SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE Layer 2 Switches Command Line Interface (CLI) V4.5

Configuration Manual

Introduction 1

General information 2

General CLI commands 3

Configuration 4

Functions specific to SCALANCE 5

System time 6

Network structures 7

Network protocols 8

Layer 2 management protocols 9

Layer 3 functions 10

Load control 11

Security and authentication 12

Diagnostics 13

Troubleshooting/FAQ 14

SCALANCE XB-200
SCALANCE XC-200
SCALANCE XF-200BA
SCALANCE XF-200G
SCALANCE XP-200 / XP-200G
SCALANCE XR-300WG

10/2023
C79000-G8976-C361-15

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C361-15
Ⓟ 10/2023 Subject to change

Copyright © Siemens AG 2015 - 2023.
All rights reserved

Table of contents

1 Introduction ... 27

1.1 Purpose of the Configuration Manual ... 27
1.2 Scope of the manual ... 27
1.3 Predefined defaults ... 28
1.4 Supplementary documentation ... 29
1.5 Further documentation ... 30
1.6 New in this version ... 30
1.7 SIMATIC NET glossary ... 30
1.8 Cybersecurity information ... 30
1.9 Firmware ... 31
1.10 Open source license conditions ... 32
1.11 Marken ... 32

2 General information ... 33

2.1 System functions hardware equipment ... 33
2.2 Configuration limits ... 36
2.3 Features not supported ... 40
2.4 Login serial interface ... 41
2.5 Initial assignment of an IP address ... 41
2.6 Working with the Command Line Interface (CLI) ... 43
2.7 Protection from brute force attacks ... 46
2.8 Structure of the Command Line Interface ... 47
2.9 The CLI command prompt ... 48
2.10 Symbols of the CLI commands ... 49
2.11 Addresses and interface names ... 50
2.11.1 Naming interfaces ... 50
2.11.2 Address types, address ranges and address masks ... 52

3 General CLI commands ... 55

3.1 clear screen ... 55
3.2 do ... 55
3.3 end ... 56
3.4 exit ... 56
3.5 Help functions and supported input ... 57

3.5.1 help ... 57
3.5.2 The command "?" ... 58
3.5.3 Completion of command entries ... 59
3.5.4 Abbreviated notation of commands ... 59
3.5.5 Reusing the last used commands ... 60
3.5.6 Working through a command sequence ... 60
3.5.7 The "show" commands ... 61
3.5.7.1 show history ... 61
3.5.8 clear history ... 61

4 Configuration ... 63

4.1 System ... 63
4.1.1 The "show" commands ... 63
4.1.1.1 show broadcast-block config ... 63
4.1.1.2 show cli-console-timeout ... 64
4.1.1.3 show coordinates ... 64
4.1.1.4 show counter discards ... 65
4.1.1.5 show counter in-errors ... 65
4.1.1.6 show device information ... 66
4.1.1.7 show environmental temperature ... 66
4.1.1.8 show ethernetip ... 67
4.1.1.9 show hardware ... 67
4.1.1.10 show im ... 68
4.1.1.11 show interfaces ... 69
4.1.1.12 show interfaces ... counters ... 70
4.1.1.13 show ip interface ... 71
4.1.1.14 show lldp neighbors ... 71
4.1.1.15 show lldp status ... 72
4.1.1.16 show multicast-block config ... 73
4.1.1.17 show nodes monitoring ... 74
4.1.1.18 show noa config ... 74
4.1.1.19 show pof status ... 75
4.1.1.20 show pof limit ... 76
4.1.1.21 show pnio ... 76
4.1.1.22 show tcp connections ... 77
4.1.1.23 show tcp listeners ... 77
4.1.1.24 show tcp retransmission details ... 78
4.1.1.25 show tcp statistics ... 78
4.1.1.26 show udp connections ... 79
4.1.1.27 show udp statistics ... 79
4.1.1.28 show unicast-block config ... 80
4.1.1.29 show usage ... 80
4.1.1.30 show versions ... 81
4.1.2 clear counters ... 82
4.1.3 clear line vty ... 83
4.1.4 configure terminal ... 83
4.1.5 disable ... 84
4.1.6 enable ... 85
4.1.7 logout ... 85
4.1.8 ping ... 86
4.1.9 Commands in the global configuration mode ... 87
4.1.9.1 interface ... 87

4.1.9.2 no interface ... 89
4.1.9.3 cli-console-timeout ... 90
4.1.9.4 no cli-console-timeout ... 91
4.1.9.5 coordinates height ... 91
4.1.9.6 coordinates latitude ... 92
4.1.9.7 coordinates longitude ... 93
4.1.9.8 environmental temperature entry ... 94
4.1.9.9 environmental diagnostics threshold monitoring ... 95
4.1.9.10 no environmental diagnostics threshold monitoring ... 96
4.1.9.11 ethernetip ... 97
4.1.9.12 ethernetip dlr ... 97
4.1.9.13 ethernetip dlr p1 p2 ... 98
4.1.9.14 ethernetip dlr vlan ... 99
4.1.9.15 pnio ... 100
4.1.9.16 pnio station-name ... 101
4.1.9.17 system contact ... 102
4.1.9.18 system location ... 103
4.1.9.19 system name ... 103
4.1.10 Commands in the interface configuration mode ... 104
4.1.10.1 alias ... 104
4.1.10.2 no alias ... 105
4.1.10.3 broadcast-block ... 106
4.1.10.4 no broadcast-block ... 106
4.1.10.5 duplex ... 107
4.1.10.6 no duplex ... 108
4.1.10.7 fsu-support ... 108
4.1.10.8 no fsu-support ... 109
4.1.10.9 lldp ... 110
4.1.10.10 no lldp ... 110
4.1.10.11 media type ... 111
4.1.10.12 multicast-block ... 113
4.1.10.13 no multicast-block ... 113
4.1.10.14 nodes monitoring action ... 114
4.1.10.15 nodes monitoring threshold ... 115
4.1.10.16 noa port config ... 115
4.1.10.17 negotiation ... 116
4.1.10.18 no negotiation ... 117
4.1.10.19 shutdown ... 117
4.1.10.20 no shutdown ... 118
4.1.10.21 power ... 119
4.1.10.22 speed ... 120
4.1.10.23 unicast-block ... 120
4.1.10.24 no unicast-block ... 121
4.1.10.25 unicast-mac flush ... 122

4.2 Load and Save ... 122
4.2.1 File list ... 123
4.2.2 The "show" commands ... 126
4.2.2.1 show loadsave minimum config-file version ... 126
4.2.2.2 show loadsave files ... 127
4.2.2.3 show loadsave stftp ... 127
4.2.2.4 show loadsave tftp ... 128
4.2.3 load ... 128

4.2.4 save ... 130
4.2.5 Commands in the global configuration mode ... 131
4.2.5.1 loadsave ... 131
4.2.6 Commands in the LOADSAVE configuration mode ... 132
4.2.6.1 delete ... 132
4.2.6.2 password ... 133
4.2.6.3 no password ... 134
4.2.6.4 tftp filename ... 135
4.2.6.5 tftp load ... 136
4.2.6.6 tftp save ... 137
4.2.6.7 tftp server ... 137
4.2.6.8 sftp filename ... 138
4.2.6.9 sftp load ... 139
4.2.6.10 sftp save ... 140
4.2.6.11 sftp server ... 141
4.2.6.12 minimum config version ... 142

4.3 Reset and Defaults ... 142
4.3.1 restart ... 143
4.3.2 Commands in global configuration mode ... 144
4.3.2.1 Introductory sentence for the global configuration mode ... 144
4.3.2.2 boot-integrity-check ... 144
4.3.2.3 cancel restart-timer ... 145
4.3.2.4 schedule restart-timer ... 146

4.4 Configuration Save & Restore ... 146
4.4.1 The "show" commands ... 147
4.4.1.1 show running-config ... 147
4.4.2 write startup-config ... 150
4.4.3 Commands in the global configuration mode ... 151
4.4.3.1 auto-save ... 151
4.4.3.2 no auto-save ... 152

4.5 DCP Discovery and Set (DaS) ... 153
4.5.1 The "show" commands ... 153
4.5.1.1 show das info ... 153
4.5.2 Commands in the global configuration mode ... 154
4.5.2.1 das delete ... 154
4.5.2.2 das discover interface ... 155
4.5.2.3 das mac ip ... 156
4.5.2.4 das mac name ... 157
4.5.2.5 das mac blink ... 158

4.6 PoE ... 159
4.6.1 The "show" commands ... 159
4.6.1.1 show poe status ... 159
4.6.1.2 show pse status ... 160
4.6.1.3 show poe schedule info ... 160
4.6.2 Commands in the global configuration mode ... 161
4.6.2.1 poe pse usage ... 161
4.6.2.2 no poe pse usage ... 162
4.6.3 Commands in the Interface Configuration mode ... 162
4.6.3.1 poe active ... 163
4.6.3.2 no poe active ... 163

4.6.3.3 poe custom maxpwr ... 164
4.6.3.4 no poe custom maxpwr ... 165
4.6.3.5 poe custom maxpwr active ... 165
4.6.3.6 no poe custom maxpwr active ... 166
4.6.3.7 poe type ... 167
4.6.3.8 no poe type ... 167
4.6.3.9 poe prio ... 168
4.6.3.10 no poe prio ... 169
4.6.3.11 poe schedule ... 169
4.6.3.12 no poe schedule ... 170
4.6.3.13 poe schedule time ... 170
4.6.3.14 no poe schedule time ... 171
4.6.3.15 poe schedule day ... 172
4.6.3.16 no poe schedule day ... 172

4.7 SINEMA ... 173
4.7.1 The "show" commands ... 173
4.7.1.1 show sinema ... 173
4.7.2 Commands in the global configuration mode ... 174
4.7.2.1 sinema ... 174
4.7.2.2 no sinema ... 175

5 Functions specific to SCALANCE ... 177

5.1 PLUG ... 177
5.1.1 The "show" commands ... 177
5.1.1.1 show plug ... 177
5.1.2 Commands in the global configuration mode ... 178
5.1.2.1 plug ... 178
5.1.3 Commands in the Plug configuration mode ... 179
5.1.3.1 factoryclean ... 179
5.1.3.2 firmware-on-plug ... 179
5.1.3.3 no firmware on plug ... 180
5.1.3.4 write ... 181

5.2 WBM ... 181
5.2.1 The "show" commands ... 181
5.2.1.1 show web-session-timeout ... 181
5.2.2 Commands in the global configuration mode ... 182
5.2.2.1 web-session-timeout ... 182
5.2.2.2 no web-session-timeout ... 183

5.3 Panel button ... 184
5.3.1 Commands in the global configuration mode ... 184
5.3.1.1 panel-button control-factory-defaults ... 184
5.3.1.2 no panel-button control-factory-defaults ... 185
5.3.1.3 panel-button control-faultmask ... 186
5.3.1.4 no panel-button control-faultmask ... 186

5.4 Signaling contact ... 187
5.4.1 The "show" commands ... 187
5.4.1.1 show signaling contact ... 187
5.4.2 Commands in the global configuration mode ... 188
5.4.2.1 signaling contact mode ... 188
5.4.2.2 signaling-contact status ... 189

6 System time ... 191

6.1 System time setting ... 191
6.1.1 The "show" commands ... 191
6.1.1.1 show dst info ... 191
6.1.1.2 show time ... 191
6.1.2 Commands in the global configuration mode ... 192
6.1.2.1 time ... 192
6.1.2.2 time set ... 193
6.1.2.3 time dst date ... 194
6.1.2.4 time dst recurring ... 195
6.1.2.5 no time dst ... 196

6.2 NTP ... 197
6.2.1 The "show" commands ... 197
6.2.1.1 show ntp info ... 197
6.2.1.2 show ntp server info ... 198
6.2.2 Commands in the global configuration mode ... 198
6.2.2.1 ntp ... 199
6.2.2.2 ntp server ... 199
6.2.2.3 no ntp server ... 200
6.2.2.4 ntp server configuration ... 200
6.2.3 Commands in the NTP configuration mode ... 201
6.2.3.1 ntp secure ... 201
6.2.3.2 no ntp secure ... 202
6.2.3.3 ntp server id ... 202
6.2.3.4 no ntp server id ... 204
6.2.3.5 ntp server id secure ... 204
6.2.3.6 ntp time diff ... 205
6.2.4 Commands in NTP server configuration mode ... 206
6.2.4.1 ntp server interface ... 206
6.2.4.2 no ntp server interface ... 208
6.2.4.3 ntp server listen interface ... 209
6.2.4.4 no ntp server listen interface ... 210
6.2.4.5 ntp server secure interface ... 211
6.2.4.6 no ntp server secure interface ... 211

6.3 SNTP client ... 212
6.3.1 The "show" commands ... 212
6.3.1.1 show sntp broadcast-mode status ... 213
6.3.1.2 show sntp status ... 213
6.3.1.3 show sntp unicast-mode status ... 214
6.3.2 Commands in the global configuration mode ... 214
6.3.2.1 sntp ... 215
6.3.3 Commands in the SNTP configuration mode ... 215
6.3.3.1 sntp client addressing-mode ... 216
6.3.3.2 sntp time diff ... 216
6.3.3.3 sntp unicast-server ipv4 ... 217
6.3.3.4 no sntp unicast-server ipv4 ... 218

6.4 PTP Client ... 219
6.4.1 The "show" commands ... 220
6.4.1.1 show ptp info ... 220
6.4.2 Commands in global configuration mode ... 220

6.4.2.1 ptp ... 221
6.4.2.2 no ptp ... 221
6.4.2.3 ptp time diff ... 222
6.4.2.4 ptp transparent-clock configuration ... 223
6.4.3 Commands in the PTP Transparent Clock configuration mode ... 223
6.4.3.1 delay-mechanism ... 224
6.4.3.2 primary-domain ... 225
6.4.3.3 vlan-id ... 225
6.4.4 Commands in interface configuration mode ... 226
6.4.4.1 ptp ... 226
6.4.4.2 no ptp ... 227
6.4.4.3 ptp transparent-clock transport-mechanism ... 228

7 Network structures ... 229

7.1 VLAN ... 229
7.1.1 The "show" commands VLAN bridge) ... 231
7.1.1.1 show mac-address-table ... 231
7.1.1.2 show mac-address-table count ... 232
7.1.1.3 show mac-address-table dynamic multicast ... 232
7.1.1.4 show mac-address-table dynamic unicast ... 233
7.1.1.5 show mac-address-table static multicast ... 234
7.1.1.6 show mac-address-table static unicast ... 235
7.1.1.7 show vlan ... 236
7.1.1.8 show vlan device info ... 237
7.1.1.9 show vlan learning params ... 237
7.1.1.10 show vlan port config ... 238
7.1.1.11 show vlan private-vlan ... 239
7.1.2 The "show" commands (Transparent Bridge) ... 240
7.1.2.1 show dot1d mac-address-table ... 240
7.1.2.2 show dot1d mac-address-table static multicast ... 241
7.1.2.3 show dot1d mac-address-table static unicast ... 241
7.1.2.4 show vlan device info ... 242
7.1.3 Commands in the global configuration mode ... 243
7.1.3.1 base bridge-mode ... 243
7.1.3.2 vlan ... 245
7.1.3.3 no vlan ... 246
7.1.3.4 interface range ... 246
7.1.3.5 no interface range ... 247
7.1.3.6 vlan range ... 248
7.1.4 Commands in the global configuration mode (VLAN bridge) ... 249
7.1.4.1 bridge-mode ... 249
7.1.4.2 vlan tag-priority override ... 250
7.1.5 Commands in the Interface configuration mode (VLAN Bridge) ... 251
7.1.5.1 alias ... 251
7.1.5.2 no alias ... 252
7.1.5.3 private-vlan mapping ... 253
7.1.5.4 no private-vlan mapping ... 254
7.1.5.5 switchport acceptable-frame-type ... 254
7.1.5.6 no switchport acceptable-frame-type ... 255
7.1.5.7 switchport access vlan ... 256
7.1.5.8 no switchport access vlan ... 257
7.1.5.9 switchport mode ... 257

7.1.5.10 no switchport mode ... 259
7.1.5.11 switchport mode private vlan ... 259
7.1.5.12 switchport mode dot1q-tunnel ... 260
7.1.5.13 no switchport mode dot1q-tunnel ... 261
7.1.5.14 switchport priority default ... 262
7.1.5.15 no switchport priority default ... 263
7.1.5.16 switchport private-vlan host-association ... 263
7.1.5.17 no switchport private-vlan host-association ... 264
7.1.5.18 switchport private-vlan mapping ... 265
7.1.5.19 no switchport private-vlan mapping ... 266
7.1.5.20 switchport pvid ... 267
7.1.5.21 no switchport pvid ... 268
7.1.5.22 tia interface ... 268
7.1.6 Commands in the VLAN configuration mode (VLAN Bridge) ... 269
7.1.6.1 name ... 269
7.1.6.2 no name ... 270
7.1.6.3 ports ... 271
7.1.6.4 no ports ... 272
7.1.6.5 priority ... 274
7.1.6.6 no priority ... 275
7.1.6.7 priority-enable ... 276
7.1.6.8 no priority-enable ... 276
7.1.6.9 private-vlan ... 277
7.1.6.10 no private-vlan ... 278
7.1.6.11 private-vlan association ... 278
7.1.6.12 no private-vlan association ... 279

7.2 Link aggregation ... 280
7.2.1 The "show" commands ... 280
7.2.1.1 show etherchannel ... 280
7.2.1.2 show interfaces etherchannel ... 281
7.2.1.3 show lacp ... 282
7.2.2 Commands in the interface configuration mode ... 283
7.2.2.1 channel-group ... 283
7.2.2.2 no channel-group ... 284
7.2.2.3 lacp timeout ... 285
7.2.2.4 no lacp timeout ... 285

7.3 Spanning Tree ... 286
7.3.1 The "show" commands ... 286
7.3.1.1 show spanning-tree ... 286
7.3.1.2 show spanning-tree active ... 287
7.3.1.3 show spanning-tree bridge ... 288
7.3.1.4 show spanning-tree detail ... 289
7.3.1.5 show spanning-tree interface ... 289
7.3.1.6 show spanning-tree interface layer2-gateway-port ... 290
7.3.1.7 show spanning-tree mst ... 291
7.3.1.8 show spanning-tree mst configuration ... 292
7.3.1.9 show spanning-tree mst interface ... 292
7.3.1.10 show spanning-tree passive-listening-compatibility ... 293
7.3.1.11 show spanning-tree root ... 294
7.3.2 clear spanning-tree detected protocols ... 295
7.3.3 clear spanning-tree counters ... 296

7.3.4 Commands in the global configuration mode ... 296
7.3.4.1 spanning-tree ... 296
7.3.4.2 no spanning-tree ... 297
7.3.4.3 spanning-tree compatibility ... 298
7.3.4.4 no spanning-tree compatibility ... 299
7.3.4.5 spanning-tree mst configuration ... 299
7.3.4.6 spanning-tree mst max-hops ... 300
7.3.4.7 no spanning-tree mst max-hops ... 301
7.3.4.8 spanning-tree mst instance-id root ... 302
7.3.4.9 no spanning-tree mst instance-id root ... 303
7.3.4.10 spanning-tree priority ... 303
7.3.4.11 no spanning-tree priority ... 304
7.3.4.12 spanning-tree passive-listening-compatibility ... 305
7.3.4.13 no spanning-tree passive-listening-compatibility ... 306
7.3.4.14 spanning-tree pathcost dynamic ... 306
7.3.4.15 no spanning-tree pathcost dynamic ... 307
7.3.4.16 spanning-tree rstp-plus ... 308
7.3.4.17 no spanning-tree rstp-plus ... 309
7.3.4.18 spanning-tree rstp-plus mrp-intercon-domain-id ... 309
7.3.4.19 spanning-tree tc-protection-backoff ... 310
7.3.4.20 Time settings for the Spanning Tree protocol ... 311
7.3.5 Commands in the interface configuration mode ... 314
7.3.5.1 spanning-tree auto-edge ... 314
7.3.5.2 no spanning-tree auto-edge ... 315
7.3.5.3 spanning-tree bpdu-receive ... 315
7.3.5.4 spanning-tree bpdu-transmit ... 316
7.3.5.5 spanning-tree bpdufilter ... 317
7.3.5.6 spanning-tree bpdu-guard ... 317
7.3.5.7 no spanning-tree bpdu-guard ... 318
7.3.5.8 spanning-tree layer2-gateway-port ... 319
7.3.5.9 no spanning-tree layer2-gateway-port ... 319
7.3.5.10 spanning-tree limited-tcn ... 320
7.3.5.11 no spanning-tree limited-tcn ... 321
7.3.5.12 spanning-tree loop-guard ... 321
7.3.5.13 no spanning-tree loop-guard ... 322
7.3.5.14 spanning-tree mst ... 323
7.3.5.15 no spanning-tree mst ... 324
7.3.5.16 spanning-tree mst hello-time ... 325
7.3.5.17 no spanning-tree mst hello-time ... 326
7.3.5.18 spanning-tree mst PseudoRootId ... 327
7.3.5.19 no spanning-tree mst PseudoRootId ... 328
7.3.5.20 spanning-tree restricted-role ... 329
7.3.5.21 no spanning-tree restricted-role ... 329
7.3.5.22 spanning-tree restricted-tcn ... 330
7.3.5.23 no spanning-tree restricted-tcn ... 330
7.3.5.24 spanning-tree ... 331
7.3.5.25 no spanning-tree ... 333
7.3.6 Commands in the MSTP configuration mode ... 334
7.3.6.1 instance ... 334
7.3.6.2 no instance ... 335
7.3.6.3 name ... 336
7.3.6.4 no name ... 337

7.3.6.5 revision ... 338
7.3.6.6 no revision ... 338

7.4 Passive Listening ... 339
7.4.1 The "show" commands ... 339
7.4.1.1 show passive-listening ... 339
7.4.2 Commands in the global configuration mode ... 340
7.4.2.1 passive-listening bpdu-vlan-flood ... 340
7.4.2.2 no passive-listening bpdu-vlan-flood ... 341
7.4.2.3 passive-listening ... 341
7.4.2.4 no passive-listening ... 342

8 Network protocols ... 345

8.1 IPv4 protocol ... 345
8.1.1 The "show" commands ... 345
8.1.1.1 show dcp forwarding ... 345
8.1.1.2 show dcp server ... 346
8.1.1.3 show dhcp snooping ... 346
8.1.1.4 show ip gateway ... 347
8.1.1.5 show ip telnet ... 347
8.1.2 Commands in the global configuration mode ... 348
8.1.2.1 dcp server ... 348
8.1.2.2 no dcp server ... 349
8.1.2.3 ip gateway ... 350
8.1.2.4 no ip gateway ... 351
8.1.2.5 ip echo-reply ... 351
8.1.2.6 no ip echo-reply ... 352
8.1.2.7 ipv4 nexthop arp_keep_alive ... 353
8.1.2.8 no ipv4 nexthop arp_keep_alive ... 353
8.1.2.9 telnet-server ... 354
8.1.2.10 no telnet-server ... 354
8.1.2.11 telnet-server port ... 355
8.1.2.12 no telnet-server port ... 356
8.1.3 Commands in the interface configuration mode ... 357
8.1.3.1 dcp forwarding ... 357
8.1.3.2 dhcp snooping ... 358
8.1.3.3 no dhcp snooping ... 358
8.1.3.4 ip address ... 359
8.1.3.5 no ip address ... 360
8.1.3.6 ip address dhcp ... 361

8.2 Domain Name System ... 361
8.2.1 The "show" commands ... 362
8.2.1.1 show ip dns ... 362
8.2.1.2 show ip dns cache ... 362
8.2.1.3 show ip dns domain name ... 363
8.2.1.4 show ip dns name-server ... 363
8.2.1.5 show ip dns statistics ... 364
8.2.2 Commands in global configuration mode ... 364
8.2.2.1 domain name ... 365
8.2.2.2 no domain name ... 365
8.2.2.3 ip domain name ... 366
8.2.2.4 no ip domain name ... 367

8.2.2.5 ip domain used server ... 368
8.2.2.6 ip domain lookup ... 369
8.2.2.7 no ip domain lookup ... 369
8.2.2.8 ip name-server ... 370
8.2.2.9 no ip name server ... 371

8.3 DHCP client ... 371
8.3.1 The "show" commands ... 371
8.3.1.1 show ip dhcp client stats ... 372
8.3.1.2 show ip dhcp client ... 372
8.3.2 Commands in the global configuration mode ... 373
8.3.2.1 ip dhcp client mode ... 373
8.3.2.2 ip dhcp client keepalive ... 374
8.3.2.3 no ip dhcp client keepalive ... 374
8.3.2.4 ip dhcp config-file-request ... 375
8.3.2.5 no ip dhcp config-file-request ... 376
8.3.2.6 ip dhcp config-file-request setup ... 376
8.3.3 Commands in the Interface configuration mode ... 377
8.3.3.1 ip address dhcp ... 377
8.3.3.2 no ip address ... 378

8.4 DHCP server ... 379
8.4.1 The "show" commands ... 379
8.4.1.1 show ip dhcp-server bindings ... 380
8.4.1.2 show ip dhcp-server pools ... 380
8.4.2 Commands in the global configuration mode ... 381
8.4.2.1 ip dhcp-server ... 381
8.4.2.2 no ip dhcp-server ... 382
8.4.2.3 ip dhcp-server icmp-probe ... 383
8.4.2.4 no ip dhcp-server icmp-probe ... 383
8.4.2.5 ip dhcp-server pool ... 384
8.4.2.6 no ip dhcp-server pool ... 385
8.4.3 Commands in the DHCPPOOL configuration mode ... 386
8.4.3.1 host ... 386
8.4.3.2 no host ... 388
8.4.3.3 lease-time ... 389
8.4.3.4 network ... 390
8.4.3.5 option value-string ... 391
8.4.3.6 Option (IP address) ... 392
8.4.3.7 no option ... 393
8.4.3.8 pool-enable ... 394
8.4.3.9 no pool-enable ... 395
8.4.3.10 ports ... 395
8.4.3.11 no ports ... 396
8.4.3.12 relay-information ... 397
8.4.3.13 no relay-information ... 398
8.4.3.14 set-interface ... 399
8.4.3.15 static-lease ... 400
8.4.3.16 no static-lease ... 401

8.5 DHCP Relay ... 402
8.5.1 The "show" commands ... 402
8.5.1.1 show dhcp server ... 402
8.5.1.2 show ip dhcp relay information ... 403

8.5.2 Commands in the Global Configuration mode ... 403
8.5.2.1 ip dhcp server ... 404
8.5.2.2 no ip dhcp server ... 404
8.5.2.3 ip dhcp relay circuit-id option ... 405
8.5.2.4 ip dhcp relay common-agent-address ... 406
8.5.2.5 no ip dhcp relay common-agent-address ... 407
8.5.2.6 ip dhcp relay common-agent-address-interface ... 408
8.5.2.7 no ip dhcp relay common-agent-address-interface ... 409
8.5.2.8 ip dhcp relay information option ... 409
8.5.2.9 no ip dhcp relay information option ... 410
8.5.2.10 service dhcp-relay ... 411
8.5.2.11 no service dhcp-relay ... 411
8.5.3 Commands in the Interface Configuration mode ... 412
8.5.3.1 ip dhcp relay circuit-id ... 412
8.5.3.2 no ip dhcp relay circuit-id ... 413
8.5.3.3 ip dhcp relay information option ... 414
8.5.3.4 no ip dhcp relay information option ... 414
8.5.3.5 ip dhcp relay remote-id ... 415
8.5.3.6 no ip dhcp relay remote-id ... 416

8.6 SNMP ... 416
8.6.1 The "show" commands ... 418
8.6.1.1 show snmp ... 418
8.6.1.2 show snmp community ... 418
8.6.1.3 show snmp engineID ... 419
8.6.1.4 show snmp filter ... 419
8.6.1.5 show snmp group ... 420
8.6.1.6 show snmp group access ... 420
8.6.1.7 show snmp inform statistics ... 421
8.6.1.8 show snmp notif ... 421
8.6.1.9 show snmp targetaddr ... 422
8.6.1.10 show snmp targetparam ... 422
8.6.1.11 show snmp tcp ... 423
8.6.1.12 show snmp user ... 423
8.6.1.13 show snmp viewtree ... 424
8.6.2 Commands in the global configuration mode ... 424
8.6.2.1 snmpagent ... 425
8.6.2.2 no snmpagent ... 425
8.6.2.3 snmpagent port ... 426
8.6.2.4 no snmpagent port ... 426
8.6.2.5 snmp access ... 427
8.6.2.6 no snmp access ... 429
8.6.2.7 snmp agent version ... 430
8.6.2.8 snmp community index ... 430
8.6.2.9 no snmp community index ... 432
8.6.2.10 snmp engineid migrate ... 432
8.6.2.11 no snmp engineid migrate ... 433
8.6.2.12 snmp group ... 434
8.6.2.13 no snmp group ... 435
8.6.2.14 snmp notify ... 436
8.6.2.15 no snmp notify ... 437
8.6.2.16 snmp targetaddr ... 437
8.6.2.17 no snmp targetaddr ... 439

8.6.2.18 snmp targetaddr remote-engine-id ... 440
8.6.2.19 snmp targetparams ... 440
8.6.2.20 no snmp targetparams ... 442
8.6.2.21 snmp user ... 443
8.6.2.22 no snmp user ... 444
8.6.2.23 snmp v1-v2 readonly ... 444
8.6.2.24 no snmp v1-v2 readonly ... 445
8.6.2.25 snmp view ... 446
8.6.2.26 no snmp view ... 447

8.7 SMTP client ... 447
8.7.1 The "show" commands ... 448
8.7.1.1 show events smtp-server ... 448
8.7.2 Commands in the Events configuration mode ... 448
8.7.2.1 smtp-server ... 449
8.7.2.2 no smtp-server ... 450
8.7.2.3 send test mail ... 451
8.7.3 Commands in SMTP server configuration mode ... 451
8.7.3.1 Introductory sentence for the SMTP server configuration mode ... 451
8.7.3.2 auth username ... 452
8.7.3.3 no auth username ... 452
8.7.3.4 port ... 453
8.7.3.5 no port ... 454
8.7.3.6 sender address ... 454
8.7.3.7 no sender address ... 455
8.7.3.8 receiver-address ... 456
8.7.3.9 no receiver-address ... 457
8.7.3.10 security ... 457
8.7.3.11 no security ... 458
8.7.3.12 smtp-server-enable ... 459
8.7.3.13 no smtp-server-enable ... 459
8.7.3.14 test ... 460

8.8 HTTP server ... 460
8.8.1 The "show" commands ... 460
8.8.1.1 show ip http server status ... 461
8.8.2 Commands in the global configuration mode ... 461
8.8.2.1 ip http ... 461
8.8.2.2 no ip http ... 462
8.8.2.3 ip http port ... 463
8.8.2.4 no ip http port ... 464

8.9 HTTPS server ... 464
8.9.1 The "show" commands ... 464
8.9.1.1 show ip http secure server status ... 464
8.9.1.2 show ssl server-cert ... 465
8.9.2 Commands in global configuration mode ... 466
8.9.2.1 ip http secure ... 466
8.9.2.2 no ip http secure ... 466
8.9.2.3 ip http secure port ... 467
8.9.2.4 no ip http secure port ... 468
8.9.2.5 ip http secure minimum tls-version ... 468

8.10 ARP ... 469

8.10.1 The "show" commands ... 469
8.10.1.1 show ip arp ... 469
8.10.2 Commands in the global configuration mode ... 470
8.10.2.1 arp timeout ... 471
8.10.2.2 no arp timeout ... 471

8.11 SSH server ... 472
8.11.1 The "show" commands ... 472
8.11.1.1 show ip ssh ... 472
8.11.1.2 show ssh-fingerprint ... 473
8.11.2 Commands in the global configuration mode ... 473
8.11.2.1 ssh-server ... 474
8.11.2.2 no ssh-server ... 474
8.11.2.3 ssh-server kex-algorithm-level ... 475
8.11.2.4 ssh-server port ... 476
8.11.2.5 no ssh-server port ... 477

9 Layer 2 management protocols ... 479

9.1 GARP ... 479
9.1.1 Commands in the global configuration mode ... 480
9.1.1.1 gmrp ... 480
9.1.1.2 no gmrp ... 481
9.1.1.3 gvrp ... 481
9.1.1.4 no gvrp ... 482

9.2 IGMP snooping ... 483
9.2.1 The "show" commands ... 483
9.2.1.1 show ip igmp snooping ... 483
9.2.1.2 show ip igmp snooping forwarding-database ... 484
9.2.1.3 show ip igmp snooping globals ... 485
9.2.1.4 show ip igmp snooping groups ... 485
9.2.1.5 show ip igmp snooping mrouter ... 486
9.2.1.6 show ip igmp snooping statistics ... 487
9.2.1.7 show ip igmp snooping switch-ip ... 487
9.2.2 Commands in the global configuration mode ... 488
9.2.2.1 ip igmp snooping clear counters ... 488
9.2.2.2 ip igmp snooping port-purge-interval ... 489
9.2.2.3 no ip igmp snooping port-purge-interval ... 490
9.2.2.4 ip igmp snooping report-forward ... 490
9.2.2.5 no ip igmp snooping report-forward ... 491
9.2.2.6 ip igmp snooping send-query ... 492
9.2.2.7 no ip igmp snooping send-query ... 492
9.2.2.8 ip igmp snooping switch-ip ... 493
9.2.2.9 ip igmp snooping version ... 494
9.2.2.10 ip igmp vlan-snooping ... 494
9.2.2.11 no ip igmp vlan-snooping ... 495
9.2.2.12 snooping report-process config-level ... 496
9.2.3 Commands in VLAN configuration mode ... 496
9.2.3.1 ip igmp snooping ... 497
9.2.3.2 no ip igmp snooping ... 498

9.3 IGMP querier ... 498
9.3.1 Commands in the Global Configuration mode ... 498
9.3.1.1 ip igmp snooping querier ... 499

9.3.1.2 no ip igmp snooping querier ... 499
9.3.2 Commands in VLAN configuration mode ... 500
9.3.2.1 Introductory sentence for the VLAN configuration mode ... 500
9.3.2.2 ip igmp snooping querier ... 500
9.3.2.3 no ip igmp snooping querier ... 501

9.4 Ring redundancy and standby connection ... 502
9.4.1 clear hrp counters ... 503
9.4.2 clear interconnection counters ... 504
9.4.3 clear ring-redundancy manager counters ... 504
9.4.4 clear standby counter ... 505
9.4.5 The "show" commands ... 505
9.4.5.1 show hrp counters ... 506
9.4.5.2 show linkcheck ... 506
9.4.5.3 show ring-redundancy ... 507
9.4.5.4 show ring-redundancy manager counters ... 507
9.4.6 Commands in the global configuration mode ... 508
9.4.6.1 ring-redundancy configuration ... 508
9.4.6.2 ring-redundancy restore-default ... 509
9.4.6.3 ring-redundancy hrpobserver ... 510
9.4.6.4 no ring-redundancy hrpobserver ... 511
9.4.6.5 ring-redundancy mode ... 511
9.4.6.6 no ring-redundancy ... 512
9.4.6.7 ring-redundancy dna-redundancy ... 513
9.4.6.8 no ring-redundancy dna-redundancy ... 513
9.4.6.9 ring-redundancy standby ... 514
9.4.6.10 no ring-redundancy standby ... 515
9.4.6.11 ring-redundancy mrpinterconnection ... 515
9.4.6.12 no ring-redundancy mrpinterconnection ... 516
9.4.7 Commands in the redundancy configuration mode ... 517
9.4.7.1 linkcheck ... 517
9.4.7.2 no linkcheck ... 519
9.4.7.3 ring ports ... 520
9.4.7.4 standby connection-name ... 523
9.4.7.5 no standby connection-name ... 524
9.4.7.6 standby force-master ... 524
9.4.7.7 no standby force-master ... 525
9.4.7.8 standby port ... 525
9.4.7.9 no standby port ... 526
9.4.7.10 standby wait-for-partner ... 527
9.4.7.11 no standby wait-for-partner ... 528
9.4.7.12 ringid ... 528
9.4.7.13 mrpinterconnection ... 529
9.4.7.14 no mrpinterconnection ... 530
9.4.8 Commands in the configuration mode for MRP multiple rings ... 531
9.4.8.1 mode ... 531
9.4.8.2 ring ports ... 532
9.4.8.3 domain-name ... 532
9.4.9 Commands in MRP Interconnection configuration mode ... 533
9.4.9.1 domain-id ... 534
9.4.9.2 domain-name ... 534
9.4.9.3 Interface ... 535
9.4.9.4 role ... 536

9.4.9.5 client-position ... 537
9.4.9.6 wait-manager ... 538
9.4.9.7 no wait-manager ... 539
9.4.9.8 Interconnection ... 539

9.5 Unicast ... 540
9.5.1 The "show" commands VLAN bridge) ... 541
9.5.1.1 show mac-address-table ... 541
9.5.1.2 show mac-address-table dynamic unicast ... 542
9.5.1.3 show mac-address-table static unicast ... 543
9.5.1.4 show unicast-block config ... 543
9.5.1.5 show unicast-mac flush config ... 544
9.5.1.6 show unicast-mac learning config ... 545
9.5.2 Commands in the global configuration mode (VLAN bridge) ... 546
9.5.2.1 mac-address-table static unicast ... 546
9.5.2.2 no mac-address-table static unicast ... 547
9.5.3 The "show" commands (Transparent Bridge) ... 548
9.5.3.1 show dot1d mac-address-table ... 548
9.5.3.2 show dot1d mac-address-table static unicast ... 549
9.5.3.3 show unicast-block config ... 550
9.5.3.4 show unicast-mac flush config ... 550
9.5.3.5 show unicast-mac learning config ... 551
9.5.4 Commands in the global configuration mode (Transparent Bridge) ... 552
9.5.4.1 mac-address-table static unicast ... 552
9.5.4.2 no mac-address-table static unicast ... 553
9.5.5 Commands in interface configuration mode ... 554
9.5.5.1 Introductory sentence for the interface configuration mode ... 554
9.5.5.2 unicast mac learning ... 554
9.5.5.3 no unicast mac learning ... 555

9.6 Multicast ... 556
9.6.1 The "show" commands VLAN bridge) ... 556
9.6.1.1 show mac-address-table ... 556
9.6.1.2 show mac-address-table dynamic multicast ... 557
9.6.1.3 show mac-address-table static multicast ... 558
9.6.1.4 show multicast-block config ... 559
9.6.2 Commands in the global configuration mode (VLAN bridge) ... 560
9.6.2.1 mac-address-table static multicast ... 560
9.6.2.2 no mac-address-table static multicast ... 561
9.6.3 The "show" commands (Transparent Bridge) ... 562
9.6.3.1 show dot1d mac-address-table ... 562
9.6.3.2 show dot1d mac-address-table static multicast ... 563
9.6.3.3 show multicast-block config ... 564
9.6.4 Commands in the global configuration mode (Transparent Bridge) ... 565
9.6.4.1 mac-address-table static multicast ... 565
9.6.4.2 no mac-address-table static multicast ... 566

10 Layer 3 functions ... 569

10.1 NAT ... 569
10.1.1 The "show" commands ... 570
10.1.1.1 show ip nat ... 570
10.1.1.2 show ip nat config ... 571
10.1.1.3 show ip nat service ... 572

10.1.1.4 show ip nat service portrange ... 573
10.1.1.5 show ip nat statistics ... 573
10.1.1.6 show ip nat summary ... 574
10.1.2 Commands in the global configuration mode ... 574
10.1.2.1 ip nat ... 575
10.1.2.2 no ip nat ... 575
10.1.2.3 ip nat timeout ... 576
10.1.2.4 no ip nat timeout ... 577
10.1.3 Commands in the Interface configuration mode ... 578
10.1.3.1 ip nat ... 578
10.1.3.2 no ip nat ... 579
10.1.3.3 ip nat napt ... 580
10.1.3.4 no ip nat napt ... 580
10.1.3.5 ip nat pool ... 581
10.1.3.6 no ip nat pool ... 582
10.1.3.7 ip nat service ... 582
10.1.3.8 no ip nat service ... 584
10.1.3.9 ip nat service portrange ... 585
10.1.3.10 no ip nat service portrange ... 586
10.1.3.11 ip nat static ... 587
10.1.3.12 no ip nat static ... 587

10.2 Single-Hop Inter-VLAN-Routing ... 588
10.2.1 Commands in the global configuration mode ... 589
10.2.1.1 ip single-hop inter-vlan-routing ... 589
10.2.1.2 no ip single-hop inter-vlan-routing ... 590

11 Load control ... 591

11.1 Rate control ... 591
11.1.1 The "show" commands ... 591
11.1.1.1 show rate-limit output ... 591
11.1.2 Commands in the interface configuration mode ... 592
11.1.2.1 rate-limit output ... 592
11.1.2.2 no rate-limit output ... 593
11.1.2.3 storm-control ... 594
11.1.2.4 no storm-control ... 595
11.1.2.5 storm-control level ... 596
11.1.2.6 no storm-control level ... 596

11.2 Static MAC filtering ... 597
11.2.1 Commands in the global configuration mode (VLAN bridge) ... 597
11.2.1.1 mac-address-table static multicast ... 598
11.2.1.2 no mac-address-table static multicast ... 599
11.2.1.3 mac-address-table static unicast ... 600
11.2.1.4 no mac-address-table static unicast ... 601
11.2.2 Commands in the global configuration mode (Transparent Bridge) ... 601
11.2.2.1 mac-address-table static multicast ... 602
11.2.2.2 no mac-address-table static multicast ... 603
11.2.2.3 mac-address-table static unicast ... 604
11.2.2.4 no mac-address-table static unicast ... 605
11.2.3 Commands in the interface configuration mode ... 605
11.2.3.1 switchport ingress-filter ... 606
11.2.3.2 no switchport ingress-filter ... 607

11.3 Dynamic MAC aging ... 607
11.3.1 The "show" commands ... 607
11.3.1.1 show mac-address-table aging-time ... 608
11.3.1.2 show mac-address-table aging-status ... 608
11.3.2 Commands in the global configuration mode ... 609
11.3.2.1 mac-address-table aging-time ... 609
11.3.2.2 no mac-address-table aging-time ... 610
11.3.2.3 mac-address-table aging ... 611
11.3.2.4 no mac-address-table aging ... 611

11.4 Flow control ... 612
11.4.1 The "show" commands ... 612
11.4.1.1 show flow-control ... 612
11.4.2 Commands in the interface configuration mode ... 613
11.4.2.1 flowcontrol ... 613

11.5 Service classes ... 614
11.5.1 The "show" commands ... 614
11.5.1.1 show qos agent-priority ... 615
11.5.1.2 show qos broadcast-priority ... 615
11.5.1.3 show qos cos-map ... 616
11.5.1.4 show qos cos-remap ... 616
11.5.1.5 show qos dscp-map ... 617
11.5.1.6 show qos scheduling mode ... 618
11.5.1.7 show qos-trust-mode ... 618
11.5.2 Commands in the Global configuration mode ... 619
11.5.2.1 qos ... 619
11.5.3 Commands in the QOS configuration mode ... 620
11.5.3.1 agent-priority ... 621
11.5.3.2 no agent-priority ... 621
11.5.3.3 broadcast-priority ... 622
11.5.3.4 no broadcast-priority ... 623
11.5.3.5 cos-map ... 623
11.5.3.6 cos-remap ... 625
11.5.3.7 no cos-remap ... 626
11.5.3.8 cos-remap-enable ... 626
11.5.3.9 no cos-remap-enable ... 627
11.5.3.10 dscp-map ... 628
11.5.3.11 qos-trust-mode ... 629
11.5.3.12 scheduling mode ... 630

12 Security and authentication ... 633

12.1 User management ... 633
12.1.1 The "show" commands ... 633
12.1.1.1 show function-rights ... 633
12.1.1.2 show password-policy ... 634
12.1.1.3 show roles ... 634
12.1.1.4 show user-accounts ... 635
12.1.1.5 show user-groups ... 636
12.1.1.6 show users ... 636
12.1.2 change password ... 637
12.1.3 whoami ... 638
12.1.4 Commands in the global configuration mode ... 638

12.1.4.1 password-policy ... 639
12.1.4.2 password-policy min-length ... 640
12.1.4.3 password-policy (parameter) ... 640
12.1.4.4 role ... 641
12.1.4.5 no role ... 643
12.1.4.6 user-account ... 643
12.1.4.7 no user-account ... 645
12.1.4.8 user-account-ext ... 646
12.1.4.9 no user-account-ext ... 647
12.1.4.10 user-name case-insensitive ... 648
12.1.4.11 no user-name case-insensitive ... 649
12.1.4.12 user-group ... 649
12.1.4.13 no user-group ... 651
12.1.4.14 username ... 652

12.2 RADIUS client ... 654
12.2.1 The "show" commands ... 654
12.2.1.1 show radius statistics ... 654
12.2.1.2 show radius server ... 654
12.2.2 Commands in the global configuration mode ... 655
12.2.2.1 login authentication ... 655
12.2.2.2 no login authentication ... 656
12.2.2.3 radius authorization-mode ... 657
12.2.2.4 radius disconnect-packet ... 658
12.2.2.5 no radius disconnect-packet ... 659
12.2.2.6 radius-server ... 659
12.2.2.7 no radius-server ... 661

12.3 Management Access Control List ... 662
12.3.1 The "show" commands ... 662
12.3.1.1 show authorized-managers ... 663
12.3.2 Commands in the Global configuration mode ... 663
12.3.2.1 authorized-manager ... 664
12.3.2.2 no authorized-manager ... 664
12.3.2.3 authorized-manager ip-source ... 665
12.3.2.4 no authorized-manager ip-source ... 667

12.4 Port Access Control List Locked Ports ... 668
12.4.1 The "show" commands ... 668
12.4.1.1 show lock port ... 668
12.4.2 Commands in the Global configuration mode ... 669
12.4.2.1 clear-all-static-unicast ... 669
12.4.2.2 auto-learn ... 670
12.4.3 Commands in the interface configuration mode ... 670
12.4.3.1 switchport lock ... 671
12.4.3.2 no switchport lock ... 671
12.4.4 Commands in the AUTOLEARN mode ... 672
12.4.4.1 start ... 672
12.4.4.2 stop ... 673

12.5 Port Based Network Access Control ... 674
12.5.1 The "show" commands ... 674
12.5.1.1 show dot1x ... 674
12.5.1.2 show dot1x guest-vlan mac-info ... 675

12.5.1.3 show dot1x mac-auth mac-info ... 675
12.5.2 Commands in the global configuration mode ... 676
12.5.2.1 dot1x guest-vlan ... 676
12.5.2.2 no dot1x guest-vlan ... 677
12.5.2.3 dot1x fallback timeout ... 677
12.5.2.4 dot1x fallback retry count ... 678
12.5.2.5 dot1x mac-auth ... 679
12.5.2.6 no dot1x mac-auth ... 679
12.5.2.7 dot1x nas-id ... 680
12.5.3 Commands in the interface configuration mode ... 681
12.5.3.1 dot1x guest-vlan ... 681
12.5.3.2 no dot1x guest-vlan ... 682
12.5.3.3 dot1x guest-vlan vlan-id ... 682
12.5.3.4 no dot1x guest-vlan vlan-id ... 683
12.5.3.5 dot1x guest-vlan reset ... 684
12.5.3.6 set dot1x guest-vlan mac-addr count ... 684
12.5.3.7 dot1x mac-auth ... 685
12.5.3.8 no dot1x mac-auth ... 687
12.5.3.9 dot1x mac-auth default-value ... 688
12.5.3.10 no dot1x mac-auth default-vlan ... 689
12.5.3.11 dot1x mac-auth port reset ... 689
12.5.3.12 dot1x mac-auth vlan-assign ... 690
12.5.3.13 no dot1x mac-auth vlan-assign ... 691
12.5.3.14 dot1x port-control ... 692
12.5.3.15 no dot1x port-control ... 693
12.5.3.16 set dot1x mac-auth mac-addr count ... 693
12.5.3.17 dot1x reauthentication ... 694
12.5.3.18 no dot1x reauthentication ... 695
12.5.3.19 dot1x timeout reauth-period ... 695
12.5.3.20 no dot1x timeout reauth-period ... 696
12.5.3.21 dot1x timeout tx-period ... 697

12.6 Brute Force Prevention ... 698
12.6.1 The "show" commands ... 698
12.6.1.1 show brute-force-prevention config ... 698
12.6.1.2 show brute-force-prevention status ... 699
12.6.2 Commands in global configuration mode ... 699
12.6.2.1 brute-force-prevention auto-reset-timer ... 700
12.6.2.2 no brute-force-prevention auto-reset-timer ... 701
12.6.2.3 brute-force-prevention ip-specific-login-attempts ... 701
12.6.2.4 no brute-force-prevention ip-specific-login-attempts ... 702
12.6.2.5 brute-force-prevention user-specific-login-attempts ... 703
12.6.2.6 no brute-force-prevention user-specific-login-attempts ... 704
12.6.2.7 brute-force-prevention trigger-interval ... 705
12.6.2.8 brute-force-prevention reset ... 706

13 Diagnostics ... 707

13.1 Event and fault handling ... 707
13.1.1 logging console ... 708
13.1.2 no logging console ... 708
13.1.3 The "show" commands ... 709
13.1.3.1 show counter log-events ... 709
13.1.3.2 show events config ... 710

13.1.3.3 show events severity ... 710
13.1.3.4 show events faults config ... 711
13.1.3.5 show events faults status ... 711
13.1.3.6 show startup-information ... 712
13.1.3.7 show logbook ... 712
13.1.3.8 show fault counter ... 713
13.1.3.9 show cabletest interface ... 714
13.1.3.10 show interface transceiver details ... 715
13.1.3.11 show power-line-state ... 715
13.1.4 clear logbook ... 716
13.1.5 clear fault counter ... 716
13.1.6 fault report ack ... 717
13.1.7 Commands in the global configuration mode ... 717
13.1.7.1 events ... 718
13.1.7.2 cabletest interface ... 719
13.1.7.3 link flap count ... 720
13.1.7.4 link flap reaction ... 720
13.1.7.5 link flap time ... 721
13.1.8 Commands in the Events configuration mode ... 722
13.1.8.1 add log ... 722
13.1.8.2 client config ... 723
13.1.8.3 no client config ... 724
13.1.8.4 event config ... 725
13.1.8.5 no event config ... 728
13.1.8.6 hrp-redundancy-loss ... 730
13.1.8.7 no hrp-redundancy-loss ... 730
13.1.8.8 link ... 731
13.1.8.9 no link ... 732
13.1.8.10 logbook alarm threshold_X ... 733
13.1.8.11 power ... 734
13.1.8.12 no power ... 734
13.1.8.13 severity ... 735
13.1.8.14 no severity ... 736
13.1.8.15 syslogserver ... 737
13.1.8.16 no syslogserver ... 738

13.2 FMP ... 739
13.2.1 The "show" commands ... 739
13.2.1.1 show fmp limit ... 740
13.2.1.2 show fmp status ... 740
13.2.2 Commands in the Interface Configuration mode ... 741
13.2.2.1 fmp ... 741
13.2.2.2 no fmp ... 742
13.2.2.3 fmp power-loss ... 743
13.2.2.4 fmp rx-power ... 744

13.3 Syslog client ... 745
13.3.1 The "show" commands ... 745
13.3.1.1 show events syslogserver ... 745
13.3.2 Commands in the Events configuration mode ... 746
13.3.2.1 syslogserver ... 746
13.3.2.2 no syslogserver ... 747

13.4 RMON ... 748

13.4.1 The "show" commands ... 748
13.4.1.1 show rmon ... 749
13.4.2 Commands in the global configuration mode ... 749
13.4.2.1 rmon ... 750
13.4.2.2 no rmon ... 751
13.4.2.3 rmon alarm ... 751
13.4.2.4 no rmon alarm ... 753
13.4.2.5 rmon collection history preset ... 754
13.4.2.6 no rmon collection history preset ... 754
13.4.2.7 rmon event ... 755
13.4.2.8 no rmon event ... 756
13.4.3 Commands in the interface configuration mode ... 757
13.4.3.1 rmon collection stats ... 757
13.4.3.2 no rmon collection stats ... 758
13.4.3.3 rmon collection history ... 758
13.4.3.4 no rmon collection history ... 759

13.5 Port Mirroring ... 760
13.5.1 The "show" commands ... 761
13.5.1.1 show monitor ... 761
13.5.1.2 show monitor barrier ... 761
13.5.1.3 show monitor session ... 762
13.5.2 Commands in the global configuration mode ... 762
13.5.2.1 monitor ... 763
13.5.2.2 no monitor ... 763
13.5.2.3 monitor barrier enabled ... 764
13.5.2.4 no monitor barrier enabled ... 765
13.5.2.5 monitor session destination ... 766
13.5.2.6 no monitor session destination ... 767
13.5.2.7 monitor session source ... 768
13.5.2.8 no monitor session source ... 769
13.5.2.9 no monitor session ... 770

13.6 Loop detection ... 771
13.6.1 The "show" commands ... 772
13.6.1.1 show loopd ... 772
13.6.1.2 show loopd interface ... 772
13.6.2 Commands in the global configuration mode ... 773
13.6.2.1 loopd ... 774
13.6.2.2 no loopd ... 774
13.6.2.3 loopd vlan mode ... 775
13.6.2.4 no loopd vlan mode ... 776
13.6.3 Commands in the Interface Configuration mode ... 776
13.6.3.1 loopd {blocked | forwarder | sender} ... 777
13.6.3.2 loopd {tx-interval | detect-threshold | reaction-timeout} ... 777
13.6.3.3 loopd port reset ... 779
13.6.3.4 no loopd port reset ... 779
13.6.3.5 loopd reaction local ... 780
13.6.3.6 no loopd reaction local ... 781
13.6.3.7 loopd reaction remote ... 781
13.6.3.8 no loopd reaction remote ... 782

14 Troubleshooting/FAQ 783
14.1 Downloading new firmware using TFTP without WBM and CLI 783
14.2 Message: SINEMA configuration not yet accepted 784
14.3 Exchange of configuration data with STEP 7 Basic/Professional using a file 785
Index 787

Introduction 1

1.1 Purpose of the Configuration Manual

This Configuration Manual is intended to provide you with the information you require to install, commission and operate IE switches. It is aimed primarily at planning, commissioning and maintenance personnel and at security officers. It provides you with the information you require to configure the IE switches.

The operating instructions of the device describe how you install and connect up the device correctly.

1.2 Scope of the manual

Validity of this configuration manual

This Configuration Manual covers the following products:

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XF-200BA
- SCALANCE XF-200G
- SCALANCE XP-200
- SCALANCE XP-200G
- SCALANCE XR-300WG

Below, the products are also called IE switch, device or network component.

There are two variants of some devices with different article numbers. The two variants differ only in their factory settings. All other properties are identical.

This Configuration Manual applies to the following software versions:

- SCALANCE XB-200 firmware as of version 4.5
- SCALANCE XC-200 firmware as of version 4.5
- SCALANCE XF-200BA firmware as of version 4.5
- SCALANCE XF-200G firmware as of version 4.5
- SCALANCE XP-200 firmware as of version 4.5
- SCALANCE XP-200G firmware as of version 4.5
- SCALANCE XR-300WG firmware as of version 4.5

1.3 Predefined defaults

PROFINET variants

- Ring Redundancy: On
- Ring Redundancy Mode: ARD Mode
- Spanning Tree Protocol (STP): Off
- Passive Listening: On
- VLAN Awareness: Off
- PROFINET Device Diagnostics: On
- IGMP Snooping: Off
- IGMP Querier: Off
- IPv4 Address Collision Detection - defense method: Never give up
- EtherNet/IP Device Diagnostics: Off
- QoS Trust Mode: Trust

EtherNet/IP variants

- Ring Redundancy: Off
- Ring Redundancy Mode: Off
- Spanning Tree Protocol (STP): On
- Passive Listening: Off
- VLAN Awareness: On
- PROFINET Device Diagnostics: Off
- IGMP Snooping: On
- IGMP Querier: On
- IPv4 Address Collision Detection - defense method: Attempt to defend
- EtherNet/IP Device Diagnostics: On
- QoS Trust Mode: Trust CoS-DSCP

Industrial Ethernet profile

- Ring Redundancy: Off
- Ring Redundancy Mode: Off
- Spanning Tree Protocol (STP): On
- Passive Listening: Off
- VLAN Awareness: On
- PROFINET Device Diagnostics: On

- IGMP Snooping: Off
- IGMP Querier: Off
- IPv4 Address Collision Detection - defense method: Never give up
- EtherNet/IP Device Diagnostics: Off
- QoS Trust Mode: Trust CoS-DSCP

1.4 Supplementary documentation

Documentation on the Internet

You can find the current version of the documents on the Internet at (https://support.industry.siemens.com/cs/de/en/ps/15273/man)

Enter the name or article number of the product in the search filter.

Orientation in the documentation

Apart from the configuration manual you are currently reading, the products also have the following documentation:

- Configuration Manual "SCALANCE Layer 2 Switches Web Based Management (WBM)" for SCALANCE XB-200/XC-200/XF-200BA/XF-200G/XP-200/XP-200G/XR-300WG
  This document is intended to provide you with the information you require to commission and configure IE switches using the Web Based Management.
- Operating Instructions "SCALANCE XB-200", "SCALANCE XC-200", "SCALANCE XF-200BA", "SCALANCE XF-200G", "SCALANCE XP-200", "SCALANCE XP-200G" and "SCALANCE XR-300WG"
  These documents contain information on installing, connecting up and approvals for the products.
  - SCALANCE XB-200 (https://support.industry.siemens.com/cs/ww/en/ps/15291/man)
  - SCALANCE XC-200 (https://support.industry.siemens.com/cs/ww/en/ps/24185/man)
  - SCALANCE XF-200BA (https://support.industry.siemens.com/cs/ww/en/ps/15287/man)
  - SCALANCE XF-200G (https://support.industry.siemens.com/cs/ww/en/ps/15285/man)
  - SCALANCE XP-200 (https://support.industry.siemens.com/cs/ww/en/ps/21869/man)
  - SCALANCE XP-200G
  - SCALANCE XR-300WG (https://support.industry.siemens.com/cs/ww/en/ps/15296/man)

See also

XP-200G (https://support.industry.siemens.com/cs/ww/en/ps/21869/man)

1.5 Further documentation

In the system manuals "Industrial Ethernet / PROFINET Industrial Ethernet" and "Industrial Ethernet / PROFINET passive network components", you will find information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network.

There, you will find among other things optical performance data of the communications partner that you require for the installation.

You will find the system manuals here:

- On the Internet pages of Siemens Industry Online Support under the following entry IDs:
  - 27069465 (https://support.industry.siemens.com/cs/de/en/view/27069465)
    Industrial Ethernet / PROFINET Industrial Ethernet System Manual
  - 84922825 (https://support.industry.siemens.com/cs/de/en/view/84922825)
    Industrial Ethernet / PROFINET - Passive network components System Manual

1.6 New in this version

Below, you will find an overview of the most important function expansions:

- Support of Fast startup of devices with gigabit ports (Page 108)
- Support of the DHCP Snooping (Page 358) function
- Downgrading the firmware version (Page 122)
- EtherNet/IP: Support of DLR VLAN ID "0" (Page 99)
- Possibility to configure an action when the number of monitored nodes is exceeded (Page 114)

Existing system functions have been released as of V4.5 for the following devices or interfaces:

- SCALANCE XR300WG: Link Aggregation
- SCALANCE XR300WG: Multiple Spanning Tree Protocol (MSTP)

1.7 SIMATIC NET glossary

The SIMATIC NET glossary describes terms that may be used in this document.

You will find the SIMATIC NET glossary in the Siemens Industry Online Support at the following address:

50305045 (https://support.industry.siemens.com/cs/ww/en/view/50305045)

1.8 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/global/en/products/services/cert.html (https://new.siemens.com/global/en/products/services/cert.html).

1.9 Firmware

Note on firmware/software support

Check regularly for new firmware/software versions or security updates and apply them. After the release of a new version, previous versions are no longer supported and are not maintained.

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

The firmware is available on the Internet pages of the Siemens Industry Online Support: (https://support.industry.siemens.com/cs/de/en/ps/15273/dl)

1.10 Open source license conditions

License conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product.

You will find license conditions in the following documents on the supplied data medium:

- OSS_Siemens_86.pdf
- OSS_SCALANCE-XB-200-XC-200-XF-200BA-XP-200-XR-300WG_86.pdf

You will find these documents on the product DVD.

1.11 Marken

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SCALANCE, C-PLUG, OLM

General information 2

2.1 System functions hardware equipment

Availability of the system functions

The following table shows the availability of the system functions on the IE switches. Note that all functions are described in this configuration manual and in the online help. Depending on your IE switch, some functions are not available.

We reserve the right to make technical changes.

Menu item in the WBM	System functions	SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
Information	ARP table	✓	✓	✓	✓	✓	✓	✓
	Log table	✓	✓	✓	✓	✓	✓	✓
	Ethernet Statistics	✓	✓	✓	✓	✓	✓	✓
	Diagnostics (temperature)	-	✓	✓	✓	✓	✓	✓
System	SMTP client	✓	✓	✓	✓	✓	✓	✓
	DHCP client	✓	✓	✓	✓	✓	✓	✓
	DHCP server	✓ 1)	✓ 1)	✓	✓	✓	✓	✓
	SNMP	✓	✓	✓	✓	✓	✓	✓
	Manual time setting	✓	✓	✓	✓	✓	✓	✓
	DST	✓	✓	✓	✓	✓	✓	✓
	SNTP	✓	✓	✓	✓	✓	✓	✓
	NTP	✓	✓	✓	✓	✓	✓	✓
	SIMATIC Time Client	✓	✓	✓	✓	✓	✓	✓
	Auto logout	✓	✓	✓	✓	✓	✓	✓
	Syslog Client	✓	✓	✓	✓	✓	✓	✓
	NOA switch functionality	-	-	✓ 4)	-	-	-	-
	Fault monitoring	✓	✓	✓	✓	✓	✓	✓
	PROFINET	✓	✓	✓	✓	✓	✓	✓
	EtherNet/IP	✓	✓	✓	✓	✓	✓	✓ 2)
	Cable tester	✓	✓	✓	✓	✓	✓	✓
	SFP Diagnostics	-	✓	✓	-	-	-	-

Menu item in the WBM	System functions	SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
Layer 2	Sending priorities	-	-	✓	✓	✓	✓	✓
	CoS Map	✓	✓	✓	✓	✓	✓	✓
	DSCP Mapping	✓	✓	✓	✓	✓	✓	✓
	QoS prioritization	✓	✓	✓	✓	✓	✓	✓
	CoS port reassignment	-	-	✓	✓	✓	✓	✓
	Load control	✓	✓	✓	✓	✓	✓	✓
	GVRP	-	-	✓	✓	✓	✓	✓
	Port-based VLAN	✓	✓	✓	✓	✓	✓	✓ 2)
	Private VLAN	-	-	✓	✓	✓	✓	-
	Provider bridge	-	-	✓	✓	✓	✓	-
	Switch-Port VLAN Trunk	-	✓	✓	✓	✓	✓	✓ 2)
	Port-based mirroring	✓	✓	✓	✓	✓	✓	✓
	Dynamic MAC aging	✓	✓	✓	✓	✓	✓	✓
	Ring redundancy	✓	✓	✓	✓	✓	✓	✓
	H-Sync support	-	-	✓	✓	✓	✓	✓
	S2 devices	-	-	✓	✓	✓	✓	✓
	CiR/H-CiR support	-	-	✓	✓	✓	✓	✓
	Ring with RSTP	✓	✓	✓	✓	✓	✓	✓
	Standby (HRP)	✓	✓	✓	✓	✓	✓	✓
	Observer (HRP)	-	-	✓	✓	✓	✓	✓
	Link Check	✓	✓	✓	-	-	-	✓
	MRP multiple rings	✓	✓	✓	-	✓	✓	-
	MRP Interconnection	✓	✓	✓	✓	✓	✓	✓
	Spanning Tree	✓	✓	✓	✓	✓	✓	✓
	RSTP	✓	✓	✓	✓	✓	✓	✓
	RSTP+	✓	✓	✓	✓	✓	✓	✓
	MSTP	-	✓	✓	✓	✓	✓	-
	Enhanced Passive Listening Compatibility	✓	✓	✓	✓	✓	✓	✓
	Loop detection	✓	✓	✓	✓	✓	✓	✓
	Link Aggregation / LACP	-	✓	✓	✓	✓	✓	✓
	DCP forwarding	✓	✓	✓	✓	✓	✓	✓

Menu item in the WBM	System functions	SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
	LLDP	✓	✓	✓	✓	✓	✓	✓
	Fiber monitoring	-	✓	✓	-	-	-	-
	Unicast filter	✓	✓	✓	✓	✓	✓	✓
	Locked ports	✓	✓	✓	✓	✓	✓	✓
	Unicast learning	✓	✓	✓	✓	✓	✓	✓
	Unicast blocking	✓	✓	✓	✓	✓	✓	✓
	Multicast groups	✓	✓	✓	✓	✓	✓	✓
	IGMP	✓	✓	✓	✓	✓	✓	✓
	GMRP	-	-	✓	✓	✓	✓	✓
	Multicast blocking	✓	✓	✓	✓	✓	✓	✓
	Broadcast blocking	✓	✓	✓	✓	✓	✓	✓
	PTP	-	-	✓ [3]	✓	-	✓	-
	RMON	✓	✓	✓	✓	✓	✓	✓
	RMON history	✓	✓	✓	✓	✓	✓	✓
Layer 3	Single-Hop Inter-VLAN-Routing	-	-	✓	✓	✓	✓	-
	DHCP relay agent	✓	✓	✓	✓	✓	✓	✓
	Common agent address	-	-	✓	✓	✓	✓	-
	NAT/NAPT	-	-	✓	✓	✓	✓	-
Security	Users	✓	✓	✓	✓	✓	✓	✓
	Passwords	✓	✓	✓	✓	✓	✓	✓
	RADIUS authentication	✓	✓	✓	✓	✓	✓	✓
	MAC authentication	✓	✓	✓	✓	✓	✓	✓
	Guest VLAN	-	-	✓	✓	✓	✓	✓
	802.1X Re-Authentication	✓	✓	✓	✓	✓	✓	✓
	Management ACL	✓	✓	✓	✓	✓	✓	✓
	Brute Force Prevention	✓	✓	✓	✓	✓	✓	✓

[1] Restricted

[2] Not with DNA devices

[3] Only SCALANCE XC-200G

[4] Only SCALANCE XC-200G EEC

Availability of hardware

The following table shows the hardware of the IE switches.

We reserve the right to make technical changes.

	SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
C-PLUG support	-	-	✓	✓	✓	✓	✓
SELECT/SET button	-	-	✓ 2) 3)	-	✓ 3)	✓ 3) 4)	-
RESET button	✓ 2)	✓ 2)	-	✓	✓ 2)	✓ 2)	-
SET button	-	-	-	-	-	-	✓ 2)
Signaling contact	-	-	✓	-	✓	✓	✓
Serial interface	✓	✓	✓	✓	✓	✓ 4)	-
Display modes	-	-	✓	-	✓	✓ 4)	-
Pluggable transceiver slots	-	-	✓	-	-	-	-
Combo ports	-	✓	✓	-	-	-	-
Bus adapter slots	-	-	-	-	-	-	✓
Power over Ethernet	-	✓ 1)	✓ 1)	-	✓ 1)	✓ 1)	-

1) "PoE" identifier in device name

2) Function of the buttons: Restore Factory Defaults

3) Function of the buttons: Set Fault Mask

4) Not with the SCALANCE XP200G PP

2.2 Configuration limits

Configuration limits of the device

The following table lists the configuration limits for Web Based Management and the Command Line Interface of the device.

Depending on your IE switch, some functions are not available.

	Configurable function	Maximum number						
		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
System	Maximum frame size (ingress)	1632 bytes	10 KB	1632 bytes / 2048 bytes / 10 KB [7]	10 KB	1632 bytes / 10 KB [8]	10 KB	1632 bytes
	Syslog server	3						
	E-mail server	3						
	DHCP pools	16 [1]	28 [1]	24				
	IPv4 addresses per DHCP pool	1		24				
	IPv4 addresses managed by the DHCP server (dynamic + static)	16 [1]	28 [1]	576				
	DHCP static assignments per DHCP pool	-		24				
	SNMPv1 trap recipient	10						
	SNMPv3 Users	48						
	SNMPv3 Groups	41						
	SNMPv3 Views (incl. 2 default views)	46						
	SNTP server	1 [9]						
	NTP server	1		4 [9]				1
	Agent/TIA interfaces [2]	1						
	Devices displayed via DCP Discovery	100						

	Configurable function	Maximum number						
		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
Layer 2	QoS priority queues	4		4/8 [6]	8	4/8 [10]	8	4
	Virtual LANs (port-based, including VLAN 1)	257 [3]						
	Private VLAN	-		1				-
	Primary PVLANs	-		1				-
	Secondary isolated PVLANs	-		24				-
	Secondary community PVLANs	-		256				-
	Mirroring sessions	1						
	Standby ports	1						
	MRP rings	4			1	4		1
	Configured MRP Interconnection connections	64						
	Enabled MRP Interconnection connections	1		2				
	Maximum number of devices with enabled MRP Interconnection in a ring	10						
	Multiple Spanning Tree instances	-	4					-
	Link aggregations	-	2/4/8 [5]					
	Ports in a link aggregation	-		8	4	8		4
	Static unicast addresses	128						
	Static multicast addresses without activated GMRP	256						
	Static multicast addresses with activated GMRP	-		50				
	Addresses learned using IGMP snooping	512						

	Configurable function	Maximum number						
		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XP-200G	SCALANCE XF-200BA
Layer 3	VLAN IP interfaces	24						
	DHCP Relay Agent interfaces	1		24				1
	DHCP Relay Agent server	4						
	NAT interfaces	-		1				-
	Dynamic NAT configurations (pools)	-		100				-
	Static NAT configurations	-		100				-
Security	Users	30 (incl. user preset in the factory "admin")						
	Roles	29						
	Groups	32						
	IP addresses of RADIUS servers	6						
	Simultaneous MAC authentications (authenticated and blocked) per device [4]	2000	-	2000				
	Simultaneous MAC authentications (authenticated and blocked) per port (configurable) [4]	200						
	Management ACLs (access rules for management)	10						

[1] With the SCALANCE XB-200 and SCALANCE XR-300WG, the number of DHCP pools and manageable IPv4 addresses depends on the number of ports. The number of ports corresponds to the maximum number of DHCP pools and manageable IPv4 addresses.

[2] This is an IP interface.

[3] Devices with Y functionality do not support VLANs.

[4] If the maximum number of MAC authentications per device is exceeded, all MAC authentications of the port at which the value was exceeded are reset.
If the maximum number of MAC authentications per port is exceeded, all MAC authentications of the port are reset.

[5] Since a link aggregation consists of at least 2 ports, the maximum number of link aggregations is dependent on the number of ports.
- For devices with up to 4 ports, a maximum of 2 link aggregations is possible.

- For devices with up to 8 ports, a maximum of 4 link aggregations is possible.
- For devices with more than 8 ports, a maximum of 8 link aggregations is possible.

6) The devices of the SCALANCE XC-200G product group support 8 queues. All other XC-200 devices support 4 queues.

7) With the following devices, the maximum frame size (ingress) is 2048 bytes:
- Devices with combo ports (suffix "C" in type designation)
- PoE variants (suffix "PoE" in type designation)

The following devices support 10 KB jumbo frames:
- All gigabit variants (suffix "G" in type designation), also those with combo ports.
- All devices that support Power over Ethernet (suffix "PoE" in type designation)
- SCALANCE XC216-4C

With all other XC-200 devices, the maximum frame size (ingress) is 1632 bytes.

8) The gigabit ports of a SCALANCE XP-200 support 10 KB jumbo frames. With all other ports, the maximum frame size is 1632 bytes.

9) Maximum number of NTP/SNTP servers that can be configured for a device.

10) The following devices of the SCALANCE XP-200 product group support 8 queues:

- 6GK5 208-0HA10-2AS6
- 6GK5 208-0HA10-2ES6
- 6GK5 208-0UA10-5ES6

All other XP-200 devices support 4 queues.

2.3 Features not supported

The following features are not supported by the IE switches with firmware version 4.5:

- IPv6
- Layer 3 routing
- Loopback
- PIM

Even if these features are listed as parameters in the documentation and are displayed by the help functions `help` and `?`, you cannot execute them with a SCALANCE XB-200, SCALANCE XC-200, SCALANCE XF-200BA, SCALANCE XF-200G, SCALANCE XP-200, SCALANCE XP-200G and SCALANCE XR-300WG.

2.4 Login serial interface

Starting the CLI via a serial connection

Follow the steps outlined below to start the Command Line Interface via a serial interface:

1. Open a serial terminal (program of your choice)
2. Connect to the serial port of the device (baud rate 115200,data/parity/stop 8N1)
3. Enter your login and password.

Note

When you log in via a serial interface you can only log in with a local user account.

2.5 Initial assignment of an IP address

Configuration options

An initial IP address for an IE switch cannot be assigned using Web Based Management (WBM) because this configuration tool can only be used if an IP address already exists.

The following options are available to assign an IP address to an unconfigured device:

- **DHCP** (factory setting)
- **SINEC PNI** (SINEC Primary Network Initialization)
  This program for initial commissioning of network devices uses the DCP protocol to detect devices in a network and assign an IP address.
  For more information, refer to PNI (https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=en-US)

- **STEP 7**
  In STEP 7, you can configure the topology, the device name and the IP address. If you connect an unconfigured IE switch to the controller, the controller assigns the configured device name and the IP address to the IE switch automatically.
  - **STEP 7**
    SCALANCE XB-200: V5.5.4 and higher
    SCALANCE XP-200: As of V5.5.4 HF9
    SCALANCE XC-200: V5.5.4 HF11 and higher
    SCALANCE XR-300WG: As of V5.6
    SCALANCE XF-200BA: As of V5.6 HF3
    SCALANCE XC-200G: As of V5.6 as HSP11
    SCALANCE XF-200G: As of V5.7 as HSP1121
    SCALANCE XP-200G: As of V5.7 SP2 as HSP1124
    For further information on the assignment of the IP address using STEP 7 refer to the documentation "Configuring Hardware and Communication Connections STEP 7", in the section "Steps For Configuring a PROFINET IO System".
  - **STEP 7 Basic or Professional**
    SCALANCE XB-200: V13 SP1 and higher
    SCALANCE XC-200: V14 and higher
    SCALANCE XP-200: V14 and higher
    SCALANCE XR-300WG: As of V15
    SCALANCE XF-200BA: As of V15
    SCALANCE XC-200G, devices with 8 ports: As of V15
    SCALANCE XC-200G, devices with more than 8 ports: As of V16
    SCALANCE XF-200G: As of V19
    SCALANCE XP-200G: As of V17 as HSP0395
    For further information on assigning the IP address using STEP 7, refer to the online help "Information system", section "Addressing PROFINET devices".
- **CLI** via the serial interface
  For more information on assigning the IP address using the CLI, refer to the documentation "SCALANCE Layer 2 Switches Command Line Interface (CLI)"
- **NCM PC**
  For further information on assigning the IP address using NCM PC, refer to the documentation "Commissioning PC stations - Manual and Quick Start", in the section "Creating a PROFINET IO system".

Note

When the product ships and after factory settings are restored, DHCP is enabled. If a DHCP server is available in the local area network, and this responds to the DHCP request of an IE switch, the IP address, subnet mask and gateway are assigned automatically when the device first starts up.

The following DHCP options are supported:

- DHCP option 3: Router IP
- DHCP option 6: DNS server IP
- DHCP option 12: Host name
- DHCP option 15: DNS domain name
- DHCP option 66: Assignment of a dynamic TFTP server name
- DHCP option 67: Assignment of a dynamic boot file name

2.6 Working with the Command Line Interface (CLI)

You can access the CLI (Command Line Interface) of the device using an SSH client. The CLI offers extended configuration options of the device. Nevertheless, also refer to the detailed explanations of the parameters in the "Web Based Management" configuration manual.

Requirements

- The device has an IP address.

  Note

  Assign an IP address to the device using DHCP or SINEC PNI.

- There is a network connection between the device and the client PC.
- The network settings of the device and of the client PC match.

  Note

  You can use a ping to check whether a connection exists and communication is possible.

- Terminal software for establishing SSH connections is available on the client PC.

Starting the CLI in a Windows console

Note

Requirement for use of the CLI

You should only use the command line interface if you are an experienced user.

Even commands that bring about fundamental changes to the configuration are executed without a prompt for confirmation.

Errors in the configuration can mean that no further operation is possible in the entire network.

Note

Command sets depend on the logged-on user. Changing configuration data is possible only with the "admin" role.

Follow the steps outlined below to start the Command Line Interface in a Windows console:

1. Open a Windows console and type in the command "ssh" followed by the IP address of the device you are configuring:
   `C:\>ssh admin@<IP address>`
2. Log in.

Log in to a device with factory settings

Note

Configuration hazard - risk of connection loss

Note that the access rights of some functions change after the first login with the default user profile **admin** and the assignment of a new password.

DCP Server:

- As long as the administrator's default password has not been changed, the device parameters can be both read and changed via DCP. Once the default password has been changed, the parameters for devices can no longer be changed via DCP. For further information, refer to the WBM, section "Configuring with Web Based Management > The "System" menu > Configuration".

DHCP client configuration file request (opt. 66, 67):

- In the delivery state and after resetting to default settings (setup), the DHCP client requests a configuration file with the next DHCP request. After the initial login with the default user profile admin and the associated assignment of a new password and loading of a configuration file, you can no longer load a configuration file from the DHCP server. For more information, refer to the WBM, chapter "Configuring with Web Based Management > The "System" menu > DHCPv4".

When you log in to a device with default settings, follow these steps:

1. Set up a SSH connection to the device and call the CLI.
   The login prompt is displayed. `login as:`
2. Enter the default user "`admin`" set at the factory and confirm with "Enter".
   With this user account, you can change the settings of the device (read and write access to the configuration data).
   The command prompt is as follows: `admin@<IP address>' password:`
3. Enter the password "`admin`" for the factory default user "admin" and confirm the entry with "Enter"
   The command prompt is: `Default admin user to be changed (y/n)?`
   You can rename the user preset in the factory "admin" once. Afterwards, renaming "admin" is no longer possible.
   - To rename the user preset in the factory "admin", enter "`y`" and confirm with "Enter".
     The command prompt is: `Enter a new non-default admin username:`".
     Continue to the next step.
   - If you do not wish to change the name of the "admin" user, enter "`n`" and confirm with "Enter".
     The command prompt is: `Default admin password must be change. Enter a new non-default admin password:`
     Skip the next two steps to change the user name.
4. Enter a new user name and confirm with "Enter". The new user name has at least 8 and maximum 250 characters.
   The command prompt is: "`Confirm new non-default admin username:`".
5. Enter the new user name again and confirm with "Enter".
   The command prompt is: "`Enter a new non-default admin username:`".
6. Enter a new password and confirm with "Enter".
   The new password must meet the password policy "High":
   - Password length: at least 8 characters, maximum 32 characters
   - At least 1 uppercase letter
   - At least 1 special character
   - At least 1 number
7. Repeat the new password.
   The command prompt is: `Confirm new non-default admin password:`
   Once you have logged in successfully, the status message "`Device transitioned to operational state. All setup functions are disabled`" appears. The command prompt is: "`CLI#`".

Log in to a configured device

1. Set up a SSH connection to the device and call the CLI.
   The login prompt is displayed. `login as:`
2. Enter the user name and confirm with "Enter".
   The command prompt is: `<User name>@<IP address>' password:`
3. Enter the password of the user and confirm with "Enter".
   Once you have logged in successfully, the command prompt is: "`CLI#`".

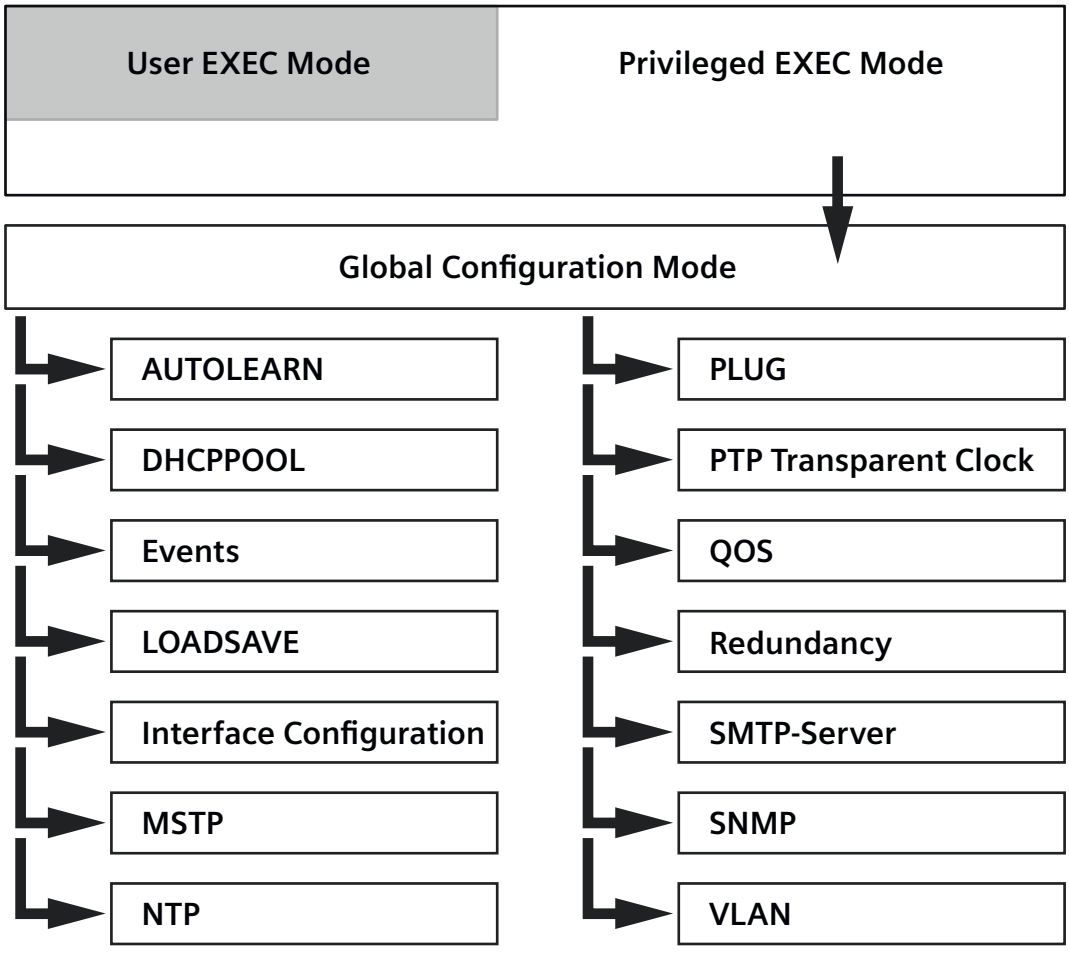
2.7 Protection from brute force attacks

To protect against brute force attacks, login to the device can be denied for a user or for the IP address of a user after a specific number of failed login attempts. The default setting for the maximum number of invalid login attempts for an IP address is "10". For users, the default value is "12". These values can be configured with the CLI commands `brute-force-prevention ip-specific-login-attempts` or `brute-force-prevention user-specific-login-attempts`.

2.8 Structure of the Command Line Interface

Grouping of the commands in the various modes

The commands of the Command Line Interface are grouped according to various modes. Apart from a few exceptions (`help`, `exit`), commands can only be called up in the mode to which they are assigned. This grouping allows different levels of access rights for each individual group of commands. The following graphic is an overview of the available modes.



User EXEC mode

This mode is active after you log in with the role "`user`" in a console window. In this mode, you can use `show` commands to display the current values of configuration parameters. It is not possible to modify parameters in this mode.

To be able to modify configuration parameters, you need to change to the Privileged EXEC mode.

Privileged EXEC mode

You change to this mode if you log in with the role "`admin`" or you enter the command `enable` in User EXEC mode. There are two ways of exiting the Privileged EXEC mode:

1. The `exit` command logs you out; the Login Prompt prompt appears.
2. The `disable` command brings you back one level from the Privileged EXEC mode to the User EXEC mode. (The `disable` command is not available in the User EXEC mode.)

Global configuration mode

In this mode, you can make basic configuration settings. In addition to this, you can also call up modes for the configuration of special interfaces or functions, for example to configure a VLAN. You change to this mode by entering `configure terminal` in the Privileged EXEC mode. To exit this mode, enter `end`.

Other configuration modes

From the Global configuration mode, you can change to other configuration modes for special tasks. These are either general configuration modes (for example line configuration, interface configuration) or protocol-specific configuration modes (SNTP, NTP).

2.9 The CLI command prompt

Overview

The Command Line Interface prompt shows the following information:

- The mode in which the CLI is currently operating.
  Most commands can only be called in a particular mode. You should therefore check the CLI mode based on the command prompt.
  - User Exec mode: `CLI>`
  - Privileged Exec mode and configuration modes: `CLI(...)#`

  Note

  Changing the system name

  When you change the system name, the command prompt also changes. The corresponding system name is then displayed instead of "`CLI`".

- The selected interface when the CLI is in an Interface Configuration mode.
  In the Interface Configuration mode, the parameters are configured for one specific interface. The command prompt is displayed in the form `CLI(config-if-$$$)#` where the placeholder `$$$` is replaced by the identifier of the Interface. You select the Interface by setting suitable parameters for the `interface` command.

- An identifier when the Trial mode is enabled.
  If you first test changes to the configuration and then want to discard them, disable the Auto save function with the `no auto-save` command. You are then in Trial mode.
  Changes to the configuration that you have not saved are indicated by an asterisk in front of the command prompt: `*CLI(...)#`.
  You save the changes to the configuration with the command `write startup-config`.
  With the `auto-save` command, you enable the Auto save function again.

Note

Upper and lower case

The Command Line Interface does not distinguish between upper case and lower case letters.

Make sure, however, that names used by the operating system or other programs are correctly written.

Blank

To use blanks in a text, enter the text in quotes, for example "H e l l o"

- Error messages
  The start of an error message is indicated by a `%` character.
- Notices
  The start of a notice is indicated by a `$` character.

2.10 Symbols of the CLI commands

Symbols for representing CLI commands

When setting parameters for CLI commands, the following characters are used:

Character	Meaning	
< ... >	mandatory parameter	Instead of the expression in parenthesis, you must enter a value
[...]	optional parameter	Instead of the expression in parenthesis, you can enter a value
(...)	Value or range of values	Enter a value to replace the expression in parenthesis
(... - ...)	Range of values	Enter a value from this range
{ ... }	Selection list	Select one more elements from the list
{ ... | ... }	exclusive selection	Select exactly one element from this list

These characters are used in combinations to describe mandatory and optional entries.

There is a general description of some of these combinations below:

Character combinations	Meaning
< variable >	Instead of the expression in parentheses<>, enter a permitted value
< variable (a - b) >	Instead of the expression in parentheses <>, enter a value from the range "a" to "b"

Character combinations	Meaning
[< variable 1 >< variable 2 >]	The parameter pair is optional. If you use the parameter assignment, you need to enter a permitted value to replace both expressions in parenthesis <>
[keyword < variable (a - b)>]	The parameter assignment is optional. If you use the keyword, you need to enter a value from the range "a" to "b" to replace the expression in parenthesis <>
[keyword < variable (a - b) unit >]	The parameter assignment is optional. If you use the keyword, you need to enter a value from the range "a" to "b" to replace the expression in parenthesis <>. "Unit" is one of the variables and is also replaced by the entry.
[keyword { A | B | C }]	The parameter assignment is optional. If you use the keyword, you need to specify exactly one of the values "A", "B" or "C"
keyword { [A] [B] [C] }	After the keyword, enter one or more of the values "A", "B" or "C"

2.11 Addresses and interface names

2.11.1 Naming interfaces

Addressing interfaces

The devices have several types of interface that are addressed in different ways.

Addressing physical interfaces

The following notation applies to all commands that address a physical interface:

- Enter the command "`interface`".
- Specify the interface type `<interface-type>`.
- After a space, enter the interface identifier, `<interface-id>`.
  The interface identifier is made up of the module number and the port number separated by a slash.

You call a Fast Ethernet interface on the second port of module 0 with the following command: `interface fa 0/2`

Addressing logical interfaces

The following notation applies to all commands that address a logical interface:

- Enter the command "`interface`".
- Enter the keyword for the logical interface.
  - `port-channel` (abbreviation: `po`)
  - `vlan`
- After a space, enter the number of the interface you assigned when you created it.
  - `<port-channel-id(1-8)>`
  - `<vlan-id(1-4094)>`

You call port channels as follows: `interface po 2`

You call VLAN ports as follows: `interface vlan 1`

Available physical interfaces

Available interface types

The devices support the following interface types:

interface-type	**Abbreviation/acronym**	**Devices**
fastethernet	fa	SCALANCE XB-200 SCALANCE XC-200 SCALANCE XF-200BA SCALANCE XF-200G SCALANCE XP-200 SCALANCE XR-300WG
gigabitethernet	gi	SCALANCE XC206-2SFP (depending on the pluggable transceivers) SCALANCE XC-200G SCALANCE XF-200G SCALANCE XP-200 SCALANCE XP-200G SCALANCE XR-300WG
extreme-ethernet	ex	SCALANCE XC-200 PoE SCALANCE XR-300WG PoE

Available interface identifiers

All physical interfaces of the devices are called module 0.

Available logical interfaces

- VLAN
  To be able to use a VLAN, create it with the `vlan` command.
- Link aggregation
  Multiple ports or connections between two devices are logically bundled together (aggregated) to achieve a higher data transmission rate and a lower failure risk.
  To add an interface to a link aggregation, use the `channel-group` command.

Identification of the interfaces in the command prompt of the Interface configuration mode

To configure the interface use the command `interface` in the global configuration mode.

Since you configure precisely one of the existing interfaces in the Interface configuration mode, the command prompt shows not only the mode but also the name of this interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

The placeholder `$$$` is replaced by the following name of the interface:

Type of interface	Command prompt
`fastethernet`	`cli(config-if-Fa$-$) #`
`gigabitethernet`	`cli(config-if-Gi$-$)#`
`extreme-ethernet`	`cli(config-if-Ex$-$)#`
`vlan`	`cli(config-if-vlan-$)#`
`port-channel`	`cli(config-if-po-$)#`

The placeholders `$` or `$-$` denote the numbering of the interface.

2.11.2 Address types, address ranges and address masks

Overview

Since the various types of addresses can be represented by different notations, the notations used in the Command Line Interface are shown below:

- IPv4 addresses
  Addresses for the Internet Protocol version 4 are written in the decimal notation of four numbers from the range 0 to 255, separated by a period.

  Note

  With leading zeros, the numbers are interpreted as octal numbers, e.g.: 192.168.070.071 → 192.168.56.57.

- Network masks
  A network mask is a series of bits that describes the network part of an IP address.
  The notation is normally decimal in keeping with the IP address.

- Alternative notation for network masks
  In contrast to the notation described above, network masks can also be represented as a number of 1 bits. The mask of the decimal representation 255.255.0.0 is then written as /16.
  The syntax is then for example: <ipaddress> / 16
  Note that there must be a space before and after the "/".
- MAC addresses
  In the syntax of the Command Line Interface, a MAC address is represented as a sequence of 6 bytes in hexadecimal format, in each case separated by a colon.
  The syntax is then, for example aa:aa:aa:aa:aa:aa
- Multicast addresses
  Layer 2 multicast addresses as used on this device use the notation of MAC addresses.
  For permitted address ranges, check the rules or ask your network administrator.

General CLI commands

3

This section describes commands that you can call up in any mode.

3.1 clear screen

Description

With this command, you clear the screen.

The command prompt is displayed.

Syntax

Call the command without parameters:

```
clear screen
```

Result

The screen is cleared.

The command prompt is displayed.

3.2 do

Description

With this command, you can execute the commands from the Privileged EXEC mode in any configuration mode.

Syntax

Call up the command with the following parameters:

```
do [command ]
```

To do this, you replace `[command ]` with the command from the Privileged EXEC mode that you want to execute.

Example

You are in the Interface configuration mode and you want to execute the `write startup-config` command from the Privileged EXEC mode.

```
cli(config-if-$$)# do write startup-config
```

Result

The command from the Privileged EXEC mode will be executed.

3.3 end

Description

With this command, you exit the configuration mode and are then in the Privileged EXEC mode.

Requirement

You are in a configuration mode.

Syntax

Call the command without parameters:

```
end
```

Result

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

3.4 exit

Description

With this command, you close the current mode.

Syntax

Call the command without parameters:

```
exit
```

Result

The current mode was exited. You are then at the next higher level.

If you are in Privileged EXEC Modus or in User EXEC Modus mode, you will be logged out.

3.5 Help functions and supported input

The Command Line Interface provides various functions that are helpful when making entries in the command line:

- `help`
- ?
- Command completion with the tab key
- Automatic completion of incomplete commands
- Paging in the list of most recently used commands
- Display of the list of most recently used commands (`show history`)

3.5.1 help

Description

With this command, you display the help entry for a command or the command list.

Syntax

Call up help with the following parameters:

```
help [command]
```

Here, you replace `[command]` with the command for which you require help.

If the command for which you require help consists of several words, enter these words without spaces.

Result

The syntax of the command is displayed.

Syntax

If you call up help without parameters, you will obtain a list of all permitted commands in the current mode:

```
help
```

Result

The mode-specific as well as the global commands are displayed.

Note

Incomplete command names

If you have specified an incomplete command when calling help, a list of all commands that start with the term you have entered is created.

3.5.2 The command "?"

Description

With this command, you call up the command list.

Syntax

Enter a question mark to obtain a list of all permitted commands in the current mode:

`?`

For this command, you do not need to press the enter key. The command executes immediately after you type the character.

Result

The mode-specific as well as the global commands are displayed.

Note

Incomplete command name

If you have specified an incomplete command when calling the help function, a list of all commands that start with the term you have entered is created.

Note

Output in pages

With long lists, the results are displayed as pages. If `-- more --` appears at the lower edge of the display, you can move to the next page with the spacebar. If the display is in pages, you cannot page back. You exit the page display with the `q` key.

3.5.3 Completion of command entries

Description

The command interpreter of the Command Line Interface supports you when you enter commands.

As soon as the first characters of the command have been entered in the input line, the system can complete the entry as long as the character string is unambiguous.

This can be repeated after entering further characters.

Procedure

Enter the first characters of the command.

Press the tab key.

Result

The command interpreter completes the input as long as the command is unambiguous.

If you enter a character string that cannot be completed to form a command, an error message is displayed.

- The command is not unique: `% Ambiguous Command`
- The command is unknown: `% Invalid Command`
- The command is incomplete: `% Incomplete command`

If the entry is not yet complete, enter further characters.

With `?`, you obtain a list of the possible commands.

Repeat this if necessary until the command is complete and can execute.

3.5.4 Abbreviated notation of commands

Description

The command interpreter of the Command Line Interface also detects commands if only the first character of the command or its parts is entered.

This is only possible if all the parts of the abbreviated input can be assigned to exactly one command or to the parts of the command.

Example

The `show event config` command can be replaced by the expression `sh e c`.

3.5.5 Reusing the last used commands

Description

The Command Line Interface saves the last 14 commands used in a list assigned to the particular mode. This can then only be called up in the relevant mode.

Example:
In the Global Configuration mode, all entered commands are saved. If you entered commands earlier in the Interface Configuration mode, these commands are not included in the list of the Global Configuration mode. You can only call up and reuse these commands in the Interface Configuration mode.

Procedure

You can page through the list of the commands most recently used using the arrow up and arrow down keys.

If the command you are looking for is displayed, you can edit the command line as required and execute the command with the enter key.

Further notes

You display the list of commands last used with the `show history` command. This function is available in every mode.

3.5.6 Working through a command sequence

Separators for multiple commands in one line

You can call up several commands one after the other in one line in the CLI.

Separate the commands with a semicolon (;).

After completing your input, start the processing of this command sequence with the enter key.

Example

The command sequence

```
CLI#conf t; int vlan 1; no ip address dhcp; ip address 192.168.1.1
255.255.255.0; end; write startup
```

has the same effect as:

```
CLI#conf t
CLI(config)#int vlan 1
CLI(config-if-vlan-1)#no ip address dhcp
CLI(config-if-vlan-1)#ip address 192.168.1.1 255.255.255.0
CLI(config-if-vlan-1)#end
CLI#write startup
```

3.5.7 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

3.5.7.1 show history

Description

This command shows the last 14 commands you entered.

The commands are listed in the order in which they were called up. The `show history` command is listed as the last command to be entered.

The list depends on the mode. In the Global configuration mode, the last 14 commands entered in this mode are displayed. These commands are not included in the list of the Interface configuration mode.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show history
```

Result

The list of used commands is displayed.

3.5.8 clear history

Description

This command deletes the last commands you entered.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
clear history
```

Result

The last commands to be input are deleted.

Further notes

You display a list of the last 14 commands entered with the `show history` command.

Configuration 4

The following is described in this section:

- System settings
- Saving and loading configurations and firmware
- Restart of the device and restoring the factory defaults
- Saving and restoring configuration backups

4.1 System

This section describes commands with which general system properties can be displayed and configured.

4.1.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.1.1.1 show broadcast-block config

Description

This command shows the broadcast blocking settings for ports.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show broadcast-block config [port <interface-type> <interface-id)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`port`	Keyword for a port description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The broadcast blocking settings for ports are displayed.

4.1.1.2 show cli-console-timeout

Description

This command shows the timeout setting of the CLI session.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show cli-console-timeout
```

Result

The timeout setting of the CLI session is displayed.

4.1.1.3 show coordinates

Description

This command shows the geographical coordinates.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show coordinates
```

Result

The geographical coordinates are displayed.

4.1.1.4 show counter discards

Description

This command shows the sum of all discarded packets within the last 24 hours as well as within the last 7 days.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

This`cli>` or `cli#`

Syntax

Call the command without parameters:
```
show counter discards
```

Result

It displays the sum of all discarded packets per time period.

4.1.1.5 show counter in-errors

Description

This command displays the sum of all received faults.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

This`cli>` or `cli#`

Syntax

Call the command without parameters:
`show counter in-errors`

Result

The sum of all received faults is displayed.

4.1.1.6 show device information

Description

This command shows information about the device.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

`show device information`

Result

The information about the device is displayed.

4.1.1.7 show environmental temperature

Description

This command shows the temperature values of internal and external modules of the device. The modules are only shown if they make temperature information available.

If the temperature value falls below or exceeds the displayed threshold values, the status changes accordingly. With the `event config` command, you can configure that you are informed of the status change by a message.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call the command without parameters:

`show environmental temperature`

Result

The temperature values are displayed.

4.1.1.8 show ethernetip

Description

This command shows the current EtherNet/IP configuration.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

`show ethernetip`

Result

The current EtherNet/IP configuration is displayed.

4.1.1.9 show hardware

Description

This command shows the type and number as well as the position of the installed interface cards of the system.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show hardware
```

Result

The table of interface cards is displayed.

The slot ID, the status and the type or name of the card is listed.

Note

With SCALANCE XB-200, SCALANCE XC-200, SCALANCE XP-200, SCALANCE XP-200G and SCALANCE XR-300WG, the slot ID is always 0. The table therefore always shows precisely one row.

4.1.1.10 show im

Description

This command shows information on device-specific vendor and maintenance data such as the article number, serial number, version numbers etc.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show im
```

Result

The information is displayed.

4.1.1.11 show interfaces

Description

This command shows the status and the configuration of one, several or all interfaces.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show interfaces [{ [<interface-type> <interface-id>]
[{ description | storm-control | flowcontrol | status }] | {vlan
<vlan-id(1-4094)> } |
port-channel <port-channel-id (1-8)> } | private-vlan mapping ]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`description`	Shows the description of the interface	-
`storm-control`	Shows the storm control settings.	-
`flowcontrol`	Shows the flow control settings.	-
`status`	Shows the status of the interface.	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`port-channel`	Keyword for a port-channel connection	-
`port-channel-id`	Number of the addressed port channel	1 ... 8
`private-vlan mapping`	Shows from which secondary PVLANs the IP interface of the primary PVLAN is reachable.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the status and configuration of all available interfaces will be displayed.

Result

The status and the configuration of the selected interfaces are displayed.

4.1.1.12 show interfaces ... counters

Description

This command shows the counters of one, several or all interfaces.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show interfaces [{ <interface-type> <interface-id> | vlan <vlan-
id(1-4094)> }] counters
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available counters.

Result

The counters of the selected interfaces are displayed.

Further notes

The counters are reset on restart or with the `clear counters` command.

4.1.1.13 show ip interface

show ip interface

Description

This command shows the configuration of one, several or all IP interfaces.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show ip interface [{vlan <vlan-id(1-4094)> | <interface-type>
<interface-id> }]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the configuration is displayed for all available IP interfaces.

Result

The configuration of the selected IP interface is displayed.

4.1.1.14 show lldp neighbors

Description

This command shows the current content of the neighborhood table.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show lldp neighbors [{brief | detail}]
```

The parameters have the following meaning:

Parameter	Description	Value range / note
`brief`	The following parameters are displayed in tabular form: • System Name • Device ID • interface	-
`detail`	The information is displayed in list form.	-

Result

The neighborhood table is displayed.

4.1.1.15 show lldp status

Description

This command shows per port whether LLDP frames are sent or received.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show lldp status [port {<interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`port`	Keyword for a port description.	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

The information is displayed.

4.1.1.16 show multicast-block config

Description

This command shows the multicast blocking settings for ports.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show multicast-block config [port <interface-type> <interface-id)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`port`	Keyword for a port description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If no parameters are specified, the settings for all ports are displayed.

Result

The multicast blocking settings for ports are displayed.

4.1.1.17 show nodes monitoring

Description

This command shows information on node monitoring of the ports or the specified port.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show nodes monitoring [port <interface-type> <interface-id>]
```

Parameter	Description	Range of values/note
`port`	Keyword for an interface.	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

Result

The number of nodes after which a warning is output is displayed for the ports or the specified port. If "-" is displayed as maximum number, this function is disabled. The number of nodes that were learned is also displayed.

4.1.1.18 show noa config

Description

This command shows the NOA configuration of the ports or the specified port.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show noa config [port <interface-type> <interface-id>]
```

Parameter	Description	Range of values/note
port	Keyword for an interface.	-
interface-type	Type or speed of the interface	Specify a valid interface.
interface-id	Module no. and port no. of the interface	

Result

The NOA configuration of the ports or of the specified port is displayed.

4.1.1.19 show pof status

Description

This command shows the current status and value of the power budget for interfaces with plastic optical fiber (POF) per port.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show pof status [port {<interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
port	Keyword for a port description.	-
interface-type	Type or speed of the interface	Specify a valid interface.
interface-id	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

Information on the current power is displayed.

4.1.1.20 show pof limit

Description

This command shows the maximum value of the power budget for interfaces with plastic optical fiber (POF) which triggers a message relating to the deterioration of the power budget.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show pof limit [port {<interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`port`	Keyword for a port description.	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

Information on the maximum power value is displayed.

4.1.1.21 show pnio

Description

This command shows the current PROFINET configuration.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

This`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show pnio
```

Result

The current PROFINET configuration is displayed.

4.1.1.22 show tcp connections

Description

With this command, you display the TCP connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show tcp connections
```

Result

The TCP connections are displayed.

4.1.1.23 show tcp listeners

Description

With this command, you display the TCP listeners.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show tcp listeners
```

Result

The TCP listeners are displayed.

4.1.1.24 show tcp retransmission details

Description

With this command, you display the details of the retransmissions.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show tcp retransmission details
```

Result

The details of the retransmissions are displayed.

4.1.1.25 show tcp statistics

Description

With this command, you display the statistical information of the TCP connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show tcp statistics
```

Result

The statistical information of the TCP connections is displayed.

4.1.1.26 show udp connections

Description

With this command, you display the UDP connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show udp connections
```

Result

The UDP connections are displayed.

4.1.1.27 show udp statistics

Description

With this command, you display the statistical information for the UDP connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show udp statistics
```

Result

The statistical information is displayed.

4.1.1.28 show unicast-block config

Description

This command shows the unicast blocking settings for ports.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show unicast-block config [port <interface-type> <interface-id)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`port`	Keyword for a port description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

The unicast blocking settings for ports are displayed.

4.1.1.29 show usage

Description

With this command, you display the CPU and RAM and flash usage as a percentage.

If the usage falls below or exceeds the displayed threshold values, the status changes accordingly. With the `event config` command, you can configure that you are informed of the status change by a message.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show usage [{cpu|ram|flash}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`cpu`	Display of the CPU usage and threshold values	-
`ram`	Display of the RAM usage and threshold values	-
`flash`	Display of the flash usage and threshold values	-

If you do not specify any parameters, the usage of CPU, RAM and flash is displayed.

Result

The information is displayed.

4.1.1.30 show versions

Description

This command shows the version information of the entire system.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show versions
```

Result

The version information of the entire system is displayed.

4.1.2 clear counters

Description

With this command, you reset the counters of an interface.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
clear counters [ <interface-type> <interface-id> ]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If no parameters are specified, the counters for all interfaces are reset.

Result

The counters of the interface are reset.

Further notes

You can display the statistical information of the interfaces with the `show interfaces ... counters` command.

4.1.3 clear line vty

Description

With this command, you close a console session on the device.

With the `forceful-clear` option, you close a session and that is not reacting.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call up the command with the following parameters:

```
clear line vty {<line-number(2-9)> | all} [forceful-clear]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`line-number`	Number of the connection that will be terminated	2 ... 9
`all`	terminates all connections	-
`forceful-clear`	closes a session that is not reacting	-

Result

The console session is closed.

Further notes

You show the logged-on users with the `show users` command.

4.1.4 configure terminal

Description

With this command, you change to the Global configuration mode.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
configure terminal
```

Result

You are now in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Further notes

You exit the Global configuration mode with the `end` command.

4.1.5 disable

With the commands `enable` and `disable` you temporarily change the function rights of the logged in user, the login data remains unchanged.

Description

With this command, you close the Privileged EXEC mode.

You are then in the User EXEC mode.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
disable
```

Result

You are in the User EXEC mode.

The command prompt is as follows:

```
cli>
```

4.1.6 enable

With the commands `enable` and `disable` you temporarily change the function rights of the logged in user, the login data remains unchanged.

Description

With this command, you change to the Privileged EXEC mode.

Requirement

You are in the User EXEC mode.

The command prompt is as follows:

```
cli>
```

Syntax

Call the command without parameters:

```
enable
```

Result

You are prompted to enter a password. After logging in successfully, you are in the Privileged EXEC mode. The command prompt is as follows:

```
cli#
```

4.1.7 logout

Description

With this command, you exit the Command Line Interface.

If you are connected to the device via telnet, the session is closed.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
logout
```

Result

The CLI session is ended and the Windows Login prompt is displayed.

4.1.8 ping

Description

With this command, you request a response from a device in the network.

This allows you to check whether or not another node is reachable.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameter assignment:

```
ping { <destination-address> | fqdn-name <FQDN> } [size
<byte(0-2080)>]
[count <packet_count (1-10)>] [timeout <seconds(1-100)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`destination-address`	Address of the device whose availability you want to check.	Enter a valid IPv4 address or a valid host name.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters If you have stored a suitable domain name, you can specify a host name.
`size`	Keyword for the size of the packets to be transferred.	-
`byte`	The size of the packets in bytes	0 ... 2080 Default: 32
`count`	Keyword for the number of packets to be requested	-

Parameter	Description	Range of values/note
`packet_count`	Number of packets	1 ... 10 Default: 3
`timeout`	Keyword for the response wait time.	-
`seconds`	Time to the timeout in seconds. If this time expires, the query is reported as "timed out".	1 ... 100 Default: 1

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default values are used.

Result

The messages relating to the response of the called node are displayed.

4.1.9 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.1.9.1 interface

Description

With this command, you change to the Interface configuration mode.

There you can edit the settings for one interface. You select the interface with the parameters of this command. If you specify a logical interface that does not exist, it will be created. The name of the selected interface is displayed in the command prompt.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
interface {vlan <vlan-id (1-4094)> | port-channel <port-channel-id
(1-8)> | <interface-type> <interface-id> }
```

The parameters have the following meaning:

Parameter	Description	Values
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094
port-channel	Keyword for a port channel connection	-
port-channel-id	Number of the addressed port channel	1 ... 8
interface-type	Type or speed of the interface	Specify a valid interface.
interface-id	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

The placeholder `$$$` is replaced by the following name of the interface:

Type of interface	Command prompt
port-channel	cli(config-if-po-$)#
vlan	cli(config-if-vlan-$)#
fastethernet	cli(config-if-Fa$-$)#
gigabitethernet	cli(config-if-Gi$-$)#
extreme-ethernet	cli(config-if-Ex$-$)#

The placeholders `$` or `$-$` denote the numbering of the interface.

The ranges of values for the logical interface VLAN and port channel can be found in the table above. You can only call up interfaces that you created with the `vlan` or `channel-group` command.

The ranges of values from the physical interfaces depend on the hardware configuration.

Additional notes

You exit the Interface configuration mode with the `end` or `exit` command.

You delete a logical interface with the `no interface` command.

You display the status and the configuration of the interfaces with the `show interfaces` command.

4.1.9.2 no interface

Description

With this command, you delete a logical interface.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no interface { vlan <vlan-id (1-4094)> | port-channel <port-channel-
id(1-8)> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`port-channel`	Keyword for a port channel connection	-
`port-channel-id`	Number of the addressed port channel	1 ... 8

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The logical interface is deleted.

Further notes

You configure an interface with the `interface` command.

You display the status and the configuration of the interfaces with the `show interfaces` command.

4.1.9.3 cli-console-timeout

Description

With this command, you activate the automatic logout and you configure the timeout setting for the CLI session.

Note

No automatic logout from the CLI

If the connection is not terminated after the set time, check the "Keep alive" setting on the Telnet client.

If the interval is shorter than the configured time, the connection is kept alive although no user data is transferred. You have set, for example, 300 seconds for the automatic logoff and the "Keep alive" function is set to 120 seconds. In this case, a packet is sent every 120 seconds that keeps the connection up.

- Turn off the "Keep alive" function. (Interval time=0)
  or
- Set the interval high enough so that the underlying connection is terminated when there is inactivity.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
cli-console-timeout [<seconds(60-600)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`seconds`	Time in seconds until automatic logout after the last entry	60 ... 600 Default: 300

Result

The time is configured and automatic logout is enabled.

Further notes

You disable automatic logout with the `no cli-console-timeout` command.

You display the current timeout setting with the `show cli-console-timeout` command.

4.1.9.4 no cli-console-timeout

Description

With this command, you disable the automatic logout.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no cli-console-timeout`

Result

Automatic logout is disabled.

Further notes

You enable automatic logout with the `cli-console-timeout` command.

You display the current timeout setting with the `show cli-console-timeout` command.

4.1.9.5 coordinates height

Description

With this command, you enter the geographical height.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

```
coordinates height <meter>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
meter	Geographical height	Max. 32 characters Enter the value for the geographical height over or under zero (sea level) in meters. To use spaces in the input, enter the height with quotation marks: `coordinates height "123 456"`

Result

The geographical height has been created.

Further notes

You display the coordinates with the `show coordinates` command.

4.1.9.6 coordinates latitude

Description

With this command, you enter the latitude.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
coordinates latitude <latitude>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`latitude`	Latitude	Max. 32 characters Enter the value for north or south latitude. To use spaces in the entry, enter the latitude in quotes: `coordinates latitude "123 456"`

Result

The latitude has been created.

Further notes

You display the coordinates with the `show coordinates` command.

4.1.9.7 coordinates longitude

Description

With this command, you enter the longitude.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
coordinates longitude <longitude>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`longitude`	Longitude	Max. 32 characters Enter the value for east or west longitude. To use spaces in the entry, enter the longitude in quotes: `coordinates longitude "123 456"`

Result

The longitude has been created.

Further notes

You display the coordinates with the `show coordinates` command.

4.1.9.8 environmental temperature entry

Description

You configure thresholds for internal and external modules of the device with this command The modules are only shown if they make diagnostic information available. If you add or remove a module, the display is automatically adapted.

If the diagnostic value falls below or exceeds the configured thresholds, the status changes accordingly. With the `event config` command, you can configure a notification of the status change via a message.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
environmental temperature entry <id> {[high {critical | warning}
<celsius(0-150)>] | [low {critical | warning} <celsius(-60 - 0)>]}
```

The parameters have the following meaning:

Parameter	Description	Values
`id`	ID of the device housing or a plugged-in pluggable transceiver. ID "0" corresponds to the device housing. Each plugged-in pluggable transceiver is automatically assigned an ID, starting with 1. You can show the Entry ID and the name of the module with the `show environmental temperature` command. The port number and the name of the SFP is output with the name.	-
`high`	Keyword for the high threshold	-
`critical`	Severity level "Critical" If the high threshold is exceeded, the status changes to "Critical".	-

Parameter	Description	Values
`warning`	Severity level "Warning" If the high threshold is exceeded, the status changes to "Warning".	-
`celsius`	Temperature in °C The value can have a tolerance of +/- 3 °C.	0 ... 150
`low`	Keyword for the low threshold	-
`critical`	Severity level "Critical" If the low threshold is fallen below, the status changes to "Critical".	-
`warning`	Severity level "Warning" If the low threshold is fallen below, the status changes to "Warning".	-
`celsius`	Temperature in °C The value can have a tolerance of +/- 3 °C.	-60 ... 0

Result

The thresholds have been specified.

Additional notes

You enable the monitoring of the thresholds with the `environmental diagnostics threshold monitoring` command.

You show the current diagnostic values and thresholds and the status with the `show environmental temperature` command.

4.1.9.9 environmental diagnostics threshold monitoring

Description

This command enables the monitoring of thresholds for internal and external modules of the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
environmental diagnostics threshold monitoring
```

Result

The monitoring of the thresholds is enabled.

Additional notes

You disable the monitoring of the thresholds with the `no environmental diagnostics threshold monitoring` command.

You configure the thresholds with the `environmental temperature entry` command.

You show the current setting with the `show environmental temperature` command.

4.1.9.10 no environmental diagnostics threshold monitoring

Description

This command disables the monitoring of thresholds for internal and external modules of the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no environmental diagnostics threshold monitoring
```

Result

The monitoring of the thresholds is disabled.

Additional notes

You enable the monitoring of the thresholds with the `environmental diagnostics threshold monitoring` command.

You show the current setting with the `show environmental temperature` command.

4.1.9.11 ethernetip

Description

With this command, you set whether EtherNet/IP will be enabled or disabled after the next device restart.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`ethernetip {off|on}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`off`	EtherNet/IP will be disabled after the next restart.	-
`on`	EtherNet/IP will be enabled after the next restart.	• When EtherNet/IP is turned on, PROFINET is turned off. The switchover from EtherNet/IP and PROFINET has no effect on DCP. • If a PROFINET connection is established; in other words the PROFINET AR status is "Online", you cannot enable EtherNet/IP.

Result

EtherNet/IP is enabled or disabled after the next restart.

Further notes

You can display the current EtherNet/IP configuration with the `show ethernetip` command.

You restore the default settings of the EtherNet/IP profile with the `restart` command.

4.1.9.12 ethernetip dlr

Description

With this command, you specify whether the Device Level Ring (DLR) protocol is enabled for the device.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command with the following parameters:

`ethernetip dlr {off | on}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`off`	Device Level Ring is disabled.	-
`on`	Device Level Ring is enabled.	-

Result

The Device Level Ring (DLR) protocol is enabled or disabled for the device.

Additional notes

You display the current EtherNet/IP configuration with the `show ethernetip` command.

You define the DLR ports with the `ethernetip dlr p1 p2` command.

You restore the default settings of the EtherNet/IP profile with the `restart` command.

4.1.9.13 ethernetip dlr p1 p2

Description

With this command, you specify which ports take on the function of the DLR ports.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command with the following parameters:

```
ethernetip dlr p1 {<interface-type> <interface-id>} p2 {<interface-
type> <interface-id>}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`p1`	Keyword for DLR port 1.	-
`interface-type`	Type or speed of DLR port 1.	Specify a valid interface.
`interface-id`	Module no. and port no. of DLR port 1.	
`p2`	Keyword for DLR port 2.	-
`interface-type`	Type or speed of DLR port 2.	Specify a valid interface.
`interface-id`	Module no. and port no. of DLR port 2.	

Result

The DLR ports are defined.

Additional notes

You display the current EtherNet/IP configuration with the `show ethernetip` command.

You enable or disable the Device Level Ring (DLR) protocol with the `ethernetip dlr` command.

You restore the default settings of the EtherNet/IP profile with the `restart` command.

4.1.9.14 ethernetip dlr vlan

Description

With this command, you assign the DLR VLAN to the interface.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ethernetip dlr vlan <vlan-id (0-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan-id`	Number of the addressed VLAN	0: DLR VLAN=0 [1)] 1 ... 4094: DLR VLAN=1

[1)] VLAN=0 is only supported by the following devices in 802.1D Transparent Bridge to a limited extent and must be configured as DLR VLAN.

6GK5 204-2AA00-2GF2	6GK5 206-2BS00-2FC2	6GK5 216-0BA00-2AC2
6GK5 204-2AA00-2YF2	6GK5 208-0BA00-2AB2	6GK5 216-0BA00-2FC2
6GK5 205-3BB00-2AB2	6GK5 208-0BA00-2AC2	6GK5 216-0BA00-2TB2
6GK5 205-3BB00-2TB2	6GK5 208-0BA00-2FC2	6GK5 216-0HA00-2AS6
6GK5 205-3BD00-2AB2	6GK5 208-0BA00-2TB2	6GK5 216-0HA00-2ES6
6GK5 205-3BD00-2TB2	6GK5 208-0HA00-2AS6	6GK5 216-0HA00-2TS6
6GK5 205-3BF00-2AB2	6GK5 208-0HA00-2ES6	6GK5 216-0UA00-5ES6
6GK5 205-3BF00-2TB2	6GK5 208-0HA00-2TS6	6GK5 224-0BA00-2AC2
6GK5 206-2BB00-2AB2	6GK5 208-0UA00-5ES6	6GK5 324-0BA00-2AR3
6GK5 206-2BB00-2AC2	6GK5 213-3BB00-2AB2	6GK5 324-0BA00-3AR3
6GK5 206-2BB00-2TB2	6GK5 213-3BB00-2TB2	6GK5 328-4FS00-2AR3
6GK5 206-2BD00-2AB2	6GK5 213-3BD00-2AB2	6GK5 328-4FS00-2RR3
6GK5 206-2BD00-2AC2	6GK5 213-3BD00-2TB2	6GK5 328-4FS00-3AR3
6GK5 206-2BD00-2TB2	6GK5 213-3BF00-2AB2	6GK5 328-4FS00-3RR3
6GK5 206-2BF00-2AB2	6GK5 213-3BF00-2TB2	6GK5 328-4SS00-2AR3
6GK5 206-2BF00-2TB2	6GK5 216-0BA00-2AB2	6GK5 328-4SS00-3AR3
6GK5 206-2BS00-2AC2		

All other devices support VLAN=0 without restrictions and do not need to be configured.

Result

The interface is added to the DLR VLAN and the corresponding VLAN ID is set.

Additional notes

You display the current EtherNet/IP configuration with the `show ethernetip` command.

You define the DLR ports with the `ethernetip dlr p1 p2` command.

You restore the default settings of the EtherNet/IP profile with the `restart` command.

4.1.9.15 pnio

Description

With this command, you configure the setting for PROFINET after the next restart of the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`pnio {off|on}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`off`	PROFINET is disabled.	If a PROFINET connection is established; in other words the PROFINET AR status is "Online", you cannot disable PROFINET.
`on`	PROFINET is activated.	When PROFINET is turned on, EtherNet/IP is turned off. The switchover from PROFINET and EtherNet/IP has no effect on DCP.

Result

PROFINET is enabled or disabled after the next restart.

Further notes

You display the current PROFINET configuration with the `show pnio` command.

You restore the default settings of the PROFINET profile with the `restart` command.

4.1.9.16 pnio station-name

Description

With this command, you enter a PROFINET device name.

Note

Activating read and write permissions on the DCP server

Before you assign a PROFINET device name, set the read and write permissions for the DCP server to read-write with the `dcp server` command.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
pnio station-name <station name>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`station name`	Input box for the name	max. 255 characters

Result

The name has been created.

Additional notes

You display the general device information with the `show pnio` command.

4.1.9.17 system contact

Description

With this command, you enter contact information for the system.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
system contact <contact info>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`contact info`	Input box for contact information	max. 255 characters

Result

The contact information is created in the system.

Further notes

You display the general device information with the `show device information` command.

4.1.9.18 system location

Description

With this command, you enter the location information for the system.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
system location <location name>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`location name`	Input box for the location information	max. 255 characters

Result

The location information is created in the system.

Further notes

You display the general device information with the `show device information` command.

4.1.9.19 system name

Description

This command, you enter a name for the system.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

`system name <system name>`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`system name`	Input box for the name	max. 255 characters

Result

The name is created in the system.

The corresponding system name is displayed instead of "`cli`" in the command prompt:
`system name``(config)#`

Further notes

You display the general device information with the `show device information` command.

4.1.10 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.1.10.1 alias

Description

With this command, you assign a name to an interface. The name only provides information and has no effect on the configuration.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`alias <interface-name>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`interface-name`	Name of the interface	max. 63 characters

Result

The interface was assigned a name.

Further notes

You delete the name of the interface with the `no alias` command.

4.1.10.2 no alias

Description

With this command, you delete the name of the interface.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

`no alias`

Result

The name of the interface is removed.

Further notes

You configure the name of the interface with the `alias` command.

4.1.10.3 broadcast-block

Description

With this command, you enable the blocking of broadcast frames on an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameter assignment:

```
broadcast-block
```

Result

Broadcast frames are blocked.

Further notes

You disable the blocking of broadcast frames with the `no broadcast-block` command.

4.1.10.4 no broadcast-block

Description

With this command, you disable the blocking of broadcast frames on an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameter assignment:

```
no broadcast-block
```

Result

The blocking of broadcast frames is disabled.

Further notes

You enable the blocking of broadcast frames with the `broadcast-block` command.

4.1.10.5 duplex

Description

Electrical interfaces can be operated in full duplex mode or half duplex mode. The options here depend on the connected device.

Optical connections are always operated in full duplex mode since they have a fiber for each transmission direction.

With this command, you configure the duplex mode of an interface. The same mode must be set for connected interfaces.

Requirement

- Autonegotiation is disabled.
- You are in the Interface configuration mode of an electrical interface.
  The command prompt is as follows:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

Parameter	Description	Range of values / note
`full`	The Interface will be operated in full duplex mode.	Default: `full`
`half`	The Interface will be operated in half duplex mode	-

Result

The duplex mode of the interface is configured.

Further notes

You can reset the duplex mode of the Interface to the default value with the `no duplex` command.

You disable autonegotiation with the `no negotiation` command.

4.1.10.6 no duplex

Description

With this command, you reset the duplex mode of an interface to the default value.

The default value is `full`.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no duplex
```

Result

The duplex mode of the Interface is reset to the default value.

Further notes

You configure the duplex mode of the interface with the `duplex` command.

4.1.10.7 fsu-support

Description

With this command, you enable accelerated connection establishment on an interface with a transmission speed of 100 Mbps. Autonegotiation and autocrossover are switched off in this case. Fast startup can only be performed for gigabit device variants. It does not work on ring, standby or interconnection ports.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

`fsu-support`

Result

The function is enabled.

Additional notes

You disable fast startup with the `no fsu-support` command.

4.1.10.8 no fsu-support

Description

With this command, you disable accelerated connection establishment on an interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

`no fsu-support`

Result

The function is disabled.

Additional notes

You enable fast startup with the `fsu-support` command.

4.1.10.9 lldp

Description

With this command, you enable the sending and receipt of LLDP packets on the interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command with the following parameters:

`lldp {transmit | receive}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`transmit`	The sending of LLDP packets is enabled.	Default: enabled
`receive`	The receipt of LLDP packets is enabled.	Default: enabled

Note
Enabling both options

When you call this command, you can only select one option.

If you want to enable both options, call up the command again.

Result

Sending or receipt of LLDP packets is enabled.

Additional notes

You disable the sending or receipt of LLDP packets with the `no lldp` command.

4.1.10.10 no lldp

Description

With this command, you disable the sending or receipt of LLDP packets on the interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`no lldp{transmit|receive}`

The parameters have the following meaning:

Parameter	Description
`transmit`	the sending of LLDP packets is disabled
`receive`	the receipt of LLDP packets is disabled

Note

Disabling both options

When you call this command, you can only select one option.

If you want to disable both options, call up the command again.

Result

Sending or receipt of LLDP packets is disabled.

Further notes

You enable the sending or receipt of LLDP packets with the `lldp` command.

4.1.10.11 media type

Description

With this command, you configure the mode of a combo port.

Note

This command only influences combo ports.

If you attempt to configure a different port with this command, an error message will be displayed.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`media-type {auto|rj45|sfp}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`auto`	The `auto` mode is enabled for the combo port. In this mode, the SFP transceiver port has priority. As soon as a pluggable transceiver is plugged in, an existing connection at the fixed RJ-45 port is terminated. If no pluggable transceiver is plugged in, a connection can be established via the built-in RJ-45 port.	Default: `auto`
`rj45`	The `rj45` mode is enabled for the combo port. In this mode, the fixed RJ-45 port is used independent of the SFP transceiver port. If a pluggable transceiver is plugged in, it is disabled and the power turned off.	-
`sfp`	The `sfp` mode is enabled for the combo port. In this mode, the SFP transceiver port is used independent of the fixed RJ-45 port. If an RJ-45 connection is established, it is terminated because the power of the RJ-45 port is turned off.	-

Result

The mode of the combo port is configured.

Further notes

You display the mode of a combo port with the command `show interface` and the parameter `status`.

4.1.10.12 multicast-block

Description

With this command, you enable the blocking of multicast frames on an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

`multicast-block`

Result

Multicast frames are blocked.

Further notes

You disable the blocking of multicast frames with the `no multicast-block` command.

4.1.10.13 no multicast-block

Description

With this command, you disable the blocking of multicast frames on an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

`no multicast-block`

Result

The blocking of multicast frames is disabled.

Further notes

You enable the blocking of multicast frames with the `mulitcast-block` command.

4.1.10.14 nodes monitoring action

Description

With this command, you define an action that is triggered when the number of monitored nodes is exceeded. The action is revoked as soon as the number is no longer exceeded.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:

```
nodes monitoring action { no | pdown | pdowntimeout }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`no`	No action when exceeded	-
`pdown`	The port is disabled.	-
`pdowntimeout`	The port is disabled. The status is checked again every 10 minutes.	-

Result

The action is specified.

Additional notes

You display information on node monitoring of the ports with the `show nodes monitoring` command.

4.1.10.15 nodes monitoring threshold

Description

With this command, you configure the number of learned MAC addresses after which a warning is output.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
nodes monitoring threshold <threshold value(0-7999)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`threshold value`	The number of learned MAC addresses after which a warning is output.	0 ... 7999 With the value "0", you disable the function.

Result

The number of learned MAC addresses after which a warning is output is configured for the port.

Additional notes

You display information on node monitoring with `show nodes monitoring`.

4.1.10.16 noa port config

Description

NOA (NAMUR Open Architecture) is a concept for data exchange in the process industry with the purpose of transferring data from the field level to a cloud. A SCALANCE XC-200 can take on the function of a NOA IT/OT switch and separate pure IT networks from pure OT networks. Communication to both networks is also possible. The switch separates the networks based on ports, i.e. a port either belongs to the IT network or to the OT network or to both networks. You use the command `noa port config` to determine which network the port belongs to.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
noa port config {otPort | itPort | itotPort}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`otPort`	The port belongs to the OT network.	-
`itPort`	The port belongs to the IT network.	-
`itotPort`	The port belongs to the OT network and the IT network.	Default

Result

The NOA functionality of the port is configured.

Additional notes

It shows the NOA configuration of the ports with the `show noa config` command.

4.1.10.17 negotiation

Description

With this command, you enable autonegotiation of connection parameters on an interface.

Autonegotiation must be set for every interface of connected interfaces.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
negotiation
```

Result

The automatic negotiation of connection parameters on an interface is activated.

Further notes

You disable the autonegotiation of connection parameters with the `no negotiation` command.

4.1.10.18 no negotiation

Description

With this command, you disable autonegotiation of connection parameters on an interface.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no negotiation
```

Result

The automatic negotiation of connection parameters on an interface is deactivated.

Further notes

You enable the autonegotiation of connection parameters with the `negotiation` command.

4.1.10.19 shutdown

Description

With this command, you shut down the interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

`shutdown [complete]`

The parameter has the following meaning:

Parameter	Description	Range of values / note
without parameters	The interface is disabled but the connection remains.	-
`complete`	The interface is disabled and the connection to the partner device is terminated.	For every optical port that you disable with the `shutdown complete` command, the current consumtion of the device is reduced by 30 mA.

Result

The Interface is shut down.

If you execute this command without parameters, a connection remains displayed. The LED for the port status flashes. However no data is sent or received.

Further notes

You activate the interface with the `no shutdown` command.

You can display the status of this function and other information with the `show interfaces`command.

4.1.10.20 no shutdown

Description

With this command, you shut down an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no shutdown
```

Result

The Interface is activated.

Further notes

You deactivate the interface with the `shutdown` command.

You can display the status of this function and other information with the `show interfaces`command.

4.1.10.21 power

Description

With this command, you enable or disable the interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:

```
power {down | up}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`down`	The interface is switched off.	-
`up`	The interface is switched on.	-

Result

The Interface is switched off or switched on.

Additional notes

You can display information about the status of the interfaces with the `show interfaces status` command.

4.1.10.22 speed

Description

With this command, you configure the transmission speed of an interface.

The transmission speed can only be configured for electrical data transfer. On optical connections, the transmission speed is fixed.

Requirement

- Autonegotiation is disabled.
- You are in the Interface configuration mode of an electrical interface.
  The command prompt is as follows:
  `cli(config-if-$$$)#`

Syntax

Call the command with the following parameters:

`speed {10 | 100 | 1000 | 2500 | 5000 | 10000}`

The parameters have the following meaning:

Parameter	Description
10	Transmission speed 10 Mbps
100	Transmission speed 100 Mbps
1000	Transmission speed 1000 Mbps
2500	Transmission speed 2500 Mbps: Only with SCALANCE XR-300WG for the 10 gigabit ports
5000	Transmission speed 5000 Mbps: Only with SCALANCE XR-300WG for the 10 gigabit ports
10000	Transmission speed 10000 Mbps

Result

The transmission speed of the interface is configured.

4.1.10.23 unicast-block

Description

With this command, you enable the blocking of unknown unicast frames on an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

`unicast-block`

Result

Unicast frames are blocked.

Further notes

You disable the blocking of unicast frames with the `no unicast-block` command.

You display the status of this function with `show unicast-block config`.

4.1.10.24 no unicast-block

Description

With this command, you disable the blocking of unknown unicast frames on an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

`no unicast-block`

Result

The blocking of unicast frames is disabled.

Further notes

You enable the blocking of unicast frames with the `unicast-block` command.

You display the status of this function with `show unicast-block config`.

4.1.10.25 unicast-mac flush

Description

With the command, you configure which addresses are deleted from the FDB (Forward Database) when a link-down occurs on a port.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
unicast-mac flush {disabled | port | full}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`disabled`	In the event of a link-down for a port, the FDB remains unchanged.	-
`port`	In the event of a link-down for a port, only the FDB entries belonging to the corresponding port are deleted.	-
`full`	In the event of a link-down for a port, all entries in the FDB are deleted.	Default

Result

In the event of a link-down for a port, the FDB is changed according to the configuration carried out.

4.2 Load and Save

This section describes commands for displaying, copying, saving and downloading files for the device.

Note

Note that during the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory configuration settings after the firmware has been installed.

4.2.1 File list

Overview of the file types

The table of file types contains the following areas.

Area	File type	Description	Upload	Save	Delete[1)]
Update	Firmware	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device. An installed firmware version can be updated to a previous version in this way. After the downgrade process is complete, the device is reset to factory settings following a restart.	X	X	--

Area	File type	Description	Upload	Save	Delete[1)]
Configuration	Config	This file contains the start configuration. Among other things, this file contains the definitions of the users, roles, groups and function rights. The passwords are stored in the "Users" file.	X	X	--
	ConfigPack	Detailed configuration information, for example, startup configuration, users, certificates, favorites, firmware of the device (if saved as well).	X	X	--
	LoginWelcome-Message	The txt file contains the desired text or the ASCII type. Only pure text files in ASCII format are supported.	X	X	X
	RunningCLI	Text file with CLI commands This file contains an overview of the current configuration in the form of CLI commands. Passwords are masked in this file as follows: [PASSWORD] You can download the text file. The file is not intended to be uploaded again unchanged.	--	X	--
	RunningSINEMA-Config	You save the current device configuration in this file type for transfer to STEP 7 Basic/Professional. The file can be imported in STEP 7 Basic/Professional and installed on a device with the same article number and firmware version. Before you can save a file, you must assign a password for the "RunningSINEMAConfig" in the WBM under "System > Load&Save > Passwords". You also need this password to import the file into STEP 7 Basic/Professional. See also "SINEMAConfig"	--	X	--
	Script	Text file with CLI commands You can upload a script file in a device. The CLI commands it contains are executed accordingly. CLI commands for saving and loading files cannot be executed with the CLI script file.	X	--	--
	SINEMAConfig	You load configuration data that was exported via STEP 7 Basic/Professional for transfer to the WBM with this file type. To load a file, you must assign a password for the "SINEMAConfig" under "System > Load&Save > Passwords". You also need this password to export the file from STEP 7 Basic/Professional. See also "RunningSINEMAConfig"	X	--	--
	Users	File with user names and passwords	X	X	--
	WBMFav	WBM favorites This file contains the favorites that you created in the WBM. You can download this file and upload it to other devices.	X	X	X

Area	File type	Description	Upload	Save	Delete[1)]
Certificate & Key	HTTPSCert	Default HTTPS certificates including key The preset and automatically created HTTPS certificates are self-signed. We strongly recommend that you create your own HTTPS certificates and make them available. We recommend that you use HTTPS certificates signed either by a reliable external or by an internal certification authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. The following file types can be loaded into the device. • .pem To successfully load an HTTPS certificate with this data type into the device, the certificate must include the unencrypted private key. • .p12 For HTTPS certificates with this file type, the private key is encrypted and secured with a password. To load the certificate successfully into the device, enter the password specified for the file on the WBM page "Passwords". **It is recommended that you use password-protected certificates in the PKCS#12 format.** The following certificates are supported: • ECDSA certificates created with secp521r1 (NIST P-521) • RSA certificates with a maximum key length of 2048 bits • ECC certificates with a key length of 256 bits	X	X	X
	SSHPrivate-KeyECDSA	SSH private key (ECDSA) The SSH key ecdsa-sha2-nistp521 is supported. There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords".	X	X	X
	SSHPrivateKeyR-SA	SSH private key (RSA) with and without password The following SSH keys are supported: • rsa-sha2-512 • rsa-sha2-256 There are files to which access is password-protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords".	X	X	X

Area	File type	Description	Upload	Save	Delete[1)]
Service & Log	Debug	This file contains information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk.	--	X	X
	DebugExt	This file contains more detailed information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk. Saving the file may take some time.	--	X	--
	LogFile	File with entries from the event log table	--	X	--
	StartupInfo	Startup log file This file contains the messages that were entered in the log file during the last startup.	--	X	--
Information	EDS	Electronic Data Sheet (EDS) Electronic data sheet for describing devices in the EtherNet/IP mode	--	X	--
	GSDML	PROFINET information on the device properties	--	X	--
	MIB	Private MSPS MIB file "Scalance_m_msps.mib"	--	X	--

1) Deletion is only possible via HTTP/HTTPS.

4.2.2 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.2.2.1 show loadsave minimum config-file version

Description

This command shows the minimum version that a configuration file must have to be loaded into the device.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show loadsave minimum config-file version
```

Result

The version is shown.

4.2.2.2 show loadsave files

Description

This command shows the current Load&Save file information.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show loadsave files
```

Result

The current Load&Save file information is displayed.

4.2.2.3 show loadsave stftp

Description

This command shows the current configuration of the SFTP server for Load&Save.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show loadsave sftp
```

Result

The current configuration of the SFTP server for Load&Save is displayed.

4.2.2.4 show loadsave tftp

Description

This command shows the current configuration of the TFTP server for Load&Save.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show loadsave tftp
```

Result

The current configuration of the TFTP server for Load&Save is displayed.

4.2.3 load

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Description

With this command, you load the files from a TFTP server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
load {tftp | sftp} {ipv4 <ucast_addr> | fqdn-name <FQDN>} [port
<tcp port (1-65535)>]
```

```
file <filename> filetype <filetype>[user <username>] [password
<password>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`tftp`	Keyword for a TFTP server	-
`sftp`	Keyword for a TFTP server	-
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	Value for an IPv4 unicast address of the server	Enter a valid IPv4 unicast address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name) of the server	Maximum of 100 characters
`port`	Keyword for the port of the server via which the TFTP/SFTP connection runs	-
`tcp port`	Number of the port	1 ... 65535 Default: • 69 (TFTP) • 22 (SFTP)
`file`	Keyword for a file name to be assigned	-
`filename`	Name of the file	Max. 100 characters
`filetype`	Keyword for the file type to be loaded	-
`filetype`	Name of the file type	Max. 100 characters

The following parameters are only available for an SFTP server:

Parameter	Description	Range of values/note
`user`	Keyword for the user name	-
`username`	The user name	Enter a valid user name.
`password`	Keyword for the password	-
`password`	The password	Enter a valid password.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The file is loaded on the device from the TFTP server.

Additional notes

With the `show loadsave files` command, you can display the file types.

4.2.4 save

Description

With this command, you save files on a TFTP server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
save filetype <filetype> {tftp | sftp} {ipv4 <ucast_addr> | fqdn-
name <FQDN>}
```

```
[port <tcp port (1-65535)>] file <filename>[user <username>]
[password <password>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`filetype`	Keyword for a file type to be loaded	-
`filetype`	Name of the file type	Max. 100 characters
`tftp`	Keyword for a TFTP server	-
`sftp`	Keyword for an SFTP server	-
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	Value for an IPv4 unicast address of the server	Enter a valid IPv4 unicast address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name) of the server	Maximum of 100 characters
`port`	Keyword for the port of the server via which the TFTP/SFTP connection runs	-
`tcp port`	Number of the port	1 ... 65535 Default: • 69 (TFTP) • 22 (SFTP)
`file`	Keyword for a file name to be assigned	-
`filename`	Name of the file	Max. 100 characters

The following parameters are only available for an SFTP server:

Parameter	Description	Range of values/note
`user`	Keyword for the user name	-
`username`	The user name	Enter a valid user name.
`password`	Keyword for the password	-
`password`	The password	Enter a valid password.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The file is saved on the TFTP server.

Additional notes

With the `show loadsave files` command, you can display the file types.

4.2.5 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.2.5.1 loadsave

Description

With this command, you change to the LOADSAVE configuration mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

`loadsave`

Result

You are now in the LOADSAVE configuration mode.

The command prompt is as follows:

`cli(config-loadsave)#`

Further notes

You exit the LOADSAVE configuration mode with the `exit` command.

4.2.6 Commands in the LOADSAVE configuration mode

This section describes commands that you can call up in the LOADSAVE configuration mode.

In global configuration mode, enter the `loadsave` command to change to this mode.

You display the valid file types for the commands in the LOADSAVE Configuration mode with the global command `show loadsave tftp`.

- If you exit the LOADSAVE configuration mode with the `exit` command, you return to the Global Configuration mode.
- If you exit the LOADSAVE configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in LOADSAVE configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

For information on the file types , refer to this list (Page 123).

4.2.6.1 delete

Description

With this command, you call up the possible files or delete a specific file.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

`cli(config-loadsave)#`

Syntax

Call up the command with the following parameters:

```
delete { showfiles | filetype <filetype> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`showfiles`	Shows the available files	-
`filetype`	Keyword for the file type to be deleted	-
`filetype`	Name of the file type	max. 100 characters

Result

The files are displayed or the file is deleted.

Further notes

With the "`show loadsave files`" command, you can display the file types.

4.2.6.2 password

Description

With this command, you activate and configure the password for a file.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

```
cli(config-loadsave)#
```

Syntax

Call up the command with the following parameters:

```
password { showfiles | filetype <filetype> [pw <password>] }
```

The parameters have the following meaning:

Parameter	Description	Values
`showfiles`	Shows the available files. The status is displayed in addition for the HTTPSCert file type. The available options are as follows: • Invalid The password does not match the certificate. The default certificate is used after a restart. • Valid The password matches the certificate. The downloaded certificate is used after a restart. • - No password was assigned. The default certificate is used after a restart.	-
`filetype`	Keyword for the file type.	-
`filetype`	Name of the file type	max. 100 characters
`pw`	Keyword for the password	-
`password`	Password	Enter the password for the file.

Result

The password for the file is configured and activated.

Additional notes

You disable the password with the `no password` command.

4.2.6.3 no password

Description

With this command, you disable the password for a file.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

```
cli(config-loadsave)#
```

Syntax

Call up the command with the following parameters:

```
no password { showfiles | filetype <filetype>}
```

The parameters have the following meaning:

Parameter	Description	Values
`showfiles`	Shows the available files	-
`filetype`	Shows that the file type follows that will be loaded	-
`filetype`	Name of the file type	max. 100 characters

Result

The password for the file is disabled.

Further notes

You enable the password for the user certificate with the `password` command.

4.2.6.4 tftp filename

Description

With this command, you assign a name to a file type.

The file type decides the type that is affected by the `tftp load` or `tftp save` action. The name decides the file to be copied to or from the TFTP server.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

```
cli(config-loadsave)#
```

Syntax

Call up the command with the following parameters:

```
tftp filename {showfiles | filetype <filetype> name <filename>}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`showfiles`	Shows the available files	-
`filetype`	Keyword for a file type to be assigned a name	-
`filetype`	Name of the file type	max. 100 characters
`name`	Keyword for a file name to be assigned to the file type	-
`filename`	Name of the file	max. 100 characters

Result

The file types are displayed or the file type is assigned a name.

Further notes

With the "`show loadsave files`" command, you can display the file types.

4.2.6.5 tftp load

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Description

With this command, you load a file from a TFTP server into the file system of the device. The TFTP protocol is used for the transfer. You can also display a list of available files.

Requirement

- The name of the file is specified
- You are in the LOADSAVE configuration mode.
  The command prompt is:
  `cli(config-loadsave)#`

Syntax

Call the command with the following parameter assignment:

```
tftp load { showfiles | filetype <filetype> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`showfiles`	Shows the available files	-
`filetype`	Keyword for a file type to be loaded	-
`filetype`	Name of the file type	max. 100 characters

Result

The file types are displayed or the file is downloaded to the device.

Additional notes

You configure the name of the file with the `tftp filename` command.

With the "`show loadsave files`" command, you can display the file types.

4.2.6.6 tftp save

Description

With this command, you copy a file from the file system of the device to a TFTP server. The TFTP protocol is used for the transfer. You can also display a list of available files.

Requirement

- The name of the file is specified
- You are in the LOADSAVE configuration mode.
  The command prompt is:
  `cli(config-loadsave)#`

Syntax

Call the command with the following parameter assignment:

```
tftp save { showfiles | filetype <filetype> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`showfiles`	Shows the available files	-
`filetype`	Keyword for a file type to be loaded	-
`filetype`	Name of the file type	max. 100 characters

Result

The file types are displayed or the file is copied.

Additional notes

You configure the name of the file with the `tftp filename` command.

With the "`show loadsave files`" command, you can display the file types.

4.2.6.7 tftp server

Description

With this command, you configure the access to a TFTP server.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

```
cli(config-loadsave)#
```

Syntax

Call the command with the following parameters:

```
tftp server { ipv4 <ucast_addr> | fqdn-name <FQDN>} [port <tcp port
(1-65535)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ipv4`	Keyword for an IPv4 address	-
`ipv4-address`	Value for an IPv4 unicast address	Enter a valid IPv4 unicast address.
`port`	Keyword for the port of the server via which the TFTP connection runs	-
`tcp port`	Number of the port	1 ... 65535

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The settings for the access to the selected TFTP server are configured.

4.2.6.8 sftp filename

Description

With this command, you assign a name to a file type.

The file type decides the type that is affected by the `sftp load` or `sftp save` action. The name decides the file to be copied to or from the SFTP server.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

```
cli(config-loadsave)#
```

Syntax

Call up the command with the following parameters:

```
sftp filename {showfiles | filetype <filetype> name <filename>}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`showfiles`	Shows the available files	-
`filetype`	Keyword for a file type to be assigned a name	-
`filetype`	Name of the file type	max. 100 characters
`name`	Keyword for a file name to be assigned to the file type	-
`filename`	Name of the file	max. 100 characters

Result

The file types are displayed or the file type is assigned a name.

Further notes

With the "`show loadsave files`" command, you can display the file types.

4.2.6.9 sftp load

Description

With this command, you load a file from an SFTP server into the file system of the device. You can also display a list of available files.

Requirement

- The name of the file is specified
- You are in the LOADSAVE configuration mode.
  The command prompt is:
  `cli(config-loadsave)#`

Syntax

Call the command with the following parameter assignment:

```
sftp load { showfiles | filetype <filetype> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`showfiles`	Shows the available files	-
`filetype`	Keyword for a file type to be loaded	-
`filetype`	Name of the file type	max. 100 characters

Result

The file types are displayed or the file is downloaded to the device.

Additional notes

You configure the name of the file with the `sftp filename` command.

With the "`show loadsave files`" command, you can display the file types.

4.2.6.10 sftp save

Description

With this command, you copy a file from the file system of the device to an SFTP server. The SFTP protocol is used for the transfer. You can also display a list of available files.

Requirement

- The name of the file is specified
- You are in the LOADSAVE configuration mode.
  The command prompt is:
  `cli(config-loadsave)#`

Syntax

Call the command with the following parameter assignment:

```
sftp save { showfiles | filetype <filetype> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`showfiles`	Shows the available files	-
`filetype`	Keyword for a file type to be loaded	-
`filetype`	Name of the file type	max. 100 characters

Result

The file types are displayed or the file is copied.

Additional notes

You configure the name of the file with the `sftp filename` command.

With the "`show loadsave files`" command, you can display the file types.

4.2.6.11 sftp server

Description

With this command, you configure the access to an SFTP server.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

```
cli(config-loadsave)#
```

Syntax

Call the command with the following parameters:

```
sftp server {ipv4 <ucast_addr> | fqdn-name <FQDN>} [port <tcp port
(1-65535)>] [user <username>] [password <password>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
ipv4	Keyword for an IPv4 address	-
ucast_addr	Value for an IPv4 unicast address	Enter a valid IPv4 unicast address.
port	Keyword for the port of the server via which the SFTP connection runs	-
tcp port	Number of the port	1 ... 65535
user	Keyword for user	-
username	User name for access to the SFTP server	Enter a valid user name. This parameter can only be used when a user with the corresponding rights has been created on the SFTP server.
password	Keyword for a password	-
password	Password of the user	Enter the password for the user.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The settings for the access to the selected SFTP server are configured.

4.2.6.12 minimum config version

Description

You use this command to specify the minimum version that a configuration file must have to be loaded into the device.

The versions differ in the signature of the file header. Configuration files of Version 2.0 have better protection against tampering.

The saving of a configuration file is independent of this setting. Configuration files that were saved with a firmware version ≤ V4.3 always equate to V1.0. Configuration files that were saved with a firmware version ≥ V4.4 always equate to V2.0.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

```
cli(config-loadsave)#
```

Syntax

Call up the command with the following parameters:

minimum config version {v10 | v20}

The parameters have the following meaning:

Parameter	Description	Range of values/note
`v10`	With this setting, you can load configuration files with V1.0 and V2.0 into the device.	Factory setting
`v20`	With this setting, you can load only configuration files with V2.0 into the device.	-

Result

The version for configuration files has been configured.

Additional notes

With the `show loadsave minimum config-file version` command, you can view the minimum version of the configuration file.

4.3 Reset and Defaults

This section describes commands for restarting the device and for restoring the original configuration.

4.3.1 restart

Description

With this command, you restart the device.

Select one of the following configuration settings:

- Device restart with the current configuration
- Device restart with the factory configuration settings.
- Device restart with the default settings of the PROFINET IO profile.
- Device restart with the default settings of the EtherNet/IP profile.
- Device restart with the default settings of the Industrial Ethernet profile.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command with the following parameters:

```
restart [{factory | pnio | ethernetip | ie}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
without parameters	The system restarts with the current configuration	• You can only restart the device with administrator privileges. • A device should only be restarted by this CLI command or the corresponding buttons in the WBM and not by a poer cycle on the device.
`factory`	Restores the factory settings of the device and restarts the device. The factory settings depend on the device.	• By resetting all the settings to the factory settings, the IP address and the passwords are also lost. The device can then only be addressed via the serial interface, SINEC PNI or via DHCP. • With the appropriate attachment, a previously correctly configured device can cause circulating frames and therefore the failure of the data traffic.

Parameter	Description	Range of values/note
`pnio`	Restores the default settings of the PROFINET IO profile and restarts the device.	• The profiles provide a preconfiguration for various use cases of the devices. • When you start a device with the default settings of a profile, the settings are reset to the factory settings and some parameters are set so that they are designed for a use case. • In contrast to resetting to the factory settings. the users and passwords are retained after the restart. The configured IP address is lost so that the device can then only be accessed via the serial interface, SINEC PNI or using DHCP. • With the appropriate attachment, a previously correctly configured device can cause circulating frames and therefore the failure of the data traffic.
`ethernetip`	Restores the default settings of the EtherNet/IP profile and restarts the device.	
`ie`	Restores the default settings of the Industrial Ethernet profile and restarts the device.	

Result

The device is restarted with the selected settings.

4.3.2 Commands in global configuration mode

4.3.2.1 Introductory sentence for the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.3.2.2 boot-integrity-check

Description

With this command, you disable checking of the firmware for errors. If an error is detected during startup of the device, the firmware is not started. The bootloader of the device waits in this status for a new firmware file that you can download by TFTP. For more information, refer to section "Downloading new firmware using TFTP without WBM and CLI (Page 783)".

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`boot-integrity-check {enabled | disabled}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`enabled`	The firmware is checked for errors on every startup	Default: Enabled
`disabled`	The firmware is not checked for errors	-

Result

Checking of the firmware is disabled.

4.3.2.3 cancel restart-timer

Description

With this command, you disable the timer.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`cancel restart-timer`

Result

The timer for the scheduled restart is disabled.

4.3.2.4 schedule restart-timer

Description

With this command, you specify the time after which the device restarts.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameter assignment:

```
schedule restart-timer <seconds(300-86400)> [force]
```

Parameter	Description	Range of values / note
`seconds`	Value for the time in seconds	300 ... 86400 (24 h)
`force`	This parameter suppresses queries so that the command can be used in a CLI script.	-

Result

When "Automatic Save" configuration mode is active, an additional message is displayed. You can specify whether the device should save the current configuration and switch to "Trial" mode. In any case, the device restarts after the specified time.

Note

Unsaved configuration is lost after restart

The scheduled restart is performed after the time has elapsed without any further message. Unsaved configuration changes are lost.

Save the current configuration with the `write startup-config` command before setting the timer for the restart.

Additional notes

You disable the scheduled restart of the device with the `cancel restart-timer` command.

4.4 Configuration Save & Restore

This section describes commands for displaying, saving and restoring configuration settings.

4.4.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.4.1.1 show running-config

Note

Depending on the device type, the IE switch does not support all described parameters; see section "Features not supported (Page 40)".

Description

This command shows configuration settings of the device.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show running-config [{ syslog | dhcp | qos | stp | la | dot1x |
vlan [ <vlan-id (1-4094)>] |
interface { port-channel <port-channel-id (1-8)> |
<interface-type> <interface-list> | vlan <vlan-id(1-4094)> } |
ssh | ssl | acl | ip | snmp | radius | rmon | igmp | sntp |
http | broadcast-blocking | multicast-blocking | locked-port |
auto-logout | time | ntp | auto-save | panel-button | cos-map |
dscp-map | output-rate-limit | unicast-blocking | ospf | vrrp |
loopd | events | redundancy | passive | umac | nat | fmp |
pim | msdp | router-advertisement-blocking | mac-learning |
mac-flush-type | noa }] [all]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`syslog`	Shows the configuration settings of the Syslog function	-
`dhcp`	shows the configuration settings of the Dynamic Host Configuration Protocol	-
`qos`	shows the configuration settings of QoS (Quality of Service)	-
`stp`	Shows the configuration settings of the Spanning Tree protocol	-
`la`	Shows the configuration settings of the Link Aggregation function	-
`dot1x`	shows the configuration settings of the port-based network access control	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface`	Keyword for a an interface description	-
`port-channel`	Keyword for a port channel connection	-
`port-channel-id`	Number of the addressed port channel	1 ... 8
`interface-type`	Type of interface	Enter a valid interface.
`interface-list`	Module no. and port no. of the interface	
`ssh`	Shows the configuration settings of the Secure Shell protocol	-
`ssl`	Shows the configuration settings of the Secure Sockets Layer protocol	-
`acl`	Shows the configuration settings of the access control lists	-
`ip`	Shows the configuration settings of the Internet Protocol	-
`snmp`	Shows the configuration settings of the Simple Network Management Protocol	-
`radius`	shows the configuration settings of the Remote Authentication Dial-In User service	-
`rmon`	Shows the configuration settings of the Remote Monitoring function	-
`igmp`	Shows the configuration settings of the Internet Group Management Protocol	-
`sntp`	Shows the configuration settings of the Simple Network Time Protocol	-
`http`	Shows the configuration settings of the Hypertext Transfer Protocol	-
`broadcast-blocking`	Shows the configuration settings of the broadcast blocking	-
`multicast-blocking`	Shows the configuration settings of the multicast blocking	-
`locked-port`	Shows the configuration settings of the locked port function	-

Parameter	Description	Range of values/note
`auto-logout`	Shows the configuration settings of the auto logout function	-
`time`	Shows the configuration settings of the system time	-
`ntp`	Shows the configuration settings of the Network Time Protocol	-
`auto-save`	Shows the configuration settings of the auto save function	-
`panel-button`	Shows the configuration settings of the Panel Button function	-
`cos-map`	Shows the configuration settings of the COS function	-
`dscp-map`	Shows the configuration settings of the DSCP map function	-
`output-rate-limit`	Shows the configuration settings of the output rate limit function	-
`unicast-blocking`	Shows the configuration settings of the unicast blocking	-
`ospf`	Shows the configuration settings of the Open Shortest Path First	-
`vrrp`	Shows the configuration settings of the Virtual Router Redundancy Protocol	-
`loopd`	Shows the configuration settings of loop detection	-
`events`	Shows the configuration settings of the events	-
`redundancy`	Shows the configuration settings of the redundancy	-
`passive`	Shows the configuration settings of passive listening	-
`umac`	Shows the configuration settings of the user configuration	-
`nat`	Shows the configuration settings of the Network Address Translation	-
`fmp`	Shows the configuration settings of the Fiber Monitoring protocol	-
`pim`	Shows the configuration settings of the Independent Multicast protocol	-
`msdp`	Shows the configuration settings of the Multicast Source Discovery protocol	-
`router-advertisement-blocking`	Shows the configuration settings of the router advertisement blocking.	-
`mac-learning`	Shows the port settings for unicast address learning	-
`mac-flush-type`	Shows the configuration settings of the "`unicast-mac flush`" command	-

Parameter	Description	Range of values/note
`noa`	Shows the configuration settings of the NOA (NAMUR Open Architecture) switch function	-
`all`	shows all configuration settings and all default parameters. Some parameters cannot be changed.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The selected configuration settings of the device are displayed.

Passwords are masked as follows: [PASSWORD]

In other "show" commands, passwords are masked as follows: `******`

4.4.2 write startup-config

Description

With this command, you save the changes to the configuration in the configuration file.

The use of this command is required in the Trial mode. It can also be used in "auto save mode".

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`*cli#` or `cli#`

Syntax

Call the command without parameter assignment:

```
write startup-config
```

Result

The changes are saved in the configuration file.

When you restart the device without parameter assignment with the `restart` command, this configuration is used.

Further notes

You enable the auto save function or disable the Trial mode with the `auto-save` command.

You disable the auto save function or enable the Trial mode with the `no auto-save` command.

4.4.3 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.4.3.1 auto-save

Description

The CLI can save changes to the configuration automatically.

If you first want to test changes made to the configuration so that you can discard them afterwards if necessary, you can disable the auto save function. You are then in the Trial mode.

Note

PROFINET IO functionality of the device is switched off when the "Auto save function" is disabled ("Trial mode"). The device then no longer responds to PROFINET requests. Consequently, a controller does not receive any PROFINET information from the device.

SINEC NMS or SINEMA Server cannot monitor the device with the PROFINET protocol when the "Auto save function" is disabled.

Changes to the configuration that you have not saved are indicated by an asterisk in front of the command prompt: `*cli(...)#`.

You save the changes to the configuration with the `write startup-config` command.

With the `auto-save` command, you enable the auto save function.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`auto-save`

As default the function is "enabled".

Result

The auto save function is enabled.

Additional notes

You save changes to the configuration in trial mode with the `write startup-config` command.

You disable the function with the `no auto-save` command.

You can display the status of this function and other information with the `show device information` command.

4.4.3.2 no auto-save

Description

With this command, you disable the auto save function.

Note

PROFINET IO functionality of the device is switched off when the "Auto save function" is disabled ("Trial mode"). The device then no longer responds to PROFINET requests. Consequently, a controller does not receive any PROFINET information from the device.

SINEC NMS or SINEMA Server cannot monitor the device with the PROFINET protocol when the "Auto save function" is disabled.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no auto-save`

Result

The auto save function is disabled. The Trial mode is activated.

Additional notes

You enable the function with the `auto-save` command.

You can display the status of this function and other information with the `show device information` command.

You save changes to the configuration in trial mode with the `write startup-config` command.

4.5 DCP Discovery and Set (DaS)

This section describes commands for displaying and setting network parameters.

4.5.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.5.1.1 show das info

Description

This command shows the devices that can be reached via the interface and support DCP. DCP Discovery only searches for devices located in the same subnet as the interface.

The result of the search is not saved permanently. Perform the search again after a restart.

Requirement

- The command `das discover interface` is executed.
- You are in the Privileged EXEC mode.
  The command prompt is as follows:
  `cli#`

Syntax

Call up the command with the following parameters:

`show das info [detail]`

The parameter has the following meaning:

Parameter	Description	Value range / note
`detail`	The information is displayed in list form.	-

Result

The available devices and their network parameters are displayed in the tabular or list form.

Further notes

You start the search for available devices with the `das discover interface` command.

You configure the network parameters of the reachable device with the `das mac ip` command.

You delete the content of the table with the `das delete` command.

You configure the PROFINET device name of the reachable device with the `das mac name` command.

4.5.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.5.2.1 das delete

Description

With this command, you delete the content of the table in which the reachable devices are saved.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
das delete {mac <aa:aa:aa:aa:aa:aa> | all }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`mac`	Deletes the selected device in the table.	`aa:aa:aa:aa:aa:aa`
`all`	Deletes the content of the entire table.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The selected device or the entire content of the table has been removed from the table.

4.5.2.2 das discover interface

Description

With this command, you start the search for devices reachable via the selected interface. The function is only available with the VLAN associated with the TIA interface.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
das discover interface { <interface-type> <interface-id> | vlan
<vlan-id(1-4094)> | port-channel <port-channel-id (1-8)}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`port-channel`	Keyword for a link aggregation	-
`port-channel-id`	Number of the addressed link aggregation	1 ... 8

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The reachable devices are searched for. On completion of the search the reachable devices are saved in a table. You display the table with the `show das info` command.

4.5.2.3 das mac ip

Description

With this command, you configure the network parameters of the selected device.

Requirement

- The command `das discover interface` is executed.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call up the command with the following parameters:

```
das mac <aa:aa:aa:aa:aa:aa> ip <ip address> {<subnet-mask> | /
<prefix-length(1-32)>} [gateway <ip address>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
–	MAC address of the reachable device	`aa:aa:aa:aa:aa:aa`
`ip`	Keyword for IPv4 address	
`ip address`	IPv4 address of the device	Enter a valid IPv4 address.
`subnet-mask`	Subnet mask	
`prefix-length`	Decimal representation of the mask as a number of "1" bits	1 ... 32

Parameter	Description	Range of values/note
`gateway`	Keyword for gateway	-
`ip address`	IPv4 address of the gateway	Enter a valid IPv4 address.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The network parameters of the selected device are configured.

To ensure that the property was applied correctly, run the `das discover interface` command again.

Further notes

You display the network parameters with the `show das info` command.

4.5.2.4 das mac name

Description

With this command, you configure the PROFINET device name of the selected device.

Requirement

- The command `das discover interface` is executed.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call the command with the following parameter assignment:

```
das mac <aa:aa:aa:aa:aa:aa> name <name(127)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
–	MAC address of the reachable device	`aa:aa:aa:aa:aa:aa`
`name`	PROFINET device name	Maximum of 127 characters The device name must be DNS-compliant.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The PROFINET device name of the selected device is configured.

To ensure that the property was applied correctly, run the `das discover interface` command again.

Additional notes

You display the configured PROFINET device name with the `show das info` command.

4.5.2.5 das mac blink

Description

With this command, you make the LEDs of the selected device or your own device flash.

Requirement

- The command `das discover interface` is executed.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call the command with the following parameter assignment:

```
das mac {<aa:aa:aa:aa:aa:aa>|own} blink [timeout <seconds(5-60)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`mac`	The LEDs of the selected device flash.	• `aa:aa:aa:aa:aa:aa` Specify the desired MAC address. • `own` The LEDs of your own device flash.
`timeout`	Keyword for the blink duration	-
`seconds`	Blink duration in seconds	5 ... 60 Default: 5 seconds

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The LEDs of the selected device flash. When the time (`timeout`) elapses, flashing stops.

4.6 PoE

4.6.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.6.1.1 show poe status

Description

This command shows specific information for all or for a selected PoE interface (PoE: Power over Ethernet).

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show poe status [interface <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

If you use the command without setting parameters, information about all PoE interfaces is displayed.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The information for the selected PoE interface is displayed.

4.6.1.2 show pse status

Description

This command shows the current settings of the PoE power supply of the device.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show pse status [<integer>]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`integer`	Number of the PSE	-

If you do not select any parameter, the entries are displayed for all available PSEs.

Result

The current settings of the PoE power supply of the device are displayed.

4.6.1.3 show poe schedule info

Description

This command shows the schedule of the PoE power supply.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show poe schedule info
```

Result

The schedule of the PoE power supply is displayed.

4.6.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.6.2.1 poe pse usage

Description

With this command, you set a value (as a percentage) for the "Usage Threshold" parameter. This specifies how many percent of the maximum power the connected devices will use. As soon as the power being used by the end devices exceeds this percentage, an event is triggered. An event is also entered in the log. You display the entries of the log with the command `show logbook`. You will find more information on this command in the section "show logbook (Page 712)".

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
poe pse <integer(1-4)> usage <integer(1-100)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`integer`	Number of the PSE	1 ... 4
`integer`	Value for "Usage Threshold" as a percentage	1 ... 100 Default: 80%

Result

The value for "Usage Threshold" is configured.

4.6.2.2 no poe pse usage

Description

With this command, you reset the "Usage Threshold" parameter to the default value.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no poe pse <integer(1-4)> usage
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`integer`	Number of the PSE	1 ... 4

Result

The "Usage Threshold" parameter is reset to the default value.

4.6.3 Commands in the Interface Configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.6.3.1 poe active

Description

With this command, you activate PoE for the interface in whose interface configuration mode you are currently working.

Requirement

You are in the Interface Configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
poe active
```

Result

PoE is activated for the corresponding interface.

4.6.3.2 no poe active

Description

With this command, you deactivate PoE for the interface in whose interface configuration mode you are currently working.

Requirement

You are in the Interface Configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no poe active
```

Result

PoE is deactivated for the corresponding interface.

4.6.3.3 poe custom maxpwr

Description

With this command you set the maximum power that a port makes available to supply a connected device.

This value is taken into account when the function is enabled with the `poe custom maxpwr active` command.

Requirement

You are in interface configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameter:

```
poe custom maxpwr <integer(0-60)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`integer`	Value for the user-defined maximum power in watts	0 ... 60

Result

The maximum power is set.

Additional notes

You enable the user-defined maximum power for the interface with the `poe custom maxpwr active` command.

You disable the user-defined maximum power for the interface with the `no poe custom maxpwr active` command.

You delete the user-defined maximum power for the interface with the `no poe custom maxpwr` command.

4.6.3.4 no poe custom maxpwr

Description

With this command, you delete the user-defined maximum power for a port.

Requirement

You are in the Interface Configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no poe custom maxpwr
```

Result

The user-defined maximum power is deleted.

Further notes

You configure the user-defined maximum power for the interface with the `poe custom maxpwr` command.

You enable the user-defined maximum power for the interface with the `poe custom maxpwr active` command.

You disable the user-defined maximum power for the interface with the `no poe custom maxpwr active` command.

4.6.3.5 poe custom maxpwr active

Description

With this command, you enable use of the user-defined maximum power for the interface.

Requirement

You are in the Interface Configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
poe custom maxpwr active
```

Result

The user-defined maximum power is enabled for the relevant interface.

Further notes

You configure the user-defined maximum power for an interface with the `poe custom maxpwr` command.

You disable the use of the user-defined maximum power with the `no poe custom maxpwr active` command.

4.6.3.6 no poe custom maxpwr active

Description

With this command, you disable use of the user-defined maximum power for the interface.

Requirement

You are in the Interface Configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no poe custom maxpwr active
```

Result

The user-defined maximum power is disabled for the relevant interface.

Further notes

You configure the user-defined maximum power for an interface with the `poe custom maxpwr` command.

You enable the use of the user-defined maximum power with the `poe custom maxpwr active` command.

4.6.3.7 poe type

Description

This command specifies a character string that describes a connected device in greater detail.

Requirement

You are in interface configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
poe type <string(256)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`string`	Description of a connected device	Max. 256 characters

Result

The description of the connected device has been specified.

4.6.3.8 no poe type

Description

With this command, you delete the description for a connected device.

Requirement

You are in the Interface Configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no poe type
```

Result

The description of the corresponding device is deleted.

4.6.3.9 poe prio

Description

With this command, you specify the priority of the power supply for an interface.

Requirement

You are in the Interface configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
poe prio {low|high|critical}
```

The parameters have the following meaning:

Parameter	Description
`low`	low priority
`high`	high priority
`critical`	highest priority

If the power of the connected power supply is inadequate to supply all connected devices, devices with a higher priority are given preference.

If the same priority is set for two ports, the port with the lower number will be preferred when necessary.

Result

The priority of the corresponding interface has been specified.

4.6.3.10 no poe prio

Description

With this command, you set the priority of an interface to the default value "low".

Requirement

You are in the Interface configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no poe prio
```

Result

The priority of the corresponding interface has been set to "low".

4.6.3.11 poe schedule

Description

This command enables the schedule of the PoE power supply. Power supply via PoE is then only possible at the defined times. You can only enable the schedule if you have already configured start and time times as well as the days of the week for the availability of the PoE power supply.

Requirement

You are in the Interface configuration mode of a PoE interface.

The command prompt is as follows:
```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:
```
poe schedule
```

Result

PoE power supply is only available within the configured times.

4.6.3.12 no poe schedule

Description

This command disables the schedule of the PoE power supply configured for this interface.

Requirement

You are in the Interface configuration mode of a PoE interface.

The command prompt is as follows:
`cli(config-if-$$$)#`

Syntax

Call the command without parameters:
`no poe schedule`

Result

The schedule for the PoE power supply is disabled.

4.6.3.13 poe schedule time

Description

This command configures the start and end times of the PoE power supply.

Requirement

You are in the Interface configuration mode of a PoE interface.

The command prompt is as follows:
`cli(config-if-$$$)#`

Syntax

Call the command with the following parameters:
`poe schedule time start <hh:mm> end <hh:mm>`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`start`	Keyword for the start of the PoE power supply.	-
`hh:mm`	Start or end time of the PoE power supply. With one-digit values for the hour or minute, a leading zero must be entered. If the value for the end time is less than the value for the start time or when both values are the same, the end of the PoE power supply is on the next weekday.	Time of day
`end`	Keyword for the end of the PoE power supply.	-

Result

The time for the start of the PoE power supply is configured.

4.6.3.14 no poe schedule time

Description

This command deletes the times for start and end of the PoE power supply. The schedule for the PoE power supply is also disabled.

Requirement

You are in the Interface configuration mode of a PoE interface.

The command prompt is as follows:
`cli(config-if-$$$)#`

Syntax

Call the command without parameters:
`no poe schedule time`

Result

The times for start and end of the PoE power supply are deleted. The schedule for the PoE power supply is disabled.

4.6.3.15 poe schedule day

Description

This command specifies the days of the week on which PoE power supply is available.

Requirement

You are in the Interface configuration mode of a PoE interface.

The command prompt is as follows:
`cli(config-if-$$$)#`

Syntax

Call the command with the following parameters:
`poe schedule day {<weekday(1-7)> | from <weekday(1-7)> to <weekday(1-7)>}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`weekday`	Consecutive number for the day of the week: Monday: 1 Tuesday: 2 etc.	1 ... 7
`from`	Keyword for the consecutive number of the day of the week from which the PoE power supply is available.	-
`to`	Keyword for the consecutive number of the day of the week until which the PoE power supply is available.	-

Result

The days of the week on which PoE power supply is available are configured.

4.6.3.16 no poe schedule day

Description

This command specifies the days of the week on which PoE power supply is not available.

Requirement

You are in the Interface configuration mode of a PoE interface.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:
`no poe schedule day {<weekday(1-7)> | from <weekday(1-7)> to <weekday(1-7)>}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`weekday`	Consecutive number for the day of the week: Monday: 1 Tuesday: 2 etc.	1 ... 7
`from`	Keyword for the consecutive number of the day of the week from which the PoE power supply is not available.	-
`to`	Keyword for the consecutive number of the day of the week until which the PoE power supply is not available.	-

Result

The days of the week on which PoE power supply is not available are configured.

4.7 SINEMA

If the SINEMA configuration interface is enabled, you can download configurations to the IE switch via STEP7 Basic/Professional.

4.7.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.7.1.1 show sinema

Description

This command shows whether the SINEMA configuration interface is enabled or disabled.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show sinema
```

Result

The setting of the SINEMA configuration interface is displayed.

4.7.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

4.7.2.1 sinema

Description

With this command, you enable the SINEMA configuration interface.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`sinema`

Result

The SINEMA configuration interface is enabled.

Further notes

You disable the SINEMA configuration interface with the `no sinema` command.

You display the setting whether the SINEMA configuration interface is enabled or disabled with the command `show sinema`.

4.7.2.2 no sinema

Description

With this command, you disable the SINEMA configuration interface.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`no sinema`

Result

The SINEMA configuration interface is disabled.

Further notes

You enable the SINEMA configuration interface with the `sinema` command.

You display the setting whether the SINEMA configuration interface is enabled or disabled with the command `show sinema`.

Functions specific to SCALANCE 5

This part contains the sections that describe functions specific to SCALANCE.

5.1 PLUG

The C-PLUG stores the configuration of a device and can therefore transfer the configuration of the old device to the new device when a device is replaced.

This section describes the commands relevant for working with the C-PLUG.

5.1.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

5.1.1.1 show plug

Description

This command shows the current information of the PLUG.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show plug
```

Result

The current information of the PLUG is diplayed.

5.1.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

5.1.2.1 plug

Description

With this command, you change to the Plug Configuration mode.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
plug
```

Result

You are now in the Plug Configuration mode.

The command prompt is as follows:

```
cli(config-plug)#
```

Further notes

You exit the Plug Configuration mode with the `end` or `exit` command.

5.1.3 Commands in the Plug configuration mode

This section describes commands that you can call up in the Plug Configuration mode.

In global configuration mode, enter the `plug` command to change to this mode.

- If you exit the Plug Configuration mode with the `exit` command, you return to the Global Configuration mode.
- If you exit the Plug Configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in Plug configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

5.1.3.1 factoryclean

Description

With this command, you delete the device configuration stored on the PLUG.

Requirement

- There is a device configuration on the PLUG.
- You are in the Plug Configuration mode.
  The command prompt is:
  `cli(config-plug)#`

Syntax

Call the command without parameters:

```
factoryclean
```

Result

The device configuration on the PLUG is deleted.

5.1.3.2 firmware-on-plug

Description

With this command, you specify that the firmware is stored on the PLUG.

Requirement

- There is a device configuration on the PLUG.
- You are in the Plug Configuration mode.
  The command prompt is:
  `cli(config-plug)#`

Syntax

Call the command without parameters:

```
firmware-on-plug
```

Result

The firmware is stored on the PLUG.

When the device starts up there is a check whether the version on the PLUG is valid and whether this version matches the version on the device. If this is not the case, the firmware is installed on the device and it is restarted. This means that automatic firmware updates/downgrades can be made with the PLUG.

Additional notes

You disable this setting with the `no firmware-on-plug` command.

5.1.3.3 no firmware on plug

Description

With this command, you disable the function. The firmware is removed from the PLUG.

Requirement

- There is a device configuration on the PLUG.
- You are in the Plug Configuration mode.
  The command prompt is:
  `cli(config-plug)#`

Syntax

Call the command without parameters:

```
no firmware-on-plug
```

Result

The firmware is removed from the PLUG.

5.1.3.4 write

Description

With this command, you format the PLUG and copy the current device configuration to it.

Requirement

You are in the Plug Configuration mode.
The command prompt is:
`cli(config-plug)#`

Syntax

Call the command without parameter assignment:

```
write
```

Result

The current device configuration has been copied to the formatted PLUG.

5.2 WBM

On the device, you can limit the time available for access with Web Based Management. If no entry is made for a specific time, the WBM session is closed.

This section describes commands relevant for the configuration of this feature.

5.2.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

5.2.1.1 show web-session-timeout

Description

This command shows the timeout setting for the WBM.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show web-session-timeout
```

Result

The timeout setting for the WBM is displayed.

5.2.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

5.2.2.1 web-session-timeout

Description

With this command, you enable the automatic logoff and you configure the timeout setting for the WBM.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`web-session-timeout [<seconds(60-3600)>]`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`seconds`	Time in seconds until automatic logout after the last entry	60 ... 3600 Default: 900

Result

The time is configured and automatic logout is enabled.

Further notes

You disable automatic logoff with the `no web-session-timeout` command.

You display the current timeout setting with the `show web-session-timeout` command.

5.2.2.2 no web-session-timeout

Description

With this command, you disable the automatic logoff.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no web-session-timeout`

Result

Automatic logoff is disabled.

Further notes

You enable automatic logoff with the `web-session-timeout` command.

You display the current timeout setting with the `show web-session-timeout` command.

5.3 Panel button

This section describes the commands relevant for working with the button.

You will find a detailed description of the function available using the button in the device operating instructions.

Availability of the buttons

Depending on your IE switch, different buttons and functions are available, see section "System functions hardware equipment (Page 33)".

5.3.1 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

5.3.1.1 panel-button control-factory-defaults

Description

With this command, you enable the following function of the button:

- When the button is pressed for more than 12 seconds in display mode A, there is a restart with the factory settings.
  This function corresponds to calling the `restart` command with the parameter `factory`.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
panel-button control-factory-defaults
```

Result

The function of the button for restarting with factory settings is enabled.

Further notes

You disable this function with the `no panel-button control-factory-defaults` command.

5.3.1.2 no panel-button control-factory-defaults

Description

With this command, you disable the following function of the button:

- When the button is pressed for more than 12 seconds in display mode A, there is a restart with the factory settings.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no panel-button control-factory-defaults
```

Result

The function of the button for restarting with factory settings is enabled or disabled.

Further notes

You enable this function with the `panel-button control-factory-defaults` command.

5.3.1.3 panel-button control-faultmask

Description

With this command, you enable the following function of the button:

- If display mode D "Fault Mask" is displayed and the button is pressed for 5 - 12 seconds, the fault mask is set.
  This function corresponds to calling the following commands in EVENTS Configuration Mode:
  - `power`
  - `link` with the parameter `down`

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
panel-button control-faultmask
```

Result

The function of the button for setting the fault mask is enabled.

Further notes

You disable this function with the `no panel-button control-faultmask` command.

5.3.1.4 no panel-button control-faultmask

Description

With this command, you disable the following function of the button:

- If display mode D "Fault Mask" is displayed and the button is pressed for 5 - 12 seconds, the fault mask is set.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

`no panel-button control-faultmask`

Result

The function of the button for setting the fault mask is disabled.

Further notes

You enable this function with the `panel-button control-faultmask` command.

5.4 Signaling contact

This section describes the commands relevant for working with the signaling contact.

5.4.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

5.4.1.1 show signaling contact

Description

This command shows the current configuration of the signaling contact.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

`show signaling-contact`

Result

The current configuration of the signaling contact is displayed.

5.4.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

5.4.2.1 signaling contact mode

Description

With this command, you specify the reaction of the signaling contact.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
signaling-contact mode {conventional | aligned}
```

The parameters have the following meaning:

Parameter	Description
`conventional`	An error/fault is displayed by the fault LED and the signaling contact is opened. When the error/fault state no longer exists, the fault LED goes off and the signaling contact is closed.
`aligned`	The way the signaling contact works does not depend on the error/fault that has occurred. The signaling contact can be opened or closed as required by user actions.

Result

The reaction of the signaling contact is specified.

Further notes

You display the setting with the `show signaling contact` command.

5.4.2.2 signaling-contact status

Description

With this command, you close or open the signaling contact.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`signaling-contact status {open | close}`

The parameters have the following meaning:

Parameter	Description
`open`	Signaling contact is opened.
`close`	Signaling contact is closed.

Result

The signaling contact is opened or closed.

Further notes

You display the setting with the `show signaling contact` command.

System time

6

6.1 System time setting

This section describes commands relevant for the configuration of the system time.

6.1.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.1.1.1 show dst info

Description

This command shows all the entries for daylight saving time stored on the device.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show dst info
```

Result

The entries for daylight saving time are displayed.

6.1.1.2 show time

Description

This command shows the settings of the system clock.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show time
```

Result

The settings for the system clock are displayed.

6.1.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.1.2.1 time

Description

With this command, you configure the way in which the system time is obtained.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

```
time { manual | ntp | sntp | sinec | ptp_tc_client}
```

The parameters have the following meaning:

Parameter	Description
`manual`	The system time is entered by the user.
`ntp`	The system time is obtained from the NTP server.
`sntp`	The system time is obtained from the SNTP server.
`sinec`	The system time is obtained using the SIMATIC Time Client .
`ptp_tc_client`	The system time is synchronized using the Precision Time Protocol.

Result

The method of obtaining the system time is configured.

Further notes

You display the settings for the system clock with the `show time` command.

You create the system time with the `time set` command.

6.1.2.2 time set

Description

With this command, you set the system time.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
time set hh:mm:ss <day (1-31)> {january|february|march|april|may|
june|july|august|september|october|november|december}
     <year (2000 - 2060)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`hh:mm:ss`	Time of day	Hour, minute, second each separated by ":"
`day`	Day of the month	1 ... 31
-	Month	january, february, march, april, may, june, july, august, september, october, november, december
`year`	Year	2000 ... 2060

Result

The system time is set.

Further notes

You display the settings for the system clock with the `show time` command.

6.1.2.3 time dst date

Description

With this command, you configure the start and end of daylight saving time.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
time dst date <name(16)> <year (1900-2099)> begin <MMDDhh> end
<MMDDhh>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`name`	Name of the entry	maximum 16 characters
`year`	Year	1900 ... 2099
`begin`	Keyword for the start of daylight saving time.	-

Parameter	Description	Range of values / note
`MMDDhh`	Time for the start of daylight saving time.	Time in the format `MM` Month `DD` Day `hh` Hour
`end`	Keyword for the end of daylight saving time.	-
`MMDDhh`	Time for the end of daylight saving time.	Time in the format `MM` Month `DD` Day `hh` Hour

Result

The entry for the start and end of daylight saving time was created.

Further notes

You display the settings for the daylight saving time changeover with the `show dst info` command.

6.1.2.4 time dst recurring

Description

With this command, you configure the start and end of daylight saving time with a generic description.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
time dst recurring <name(16)> begin {<week(1-5)> | last} <weekday>
<month> <hour> end {<week(1-5)> | last} <weekday> <month> <hour>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`name`	Name of the entry	maximum 16 characters
`begin`	Keyword for the start of daylight saving time.	-
`week`	Calendar week in a month	1 ... 5
`last`	Keyword for the last calendar week in a month	-
`weekday`	Weekday	monday, tuesday, wednesday, thursday, friday, saturday, sunday
`month`	Month	january, february, march, april, may, june, july, august, september, october, november, december
`hour`	Hour	0 ... 23
`end`	Keyword for the end of daylight saving time.	-

Result

The entry for the start and end of daylight saving time was created.

Further notes

You display the settings for the daylight saving time changeover with the `show dst info` command.

6.1.2.5 no time dst

Description

With this command you delete the entry for the start and end of daylight saving time with the specified name. If you do not specify a name as the parameter, all entries are deleted.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no time dst [<name(16)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`name`	Name of the entry	maximum 16 characters

Result

One entry or the entries for the start and end of daylight saving time was/were deleted.

Additional notes

You display the settings for the daylight saving time changeover with the `show dst info` command.

6.2 NTP

This section describes commands for configuration of the NTP server and the NTP client.

6.2.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.2.1.1 show ntp info

Description

This command shows the current settings for the Network Time Protocol (NTP).

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ntp info
```

Result

The current NTP settings are displayed.

6.2.1.2 show ntp server info

Description

This command shows the current settings for the NTP server.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call the command without parameters:

`show ntp server info`

Result

The current NTP server settings are displayed.

6.2.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.2.2.1 ntp

Description

With this command, you change to the Network Time Protocol (NTP).

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`ntp`

Result

You are now in the NTP configuration mode.

The command prompt is as follows:

`cli(config-ntp)#`

Further notes

You exit the NTP configuration mode with the `end` or `exit` command.

6.2.2.2 ntp server

Description

With this command, you enable the NTP server service.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`ntp server`

Result

The NTP server service is configured.

Further notes

You disable the service with the `no ntp server` command.

6.2.2.3 no ntp server

Description

With this command, you disable the NTP server service.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ntp server
```

Result

The NTP server service is disabled.

Further notes

You enable the service with the `ntp server` command.

6.2.2.4 ntp server configuration

Description

With this command, you change to the configuration mode of the NTP server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

`ntp server configuration`

Result

You are now in the NTP Server configuration mode.

The command prompt is as follows:

`cli(config-ntp-server)#`

Further notes

You exit the NTP Server configuration mode with the command `end` or `exit`.

6.2.3 Commands in the NTP configuration mode

This section describes commands that you can call up in the NTP configuration mode.

In global configuration mode, enter the `ntp` command to change to this mode.

- If you exit the NTP configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the NTP configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in NTP configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.2.3.1 ntp secure

Description

With this command, you enable the "Secure NTP Client only" function. The device receives the system time from a secure NTP server.

Requirement

- You are in NTP configuration mode.
  The command prompt is as follows:
  `cli(config-ntp)#`
- The parameters for authentication (key ID, hash algorithm, key) are configured.

Syntax

Call up the command with the following parameters:

`ntp secure`

Result

The function is enabled.

Additional notes

You disable the function with the `no ntp secure` command.

You configure the parameters for authentication with the `ntp server id` command.

6.2.3.2 no ntp secure

Description

With this command, you disable the "Secure NTP Client only" function.

Requirement

You are in NTP configuration mode.

The command prompt is as follows:

`cli(config-ntp)#`

Syntax

Call up the command with the following parameters:

`no ntp secure`

Result

The function is disabled.

Additional notes

You enable the function with the `ntp secure` command.

6.2.3.3 ntp server id

Description

With this command, you configure the connection to a server on the NTP client.

Requirement

You are in the NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Syntax

Call up the command with the following parameters:

```
ntp server id <1-4> { ipv4 <ip_addr> | fqdn-name <FQDN> } [port
{ <1025-36564> | default}] [poll <seconds(64-1024)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
id	Number of the NTP server.	1 ... 4 The NTP servers are queried in the order of the NTP Server Index. The time of the server that is found first is applied. If time frames of an NTP server with a smaller stratum value are received, this time is applied. The switchover to the time with the smaller stratum takes about 30 minutes.
ipv4	Keyword for an IPv4 address	-
ip_addr	Value for the IPv4 address of the time server	Enter a valid IPv4 address.
fqdn-name	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters If you have stored a suitable domain name, you can specify a host name.
port	UDP port of the time server	1025 ... 36564
default	Default value for the UDP port	123
poll	Keyword for the time after which the time of day is requested again	-
seconds	Value for the time in seconds	64 ... 1024

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The connection to a server is configured on the NTP client.

Additional notes

You delete the connection to a server with the `no ntp server id` command.

6.2.3.4 no ntp server id

Description

With this command, you delete the connection to a server on the NTP client.

Requirement

You are in the NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Syntax

Call up the command with the following parameters:

```
no ntp server id <1-4>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`id`	Number of the NTP server.	1 ... 4

Result

The connection to a server is deleted on the NTP client.

Further notes

You configure the connection to a server with the `ntp server id` command.

6.2.3.5 ntp server id secure

Description

With this command, you configure the parameters for authentication.

Requirement

You are in the NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Syntax

Call up the command with the following parameters:

```
ntp server id <1-4> secure [ntpkeyid <1-65534>] [hashalg {des-cbc|
md5|sha1}] [ntp-key <secret-key-string(1-128)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`id`	NTP server index to which the parameters relate	1 ... 4
`secure`	Key for the authentication	-
`keyid`	Authentication key ID	The entry must exist on the NTP server. 1 ... 65534
`hashalg`	Authentication key format	des-cbc md5 sha1
`ntp-key`	Keyword for the authentication key	-
`secret-key-string`	Authentication key	The key can only contain printable ASCII characters. The entry must match the key stored on the NTP server.

Result

The parameters are configured.

Further notes

You display the settings and other information with the `show ntp server` command.

6.2.3.6 ntp time diff

Description

With this command, you configure the time difference between the device and the NTP server.

Requirement

You are in the NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Syntax

Call up the command with the following parameters:

```
ntp time diff <(+/-hh:mm)>
```

The parameter has the following meaning:

Parameter	Description
+	Time zones to the west of the NTP server time zone
–	Time zones to the east of the NTP server time zone
hh	Number of hours difference
mm	Number of minutes difference

Enter the time difference as follows:

- with sign
- without spaces
- Hours and minutes both two digits (with leading zero)

Default: No time difference.

Result

The time difference between the device and the NTP server is configured.

6.2.4 Commands in NTP server configuration mode

This section describes commands that you can call up in the NTP Server configuration mode.

In the Global configuration mode, enter the `ntp server configuration` command to change to this mode.

- If you exit the NTP Server configuration mode with the `exit` command, you return to the global configuration mode.
- If you exit the NTP Server configuration mode with the `end` command, you return to the Privileged EXEC mode.

6.2.4.1 ntp server interface

Description

With this command, you configure the NTP server for an interface. The other devices can call up the time via these interfaces.

Requirement

You are in NTP Server configuration mode.

The command prompt is as follows:

```
cli(config-ntp-server)#
```

Syntax

Call up the command with the following parameters:

```
ntp server interface { <interface-type> <interface-id> | vlan <vlan-
id(1-4094)> | all }
[port {<1025-36564> | default}][secure ntpkeyid <1-65534> hashalg
{des-cbc|md5|sha1} ntp-key <secret-key-string(1-128)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`all`	Enables the function on all available interfaces.	-
`port`	NTP Server Port	• 1025 ... 36564 • default (123)
`secure`	The following parameters are only relevant for "NTP (secure)".	-
`ntpkeyid`	Authentication key ID	1 ... 65534
`hashalg`	Hash algorithm for the authentication key	• des-cbc • md5 • sha1
`ntp-key`	Keyword for the authentication key	-
`secret-key-string`	Authentication key	The length of the authentication key depends on the hash algorithm. • DES: ASCII 8 characters • MD5: ASCII 16 – 128 characters • SHA1: ASCII 20 – 128 characters

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The NTP server is configured for an interface.

Further notes

You display the settings and other information with the `show ntp server info` command.

You delete the configuration of the NTP server for an interface with the `no ntp server interface` command.

You enable "NTP (secure)" with the `ntp server secure interface` command.

6.2.4.2 no ntp server interface

Description

With this command, you delete the configuration of the NTP server for one or all interfaces.

Requirement

You are in NTP Server configuration mode.

The command prompt is as follows:

```
cli(config-ntp-server)#
```

Syntax

Call the command with the following parameters:

```
no ntp server interface {<interface-type> <interface-id> | vlan
<vlan-id(1-4094)> | all}
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`all`	Keyword with which you delete the configuration information for all interfaces.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The configuration of the NTP server for the specified interface or all interfaces has been deleted.

Additional notes

You display the settings and other information with the `show ntp server info` command.

You create the configuration of the NTP server for an interface with the `ntp server interface` command.

6.2.4.3 ntp server listen interface

Description

This command enables the time-of-day synchronization with NTP for the specified interface.

Requirement

- You are in NTP Server configuration mode.
  The command prompt is as follows:
  `cli(config-ntp-server)#`
- You have created a configuration for the NTP server for the relevant interface with the `ntp server interface` command.

Syntax

Call the command with the following parameters:

```
ntp server listen interface {<interface-type> <interface-id> | vlan
<vlan-id(1-4094)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

Time-of-day synchronization with NTP is activated for the specified interface.

Additional notes

You display the settings and other information with the `show ntp server info` command.

You disable the NTP server for an interface with the `no ntp server listen interface` command.

6.2.4.4 no ntp server listen interface

Description

This command disables the time-of-day synchronization with NTP for the specified interface. The configuration of the NTP server for this interface is retained.

Requirement

You are in NTP Server configuration mode.

The command prompt is as follows:

```
cli(config-ntp-server)#
```

Syntax

Call the command with the following parameters:

```
no ntp server listen interface {<interface-type> <interface-id> |
vlan <vlan-id(1-4094)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

Time-of-day synchronization with NTP is deactivated for the specified interface.

Additional notes

You display the settings and other information with the `show ntp server info` command.

You enable the NTP server for an interface with the `ntp server listen interface` command.

6.2.4.5 ntp server secure interface

Description

With this command, the NTP server becomes an NTP server of the type "NTP (secure)".

Requirement

You are in NTP Server configuration mode.

The command prompt is as follows:

```
cli(config-ntp-server)#
```

Syntax

Call the command with the following parameters:

```
ntp server secure interface {<interface-type> <interface-id> | vlan
<vlan-id(1-4094)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The NTP server of the type "NTP (secure)" is enabled.

Additional notes

You display the settings and other information with the `show ntp server info` command.

You disable the function with the `no ntp server secure interface` command.

6.2.4.6 no ntp server secure interface

Description

With this command, you disable NTP (secure).

Requirement

You are in NTP Server configuration mode.

The command prompt is as follows:

```
cli(config-ntp-server)#
```

Syntax

Call the command with the following parameters:

```
no ntp server secure interface {<interface-type> <interface-id> |
vlan <vlan-id(1-4094)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The function is disabled on the interfaces.

Additional notes

You display the settings and other information with the `show ntp server info` command.

You enable the function with the `ntp server secure interface` command.

6.3 SNTP client

This section describes commands relevant for configuration of the SNTP client.

6.3.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.3.1.1 show sntp broadcast-mode status

Description

This command shows the current configuration of the broadcast mode of SNTP.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show sntp broadcast-mode status
```

Result

The current SNTP broadcast configuration is displayed.

See also

show sntp status (Page 213)

6.3.1.2 show sntp status

Description

This command shows the settings of the Simple Network Time Protocol.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show sntp status
```

Result

The settings of SNTP are displayed.

6.3.1.3 show sntp unicast-mode status

Description

This command shows the current configuration of the unicast mode of SNTP.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show sntp unicast-mode status
```

Result

The current SNTP unicast configuration is displayed.

6.3.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.3.2.1 sntp

Description

With this command, you change to the SNTP configuration mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`sntp`

Result

You are now in the SNTP configuration mode.

The command prompt is as follows:

`cli(config-sntp)#`

Further notes

You exit the SNTP configuration modewith the `end` or `exit` command.

6.3.3 Commands in the SNTP configuration mode

This section describes commands that you can call up in the SNTP configuration mode.

In global configuration mode, enter the `sntp` command to change to this mode.

- If you exit the SNTP configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the SNTP configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in SNTP configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.3.3.1 sntp client addressing-mode

Description

With this command, you configure the addressing mode of the SNTP client as unicast or broadcast.

Requirement

- The SNTP client is activated.
- You are in the SNTP Configuration mode.
  The command prompt is:
  `cli(config-sntp)#`

Syntax

Call up the command with the following parameters:

`sntp client addressing-mode{unicast|broadcast}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`unicast`	configures the SNTP client in unicast mode	Default: unicast enabled
`broadcast`	configures the SNTP client in broadcast mode	Supports only IPv4 addresses

Result

The addressing mode of the SNTP client is configured.

Further notes

You display this setting and other information with the `show sntp status` command.

You display the settings for the unicast mode with the `show sntp unicast-mode status` command.

You display the settings for the broadcast mode with the `show sntp broadcast-mode status` command.

6.3.3.2 sntp time diff

Description

With this command, you configure the time difference of the system time relative to the UTC time.

Requirement

- You are in the SNTP Configuration mode.
  The command prompt is:
  `cli(config-sntp)#`

Syntax

Call up the command with the following parameters:

`sntp time diff <(+/-hh:mm)>`

The parameter has the following meaning:

Parameter	Description
+	Time zones to the west of the SNTP server time zone
–	Time zones to the east of the SNTP server time zone
hh	Number of hours difference
mm	Number of minutes difference

Enter the time difference as follows:

- with sign
- without spaces
- Hours and minutes both two digits (with leading zero)

Default: no time difference

Result

The time zone of the system time is configured.

Further notes

You can display the settings of this function and other information with the `show sntp status` command.

6.3.3.3 sntp unicast-server ipv4

Description

With this command, you configure an SNTP unicast server.

Note

To avoid time jumps, make sure that there is only one time server in the network.

Requirement

- The addressing mode of the SNTP client is configured as "unicast".
- You are in the SNTP configuration mode.
  The command prompt is:
  `cli(config-sntp)#`

Syntax

Call up the command with the following parameters:

```
sntp unicast-server { ipv4 <ucast_addr> | fqdn-name <FQDN> } [port
<(1025-36564)>] [poll <seconds(16-16284)>] [secondary]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ipv4`	Keyword for an IP address	-
`ucast_addr`	Value for an IPv4 unicast address	Enter a valid IPv4 unicast address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters If you have stored a suitable domain name, you can specify a host name.
`port`	UDP port of the time server	1025 ... 36564 Default: 123
`poll`	Keyword for the time after which the time of day is requested again	-
`seconds`	Value for the time in seconds	16 ... 16284

Result

The SNTP unicast server is configured.

Further notes

You can reset the setting to the default with the `no sntp unicast-server ipv4` command.

You display this setting and other information with the `show sntp unicast-mode status` command.

6.3.3.4 no sntp unicast-server ipv4

Description

With this command, you delete the attributes for an SNTP unicast server and reset the address.

Requirement

You are in the SNTP configuration mode.

The command prompt is as follows:

```
cli(config-sntp)#
```

Syntax

Call up the command with the following parameters:

```
no sntp unicast-server {ipv4 <ucast_addr> | fqdn-name <FQDN> }
```

The parameters have the following meaning:

Parameter	Description	Range of values
`ucast_addr`	Value for an IPv4 unicast address	Enter a valid IPv4 unicast address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters If you have provided a suitable domain name, you can specify a host name.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The SNTP unicast server is reset to the default value.

Further notes

You configure the setting with the `sntp unicast-server ipv4` command.

You display this setting and other information with the `show sntp unicast-mode status` command.

6.4 PTP Client

The following devices support time-of-day synchronization with PTP:

- SCALANCE XC-200G
- SCALANCE XP-200G
- SCALANCE XP-200 with the following article numbers:
  - 6GK5 208-0HA10-2AS6
  - 6GK5 208-0HA10-2TS6
  - 6GK5 208-0HA10-2ES6

6.4.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.4.1.1 show ptp info

Description

This command shows the current settings for the Precision Time Protocol (PTP).

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show ptp info [ interfaces [<interface-type> <interface-id>] ]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interfaces`	Keyword for a an interface name.	-
`interface-type`	Type or speed of the interface.	Enter a valid interface name.
`interface-id`	Slot no. and port no. of the interface.	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The current settings for the Precision Time Protocol (PTP) are displayed.

6.4.2 Commands in global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.4.2.1 ptp

Description

With this command, you enable the PTP Transparent Clock :function on the device.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ptp
```

Result

The PTP Transparent Clock function is enabled.

Additional notes

You show the current settings for the Precision Time Protocol (PTP) with the `show ptp info` command.

You disable the PTP Transparent Clock function on the device with the `no ptp` command.

6.4.2.2 no ptp

Description

With this command, you disable the PTP Transparent Clock :function on the device.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no ptp`

Result

The PTP Transparent Clock function is disabled.

Additional notes

You show the current settings for the Precision Time Protocol (PTP) with the `show ptp info` command.

You enable the PTP Transparent Clock function on the device with the `ptp` command.

6.4.2.3 ptp time diff

Description

With this command, you set the time zone for the Precision Time Protocol.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command with the following parameters:

`ptp time diff <(+/-hh:mm)>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`+/-hh:mm`	The value for the time difference.	Hours and minutes specified in the format `+/-hh:mm`

Result

The time zone for the Precision Time Protocol is specified.

Additional notes

You show the current settings for the Precision Time Protocol (PTP) with the `show ptp info` command.

6.4.2.4 ptp transparent-clock configuration

Description

With this command you change to the PT Transparent Clock configuration mode.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
ptp transparent-clock configuration
```

Result

You are in the PTP Transparent Clock configuration mode.

The command prompt is as follows:

```
cli(config-ptp-tc)#
```

Additional notes

You show the current settings for the Precision Time Protocol (PTP) with the `show ptp info` command.

6.4.3 Commands in the PTP Transparent Clock configuration mode

This section describes commands that you can call up in the PTP Transparent Clock configuration mode.

In the Global configuration mode, enter the `ptp transparent-clock configuration` command to change to this mode.

- If you exit the PTP Transparent Clock configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the PTP Transparent Clock configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in PTP Transparent Clock configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.4.3.1 delay-mechanism

Description

With this command, you specify which correction mechanism the Precision Time Protocol uses.

Requirement

You are in the PTP Transparent Clock configuration mode.

The command prompt is as follows:

```
cli(config-ptp-tc)#
```

Syntax

Call up the command with the following parameters:

```
delay-mechanism { end-to-end | peer-to-peer }
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`end-to-end`	The device operates as an end-to-end transparent clock.	With end-to-end synchronization with more than 2 slaves, freak values > 100 ns can occur in the offset.
`peer-to-peer`	The device operates as a peer-to-peer transparent clock.	-

Result

The correction mechanism for the Precision Time Protocol is specified.

Additional notes

You show the current settings for the Precision Time Protocol (PTP) with the `show ptp info` command.

You specify the primary domain with the `primary-domain` command.

6.4.3.2 primary-domain

Description

With this command, you specify the primary domain.

Requirement

You are in the PTP Transparent Clock configuration mode.

The command prompt is as follows:

```
cli(config-ptp-tc)#
```

Syntax

Call up the command with the following parameters:

```
primary-domain <domain-id (0-255)>}
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`domain-id`	The identifier of the primary domain.	0 ... 255

Result

The primary domain is specified.

Additional notes

You show the current settings for the Precision Time Protocol (PTP) with the `show ptp info` command.

You define the correction mechanism for the Precision Time Protocol with the `delay-mechanism` command

6.4.3.3 vlan-id

Description

With this command you specify the VLAN in which the device is to synchronize itself.

Requirement

You are in the PTP Transparent Clock configuration mode.

The command prompt is as follows:

```
cli(config-ptp-tc)#
```

Syntax

Call the command with the following parameters:

```
vlan-id <IEEE1588 vlan-id(0-4095)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`IEEE1588 vlan-id`	The ID of the VLAN in which the device is to synchronize itself.	0 ... 4095

Result

The VLAN in which the device is to synchronize itself has been specified.

Additional notes

You show the current settings for the Precision Time Protocol (PTP) with the `show ptp info` command.

6.4.4 Commands in interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

6.4.4.1 ptp

Description

With this command, you enable the PTP Transparent Clock function for an interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
ptp
```

Result

The PTP Transparent Clock function is enabled.

Additional notes

You show the current settings for the Precision Time Protocol (PTP) with the `show ptp info` command.

You disable the PTP Transparent Clock function for an interface with the `no ptp` command.

6.4.4.2 no ptp

Description

With this command, you disable the PTP Transparent Clock function for an interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no ptp
```

Result

The PTP Transparent Clock function is disabled.

Additional notes

You show the current settings for the Precision Time Protocol (PTP) with the `show ptp info` command.

You enable the PTP Transparent Clock function for an interface with the `ptp` command.

6.4.4.3 ptp transparent-clock transport-mechanism

Description

With this command you choose how this port will handle PTP message data traffic. You can make different settings for the ports of a device, however, the relevant communications partner must support the selected transport mechanism.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
ptp transparent-clock transport-mechanism { udp-ip-v4 | ethernet }
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`udp-ip-v4`	The device uses UDP as the transport mechanism.	Factory setting
`ethernet`	The device uses Ethernet as the transport mechanism.	-

Result

The transport mechanism is specified.

Network structures 7

This part contains the sections that describe the commands for configuring and managing various network structures.

The following technologies are available:

- The establishment of independent structures even across the boundaries of subnets using virtual networks (VLANs)
  This can result in the following advantages:
  - Administration:
    Devices can be grouped together to form a logical units regardless of their physical location
  - Performance:
    By prioritizing, time-critical data (process data, streams) can be given priority for transfer
  - Security:
    The transition between VLANs can only be controlled by an administrator
- Bundling of interfaces or connections between devices to increase the data transmission rate and reliability (link aggregation)
- Improved reliability by adapting the tree structure if transmission is disrupted (Spanning Tree)

7.1 VLAN

This section describes commands for configuring and managing virtual networks (VLANs).

With the following commands, note which "Base bridge mode" you are in. If you are in the "Transparent Bridge" mode, all settings relate to the management VLAN: VLAN 1.

You change the mode with the `base bridge-mode` command.

Commands for configuring and managing private VLANs are also described.

With a private VLAN (PVLAN) you can divide up the layer 2 broadcast domains of a VLAN.

A private VLAN consists of the following units:

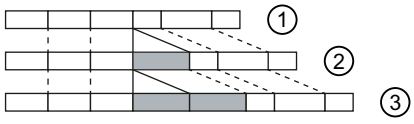
- A primary private VLAN (primary PVLAN)
  The VLAN that is divided up is called primary private VLAN.
- Secondary private VLANs (secondary PVLAN)
  Secondary PVLANs exist only within a primary PVLAN. Every secondary PVLAN has a specific VLAN ID and is connected to the primary PVLAN.
  Secondary PVLANs are divided into the following types:
  - Isolated Secondary PVLAN
    Devices within an Isolated Secondary PVLAN cannot communicate with each other via layer 2.
  - Community Secondary PVLAN
    Devices within a Community Secondary PVLAN can communicate with each other directly via layer 2. The devices cannot communicate with devices in other communities of the PVLAN via layer 2.

In addition, commands are described for configuring the VLAN tunnel.

With the Q-in-Q VLAN tunnel function it is possible to forward the data traffic from various customer networks with a VLAN tunnel via a provider network. Each customer network can have the total number VLANs available.

A VLAN tunnel is established between provider switches configured on the boundaries of a provider network. A provider switch has the following types of port:

- Access port
  The provider switch is connected to a customer network via an access port.
  - Incoming data traffic
    The incoming data traffic at an access port is treated as if it were untagged ①. All incoming frames are expanded by a tag with the port VID of the access port ②. With frames that are already tagged this means that they are expanded by a second 802.1Q tag ③, the outer VLAN tag.



  - Outgoing data traffic
    With outgoing data traffic at an access port the outer VLAN tag is removed again.
- Core port
  The provider switch is connected to a provider network via a core port.
  Core ports are members in the port VLAN of the access port or are configured with the port type "Switch-Port VLAN Trunk".

When the frames reach the relevant access port, they are expanded by a tag with the port VID of the access port and tunneled through the provider network. As soon as the frames leave the provider network, the outer VLAN tag (PVID) is removed again. The frames are forwarded in their original form. The priority of the frame is retained.

7.1.1 The "show" commands VLAN bridge)

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.1.1.1 show mac-address-table

Description

This command shows the table with the static and dynamic unicast MAC addresses and multicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table [vlan <vlan-range>] [address
<aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN or VLAN range	-
`vlan-range`	Number of the addressed VLAN or VLAN range	1 ... 4094 Enter the range limits with a hyphen or a space.
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The entries of the MAC addresses table are displayed.

7.1.1.2 show mac-address-table count

Description

With this command, you show the number of MAC addresses for all or a selected VLAN.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table count [vlan <vlan-id(1-4094)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

If you do not select any parameter from the parameter list, the total number of entries is displayed for all VLANs.

Result

The number of MAC addresses for the selected VLAN is displayed.

7.1.1.3 show mac-address-table dynamic multicast

Description

This command shows the table with the dynamic multicast MAC addresses assigned by the device.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table dynamic multicast[vlan<vlan-range>]
     [address<aa:aa:aa:aa:aa:aa>]
     [{interface<interface-type><interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan`	Keyword for a VLAN connection	-
`vlan-range`	Number of the addressed VLAN	1 ... 4094
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type of interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The dynamic multicast MAC addresses are displayed.

7.1.1.4 show mac-address-table dynamic unicast

Description

This command shows the table with the dynamic unicast MAC addresses learned by the switch based on the MAC address of the sender of received frames on its Ethernet ports.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table dynamic unicast[vlan<vlan-range>]
     [address<aa:aa:aa:aa:aa:aa>][{interface<interface-type>
     <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
vlan	Keyword for a VLAN connection	-
vlan-range	Number of the addressed VLAN	1 ... 4094 Enter the range limits with a hyphen without spaces.
address	Keyword for a MAC address	-
aa:aa:aa:aa:aa:aa	MAC address	-
interface	Keyword for a an interface description	-
interface-type	Type or speed of the interface	Enter a valid interface
interface-id	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The dynamic unicast MAC addresses are displayed.

7.1.1.5 show mac-address-table static multicast

Description

This command shows the table with the static multicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

cli> or cli#

Syntax

Call up the command with the following parameters:

```
show mac-address-table static multicast[vlan<vlan-range>]
  [address<aa:aa:aa:aa:aa:aa>][{interface<interface-type><interface-
id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan`	Keyword for a VLAN connection	-
`vlan-range`	Number of the addressed VLAN	1 ... 4094 Enter the range limits with a hyphen without spaces.
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The static multicast MAC addresses are displayed.

7.1.1.6 show mac-address-table static unicast

Description

This command shows the table with the static unicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table static unicast[vlan<vlan-range>]
  [address<aa:aa:aa:aa:aa:aa>][{interface<interface-type><interface-
id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan`	Keyword for a VLAN connection	-
`vlan-range`	Number of the addressed VLAN	1 ... 4094 Enter the range limits with a hyphen without spaces.
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The static unicast MAC addresses are displayed.

7.1.1.7 show vlan

Description

This command shows the specific information for all or a selected VLAN.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show vlan [brief | id <vlan-range> | summary]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`brief`	Shows brief information about all VLANs	-
`id`	Keyword for a VLAN or VLAN range	-

Parameter	Description	Range of values / note
`vlan-range`	Number of the addressed VLAN or VLAN range	1 ... 4094 Enter the range limits with a hyphen or a space.
`summary`	Shows a summary of the VLANs	

If you do not select any parameter from the parameter list, the entries of all available interfaces are displayed.

Result

The information for the selected VLAN is displayed.

7.1.1.8 show vlan device info

Description

This command shows all the global information that is valid for all VLANs.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show vlan device info
```

Result

The global information is displayed.

7.1.1.9 show vlan learning params

Description

This command shows the parameters for the automatic learning of addresses for selected or all VLANs (active and inactive VLANs).

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show vlan learning params [vlan <vlan-range>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan`	Keyword for a VLAN or VLAN range	-
`vlan-range`	Number of the addressed VLAN or VLAN range	1 ... 4094 Enter the range limits with a hyphen or a space.

If you do not select any parameter from the parameter list, the entries of all available interfaces are displayed.

Result

The settings for the automatic learning of addresses are displayed.

7.1.1.10 show vlan port config

Description

This command shows the VLAN-specific information for ports.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show vlan port config [{port <interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`port`	Keyword for a port	-
`interface-type`	Type of interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on identifiers of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries of all available interfaces are displayed.

Result

The information about the ports is displayed.

7.1.1.11 show vlan private-vlan

Description

This command shows the specific information for all or for a selected private VLAN type.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

`show vlan private-vlan [{primary|isolated|community}]`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`pvlan-type`	Displays information on all PVLAN types.	-
`primary`	Displays information on the Primary PVLAN.	-
`isolated`	Displays information on the Isolated Secondary PVLANs.	-
`community`	Displays information on the Community Secondary PVLANs.	-

If you do not select any parameter from the parameter list, the entries of all available types are displayed.

Result

The information for the selected private VLAN type is displayed.

Further notes

You define a private VLAN type `private-vlan` command.

7.1.2 The "show" commands (Transparent Bridge)

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.1.2.1 show dot1d mac-address-table

Description

This command shows the table with the static and dynamic unicast entries and the dynamic multicast entries.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
show dot1d mac-address-table [address <aa:aa:aa:aa:aa:aa>]
     [{interface <interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	Specify a valid MAC address.
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The entries are displayed.

7.1.2.2 show dot1d mac-address-table static multicast

Description

This command shows the table with the static multicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show dot1d mac-address-table static multicast [address
<aa:aa:aa:aa:aa:aa>]
     [{interface <interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The static multicast MAC addresses are displayed.

7.1.2.3 show dot1d mac-address-table static unicast

Description

This command shows the table with the static unicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show dot1d mac-address-table static unicast [address
<aa:aa:aa:aa:aa:aa>]
     [{interface <interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The static unicast MAC addresses are displayed.

7.1.2.4 show vlan device info

Description

This command shows all the global information that is valid for all VLANs.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show vlan device info
```

Result

The global information is displayed.

7.1.3 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.1.3.1 base bridge-mode

Description

With this command, you configure whether or not the device forwards frames with VLAN tags transparently (IEEE 802.1D/Transparent Bridge) or takes VLAN information into account (IEEE 802.1Q/VLAN Bridge).

Note

Changing base bridge mode

Note the section "Changing base bridge mode". This section describes how a change affects the existing configuration. Before device mode is switched, a security prompt takes place.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
base bridge-mode {dot1d-bridge|dot1q-vlan} [force]
```

The parameters have the following meaning:

Parameter	Description	Range of values / notes
`dot1d-bridge`	Sets the mode "Transparent Bridge" for the device. VLAN tags are not taken into account or changed but are forwarded transparently. In this mode, you cannot create any VLANs. Only a management VLAN is available: VLAN 1.	Default setting with PROFINET variants
`dot1q-vlan`	Sets the mode "VLAN Bridge" for the device. VLAN information is taken into account.	Default setting with EtherNet/IP variants
`force`	When this parameter is executed, there is no security prompt when you switch device mode. This enables you to integrate the command in a script.	Take note of the effects on the existing configuration described in the section "Changing base bridge mode".

Result

The device mode is configured.

Changing base bridge mode

802.1D Transparent Bridge → 802.1Q VLAN Bridge

If you change the Base bridge mode from Transparent Bridge to VLAN Bridge, this has the following effects

- All static and dynamic unicast entries are deleted.
- All static and dynamic multicast entries are deleted.
- With spanning tree you can set the following protocol compatibility: STP, RSTP and MSTP

802.1Q VLAN Bridge → 802.1D Transparent Bridge

If you change the Base bridge mode from VLAN Bridge to Transparent Bridge, this has the following effects

- All VLAN configurations are deleted.
- A management VLAN is created: VLAN 1.
- All static and dynamic unicast entries are deleted.
- All static and dynamic multicast entries are deleted.
- With spanning tree you can set the following protocol compatibility: STP and RSTP
- You cannot use GVRP.
- You cannot use guest VLAN.
- The VLAN assignment cannot be adopted from the RADIUS server.

- You cannot configure the port type.
- Defined access rules must be valid for all VLANs: `authorized-manager ip-source`

Further notes

You can display the status of this function and other VLAN information with the `show vlan device info` command.

7.1.3.2 vlan

Description

With this command, you create a VLAN on the device and change to the VLAN configuration mode. The command only has an effect in the 802-1Q-VLAN bridge mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
vlan <vlan-id(1-4094)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`vlan-id`	Number of the addressed VLAN	1 ... 4094 In the transparent bridge mode only VLAN 1 is available.

Do not enter any leading zeros with the number of the VLAN.

Result

You are now in the VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-1)#
```

Further notes

You can display information about the VLAN with the `show vlan device info` command.

7.1.3.3 no vlan

Description

With this command, you delete a VLAN on the device.

Requirement

- The VLAN must not be assigned to a physical port.
- You are in the Global Configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call up the command with the following parameter:

`no vlan <vlan-id(1-4094)>`

Parameter	Description	Range of values / note
`vlan-id`	Number of the addressed VLAN	1 ... 4094

The VLAN with number 1 cannot be deleted.

Result

The VLAN is deleted

Further notes

With the `vlan` command, you create a VLAN on the device.

You can display information about the VLAN with the `show vlan` command.

7.1.3.4 interface range

Description

With this command, you can put several interfaces or the interfaces of VLANs together and configure them together. The configurations are valid for all interfaces of the specified range.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

```
interface range {[<interface-type> <0/a-b,0/c,...>] |
[{vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>}]}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Keyword for an interface	Enter a valid interface.
`0/a-b, 0/c,...`	Module no. and port no. of the interface	
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`vlan-id`	Number of the addressed VLAN	2 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you want to address several VLANs with this command, you must insert a blank before and after the hyphen, for example `interface range vlan 5 - 10`.

Result

The interfaces or interfaces of VLANs were put together to form an interface range.

The command prompt is as follows:

```
cli(config-if-vlan-range)#
```

The configuration commands you enter in a mode apply to all interfaces of this area.

Further notes

With the `no interface range` command, you remove VLANs from this range or break it up.

7.1.3.5 no interface range

Description

With this command, you remove the interfaces or interfaces of VLANs from the interface range or break it up if you first remove all previously added interfaces.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no interface range vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`vlan-id`	Number of the addressed VLAN	2 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you address several VLANs, you must insert a blank before and after the hyphen, for example `no interface range vlan 5 - 10`.

Result

The VLANs have been removed from the specified interface area.

Further notes

With the `interface range` command, you can put several interfaces or VLANs together to be able to configure them together.

7.1.3.6 vlan range

Description

With this command, you can select several VLANs and configure them together. The configurations are valid for all selected VLANs.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
vlan range <vlan-id(1-4094)> - <vlan-id(2-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`vlan-id`	Number of the addressed VLAN	2 ... 4094

Enter a space before and after the hyphen, e.g. `vlan range 5 - 10`.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The command prompt is as follows:

`CLI(config-vlan-range)#`

Configuration commands you enter with this command prompt apply to all selected VLANs.

Further notes

With the command `exit`, you return to the Global configuration mode.

7.1.4 Commands in the global configuration mode (VLAN bridge)

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.1.4.1 bridge-mode

Description

With this command you assign the device a role therefore specifying whether or not the device can manage outer VLAN tags.

If you change the role, the layer 2 port settings (VLAN, spanning tree) are reset to the factory settings and the device is restarted.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`bridge-mode {customer | provider }`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`customer`	The device behaves like a standard IE switch.	-
`provider`	In addition to the properties of the role "Customer" the device also has the possibility of managing outer VLAN tags. In this role, you can use the function Q-in-Q VLAN tunnel.	The "Provider" role has the following effects on the VLAN tag: All data packets that are not sent from an access port receive a VLAN tag. If the VLAN configuration of the other devices is not adapted accordingly, network loops can occur or network segments may no longer be reachable.

Result

The role of the device is specified.

Further notes

You display the role of the device with the `show vlan device info` command.

7.1.4.2 vlan tag-priority override

Description

With this command, you specify whether the priority of an incoming frame is overwritten by the priority configured for a VLAN.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`vlan tag-priority override {enable | disable}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`enable`	The priority configured for a VLAN replaces the priority existing in the VLAN tag of the frame.	-
`disable`	The VLAN tag of the frame remains unchanged.	-

Result

Overwriting of the VLAN tag is enabled or disabled.

Additional notes

You configure the priority of a VLAN with the `priority` command.

You reset the priority of a VLAN to the default value with the `no priority` command.

7.1.5 Commands in the Interface configuration mode (VLAN Bridge)

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.1.5.1 alias

Description

With this command, you assign a name to an interface. The name only provides information and has no effect on the configuration.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
alias <interface-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`interface-name`	Name of the interface	max. 63 characters

Result

The interface was assigned a name.

Further notes

You delete the name of the interface with the `no alias` command.

7.1.5.2 no alias

Description

With this command, you delete the name of the interface.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameter assignment:

```
no alias
```

Result

The name of the interface is removed.

Further notes

You configure the name of the interface with the `alias` command.

7.1.5.3 private-vlan mapping

Description

With this command you specify from which secondary PVLANs the IP interface of the primary PVLAN will be reachable.

Requirement

- The interface is configured as an IP interface.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`private-vlan mapping [{add | remove}] <vlan-list>`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`add`	Adds secondary PVLANs.	-
`remove`	Removes secondary PVLANs.	-
`vlan-list`	VLAN ID of the secondary PVLAN	Separate the PVLANs with commas if you specify several PVLANs.

Result

The IP interface of the primary PVLAN can be reached from the selected secondary PVLANs.

Further notes

You delete the link between secondary PVLANs and the IP interface of the primary PVLAN with the command `no private-vlan mapping`.

You display this setting with the `show interfaces` command with the `private-vlan mapping` parameter.

7.1.5.4 no private-vlan mapping

Description

With this command you delete the link between secondary PVLANs and the IP interface of the primary PVLAN with the command .

Requirement

- The interface is configured as an IP interface.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

```
no private-vlan mapping
```

Result

The IP interface of the primary PVLAN cannot be reached from the selected secondary PVLANs.

Further notes

You configure a link between secondary PVLANs and the IP interface of the primary PVLAN with the command `private-vlan mapping`.

You display this setting with the `show interfaces` command with the `private-vlan mapping` parameter.

7.1.5.5 switchport acceptable-frame-type

Description

With this command, you configure which types of frames are accepted.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`all`	All frames are accepted.	Default On a ring port only the parameter "`all`" is supported.
`tagged`	The device discards all untagged frames. The device forwards all tagged frames.	-
`untaggedAndPrioritytagged`	The device discards all tagged frames. The device forwards all untagged frames and frames with a priority.	-

Result

The setting is enabled.

Further notes

You can reset the setting to the default with the `no switchport acceptable-frame-type` command.

You can display the status of this function and other information with the `show vlan port config` command.

7.1.5.6 no switchport acceptable-frame-type

Description

With this command, you reset the setting for the types of frames accepted by the interface to the default value.

The default value is `all`.

The interface accepts tagged and untagged frames.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

```
no switchport acceptable-frame-type
```

Result

The setting is reset to the default value.

Further notes

You configure the setting with the `switchport acceptable-frame-type` command.

You can display the status of this function and other information with the `show vlan port config`command.

7.1.5.7 switchport access vlan

Description

With this command, you assign an VLAN to an interface and configure the port VLAN identifier (PVID) for it.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
switchport access vlan <vlan-id(1-4094)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`vlan-id`	Number of the addressed VLAN	1 ... 4094

Result

The Interface is added to the VLAN as an untagged port and the corresponding VLAN ID is set.

Further notes

You can reset the setting to the default with the `no switchport access vlan` command.

You display the setting and other information with the `show vlan port config` command.

7.1.5.8 no switchport access vlan

Description

With this command, you reset the setting for the port VLAN identifier (PVID) for an interface to the default value.

The default value is 1.

Requirement

You are in the interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no switchport access vlan
```

Result

The setting is reset to the default value.

Further notes

You configure the setting with the `switchport access vlan` command.

You can display the status of this function and other information with the `show vlan port config`command.

7.1.5.9 switchport mode

Description

With this command, you specify the operating mode for the switch port.

Requirement

- The interface is configured as a switch port.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`switchport mode { access | trunk | hybrid }`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`access`	Configures the port as an access port. Access ports belong to a provider switch that supports the function Q-in-Q VLAN-Tunnel. Connect a customer network to access ports.	GVRP must be disabled on the port. On the port for the `acceptable-frame-type` the value `untaggedAndPrioritytagged` must be set.
`trunk`	Configures the port as a trunk port that only forwards tagged frames. The port can then only be configured as the trunk port if the port is not entered in any VLAN that exchanges untagged frames. For the trunk port to forward tagged frames, all VLAN IDs to which the trunk port forwards frames must be stored. If a new VLAN is created, the VLAN ID is automatically entered at the trunk port. With a trunk port, the VLAN assignment is dynamic. Static configurations can only be created if, in addition to the trunk port property, the port is also entered statically as a member in the VLANs involved. An example of a static configuration is the assignment of the multicast groups in certain VLANs. If you execute the "`acceptable frame-type all`" command at the trunk port, the port also receives untagged frames.	-
`hybrid`	Configures the port as a hybrid port that accepts tagged and untagged frames.	Default: `hybrid`

Result

The operating mode is configured.

Further notes

You reset the operating mode to the default with the `no switchport mode` command.

You display this setting and other information with the `show vlan port config` command.

You configure the interface as a switch port with the `switchport` command.

7.1.5.10 no switchport mode

Description

With this command, you reset the operating mode for the switch port to the default.

The default value is Hybrid.

Requirement

- The interface is configured as a switch port.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameters:

```
no switchport mode
```

Result

The setting is reset to the default value.

Further notes

You configure the operating mode with the `switchport mode` command.

You display this setting and other information with the `show vlan port config` command.

You configure the interface as a switch port with the `switchport` command.

7.1.5.11 switchport mode private vlan

Description

With this command, you specify the operating mode for the private VLAN port.

Requirement

- The interface is configured as a switch port.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`switchport mode private-vlan {promiscuous | host}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`promiscuous`	Configures the port as a promiscuous port. Promiscuous ports belong to a primary PVLAN. Connect devices to promiscuous ports that are intended to communicate with all other devices of the PVLAN.	GVRP must be disabled on the port.
`host`	Configures the port as a host port. Host ports belong to a secondary PVLAN. Connect devices to host ports that are only intended to communicate with certain devices of the PVLAN.	

Result

The operating mode for the private VLAN port is configured.

Further notes

You display this setting and other information with the `show vlan port config` command.

You configure the interface as a switch port with the `switchport` command.

You configure a host port with the `switchport private-vlan host-association` command.

You configure a promiscuous port with the `switchport private-vlan mapping` command.

7.1.5.12 switchport mode dot1q-tunnel

Description

With this command, you enable the Q-in-Q VLAN tunnel function. Frames received at the port are expanded with an outer VLAN tag, the PVID of the port.

Requirement

- The port is configured as an access port.
- Spanning tree is disabled on the port.
- GMRP is disabled on the port.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

```
switchport mode dot1q-tunnel
```

Result

The Q-in-Q VLAN tunnel function is enabled.

Further notes

You disable the function with the `no switchport mode dot1q-tunnel` command.

You display this setting and other information with the `show vlan port config` command.

You configure the PVID with the `switchport pvid` command.

You configure the operating mode of a port with the `switchport mode` command.

You disable the spanning tree function with the `no spanning tree` command.

If you want to enable or disable the GMRP function for a specific interface on the device, use the `no gmrp` command in the Interface configuration mode.

7.1.5.13 no switchport mode dot1q-tunnel

Description

With this command, you disable the Q-in-Q VLAN tunnel function.

Requirement

You are in the Interface configuration mode.
The command prompt is:
`cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

```
no switchport mode dot1q-tunnel
```

Result

The Q-in-Q VLAN tunnel function is disabled.

Further notes

You enable the function with the `switchport mode dot1q-tunnel` command.

You display this setting and other information with the `show vlan port config` command.

7.1.5.14 switchport priority default

Description

With this command, you configure the priority default for the interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
switchport priority default <(0-7)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
–	Value for the priority default	0 ... 7 Default: 0

Result

The setting for the default priority of the interface is configured.

Further notes

You reset the priority default to the original default with the `no switchport priority default` command.

You display this setting and other information with the `show vlan port config` command.

7.1.5.15 no switchport priority default

Description

With this command, you reset the priority default for the interface to the default value.

The default value is 0.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

`no switchport priority default`

Result

The setting is reset to the default value.

Further notes

You configure the priority default with the `switchport priority default` command.

You display this setting and other information with the `show vlan port config` command.

7.1.5.16 switchport private-vlan host-association

Description

With this command, you configure a host port.

The following settings are made:

- The interface becomes an untagged member of the primary PVLAN and its secondary PVLANs.
- With incoming untagged frames, the port VLAN-ID of the secondary VLAN is set.
- Ingress filtering is enabled.

Requirement

- The interface is configured as a host port.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

```
switchport private-vlan host-association <primary-vlan-id (1-4094)>
<secondary-vlan-id (1-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`primary-vlan-id`	VLAN ID of the primary PVLAN	1 ... 4094
`secondary-vlan-id`	VLAN ID of the secondary PVLAN	1 ... 4094

Result

The interface is configured.

Further notes

You delete the configuration with the `no switchport private-vlan host-association` command.

You display this setting and other information with the commands `show vlan port config`, `show vlan` and `show vlan private-vlan`.

You configure the interface as a host port with the `switchport mode` command.

7.1.5.17 no switchport private-vlan host-association

Description

With this command, you delete the configuration of a host port.

Requirement

- The interface is configured as a host port.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

```
no switchport private-vlan host-association
```

Result

The configuration is deleted.

Further notes

You configure a host port with the `switchport private-vlan host-association` command.

You display this setting and other information with the commands `show vlan port config`, `show vlan` and `show vlan private-vlan`.

You configure the interface as a host port with the command.

7.1.5.18 switchport private-vlan mapping

Description

With this command, you configure a promiscuous port.

The following settings are made:

- The interface becomes an untagged member of the primary PVLAN and all secondary PVLANs.
- With incoming untagged frames, the port VLAN-ID of the primary VLAN is set.
- Ingress filtering is enabled.

Requirement

- The interface is configured as a promiscuous port.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

```
switchport private-vlan mapping <primary-vlan-id (1-4094)> [{add |
remove}] [<secondary_vlan_list>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`primary-vlan-id`	VLAN ID of the primary PVLAN	1 ... 4094
`add`	Adds secondary PVLANs.	-
`remove`	Removes secondary PVLANs.	-
`secondary_vlan_list`	VLAN ID of the secondary PVLAN	1 ... 4094 Separate the PVLANs with commas if you specify several PVLANs.

Result

The interface is configured.

Further notes

You delete the configuration with the `no switchport private-vlan mapping` command.

You display this setting and other information with the commands `show vlan port config`, `show vlan` and `show vlan private-vlan`.

You configure the interface as a promiscuous port with the `switchport mode` command.

7.1.5.19 no switchport private-vlan mapping

Description

With this command, you delete the configuration of a promiscuous port.

Requirement

- The interface is configured as a promiscuous port.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

```
no switchport private-vlan mapping
```

Result

The configuration is deleted.

Further notes

You configure a promiscuous port with the `switchport private-vlan mapping` command.

You display this setting and other information with the commands `show vlan port config`, `show vlan` and `show vlan private-vlan`.

You configure the interface as a promiscuous port with the `switchport mode` command.

7.1.5.20 switchport pvid

Description

With this command, you assign an interface to a VLAN and configure the port VLAN identifier (PVID) for it. If a received frame has no VLAN tag, it has a tag added with the VLAN ID specified here and is sent according to the switch rules for the port.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:

```
switchport pvid <vlan-id(1-4094)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`vlan-id`	Number of the addressed VLAN	1 ... 4094

Result

The PVID is configured

Additional notes

You can reset the setting to the default with the `no switchport pvid` command.

You configure the VLAN ID and assign a VLAN to the interface with the `switchport access vlan` command.

You display the setting and other information with the `show vlan port config` command.

7.1.5.21 no switchport pvid

Description

With this command, you reset the setting for the port VLAN identifier (PVID) for an interface to the default value.

The default value is 1.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no switchport pvid
```

Result

The setting is reset to the default value.

Additional notes

You configure the setting with the `switchport pvid` command.

You configure the VLAN ID and assign a VLAN to the interface with the `switchport access vlan` command.

You can display the status of this function and other information with the `show vlan port config` command.

7.1.5.22 tia interface

Description

With this command, you enable or disable the property TIA interface. The TIA interface defines the VLAN on which the PROFINET functionalities are available. This mainly affects the device search with or via DCP.

Requirement

- The interface is enabled.
- You are in the Interface configuration mode of the VLAN interface.
  The command prompt is:
  `cli (config-if-vlan-$$$) #`
  $$$ stands for the numbering of the interface.

Syntax

Call the command without parameters:
`tia-interface`

Result

The TIA interface property is enabled exclusively for the specified VLAN. The function was disabled on the other interfaces.

Further notes

Note that only one VLAN interface can become the TIA interface.

7.1.6 Commands in the VLAN configuration mode (VLAN Bridge)

This section describes commands that you can call up in the VLAN Configuration mode.

In global configuration mode, enter the `vlan $$$` command to change to this mode. When doing this, you need to replace the `$$$` placeholders with the relevant VLAN ID.

Commands relating to other topics that can be called in the VLAN Configuration mode can be found in the relevant sections.

- If you exit the VLAN Configuration mode with the `exit` command, you return to the Global Configuration mode.
- If you exit the VLAN Configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in VLAN configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.1.6.1 name

Description

With this command, you assign a name to the VLAN.

Requirement

You are in the VLAN Configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call up the command with the following parameters:

```
name <vlan-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`vlan-name`	Name that will be assigned to the VLAN	max. 32 characters

Result

The VLAN is assigned a name.

Further notes

You delete name assignment for a VLAN with the `no name` command.

7.1.6.2 no name

Description

With this command, you delete the name assignment for a VLAN.

Requirement

You are in the VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call the command without parameters:

```
no name
```

Result

The name of the VLAN is deleted.

Further notes

You assign the VLAN a name with the command `name`.

7.1.6.3 ports

Description

With this command, you generate a list that specifies the behavior of the interfaces and replaces the existing VLAN configuration.

- Member Port (tagged port)
  The interface is added permanently to the list of incoming and outgoing connections. Tagged and untagged frames are transferred.
- Untagged Port
  The interface transfers untagged frames. If the VLAN ID (PVID) is set, incoming untagged frames are given a tag with the VLAN ID specified there. Received frames with a VLAN ID are forwarded according to the VLAN ID. With outgoing frames, the tag with the VLAN ID is removed.
- Forbidden Ports
  This interface is not used for communication in a VLAN.

The "tagged port" and "untagged port" you specify with this command are used for outgoing data traffic.

Requirement

You are in the VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call up the command with the following parameters:

```
ports
   (
    [<interface-type><0/a-b,0/c,...>]
    [<interface-type><0/a-b,0/c,...>]
    [port-channel<a,b,c-d>]
   )
   [
    untagged<interface-type> <0/a-b,0/c,...>
    (
     [<interface-type><0/a-b,0/c,...>]
     [port-channel <a,b,c-d>]
     [all]
    )
   ]
```

```
[
 forbidden<interface-type><0/a-b,0/c,...>
 [<interface-type><0/a-b,0/c,...>]
 [portchannel<a,b,c-d>]
]
[name<vlan-name>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Enter a valid interface.
`/a-b,0/c,...`	Port no. of the interface	
`port-channel`	Keyword for a port channel	-
`a,b,c-d`	Port no. of the interface	Enter a valid interface name
`untagged`	Keyword for interfaces or ports that transfer data packets without VLAN marking	-
`all`	Specifies that all interfaces or ports are set to "untagged"	-
`forbidden`	Keyword for forbidden interfaces or ports	-
`name`	Keyword for the name assignment	-
`vlan-name`	Name of the VLAN	max. 32 characters

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The existing VLAN configuration is replaced. To add individual interfaces, you need to recreate the full list.

Further notes

You display details of the function with the `show vlan` command.

You reset the settings with the `no ports` command.

7.1.6.4 no ports

Description

With this command you remove all ports i.e. Member Ports (M), Untagged Member Ports (U) and Forbidden Ports (F) from a VLAN.

Requirement

You are in VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no ports
[<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/
c,...>]
[port-channel <a,b,c-d>] [all] [untagged ([<interface-type> <0/a-
b,0/c,...>]
 [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]
[all])]
[forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/
a-b,0/c,...>]
[port-channel <a,b,c-d>] [all])]
[name <vlan-name>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type of interface	Enter a valid interface.
`/a-b,0/c,...`	Port no. of the interface	
`port-channel`	Keyword for a port channel	-
`a,b,c-d`	Port no. of the interface	Enter a valid interface.
`untagged`	Keyword for interfaces or ports that transfer data packets without VLAN marking	-
`all`	This parameter appears at several points in the command. • `no ports all` This command removes all Member Ports (Tagged Member - M) from the VLAN. • `no ports untagged all` This command removes all Untagged Member Ports (U) from the VLAN. Afterwards the ports are Tagged Members (M) in the VLAN. • `no ports forbidden all` This command removes all Forbidden Ports (F) from the VLAN.	-
`forbidden`	Keyword for forbidden interfaces or ports	-
`name`	Keyword for the name assignment	-
`vlan-name`	Name of the VLAN	max. 32 characters

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The ports are removed from the VLAN configuration.

Additional notes

It is possible to remove individual ports from a VLAN configuration without needing to rewrite the entire configuration.

You display details of the function with the `show vlan` command.

You configure the setting with the `ports` command.

7.1.6.5 priority

Description

With this command, you specify which Class of Service (COS) is assigned to the package on transmission. This does not change the Tag Control Information (TCI) of the package, however. If you want to overwrite the COS information in the package, you need to specify the `update-tag-priority` parameter.

Requirement

You are in VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call up the command with the following parameters:

```
priority <prio (0-7)> [update-tag-priority]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`prio`	Value of the priority	0 ... 7 Default: 0
`update-tag-priority`	Keyword for overwriting class of service information in the package.	-

Result

The VLAN has been assigned a priority.

Additional notes

You reset the priority to the default value with the `no priority` command.

You enable the priority with the `priority-enable` command.

You disable the priority with the `no priority-enable` command.

You display the current priority with the `show vlan` command.

You configure the assignment of the priority to a queue with the `cos-map` command.

7.1.6.6 no priority

Description

With this command, you reset the priority of the VLAN back to the default value 0.

Requirement

You are in VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call the command without parameter assignment:

```
no priority
```

Syntax

Call the command with the following parameters:

```
no priority [update-tag-priority]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`update-tag-priority`	Keyword for overwriting class of service information in the package.	-

Result

The priority of the VLAN is reset to the default value.

Additional notes

You change the priority with the `priority` command.

You enable the priority with the `priority-enable` command.

You disable the priority with the `no priority-enable` command.

You display the current priority with the `show vlan` command.

You configure the assignment of the priority to a queue with the `cos-map` command.

7.1.6.7 priority-enable

Description

With this command, you enable the priority of a VLAN.

Requirement

You are in the VLAN Configuration mode.

The command prompt is as follows:

`cli(config-vlan-$$$)#`

Syntax

Call the command without parameter assignment:

`priority-enable`

Result

The priority of the VLAN is enabled.

Further notes

You disable the priority with the `no priority-enable` command.

You change the priority with the `priority`command.

You reset the priority to the default value with the `no priority` command.

You display the current priority with the `show vlan` command.

7.1.6.8 no priority-enable

Description

With this command, you disable the priority of a VLAN.

Requirement

You are in the VLAN Configuration mode.

The command prompt is as follows:

`cli(config-vlan-$$$)#`

Syntax

Call the command without parameter assignment:

```
no priority-enable
```

Result

The priority of the VLAN is disabled.

Further notes

You enable the priority with the `priority-enable` command.

You change the priority with the `priority`command.

You reset the priority to the default value with the `no priority` command.

You display the current priority with the `show vlan` command.

7.1.6.9 private-vlan

Description

With this command you define a VLAN as a private VLAN and specify the PVLAN type.

Requirement

You are in the VLAN Configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call up the command with the following parameters:

```
private-vlan { primary | isolated | community }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`primary`	With this type, you define a primary PVLAN. The primary PVLAN uses the VLAN ID of the VLAN.	-
`isolated`	With this type, you define a secondary PVLAN. Devices within an Isolated Secondary PVLAN cannot communicate with each other via layer 2. The secondary PVLAN has a specific VLAN ID.	-
`community`	With this type, you define a secondary PVLAN. The devices in this secondary PVLAN can communicate with each other via layer 2. The secondary PVLAN has a specific VLAN ID.	-

Result

The PVLAN is defined and the PVLAN type specified.

Additional notes

You delete the configuration as a private VLAN with the `no private-vlan` command.

You display this setting with the `show vlan private-vlan` command.

7.1.6.10 no private-vlan

Description

With this command, you delete the configuration as a private VLAN.

Requirement

You are in the VLAN Configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call the command without parameter assignment:

```
no private-vlan
```

Result

The VLAN is not a private VLAN.

Further notes

You define a VLAN as a private VLAN and specify the PVLAN type with the command `private-vlan`.

You display this setting with the `show vlan private-vlan` command.

7.1.6.11 private-vlan association

Description

With this command, you assign secondary PVLANs to a primary PVLAN.

Requirement

- The interface is configured as a primary PVLAN.
- You are in VLAN configuration mode.
  The command prompt is as follows:
  `cli(config-vlan-$$$)#`

Syntax

Call the command with the following parameters:

`private-vlan association [{add|remove}] <secondary_Vlan_list>`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`add`	Adds a secondary PVLAN..	-
`remove`	Removes a secondary PVLAN..	-
`secondary_Vlan_list`	Number of the secondary PVLAN	Separate the PVLANs with commas if you specify several PVLANs.

Result

The secondary PVLANs are assigned to the primary PVLAN.

Additional notes

You delete the link between secondary PVLANs and a primary PVLAN with the command `no private-vlan association`.

You display this setting with the `show vlan private-vlan` command.

You configure a an interface as a primary PVLAN with the `private-vlan` command.

7.1.6.12 no private-vlan association

Description

With this command you delete the link between secondary PVLANs and a primary PVLAN.

Requirement

- The interface is configured as a primary PVLAN.
- You are in VLAN configuration mode.
  The command prompt is as follows:
  `cli(config-vlan-$$$)#`

Syntax

Call the command without parameter assignment:

`no private-vlan association`

Result

The secondary PVLANs are not assigned to the primary PVLAN.

Additional notes

You assign secondary PVLANs to a primary PVLAN with the command `private-vlan association`.

You display this setting with the `show vlan private-vlan` command.

You configure a an interface as a primary PVLAN with the `private-vlan` command.

7.2 Link aggregation

This section describes commands that configure or manage the bundling of interfaces or connections between devices.

7.2.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.2.1.1 show etherchannel

Description

This command shows the settings of link aggregations.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show etherchannel [[channel-group-number]
     { detail | load-balance | port | port-channel | summary |
protocol}]
```

The parameters have the following meaning:

Parameter	Description
`channel-group-number`	Number of the link aggregation
`detail`	Detailed display of the settings
`load-balance`	Shows which load balancing method is enabled
`port`	Information on the port of the link aggregation
`port-channel`	Information on the link aggregation
`summary`	Brief overview of the settings of a link aggregation
`protocol`	Specification of the protocol set for a link aggregation

If you do not select any parameters from the parameter list, the settings of all channels will be displayed in detail.

Result

The settings of the link aggregation are displayed.

7.2.1.2 show interfaces etherchannel

Description

This command shows the interface-specific information for a link aggregation.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show interfaces [<interface-type> <interface-id> ] etherchannel
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select an interface, information for all interfaces is displayed.

Result

The interface-specific information for a link aggregation is displayed.

Note

When a port is assigned to a link aggregation but is not active (e.g. link down), the values displayed may differ from the values configured for the link aggregation.

If the port in the link aggregation becomes active, individual port configurations such as DCP forwarding are overwritten with the configured values of the link aggregation.

7.2.1.3 show lacp

Description

This command shows the information about the settings and information about the ports involved in the link aggregation. The number of sent and received packets is also displayed.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show lacp [<port-channel(1-8)>] { counters | neighbor [detail] }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`port-channel`	Number of the link aggregation	1 ... 8
`counters`	Shows the values of the counters.	-

Parameter	Description	Range of values/note
`neighbor`	Displays information on neighbor ports.	-
`detail`	Displays detailed information on neighbor ports.	-

If you do not select a link aggregation, information for all available interfaces is displayed.

Result

The information is displayed.

7.2.2 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.2.2.1 channel-group

Description

With this command, you add an interface to a link aggregation.

Requirement

- With the `interface po <channel-group-id(1-8)>` command, you have already generated a logical interface for a link aggregation.
- You are in the Interface configuration mode.
  The command prompt is as follows:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

```
channel-group <channel-group-number(1-8)> mode{on|active|passive}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`channel-group-number`	Number of the link aggregation	1 ... 8
`on`	Adds the interface without LACP to a link aggregation. This corresponds to manual bundling.	If you add a configured port to a link aggregation, the port adopts the configuration of the link aggregation. If you take the port out of the link aggregation, the settings of the port are reset to the factory settings.
`active`	The negotiation of a connection via LACP is started unconditionally.	-
`passive`	The negotiation of a connection via LACP is started when an LACP packet arrives from the connection partner.	-

Result

The link aggregation is configured.

7.2.2.2 no channel-group

Description

With this command, you remove the interface from a link aggregation.

Requirement

You are in the interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no channel-group
```

Result

The interface is deleted from the link aggregation.

7.2.2.3 lacp timeout

Description

With this command, you configure the length of the LACP timeout.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:

```
lacp timeout {long|short}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`long`	The length of the LACP timeout is set to 90 seconds.	Default
`short`	The length of the LACP timeout is set to 3 seconds.	-

Note

The timeout is always three times the send period. This means that the send period lasts 30 seconds with the "`long`" timeout and one second with the "`short`" timeout.

Result

The length of the LACP timeout is specified.

7.2.2.4 no lacp timeout

Description

With this command, you set the LACP timeout to the default value (90 seconds).

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

`no lacp timeout`

Result

The length of the LACP timeout is 90 seconds.

7.3 Spanning Tree

The Spanning Tree Protocol is used to monitor a LAN for redundant connections. These are blocked and reactivated when necessary if there are changes to the network topology.

This section describes the commands of the Spanning Tree Protocol (STP), the Rapid Spanning Tree Protocol (RSTP) and the Multiple Spanning Tree Protocol (MSTP).

Note

Avoiding bad configurations

When using the commands in this section, you should take particular care because a bad configuration of this function can have serious negative affects on the network.

7.3.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.3.1.1 show spanning-tree

Description

This command shows the settings of the spanning tree function.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

`show spanning-tree [{ summary | blockedports | pathcost method }]`

The parameters have the following meaning:

Parameter	Description
`summary`	Shows a summary
`blockedports`	Shows the blocked ports
`pathcost method`	Shows whether 16-bit (short) or 32 bit (long) values are used in the calculation

Result

The settings for the spanning tree function are displayed.

Further notes

You can show further settings for special aspects of the Spanning Tree Protocol with the following commands:

- `show spanning-tree active`
- `show spanning-tree bridge`
- `show spanning-tree detail`
- `show spanning-tree interface`
- `show spanning-tree root`
- `show spanning-tree mst`

7.3.1.2 show spanning-tree active

Description

This command shows the settings for the active ports of the spanning tree function.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

`show spanning-tree active [detail]`

The parameter has the following meaning:

Parameter	Description
`detail`	Shows settings in detail

Result

The settings for the active ports of the spanning tree function are displayed.

7.3.1.3 show spanning-tree bridge

Description

This command shows the settings of the spanning tree function of the bridge.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show spanning-tree bridge
 [{ address | forward-time | hello-time | id | max-age | protocol |
priority | detail }]
```

The parameters have the following meaning:

Parameter	Description
`address`	Shows the MAC address of the bridge
`forward-time`	Shows the time that the bridge is in the listening mode when changing from the blocking mode to the learning mode
`hello-time`	Shows the time after which the bridge sends configuration frames (BPDUs)
`id`	Shows the ID of the bridge
`max-age`	Shows the maximum age of the data packet after which it is deleted
`protocol`	Shows the protocol used
`priority`	Shows the priority of the bridge
`detail`	Shows detailed information about the Spanning Tree settings of the bridge

Result

The settings for the spanning tree function of the bridge are displayed.

7.3.1.4 show spanning-tree detail

Description

This command shows the detailed settings of the spanning tree function.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show spanning-tree detail
```

Result

The detailed settings for the spanning tree function are displayed.

7.3.1.5 show spanning-tree interface

Description

This command shows the settings of the ports for the spanning tree function.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show spanning-tree interface <interface-type> <interface-id>
 [{ cost | priority | portfast | rootcost | restricted-role |
 restricted-tcn | state | stats | detail }]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	
`cost`	Shows the port costs used to calculate the lowest-cost path.	-
`priority`	Shows the priority of the port.	-
`portfast`	Shows whether `spanning-tree portfast` is enabled.	-
`rootcost`	Shows the costs of the path to the root bridge.	-
`restricted-role`	Shows whether `spanning-tree restricted-role` is enabled.	-
`restricted-tcn`	Shows whether `spanning-tree restricted-tcn` is enabled.	-
`state`	Shows the status of the interface.	-
`stats`	Shows the counters of the various BPDU transmissions.	-
`detail`	Shows detailed information about the spanning tree settings of the interface.	-

For information on identifiers of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The settings of the ports for the spanning tree function are displayed.

7.3.1.6 show spanning-tree interface layer2-gateway-port

Description

This command shows the settings of Layer 2 Gateway Port (L2GP). For example the priority, the MAC address and the status of L2GP are displayed.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show spanning-tree interface [<interface-type> <interface-id>]
layer2-gateway-port
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The settings for Layer 2 Gateway Port (L2GP) are displayed.

7.3.1.7 show spanning-tree mst

Description

This command shows various settings of the spanning tree configuration specific to a Common Internal Spanning Tree (CIST) instance or a selected instance of the Multiple Spanning Tree Protocol.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with one of the following parameter assignments:

```
show spanning-tree mst[<instance-id(1-64|4094)>][detail]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`instance-id`	Number of the instance or range of instances whose settings are displayed	• 1 ... 64 • 4094
`detail`	Shows detailed information about the selected interface	-

Result

The settings for the spanning tree configuration are displayed.

Further notes

You display the general settings for the Spanning Tree Protocol with the `show spanning-tree` command.

7.3.1.8 show spanning-tree mst configuration

Description

This command shows various settings for an instance of the Multiple Spanning Tree Protocol.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show spanning-tree mst configuration
```

Result

The settings of an instance of the Multiple Spanning Tree protocol are displayed.

Further notes

You display the general settings for the Spanning Tree Protocol with the `show spanning-tree` command.

7.3.1.9 show spanning-tree mst interface

Description

This command shows port-specific settings of a Multiple Spanning Tree configuration.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with one of the following parameter assignments:

```
show spanning-tree mst [<instance-id(1-64|4094)>] interface
<interface-type> <interface-id>
   [{ stats | hello-time | detail }]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`instance-id`	Number of the instance or range of instances whose settings are displayed	• 1 ... 64 • 4094
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	
`stats`	Shows the number of incoming and outgoing packets for each path of the interface	-
`hello-time`	Shows the intervals at which the root switch sends its "Hello" message to the other switches	-
`detail`	Shows detailed information about the selected interface	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The port-specific settings are displayed.

Further notes

You display the general settings for the Spanning Tree Protocol with the `show spanning-tree` command.

7.3.1.10 show spanning-tree passive-listening-compatibility

Description

This command shows whether or not the "Enhanced Passive Listening Compatibility" function is enabled or disabled.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameter assignment:

`show spanning-tree passive-listening-compatibility`

Result

The setting for the "Enhanced Passive Listening Compatibility" function is displayed.

Further notes

You enable the "Enhanced Passive Listening Compatibility" function with the `spanning-tree passive-listening-compatibility` command.

You disable the "Enhanced Passive Listening Compatibility" function with the `no spanning-tree passive-listening-compatibility` command.

7.3.1.11 show spanning-tree root

Description

This command shows the settings of the root bridge for the spanning tree function.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show spanning-tree root [{ address | cost | forward-time | id |
max-age | port | priority | detail }]
```

The parameters have the following meaning:

Parameter	Description
`address`	Shows the MAC address of the root bridge
`cost`	Shows the costs of the connection to the root bridge.
`forward-time`	Shows the time that the bridge is in the listening mode when changing from the blocking mode to the learning mode
`id`	Shows the ID of the root bridge
`max-age`	Shows the maximum age of the data packet after which it is deleted
`port`	Shows the interface via which the spanning tree is set up

Parameter	Description
`priority`	Shows the priority of the bridge
`detail`	Shows detailed information about the root bridge

Result

The settings of the root bridge for the spanning tree function are displayed.

7.3.2 clear spanning-tree detected protocols

Description

With this command, you restart the protocol transmission process on a specific or on all interfaces and force renegotiation of the connection settings with the neighboring devices.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
clear spanning-tree detected protocols
   [{interface<interface-type><interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the process is restarted for all interfaces.

Result

The connection settings for spanning tree are renegotiated.

7.3.3 clear spanning-tree counters

Description

With this command, you reset all the statistical counters of the spanning tree function at the device and port level.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
clear spanning-tree counters
```

Result

The spanning tree counters are reset.

7.3.4 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.3.4.1 spanning-tree

Description

The Spanning Tree Protocol is used to monitor a LAN for redundant connections. These are blocked and reactivated when necessary if there are changes to the network topology.

With this command, you enable the spanning tree function.

Requirement

- The ring redundancy is disabled.
- You are in the Global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call the command without parameters:

`spanning-tree`

Result

The spanning tree function is enabled.

If you enable Spanning Tree, passive listening is disabled.

Further notes

The default setting of the function with PROFINET variants is "disabled".

The default setting of the function with EtherNet/IP variants is "enabled".

You disable the ring redundancy function with the `no ring-redundancy` command.

You disable the spanning tree function with the `no spanning-tree` command.

You can display the status of this function and other information with the `show spanning-tree detail`command.

You can display information about active ports with the `show spanning-tree active` command.

7.3.4.2 no spanning-tree

Description

With this command, you disable the spanning tree function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

```
no spanning-tree
```

Result

The spanning tree function is disabled.

Further notes

You enable the spanning tree function with the `spanning-tree` command.

You can display the status of this function and other information with the `show spanning-tree detail`command.

You can display information about active ports with the `show spanning-tree active` command.

7.3.4.3 spanning-tree compatibility

Description

With this command, you configure the compatibility version of the protocol that will be used by the spanning tree function.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree compatibility {stp|rst|mst}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`stp`	The version is compatible with the Spanning Tree protocol	-
`rst`	The version is compatible with the Rapic Spanning Tree protocol	Default: enabled
`mst`	The version is compatible with the Multiple Spanning Tree protocol	-

Result

The compatibility version of the protocol is selected.

Further notes

With the `no spanning-tree compatibility` command, you can reset the setting to the default value `rst`.

You can display the status of this function and other information with the `show spanning tree detail` command.

You can display information about active ports with the `show spanning tree active` command.

7.3.4.4 no spanning-tree compatibility

Description

With this command, you reset the compatibility version of the protocol of the spanning tree function to the default value.

The default value is RST.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no spanning-tree compatibility
```

Result

The compatibility version is reset to the default value.

Further notes

You configure the setting with the `spanning-tree compatibility` command.

You can display the status of this function and other information with the `show spanning tree detail` command.

7.3.4.5 spanning-tree mst configuration

Description

With this command, you change to the MSTP configuration mode.

Requirement

- MSTP is enabled
- Compatibility mode: MSTP

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
spanning-tree mst configuration
```

Result

You are now in the MSTP configuration mode.

The command prompt is as follows:

```
cli(config-mst)#
```

Further notes

You exit the MSTP configuration mode with the `end` or `exit` command.

7.3.4.6 spanning-tree mst max-hops

Description

With this command, you configure the maximum number of nodes (hops) that a path can run through in an MST.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree mst max-hops <value(6-40)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`value`	Maximum number of hops that a path can run through in an MST	6 ... 40 Default: 20

Result

The setting for the maximum number of hops is configured.

Further notes

You can reset the setting for the maximum number of nodes to the default with the `no spanning-tree mst max-hops` command.

You display this setting and other information with the `show spanning-tree mst` command.

7.3.4.7 no spanning-tree mst max-hops

Description

With this command, you reset the maximum number of hops that a path in an MST can run through to the default value.

The default value is 20.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no spanning-tree mst max-hops
```

Result

The setting for the maximum number of nodes is reset to the default value.

Further notes

You can configure the setting for the maximum number of nodes with the `spanning-tree mst max-hops` command.

You display this setting and other information with the `show spanning-tree mst` command.

7.3.4.8 spanning-tree mst instance-id root

Description

With this command you specify whether the device is a root bridge (primary) or a substitute root bridge (secondary).

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree mst {instance-id <instance-id(1-64)>} root {primary |
secondary}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`instance-id`	Keyword for the instance	-
`instance-id`	Number of the instance	1 ... 64
`primary`	The priority of the device is set to a low value so that the device can become the root bridge (primary) of the Spanning Tree instance. The lower the value, the higher the priority.	The priority is set to the value 24576.
`secondary`	The priority of the device is set to a low value so that the device becomes the substitute root bridge (secondary) of the Spanning Tree instance. If the root bridge (primary) fails, the substitute root bridge (secondary) takes over the task of the root bridge without delay.	The priority is set to the value 28672.

Result

The function of the device is specified.

Additional notes

You disable the root bridge with the `no spanning-tree mst instance-id root` command.

You display this setting and other information with the commands that start with `show spanning-tree ....`

7.3.4.9 no spanning-tree mst instance-id root

Description

With this command, you disable the "root bridge" function on the device.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no spanning-tree mst{instance-id<instance-id(1-64)>}root
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`instance-id`	Keyword for the instance	-
`instance-id`	Number of the instance	1 ... 64

Result

The "root bridge" function is disabled.

Further notes

You enable the root bridge function with the `spanning-tree mst instance-id root` command.

You display this setting and other information with the commands that start with `show spanning tree ....`

7.3.4.10 spanning-tree priority

Description

With this command, you configure the priority of the device. Which device becomes the root bridge is decided based on the priority. The bridge with the highest priority becomes the root bridge. The lower the value, the higher the priority.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree [mst <instance-id(1-64)>] priority <value(0-61440)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mst`	Keyword for a Multiple Spanning Tree instance	-
`instance-id`	Number of the instance	1 ... 64
`priority`	Keyword for the priority	-
`value`	Value for the priority	0 ... 61440 Default: 32768

You can only change the value for the priority in the steps of 4096.

Result

The priority of the device is configured.

Further notes

You can reset the setting to the default with the `no spanning-tree priority` command.

You display this setting and other information with the commands that start with `show spanning-tree ....`

7.3.4.11 no spanning-tree priority

Description

With this command, you reset the priority of the device back to the default value.

The default value is 32768.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no spanning-tree[mst <instance-id(1-64)>]priority
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mst`	Keyword for a Multiple Spanning Tree instance	-
`instance-id`	Number of the instance	1 ... 64

Result

The priority of the device is reset to the default value.

Further notes

You configure the setting with the `spanning-tree priority` command.

You display this setting and other information with the commands that start with `show spanning-tree ....`

7.3.4.12 spanning-tree passive-listening-compatibility

Description

With this command you enable the "Enhanced Passive Listening Compatibility" function.

If you enable the "Enhanced Passive Listening Compatibility" function, the IE switch sends topology change frames via the (R)STP edge port that caused the topology change.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
spanning-tree passive-listening-compatibility
```

Result

The "Enhanced Passive Listening Compatibility" function is enabled.

Further notes

You disable the function with the `no spanning-tree passive-listening-compatibility` command.

You can display the status of this function with the `show spanning-tree passive-listening-compatibility`command.

7.3.4.13 no spanning-tree passive-listening-compatibility

Description

With this command you disable the "Enhanced Passive Listening Compatibility" function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no spanning-tree passive-listening-compatibility
```

Result

The "Enhanced Passive Listening Compatibility" function is disabled.

Further notes

You enable the function with the `spanning-tree passive-listening-compatibility` command.

You can display the status of this function with the `show spanning-tree passive-listening-compatibility`command.

7.3.4.14 spanning-tree pathcost dynamic

Key statement

Use this command to specify that the path cost of ports for spanning tree is adapted dynamically depending on the port speed. You can use an optional parameter to specify that the path cost of a link aggregation is also adapted dynamically.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command with the following parameters:

`spanning-tree pathcost dynamic [lag-speed]`

The parameter has the following meaning:

Parameter	Description
`lag-speed`	The spanning tree path cost of a link aggregation is adapted dynamically. The bandwidth currently available in the link aggregation is decisive.

Result

The spanning tree path cost is adapted dynamically.

Additional notes

You display the configuration of Spanning Tree with the `show spanning tree` command.

7.3.4.15 no spanning-tree pathcost dynamic

Key statement

Use this command to disable dynamic adaptation of spanning tree path costs.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command with the following parameters:

`no spanning-tree pathcost dynamic [lag-speed]`

The parameter has the following meaning:

Parameter	Description
`lag-speed`	The spanning tree path cost of a link aggregation is not adapted dynamically. This does not affect the dynamic adaptation of the path cost of individual ports.

Result

The spanning tree path cost is independent of the bandwidth of the port in question.

Additional notes

You display the configuration of Spanning Tree with the `show spanning tree` command.

7.3.4.16 spanning-tree rstp-plus

Description

With this command, you enable RSTP+.

RSTP+ enables the linking of a network segment in which Spanning Tree is activated with an MRP ring. Make sure that the following requirements have been met before executing this command:

- MRP must be activated as redundancy method.
- If ring redundancy is activated, you need to disable the ring ports for Spanning Tree.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
spanning-tree rstp-plus
```

Result

RSTP+ is enabled.

Additional notes

You can display the status of this function and other information with the `show spanning-tree` command.

7.3.4.17 no spanning-tree rstp-plus

Description

With this command, you disable RSTP+.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no spanning-tree rstp-plus
```

Result

RSTP+ is disabled.

Additional notes

You can display the status of this function and other information with the `show spanning-tree` command.

7.3.4.18 spanning-tree rstp-plus mrp-intercon-domain-id

Description

With this command, you configure the MRP Interconnection Domain ID for RSTP+.

The RSTP+ MRP Interconnection Domain ID must be unique throughout the network and must differ from any MRP Interconnection Domain ID that may need to be configured. Different IDs are necessary to distinguish TCNs (Topology Change Notifications) of the RSTP network from TCNs of the MRP ring. This assignment makes it possible to only delete those FDB entries (Forwarding Database entries) that are affected by the topology change.

Each device checks whether different values were configured for these two parameters. If the IDs are identical, the device outputs an error message. The network administrator is responsible for making sure that these IDs are also unique throughout the network. An individual device cannot make such a check.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree rstp-plus mrp-intercon-domain-id <mrp-intercon-domain-
id (1-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`mrp-intercon-domain-id`	The MRP Interconnection Domain ID for RSTP+. This value must not match the MRP Interconnection Domain ID configured for the active MRP Interconnection connection.	1 ... 65535

Result

The MRP Interconnection Domain ID for RSTP+ is configured.

Additional notes

You can display the status of this function and other information with the `show spanning-tree detail` command.

You can display information about active ports with the `show spanning-tree active` command.

7.3.4.19 spanning-tree tc-protection-backoff

Description

Use this command to configure the Topology Change Protection Backoff function.

The function can be activated in case of frequent changes or faulty connections (shaky link) in large RSTP/ MSTP networks to avoid overloading the network components during the processing of many simultaneously arriving topology change frames. When activated, the basic processing of TC frames remains unchanged, but the address tables are only processed at set time intervals. This significantly reduces the actions that the switch has to perform when it receives a large number of topology changes at the same time. The basic RSTP/MSTP behavior is not affected by this feature.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`spanning-tree tc-protection-backoff <seconds(0-60)>`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`tc-protection-backoff`	Keyword for Topology Change Protection Backoff	-
`seconds`	Specify the time interval in which the switch deletes FDB (Forwarding Database) entries in the address tables after it has received TC frames.	0 ... 60 0: The function is disabled Default: 6

Result

The Topology Change Protection Backoff function is configured.

Further notes

You display the configuration of Spanning Tree with the `show spanning tree` command.

7.3.4.20 Time settings for the Spanning Tree protocol

spanning-tree (time settings)

Description

With this command, you configure the various time settings of the spanning tree function:

- With the `forward-time` option, you configure the time after which a port changes its spanning tree status from "Blocking" to "Forwarding".
- With the `hello-time` option, you configure the time after which the bridge sends its configuration frames (BPDUs).
- With the `max-age` option, you configure the time after which the information of the BPDUs becomes invalid.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree {forward-time <seconds(4-30)> | hello-time
<seconds(1-2)> | max-age <seconds(6-40)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`forward-time`	Keyword for the time after which a port changes its spanning tree status from "Blocking" to "Forwarding"	-
`seconds`	Time after which the changeover takes place	4 ... 30 Default: 15
`hello-time`	Keyword for the time after which the bridge sends its configuration BPDUs	-
`seconds`	Time after which they are sent	1 ... 2 Default: 2
`max-age`	Keyword for the time after which the information of the BPDUs becomes invalid	-
`seconds`	Maximum age of the BPDUs in seconds	6 ... 40 Default: 20

Note

Dependencies when setting the timing

If you specify the time settings for spanning tree, you need to keep to the following two rules:

- 2 * (`forward-time` - 1) ≥ `max-age`
- `max-age` ≥ 2 * (`hello-time` + 1)

Result

The selected setting for the time is configured.

Further notes

You reset the time settings to the default values with the `no spanning-tree forward-time`, `no spanning-tree hello-time` or `no spanning-tree max-age`.

If you call the `no spanning-tree` command without parameters, you disable the spanning tree function. The configured time settings are retained.

If you call the `restart factory` command, the system restarts with the factory configuration settings All rime settings are reset.

You display these settings and other information with the commands that start with `show spanning-tree ....`

no spanning-tree (time settings)

Description

With this command in conjunction with the relevant parameter you reset the time settings of the spanning tree function to the default values.

If you call the command without parameters, you disable the spanning tree function. The configured time settings are retained.

If you call the `restart factory` command, the system restarts with the factory configuration settings All rime settings are reset.

The default values are as follows:

Parameter	Default value
`forward-time`	15 seconds
`hello-time`	2 seconds
`max-age`	20 seconds

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no spanning-tree{forward-time|hello-time|max-age}
```

The parameters have the following meaning:

Parameter	Description
`forward-time`	Time after which a port changes its spanning tree status from "Blocking" to "Forwarding"
`hello-time`	Time after which the bridge sends its configuration frames (BPDUs)
`max-age`	Time after which the information of the BPDUs becomes invalid

Result

The selected setting for the time is reset to the default value.

Further notes

You configure the time with the `spanning-tree` command (time settings).

You display these settings and other information with the commands that start with `show spanning-tree ....`

7.3.5 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.3.5.1 spanning-tree auto-edge

Description

With this command, you enable automatic discovery of a bridge connected to the interface.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

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

Result

The automatic discovery of a bridge on the interface is enabled.

Further notes

The automatic discovery of a bridge on the interface is disabled with the `no spanning-tree auto-edge` command.

7.3.5.2 no spanning-tree auto-edge

Description

With this command, you disable automatic discovery of a bridge connected to the interface.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no spanning-tree auto-edge
```

Result

The automatic discovery of a bridge on the interface is disabled.

Further notes

The automatic discovery of a bridge on the interface is enabled with the `spanning-tree auto-edge` command.

7.3.5.3 spanning-tree bpdu-receive

Description

With this command, you enable or disable the BPDU receive status at the port.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree bpdu-receive {enabled | disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`enabled`	BPDU packets are received at the port	Default: enabled
`disabled`	BPDU packets are ignored at the port	-

Result

The BPDU receive status is enabled or disabled.

Further notes

You can display the status of this function and other information with the `show spanning-tree interface` command with the `detail` option.

7.3.5.4 spanning-tree bpdu-transmit

Description

With this command, you enable or disable the BPDU transmit status at the port.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree bpdu-transmit {enabled | disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`enabled`	BPDU packets are transmitted at the port	Default: enabled
`disabled`	BPDU packets are not transmitted at the port	-

Result

The BPDU transmit status has switched over.

Further notes

You can display the status of this function and other information with the `show spanning-tree interface` command with the `detail` option.

7.3.5.5 spanning-tree bpdufilter

Description

With this command, you configure the BPDU transmit status for a port.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree bpdufilter {disable | enable}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`disable`	The transfer of BPDU packets is disabled for the port	Default: disabled
`enable`	The transfer of BPDU packets is enabled for the port	-

Result

The BPDU transmit status is configured.

7.3.5.6 spanning-tree bpdu-guard

Description

With this command, you enable BPDU protection on the selected port. If MSTP-BPDU packets are received at this port, the port is disabled.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

`spanning-tree bpdu-guard`

Result

BPDU protection is enabled on the interface.

Additional notes

You disable BPDU protection with the `no spanning-tree bpdu-guard` command.

You display the status of this function and other information with the `show spanning-tree interface` command with the `detail` option.

7.3.5.7 no spanning-tree bpdu-guard

Description

With this command, you disable BPDU protection on the selected port.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

`no spanning-tree bpdu-guard`

Result

BPDU protection is enabled on the interface.

Additional notes

You enable BPDU protection with the `spanning-tree bpdu-guard` command.

You display the status of this function and other information with the `show spanning-tree interface` command with the `detail` option.

7.3.5.8 spanning-tree layer2-gateway-port

Description

With this command, you configure a port as a layer 2 gateway port.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
spanning-tree layer2-gateway-port
```

Result

The port is configured as a layer 2 gateway port.

Further notes

You delete the configuration of a port as a layer 2 gateway port with the command`no spanning-tree layer2-gateway-port`.

You can display other information with the `show spanning-tree interface` command with the `detail` option.

7.3.5.9 no spanning-tree layer2-gateway-port

Description

With this command, you delete the configuration of the port as a layer 2 gateway port.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no spanning-tree layer2-gateway-port
```

Result

The configuration of the port as a layer 2 gateway port is deleted.

Further notes

You configure a port as a layer 2 gateway port with the command`spanning-tree layer2-gateway-port`.

You can display other information with the `show spanning-tree interface` command with the `detail` option.

7.3.5.10 spanning-tree limited-tcn

Description

With this command, you specify that the port accepts received and detected topology changes but does not forward them to other ports. This command only takes effect when the following requirements are met:

- RSTP+ must be enabled.
- The port cannot be blocked for Topology Change Notifications. You release a port blocked for TCN with the command `no spanning-tree restricted-tcn`.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
spanning-tree limited-tcn
```

Result

The port accepts topology changes but does not forward them to other ports.

Additional notes

You cancel the block with the `no spanning-tree limited-tcn` command.

You can display the status of this function and other information with the `show spanning-tree detail` command.

7.3.5.11 no spanning-tree limited-tcn

Description

With this command, you specify that the port accepts received and detected topology changes and forwards them to other ports.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no spanning-tree limited-tcn
```

Result

The port forwards TCN to other ports.

Additional notes

You block the forwarding of Topology Change Notifications with the command `spanning-tree limited-tcn`. However, the port accepts received and detected topology changes.

You can display the status of this function and other information with the `show spanning-tree detail` command.

7.3.5.12 spanning-tree loop-guard

Description

This function prevents alternative ports or root ports becoming designated ports if there is a disruption of a one-way link.

With this command, you enable the function.

Requirement

- Spanning tree is enabled.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameters:

```
spanning-tree loop-guard
```

Result

The "Spanning Tree Loop Guard" function is enabled.

Further notes

You disable the setting with the `no spanning-tree loop-guard` command.

You can display the status of this function and other information with the following commands:

- `show spanning-tree detail`
- `show spanning-tree active detail`
- `show spanning-tree interface`

7.3.5.13 no spanning-tree loop-guard

Description

This function prevents alternative ports or root ports becoming designated ports if there is a disruption of a one-way link.

With this command, you disable the function.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

```
no spanning-tree loop-guard
```

Result

The "Spanning Tree Loop Guard" function is disabled.

Further notes

You enable the setting with the `spanning-tree loop-guard` command.

You can display the status of this function and other information with the following commands:

- `show spanning-tree detail`
- `show spanning-tree active detail`
- `show spanning-tree interface`

7.3.5.14 spanning-tree mst

Description

With this command, you configure the various properties of the Multiple Spanning Tree function:

- With the `cost` option, you configure the port costs used to calculate the lowest-cost path.
- With the `port-priority` option, you configure the priority of the interface for negotiating a Multiple Spanning Tree configuration.
- With the `disable` option, you disable the interface for the Multiple Spanning Tree function.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree mst <instance-id(1-64)> { cost <(1-200000000)>|
port-priority <(0-240)> | disable }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`instance-id`	Number of the addressed instance	1 ... 64
`cost`	Costs of the port for calculating the lowest cost path.	1 ... 200000000 Default: • 200000 for physical interfaces • 199999 for port channels

Parameter	Description	Range of values / note
`port-priority`	Priority of the interface	0 ... 240 in steps of 16 Default: 128
`disable`	Disables the interface for multiple spanning tree	Default: MST is disabled, RST is enabled

Note

Configure multiple properties

With each call of the command, you can configure precisely one property.
If you want to configure several properties, call the command several times.

Result

The selected property is configured.

Further notes

You can reset the setting to the default with the `no spanning-tree mst` (properties) command.

You display these settings and other information with the commands that start with `show spanning tree ....`

7.3.5.15 no spanning-tree mst

Description

With this command, you reset the various properties of the Multiple Spanning Tree function to the default value.

The default values are as follows:

Parameter	Default value
`cost`	• 200000 for physical interfaces • 199999 for port channels
`port-priority`	128
`disable`	MST is disabled, RST is enabled

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

`no spanning-tree mst<instance-id(1-64)>{cost|port-priority|disable}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`instance-id`	Number of the addressed instance	1 ... 64
`cost`	Keyword for the costs of the port for calculating the lowest-cost path.	-
`port-priority`	Keyword for the priority of the interface	-
`disable`	Enables the interface for multiple spanning tree.	-

Note

Configure multiple properties

With each call of the command, you can configure precisely one property.
If you want to configure several properties, call the command several times.

Result

The selected setting is reset to the default value.

Additional notes

You configure the setting with the `spanning-tree mst` command (properties).

You display these settings and other information with the commands that start with `show spanning tree ....`

7.3.5.16 spanning-tree mst hello-time

Description

With this command, you configure the Hello time after which the bridge sends its configuration frames (BPDUs).

A change to this value applies to all MST instances active on this interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

```
spanning-tree mst hello-time<seconds(1-2)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`seconds`	Time after which the bridge sends its configuration frames (BPDUs)	1 ... 2 Default: 2

Result

The setting for the hello time is configured.

Further notes

You can reset the setting for the hello time to the default with the `no spanning-tree mst hello-time` command.

You display this setting and other information with the commands that start with `show spanning-tree ....`

7.3.5.17 no spanning-tree mst hello-time

Description

With this command, you reset the hello time after which the bridge sends its configuration BPDUs to the default value.

The default value is 2 seconds.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no spanning-tree mst hello-time
```

Result

The setting for the hello time is reset to the default value.

Further notes

You can configure the setting for the hello time with the `spanning-tree mst hello-time` command.

You display this setting and other information with the commands that start with `show spanning-tree ....`

7.3.5.18 spanning-tree mst PseudoRootId

Description

With this command, you configure a pseudoroot MAC address and the priority for a spanning tree configuration. The command is used in conjunction with the layer 2 gateway port.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
spanning-tree [mst <instance-id(1-64)>] pseudoRootId priority
<value(0-61440)>
    mac-address <ucast_mac>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mst`	Keyword for a spanning tree instance	-
`instance-id`	Number of the instance	1 ... 64
`priority`	Keyword for the priority	-
`value`	Value for the priority	0 ... 61440 Default: Priority of the device
`mac-address`	Keyword for the pseudoroot unicast MAC address	-
`ucast_mac`	MAC address of the interface	aa:aa:aa:aa:aa:aa Default: MAC address of the device

You can only change the value for the priority in the steps of 4096.

Result

The pseudoroot MAC address and the priority are configured.

Further notes

You can reset the settings to the default values with the `no spanning-tree mst pseudoRootId`command.

You display this setting and other information with the commands that start with `show spanning tree ....`

7.3.5.19 no spanning-tree mst PseudoRootId

Description

With this command, you reset a pseudoroot MAC address and the priority of the spanning tree configuration to the default values.

The default values are as follows:

- The priority is configured to the priority of the device.
- The MAC address is configured to the MAC address of the device.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no spanning-tree[mst<instance-id(1-64)>]pseudoRootId
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mst`	Keyword for a spanning tree instance	-
`instance-id`	Number of the instance	1 ... 64

Result

The pseudoroot MAC address and the priority are rest to the defaults.

Further notes

You configure the settings with the `spanning-tree mst pseudoRootId` command.

You display this setting and other information with the commands that start with `show spanning tree ....`

7.3.5.20 spanning-tree restricted-role

Description

With this command, you prevent the port adopting the role of root port.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

`spanning-tree restricted-role`

As default the function is "disabled".

Result

The port is prevented from adopting the role of root port.

Further notes

You cancel the lock with the `no spanning-tree restricted-role` command.

You can display the status of this function and other information with the `show spanning-tree detail`command.

7.3.5.21 no spanning-tree restricted-role

Description

With this command, you release the port for the role as root port.

Requirement

You are in the interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

```
no spanning-tree restricted-role
```

Result

The port is released for the role of root port.

Further notes

You prevent the port adopting the role of the root port with the `spanning-tree restricted-role` command.

7.3.5.22 spanning-tree restricted-tcn

Description

With this command, you restrict the port for the Topology Change Notification (TCN) function. The port cannot initiate any modifications to the network topology.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

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

Result

The port is prevented from using the TCN function.

Further notes

You cancel the lock with the `no spanning-tree restricted-tcn` command.

You can display the status of this function and other information with the `show spanning-tree detail`command.

7.3.5.23 no spanning-tree restricted-tcn

Description

With this command, you release the port for the TCN function.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

`no spanning-tree restricted-tcn`

Result

The port is released for the TCN function.

Further notes

You restrict the port for the TCN function with the `spanning-tree restricted-tcn` command.

7.3.5.24 spanning-tree

Description

With this command, you configure the various properties of the spanning tree function:

- With the `cost` option, you configure the port costs used to calculate the lowest-cost path.
- With the `disable` option, you disable the interface for the spanning tree function.
- With the `link-type` option, you configure the connection status of the following network segment. The following settings are possible:
  - `point-to-point` – the interface communicates with precisely one network component
  - `shared` - the interface is connected to more than one network component
- With the `portfast` option, you enable the PortFast function on the interface. The interface is connected to an end device and can therefore ignore the waiting time before changing to Forwarding mode.
- With the `port-priority` option, you configure the priority of the interface for negotiating a spanning tree configuration.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command with the following parameterization:

```
spanning-tree {cost <(0-200000000)>|disable|
link-type{point-to-point|shared}|portfast|
port-priority <(0-240)>}
```

The parameters have the following meaning:

Parameter	Description	Value range / note
`cost`	Keyword Describes the costs of the port for calculating the lowest cost path.	0 ... 200000000 Default: if dynamic calculation of the path costs is not enabled: • 200000 for physical interfaces • 199999 for port channels
`disable`	disables the interface for spanning tree	- Default: The spanning tree function is enabled on the interface
`link-type`	Connection status of the following network segment	• `point-to-point` • `shared` Default: • `point-to-point` The connection is configured as `full-duplex` • `shared` in all other cases
`portfast`	Enables the PortFast function	- Default: disabled
`port-priority`	Priority of the interface	0 ... 240 in increments of 16 Default: 128

Note

Configure multiple properties

With each call of the command, you can configure precisely one property.
If you want to configure several properties, call the command several times.

Result

The selected property is configured.

Further notes

You can reset the setting to the default with the `no spanning-tree` (properties) command.

You display these settings and other information with the commands that start with `show spanning-tree ....`

7.3.5.25 no spanning-tree

Description

With this command, you reset the various properties of the spanning tree function to the default value:

The default values are as follows:

Parameter	Default value
`cost`	if dynamic calculation of the path costs is not enabled: • 200000 for physical interfaces • 199999 for port channels
`disable`	The spanning tree function is enabled on the interface
`link-type`	• `point-to-point` The connection is configured as `full-duplex` • `shared` in all other cases
`portfast`	disabled
`port-priority`	128

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no spanning-tree {cost|disable|link-type|portfast|port-priority}
```

The parameters have the following meaning:

Parameter	Description
`cost`	Keyword for the costs of the port for calculating the lowest-cost path.
`disable`	Enables the interface for spanning tree.
`link-type`	Connection status of the following network segment
`portfast`	Disables the PortFast function.
`port-priority`	Keyword for the priority of the interface

Note

Configure multiple properties

With each call of the command, you can configure precisely one property.
If you want to configure several properties, call the command several times.

Result

The selected setting was reset to the default value.

Further notes

You configure the setting with the `spanning-tree` command (properties).

You display these settings and other information with the commands that start with `show spanning-tree ...`.

7.3.6 Commands in the MSTP configuration mode

This section describes commands that you can call up in the MSTP configuration mode.

In global configuration mode, enter the `spanning-tree mst configuration` command to change to this mode.

- If you exit the MSTP configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the MSTP configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in MSTP configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.3.6.1 instance

Description

With this command, you assign a range of VLANs to an MST instance.

Requirement

You are in the MSTP configuration mode.

The command prompt is as follows:

```
cli(config-mst)#
```

Syntax

Call up the command with the following parameters:

`instance <instance-id(1-64)> vlan <vlan-range>`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`instance-id`	Number of the instance	1 ... 64 You can define up to 16 MSTP instances. Default: The VLANs 1 ... 4094 are assigned to instance "0"
`vlan`	Keyword for a VLAN connection	-
`vlan-range`	Range of VLANs assigned to an instance	1 ... 4094 Enter the range limits with a hyphen without a space.

Result

The range of VLANs is assigned to the MST instance.

Further notes

You cancel the assignment of the VLAN to an MST instance with the `no instance` command.

You delete the MST instance with the `no instance` command.

You display this setting and other information with the `show spanning-tree mst configuration` command.

7.3.6.2 no instance

Description

With this command, you cancel the assignment of a VLAN to an MST instance or delete the MST instance.

Requirement

You are in the MSTP Configuration mode.

The command prompt is as follows:

`cli(config-mst)#`

Syntax

Call up the command with the following parameters:

```
no instance <instance-id (1-64)> [vlan <vlan-range>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`instance-id`	Number of the MST instance	1 ... 64
`vlan`	Keyword for a VLAN connection	-
`vlan-range`	Range of VLANs that will be deleted from the instance	1 ... 4094 Enter the range limits with a hyphen or a space.

If you specify a VLAN or a VLAN range, the assignment to an MST instance is canceled.

If you do not specify a VLAN, the MST instance is deleted.

Result

The assignment of a VLAN to an MST instance is canceled or the MST instance is deleted.

Further notes

You assign a VLAN to an MST instance with the `instance` command.

You display this setting and other information with the `show spanning-tree mst configuration` command.

7.3.6.3 name

Description

With this command, you configure a name for the MST region.

Requirement

You are in the MSTP Configuration mode.

The command prompt is as follows:

```
cli(config-mst)#
```

Syntax

Call up the command with the following parameters:

```
name <region-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`region-name`	Name of the MST region	Max. 32 characters

The default value of the name is the MAC address of the device.

Result

The name is configured.

Further notes

You delete the name of the MST region with the `no name` command.

You display this setting and other information with the `show spanning-tree mst configuration` command.

7.3.6.4 no name

Description

With this command, you reset the name for the MST region to the default value.

The default value is:

- The MAC address of the device is configured as name.

Requirement

You are in the MSTP Configuration mode.

The command prompt is as follows:

```
cli(config-mst)#
```

Syntax

Call the command without parameters:

```
no name
```

Result

The name is reset to the default value.

Further notes

You configure the name of the MST region with the `name` command.

You display this setting and other information with the `show spanning-tree mst configuration` command.

7.3.6.5 revision

Description

With this command, you assign a revision number to the MST region.

Requirement

You are in the MSTP Configuration mode.

The command prompt is as follows:

```
cli(config-mst)#
```

Syntax

Call up the command with the following parameters:

```
revision <revision-no(0-65535)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`revision-no`	Value of the revision number	0 ... 65535 Default: 0

Result

The MST region is assigned a revision number.

Further notes

You delete a revision number with the `no revision` command.

You display this setting and other information with the `show spanning-tree mst configuration` command.

7.3.6.6 no revision

Description

With this command, you reset the revision number of the MST region to the default value.

The default value is 0.

Requirement

You are in the MSTP Configuration mode.

The command prompt is as follows:

```
cli(config-mst)#
```

Syntax

Call the command without parameters:

```
no revision
```

Result

The revision number of the MST region is reset to the default value.

Further notes

You assign a revision number to the MST region with the `revision` command.

You display this setting and other information with the `show spanning-tree mst configuration` command.

7.4 Passive Listening

This section describes commands of the passive listening function.

If you enable passive listening, the IE switch forwards (R)STP configuration frames (BPDUs) transparently even when (R)STP is disabled for it. The IE switch also reacts to topology change frames. When the IE switch receives a TC frame, it deletes the MAC address table.

7.4.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.4.1.1 show passive-listening

Description

This command shows whether or not "passive listening" is enabled.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show passive-listening
```

Result

`disabled` is displayed if "passive listening" is disabled. If "passive listening" is enabled, `enabled` is displayed.

7.4.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

7.4.2.1 passive-listening bpdu-vlan-flood

Description

With this command you enable forwarding of BPDUs for specific VLANs; in other words, to all ports of the receiver VLAN of the BPDU.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
passive-listening bpdu-vlan-flood
```

As default the function is "enabled".

Result

BPDUs for specific VLANs.

Further notes

You disable this function with the `no passive-listening bpdu-vlan-flood` command.

You display the status of "passive listening" with the `show passive-listening` command.

7.4.2.2 no passive-listening bpdu-vlan-flood

Description

With this command you enable the flooding of BPDUs to all available ports of the device regardless of the configured VLANs.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no passive-listening bpdu-vlan-flood
```

Result

BPDUs are flooded to all available ports.

Further notes

You enable this function with the `passive-listening bpdu-vlan-flood` command.

You display the status of "passive listening" with the `show passive-listening` command.

7.4.2.3 passive-listening

Description

This command enables "passive listening".

Requirement

Note
No simultaneous operation with spanning tree
"Passive listening" can only be enabled when spanning tree is disabled.

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`passive-listening`

Result

The "passive listening" function is enabled.

Further notes

You disable "passive listening" with the `no passive-listening` command.

You display the status of "passive listening" with the `show passive-listening` command.

7.4.2.4 no passive-listening

Description

This command disables "passive listening".

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no passive-listening`

Result

The "passive listening" function is disabled.

Further notes

You enable "passive listening" with the `passive-listening` command.

You display the status of "passive listening" with the `show passive-listening` command.

Network protocols 8

This part contains the sections that describe the commands for working with the various network protocols.

8.1 IPv4 protocol

This section describes commands of the Internet Protocol (IP) version 4.

8.1.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.1.1.1 show dcp forwarding

Description

This command shows an overview of the DCP forwarding behavior on one or all interfaces.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show dcp forwarding [port <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`port`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The overview of the DCP forwarding behavior is displayed.

8.1.1.2 show dcp server

Description

This command shows whether or not the DCP function is enabled on the device.

If the DCP function is enabled, the read and write permissions are displayed.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show dcp server
```

Result

The overview of the status of the DCP function and access rights is displayed.

8.1.1.3 show dhcp snooping

Description

This command shows the configured setting for DHCP snooping at one or all interfaces.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show dhcp snooping [port <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
port	Keyword for a an interface description	-
interface-type	Type or speed of the interface	Enter a valid interface.
interface-id	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The overview of the DCP snooping configuration is displayed.

8.1.1.4 show ip gateway

Description

This command shows the default gateway configured for the device.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip gateway
```

Result

The default gateway is displayed.

8.1.1.5 show ip telnet

Description

This command shows the admin status and the port number of the Telnet server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip telnet
```

Result

The admin status and the port number of the Telnet server are displayed.

8.1.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.1.2.1 dcp server

Description

This command is used to configure the read and write permissions for the DCP server and enable it.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`dcp server {read-only | read-write | read-setup}`

The parameters have the following meaning:

Parameter	Description	Value range / note
`read-only`	Only reading is permitted on the DCP server	-
`read-write`	Reading and writing are permitted on the DPC server	-
`read-setup`	As long as the default password of the administrator is not changed, reading and writing on the DCP server is allowed. After changing the default password, only reading is allowed on the DCP server.	Default

Result

The read and write permissions for the DCP server are configured.

The DCP server is enabled.

Further notes

You disable the DCP server with the `no dcp server` command.

8.1.2.2 no dcp server

Description

With this command, you disable the DCP server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no dcp server`

Result

The DCP server is disabled.

Further notes

You enable and configure the DCP server with the `dcp server` command.

8.1.2.3 ip gateway

Description

With this command, you configure the default gateway.

Note

If you configure a static IP address for the default gateway, DHCP is automatically disabled for the TIA interface. This prevents the gateway address from being overwritten by DHCP. If necessary, you can enable DHCP again subsequently.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ip gateway <gateway>
```

The parameter has the following meaning:

Parameter	Description	Range of values
`gateway`	Specifies the IP address of the gateway	enter a valid IP address

Result

The entry is configured.

Additional notes

You delete the default gateway with the `no ip gateway` command.

You show the default gateway with the `show ip gateway` command.

8.1.2.4 no ip gateway

Description

With this command, you delete the default gateway.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`no ip gateway <gateway>`

The parameter has the following meaning:

Parameter	Description	Range of values
`gateway`	Specifies the IP address of the gateway.	Specify a valid IP address.

Result

The entry is deleted.

Further notes

You configure the default gateway with the `ip gateway` command.

You show the default gateway with the `show ip gateway` command.

8.1.2.5 ip echo-reply

Description

To check the availability of a network node, packets of the Internet Control Message Protocol (ICMP) can be sent to it. These packets of type 8 request the recipient to send a packet back to the sender (echo reply).

With this command you enable the network node to react to ping queries.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip echo-reply
```

Result

"ICMP echo reply messages" are enabled. The network node reacts to ping queries.

Further notes

You disable the setting with the `no ip echo-reply` command.

8.1.2.6 no ip echo-reply

Description

With this command you stop the network node reacting to ping queries.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip echo-reply
```

Result

"ICMP echo reply messages" are disabled. The network node does not react to ping queries.

Further notes

You change the setting with the `ip echo-reply` command.

8.1.2.7 ipv4 nexthop arp_keep_alive

Description

With this command, you enable the device to check all entries in the routing table to establish whether there is an entry for the specified gateway (Next Hop) in the ARP table. If there is no entry in the ARP table, the device sends an ARP query. With the optional parameter "interval", you specify the interval at which these cyclic checks take place.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ipv4 nexthop arp_keep_alive [interval <integer(30-86400)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`interval`	Interval in seconds at which the check is performed	30 ... 86400 Default: 30

Result

The check is performed at the specified interval.

Additional notes

You disable the check with the `no ipv4 nexthop arp_keep_alive` command.

8.1.2.8 no ipv4 nexthop arp_keep_alive

Description

With this command, you disable the check for entries for gateways (next hop) in the ARP table.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

`no ipv4 nexthop arp_keep_alive`

Result

The check is disabled.

Further notes

You enable the check with the `ipv4 nexthop arp_keep_alive` command.

8.1.2.9 telnet-server

Description

With this command, you enable the Telnet server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`telnet-server`

As default the function is "enabled".

Result

The Telnet server is enabled.

Further notes

You disable the Telnet server with the `no telnet-server` command.

8.1.2.10 no telnet-server

Description

With this command, you disable the Telnet server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no telnet-server`

Result

The Telnet server is disabled.

Further notes

You enable the Telnet server with the `telnet-server` command.

8.1.2.11 telnet-server port

Description

With this command you specify the port for Telnet access to the CLI.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`telnet-server port <port-number(1024-65535)>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`port-number`	Port number	1024 ... 65535 Default: 23 (standard port)

Note

Used ports

Some ports are permanently reserved. Make sure that the specified port is not already in use. You can find the ports used in the "List of available services".

Result

The port for Telnet access has been changed. Access the CLI with the changed port.

Further notes

You reset the port to the standard port with the `no telnet-server port` command.

8.1.2.12 no telnet-server port

Description

With this command, you reset the port to the standard port.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no telnet-server port
```

Result

The port is reset to the standard port 23.

Additional notes

You configure the port for Telnet access with the `telnet-server port.` command

8.1.3 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.1.3.1 dcp forwarding

Description

With this command, you configure the forwarding behavior of the interface for DCP frames.

Note

PROFINET configuration

Since DCP is a PROFINET protocol, the configuration created here is only effective with the VLAN associated with the TIA interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameterization:

```
dcp forwarding { block | forward }
```

The parameters have the following meaning:

Parameter	Description	Value range / note
`block`	DCP frames are discarded	-
`forward`	DCP frames are forwarded	Default: `forward`

Result

The forwarding behavior of the interface for DCP frames is configured.

8.1.3.2 dhcp snooping

Description

With this command, you specify the reaction of the Ethernet interface on receipt of packets from the DHCP server or DHCP client.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:

```
dhcp snooping { client | client-react | server | server-react }
```

The parameters have the following meaning:

Parameter	Description
client	Messages received from the DHCP server are logged.
client-react	Messages received from the DHCP server are logged and the port is turned off.
server	Messages received from the DHCP client are logged.
server-react	Messages received from the DHCP client are logged and the port is turned off.

Result

The behavior of the Ethernet interface for received packets from the DHCP server or client is configured.

8.1.3.3 no dhcp snooping

Description

With this command, you disable checking of packets from the DHCP server or DHCP client at an Ethernet interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameter assignment:

```
no dhcp snooping
```

Result

The DHCP snooping function is disabled.

8.1.3.4 ip address

Description

With this command, you assign an IP address.

Requirement

You are in the Interface Configuration mode of VLAN.

The command prompt is as follows:

```
cli(config-if-vlan-$$$)#
```

Syntax

Call up the command with the following parameters:

```
ip address <ip-address> {<subnet-mask>| / <prefix-length(1-32)>}
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
ip-address	IP address	Specify a valid IP address.
subnet-mask	Subnet mask	Enter a valid subnet mask.
prefix-length	Decimal representation of the mask as a number of "1" bits	1 ... 32

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The IP address is assigned.

Note

Effectiveness of the command

The command is effective immediately. If you configure the interface via which you access the device, the connection will be lost!

Further notes

You delete the setting with the `no ip address` command.

8.1.3.5 no ip address

Description

With this command, you delete the assignment of an IP address and disable DHCP.

Requirement

You are in the Interface Configuration mode of VLAN.

The command prompt is as follows:

```
cli(config-if-vlan-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no ip address [{ <ucast_addr> | dhcp }]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`ucast-addr`	Value for an IPv4 unicast address	Enter a valid IPv4 unicast address.
`dhcp`	Specify this parameter if you want to disable the DHCP function explicitly.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

If DHCP was enabled on this interface, DHCP is now disabled. Any existing dynamically learned IP address will be automatically converted to a static IP address.

If static IP addresses were configured and if no explicit IP address was transferred as a parameter, all static IP addresses will be deleted from this interface.

If a static IP address was specified explicitly, this address is deleted from this interface.

Note
Effectiveness of the command
The command is effective immediately.
If you configure the interface via which you access the device, you can lose the connection!

Further notes

You assign an IP address with the `ip address` or `ip address dhcp` command.

8.1.3.6 ip address dhcp

Description

With this command, the VLAN interface obtains the IPv4 address via DHCP.

Requirement

You are in the Interface Configuration mode of VLAN.
The command prompt is as follows:

```
cli(config-if-vlan-$$$)#
```

Syntax

Call the command without parameters:

```
ip address dhcp
```

Result

The DHCP assigns the IP address to the VLAN interface.

Further notes

You delete the settings with the `no ip address` command.
You display this setting and other information with the `show ip interface` command.

8.2 Domain Name System

This section describes commands of the Domain Name System (DNS).

8.2.1 The "show" commands

8.2.1.1 show ip dns

Description

This command shows information about the DNS client, for example the status of the DNS client and parameters for querying the DNS server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip dns
```

Result

Information on the DNS client is displayed.

8.2.1.2 show ip dns cache

Description

This command shows the content of the DNS cache. The DNS cache buffers replies of the DNS server for a brief time. This allows other queries for the same name to be replied to directly without sending another query to the DNS server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip dns cache
```

Result

The content of the DNS cache is displayed.

8.2.1.3 show ip dns domain name

Description

This command shows the list of configured domain names.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip dns domain name
```

Result

The list of domain names is displayed.

8.2.1.4 show ip dns name-server

Description

This command shows information about the DNS servers configured on the device. The table contains the index, the address type (e.g. IPv4) as well as the IP address and the origin.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip dns name-server
```

Result

The table with the information about the DNS servers is displayed.

8.2.1.5 show ip dns statistics

Description

This command shows DNS statistics. It provides information about the type and number of queries to the DNS server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip dns statistics
```

Result

Information about the communication with the DNS server is displayed.

8.2.2 Commands in global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.2.2.1 domain name

Description

With this command, you can store a domain name.

In total, 4 domain names can be stored on the device. In the order in which the domain names are created or learned, they are assigned an index from 2 to 4. Index 1 can only be manually configured with the `ip domain name` command.

With several domain names, the index specifies the order in which the domain names are used. The domain name with the lowest index is queried first.

If domain names are stored, with several IP address fields you have the option of entering the host name.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
domain name <domain-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`domain-name`	Domain name	Enter a domain name.

Result

The domain name is stored.

Additional notes

You delete a domain name with the `no domain name` command.

You define the first domain name with the `ip domain name` command.

You display the defined domain names with the `show ip dns domain name` command.

8.2.2.2 no domain name

Description

With this command, you delete a domain name.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command with the following parameters:

`no domain name <domain-name>`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`domain-name`	Domain name	Enter a domain name.

Result

The domain name is deleted.

Additional notes

You store a domain name with the `domain name` command.

You define the first domain name with the `ip domain name` command.

You display the defined domain names with the `show ip dns domain name` command.

8.2.2.3 ip domain name

Description

With this command, you store the primary domain name with the index 1. This domain name is used first to resolve a host name.

In total, 4 domain names can be stored on the device. Index 1 can only be configured manually. The index entries 2 to 4 can be learned or configured manually with the `domain name` command.

With several domain names, the index specifies the order in which the domain names are used. The domain name with the lowest index is queried first.

If domain names are stored, with several IP address fields you have the option of entering the host name.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip domain name <domain-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
domain-name	Domain name	Enter a domain name.

Result

The domain name with the index 1 is stored. If a host name is entered in an IP address field, first an attempt is made to resolve the address with this domain name.

Additional notes

You delete the first domain name with the `no ip domain name` command.

You define further domain names with the `domain name` command.

You display the defined domain names with the `show ip dns domain name` command.

8.2.2.4 no ip domain name

Description

With this command you delete the domain name with the index 1.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no ip domain name
```

Result

The domain name with the index 1 is deleted.

Additional notes

You store the first domain name with the `ip domain name` command.

You define further domain names with the `domain name` command.

You display the defined domain names with the `show ip dns domain name` command.

8.2.2.5 ip domain used server

Description

This command specifies which DNS server the device uses.

Note

Only resource records of type A (IPv4 address of a host) are supported.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ip domain used server {learned-only | manually-only | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`learned-only`	The device uses only the DNS servers assigned by DHCP.	-
`manually-only`	The device uses only the manually configured DNS servers. A maximum of three DNS servers can be configured.	-
`all`	The device uses all available DNS servers.	-

Result

The device uses the DNS servers specified in the configuration.

8.2.2.6 ip domain lookup

Description

This command enables the DNS client of the device. To be able to use the function, a DNS server must be reachable.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip domain lookup
```

Result

The DNS client of the device is enabled and when necessary sends queries to the DNS server.

8.2.2.7 no ip domain lookup

Description

This command disables the DNS client of the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip domain lookup
```

Result

The DNS client of the device is disabled.

8.2.2.8 ip name-server

Description

With this command, you can manually configure up to 3 DNS servers with IPv4 addresses. You can assign manually configured DNS servers the optional parameter `index` with the range of values 1 to 3. If you configure a DNS server without specifying an index, the server that currently has index 1 will be overwritten.

Using DHCP, the device can learn two DNS servers with IPv4 addresses. Learned DNS servers are automatically assigned an index from 4 to 5.

If there is more than one DNS server, the index specifies the order in which the servers are queried. The server with the lowest index is queried first. A total of five DNS servers can be configured on the device. Manually configured DNS servers are given preference.

The DNS server (Domain Name System) assigns a domain name to an IP address so that a device can be uniquely identified.

If this function is enabled, the device can communicate with a DNS server as a DNS client. You have the option of entering names in IP address fields.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip name-server ipv4 <ucast_addr> [index <id(1-3)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	IPv4 address of the DNS server	Enter a valid IPv4 address.
`index`	Keyword for the index	-
`id`	Index of the DNS server	1 ... 3

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The IP address and, if specified, the index for a DNS server have been set.

8.2.2.9 no ip name server

Description

This command deletes the entry with the specified index for a DNS server. If you do not specify an index, all entries are deleted.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no ip name-server ipv4 <ucast_addr> [index <id(1-3)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ipv4`	Keyword for IPv4	-
`ucast_addr`	IP address of the DNS server	enter a valid IPv4 address
`index`	Keyword for the index	-
`id`	Index of the DNS server	1 ... 3

Result

The specified entries for the DNS servers were deleted.

8.3 DHCP client

This section describes commands of the Dynamic Host Configuration Protocol (DHCP).

8.3.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.3.1.1 show ip dhcp client stats

Description

With this command, you display the statistical counters of the DHCP client.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip dhcp client stats
```

Result

The counters are displayed.

8.3.1.2 show ip dhcp client

Description

With this command, you display the configuration settings of the DHCP client.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip dhcp client
```

Result

The configuration settings of the DHCP client are displayed.

8.3.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.3.2.1 ip dhcp client mode

Description

With this command, you configure the type of identifier with which the DHCP client logs on with its DHCP server.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip dhcp client mode {mac | client-id <client-id> | sysname | pnio-
name-of-station}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`mac`	Keyword for logon with the MAC address.	-
`client-id`	Keyword for logon with the Client ID.	-
`client-id`	The ID of the DHCP client.	Max. 254 characters
`sysname`	Keyword for logon with the system name.	-
`pnio-name-of-station`	Keyword for logon with the PROFINET name. The device name is assigned via SINEC PNI, for example.	-

Result

The registration mode of the DHCP client is configured.

8.3.2.2 ip dhcp client keepalive

Description

Use this command to enable the Keep Alive function, to retain the IP address in the event of a connection failure.

If enabled, the IP address is kept alive when the connection to the DHCP server is lost and is not reset to 0.0.0.0.

Keep Alive is enabled by default.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip dhcp client keepalive
```

Result

The function is enabled.

Further notes

You disable the option with the `no ip dhcp client keepalive` command.

8.3.2.3 no ip dhcp client keepalive

Description

With this command, you disable the Keep Alive function. The IP address is then reset to 0.0.0.0 when the connection to the DHCP server is lost.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip dhcp client keepalive
```

Result

The function is disabled.

Further notes

You enable the option with the `ip dhcp client keepalive` command.

8.3.2.4 ip dhcp config-file-request

Description

If the DHCP config file request option is set, the device requests the TFTP address and the name of a configuration file from the DHCP server. If the device is restarted following the completed download, the configuration settings are read from this file.

With this command, you enable the DHCP config file request option.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip dhcp config-file-request
```

Result

The DHCP config file request option is enabled.

Further notes

You disable the DHCP config file request option with the `no ip dhcp config-file-request` command.

8.3.2.5 no ip dhcp config-file-request

Description

With this command, you disable the DHCP config file request option.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip dhcp config-file-request
```

Result

The DHCP config file request option is disabled.

Further notes

You enable the DHCP config file request option with the `ip dhcp config-file-request` command.

8.3.2.6 ip dhcp config-file-request setup

Description

The function depends on the status of the device.

- In the delivery state and after resetting to default settings, the DHCP client requests a configuration file with the next DHCP request.
- The following events trigger a status change of the device: The first login with the default user profile admin and the associated assignment of a new password as well as the loading of a configuration file. After that, the device is in safe operating state and the function is disabled for all DHCP client interfaces.

With this command, you disable the default setting.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip dhcp config-file-request setup
```

Result

The "`ip dhcp config-file-request setup`" option is enabled.

Further notes

You disable the option with the `no ip dhcp config-file-request setup` command.

8.3.3 Commands in the Interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.3.3.1 ip address dhcp

Description

With this command, you assign an IP address using DHCP.

Requirement

You are in the VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call the command without parameter assignment:

```
ip address dhcp
```

Result

The IP address is assigned using DHCP.

Further notes

You delete the setting with the `no ip address` command.

8.3.3.2 no ip address

Description

With this command, you delete the assignment of an IP address and disable DHCP.

Requirement

You are in the Interface Configuration mode of VLAN.

The command prompt is as follows:

```
cli(config-if-vlan-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no ip address [{ <ucast_addr> | dhcp }]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`ucast-addr`	Value for an IPv4 unicast address	Enter a valid IPv4 unicast address.
`dhcp`	Specify this parameter if you want to disable the DHCP function explicitly.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

If DHCP was enabled on this interface, DHCP is now disabled. Any existing dynamically learned IP address will be automatically converted to a static IP address.

If static IP addresses were configured and if no explicit IP address was transferred as a parameter, all static IP addresses will be deleted from this interface.

If a static IP address was specified explicitly, this address is deleted from this interface.

Note

Effectiveness of the command

The command is effective immediately.

If you configure the interface via which you access the device, you can lose the connection!

Further notes

You assign an IP address with the `ip address` or `ip address dhcp` command.

8.4 DHCP server

You can operate the device as a DHCP server. This allows IP addresses to be assigned automatically to the connected devices. The IP addresses are either distributed dynamically from an address band (pool) you have specified or a specific IP address is assigned to a particular device.

Both with the dynamic and static assignment a pool is selected based on the following criteria:

1. With the DHCP query option 82 is enabled.
   The DHCP server checks whether there is a pool with option 82. You configure this criterion with the `relay-information` command.
2. The DHCP query was received via a relay agent.
   The DHCP server checks whether the relay agent is located in the subnet of a pool.
3. The port via which the DHCP query was received is enabled in the Port Range.
   The DHCP server checks whether the IP interface of the port is located in the subnet of a pool. You configure this criterion with the `ip address` command.

This section describes commands relevant for configuring the DHCP server.

Requirement

The connected devices are configured so that they obtain the IPv4 address from a DHCP server.

8.4.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.4.1.1 show ip dhcp-server bindings

Description

This command shows the current assignments of IPv4 addresses of the DHCP server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameterization:

```
show ip dhcp-server bindings [detail]
```

The parameter has the following meaning:

Parameter	Description	Value range / note
`detail`	The information is displayed in list form.	-

Result

The information is displayed.

8.4.1.2 show ip dhcp-server pools

Description

The command shows the DHCP server configuration of a specific IPv4 address band or all IPv4 address bands.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show ip dhcp-server pools [pool-id (1-24)]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`pool-id`	ID of the addressed IPv4 address band	1 ... 24

If no parameters are specified, the settings for all address bands are displayed.

Result

The configuration of the DHCP server is displayed.

8.4.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.4.2.1 ip dhcp-server

Description

With this command, you enable the DHCP server on the device.

Note

To avoid conflicts with IPv4 addresses, only one device may be configured as a DHCP server in the network.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

`ip dhcp-server`

Result

The DHCP server is enabled.

Further notes

You disable the DHCP server with the `no ip dhcp-server` command.

8.4.2.2 no ip dhcp-server

Description

With this command, you disable the DHCP server on the device.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`no ip dhcp-server`

Result

The DHCP server is disabled.

Further notes

You enable the DHCP server with the `ip dhcp-server` command.

8.4.2.3 ip dhcp-server icmp-probe

Description

With this command you enable the function "Probe address with ICMP echo before offer". The DHCP server checks whether or not the IPv4 address has already been assigned. If no reply is received, the DHCP server can assign the IPv4 address.

Note

With static assignments, this check is not made.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`ip dhcp-server icmp-probe`

Result

The function is enabled.

Further notes

You disable the function with the `no ip dhcp-server icmp-probe` command.

8.4.2.4 no ip dhcp-server icmp-probe

Description

With this command you disable the function "Probe address with ICMP echo before offer".

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

```
no ip dhcp-server icmp-probe
```

Result

The function is disabled.

Further notes

You enable the function with the `ip dhcp-server icmp-probe` command.

8.4.2.5 ip dhcp-server pool

Description

With this command, you have three options of changing to the DHCPPOOL configuration mode and to assign an interface to the IPv4 address band.

1. If you call the command `ip dhcp-server pool` with the parameter `pool-id (1-24)`, you change to the corresponding DHCPPOOL configuration mode. The corresponding pool ID must have already been created.
2. If you call the `ip dhcp-server pool` command with the parameter `vlan` or `interface-type/interface-id`, an IPv4 address band with the next free pool ID is created and the specified interface assigned directly to it. This is followed by a change to the DHCPPOOL configuration mode. You then configure the other settings in the DHCPPOOL configuration mode.
3. If you call the `ip dhcp-server pool` command without parameters, and IPv4 address band with the next free pool ID is created and you change directly to the corresponding DHCPPOOL configuration mode.
   You then configure the interface and the other settings in the DHCPPOOL configuration mode.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip dhcp-server pool [{ <pool-id (1-24)> | [{ vlan <vlan-id
(1-4094)> | <interface-type> <interface-id> }]}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`pool-id`	ID of the addressed IPv4 address band	1 ... 24
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface-type`	Type of interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The ID of the addressed IPv4 address band is configured.

You are now in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Additional notes

You exit the DHCPPOOL configuration mode with the `exit` command.

You delete the entry with the `no ip dhcp-server pool` command.

8.4.2.6 no ip dhcp-server pool

Description

With this command, you delete the required IPv4 address band.

Requirement

- The IPv4 address band is not enabled.
- You are in the Global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call up the command with the following parameters:

```
no ip dhcp-server pool <pool-id (1-24)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`pool-id`	ID of the addressed IPv4 address band	1 ... 24

Result

The required IPv4 address band is deleted.

Further notes

You create an IPv4 address band with the `ip dhcp-server pool`command.

8.4.3 Commands in the DHCPPOOL configuration mode

This section describes commands that you can call up in the DHCPPOOL Configuration mode.

In global configuration mode, enter the `ip dhcp-server pool` command to change to this mode.

- If you exit the DHCPPOOL Configuration mode with the `exit` command, you return to the Global Configuration mode.
- If you exit the DHCPPOOL Configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in DHCPPOOL configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.4.3.1 host

Description

With this command, you configure a DHCP option for a statically assigned IP address.

Note

This command is not available with the following devices:

- SCALANCE XB-200
- SCALANCE XR-300WG

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
 host { mac <mac-address> | client-id <string> } option <code
(1-2147483647)>
{ value-string <dhcp-param> | ip <address> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
mac	Keyword for the MAC address.	-
mac-address	The MAC address of the device for which a DHCP option is to be set.	Specify a valid MAC address.
client-id	Keyword for the client ID	-
string	The DHCP client ID	String, maximum of 254 characters
option	Keyword for the DHCP option	-
code	The number of the DHCP option	1 ... 2147483647
value-string	Keyword for a parameter in string format	-
dhcp-param	Value of the parameter	String
ip	Keyword for an IP address	-
address	The IP address that is used for the DHCP option.	Specify a valid IP address.

Result

The DHCP option is configured.

Additional notes

You display the setting with the `show ip dhcp-server pools` command.

You disable a DHCP option for a static IP address with the `no host` command.

8.4.3.2 no host

Description

With this command, you disable a DHCP option for a statically assigned IP address.

Note

This command is not available with the following devices:

- SCALANCE XB-200
- SCALANCE XR-300WG

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
no host { mac <mac-address> | client-id <string> } option <code
(1-2147483647)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
mac	Keyword for the MAC address	-
mac-address	The MAC address of the device for which a DHCP option is to be specified.	Specify a valid MAC address.
client-id	Keyword for the client ID	-
string	The DHCP client ID	String, maximum of 254 characters
option	Keyword for the DHCP option	-
code	The number of the DHCP option	1 ... 2147483647

Result

The specified DHCP option is disabled.

Additional notes

You display the setting with the `show ip dhcp-server pools` command.

You configure a DHCP option for a static IP address with the `host` command.

8.4.3.3 lease-time

Description

With this command, you specify how long the assigned IPv4 address remains valid. When half the period of validity has elapsed. the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
lease-time <seconds (60-31536000)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`seconds`	Time until renewal of the assigned IPv4 address in seconds	60 ... 31536000

Result

The time is configured.

Further notes

You display the setting with the `show ip dhcp-server pools` command.

8.4.3.4 network

Description

With this command you configure the IPv4 address band from which the DHCP client receives any IPv4 address.

Note

Assignment of IP addresses

When assigning IP addresses from a local address band, the IPv4 address of the interface must be located within the IPv4 address band. If this is not the case, the interface does not assign any IPv4 addresses.

The IP address does not need to be within the IPv4 address band if relay agent information is configured for the address band.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
network <lower-IP> <upper-IP> { <subnet-mask> | / <prefix-length
(1-32)> }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`lower-IP`	Start of the IPv4 address band	Enter a valid IPv4 address.
`upper-IP`	End of the IPv4 address band	Enter a valid IPv4 address.
`subnet-mask`	Subnet mask of the corresponding subnet	Enter a valid subnet mask.
`prefix-length`	Decimal representation of the mask as a number of "1" bits	1 ... 32

Result

The IPv4 address band is configured. The DHCP options 1, 3, 6, 66 and 67 are created automatically. With the exception of option 1, the options can be deleted.

Further notes

You display the setting with the `show ip dhcp-server pools` command.

You assign an IP address to an interface with the `set interface` command.

You configure the DHCP option 67 with the `option value-string` command.

You configure the DHCP options 3, 6 and 66 with the `option` command.

You delete the DHCP option with the `no option` command.

8.4.3.5 option value-string

Description

With this command, you configure DHCP options 12, 15 and 67 that contain a string as DHCP parameter. The DHCP options 66 and 67 are created automatically when the IPv4 address band is created.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call the command with the following parameters:

```
option <option-code> value-string <dhcp-param>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`option-code`	Code of the DHCP option	• 12 (host name) • 15 (domain name) • 67 (bootfile name)
`dhcp-param`	Parameter value of the DHCP option	Enter the parameter value in String format.

Result

The DHCP option is configured.

Additional notes

You display the setting with the `show ip dhcp-server pools` command.

You delete the DHCP option with the `no option` command.

You configure the DHCP options 3 and 6 with the `option` (IP address) command.

You disable the IPv4 address band with the `no pool-enable` command.

8.4.3.6 Option (IP address)

Description

With this command you configure the DHCP options 3 and 6 that contain an IPv4 address as DHCP parameter. The DHCP options 3 and 6 are created automatically when the IPv4 address band is created.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call the command with the following parameters:

```
option <option-code> { <ip-address-list> | int-ip }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`option-code`	Code of the DHCP option	• 3 - Default gateway • 6 - DNS server • 66 - TFTP server
`ip-adress-list`	IPv4 address or IPv4 address list	• DHCP option 3 (default gateway): Enter the DHCP parameter as an IPv4 address, e.g. 192.168.100.2. • DHCP option 6 (name server): Enter the DHCP parameter as an IPv4 address, e.g. 192.168.100.2. You can specify up to three IPv4 addresses separated by commas. • DHCP option 66 (TFTP server) Enter the DHCP parameter as an IPv4 address, e.g. 192.168.100.2.
`int-ip`	Uses IPv4 address of the interface that is assigned to the IPv4 address band.	Only with DHCP option 3

Result

The DHCP option is created.

Additional notes

You display the setting with the `show ip dhcp-server pools` command.

You disable the IPv4 address band with the `no pool-enable` command.

You delete the DHCP option with the `no option` command.

You configure the DHCP options 12, 66 and 67 with the `option value-string` command.

You configure the interface with the `set interface` command.

8.4.3.7 no option

Description

With this command, you delete the DHCP option with the specified number.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call the command with the following parameters:

```
no option <option-code>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`option-code`	Code of the DHCP option	Enter a valid DHCP option code.

Result

The specified DHCP option is deleted.

Additional notes

You configure the DHCP options 3, 6 and 66 with the `option` command.

You configure the DHCP options 12, 15, 43, and 67 with the `option value-string` command.

8.4.3.8 pool-enable

Description

With this command you specify that this IPv4 address band will be used.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

`cli(config-dhcp-pool-<ID>)#`

Syntax

Call the command without parameter assignment:

`pool-enable`

Result

The setting is enabled.

Note

If the IPv4 address band is enabled, the following parameters can no longer be edited:

- DHCP options (`option` ...)
- Port Range (`ports`)
- Relay Agent Information (`relay-information`)
- Static Leases (`static-lease`)

Further notes

You display the setting with the `show ip dhcp-server pools` command.

You disable the setting with the `no pool-enable` command.

8.4.3.9 no pool-enable

Description

With this command you specify that this IPv4 address band will not be used.

Note

Deleting DHCP server bindings

If you disable or delete an IPv4 address band or you switch the DHCP server off and on again, the DHCP server bindings are deleted. You display the DHCP server bindings with the `show ip dhcp-server bindings` command.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call the command without parameter assignment:

```
no pool-enable
```

Result

The setting is disabled.

Further notes

You display the setting with the `show ip dhcp-server pools` command.

You enable the setting with the `pool-enable` command.

8.4.3.10 ports

Description

With this command you enable the ports via which the IPv4 addresses of an address band in the local subnet are assigned.

After you have created an IPv4 address band, all ports are selected that are currently located in the corresponding VLAN. If you add ports to the VLAN later, these ports are not automatically enabled.

With address assignments via a relay agent, you cannot restrict the ports.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
ports [<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-
b, 0/c, ...>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Enter a valid interface
`0/a-b,0/c,...`	Port no. of the interface	

For information on identifiers of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The selected ports will be enabled. Before the IPv4 address band can be used, it still needs to be activated.

Further notes

You disable the ports with the `no ports` command.

You display the setting with the `show ip dhcp-server pools` command.

You enable the IPv4 address band with the `pool-enable` command.

8.4.3.11 no ports

Description

With this command you disable the ports via which the IPv4 addresses of an address band in the local subnet are assigned.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call the command with the following parameters:

```
no ports [<interface-type> <0/a-b, 0/c, ...>] [<interface-type>
<0/a-b, 0/c, ...>] [all]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Enter a valid interface
`0/a-b,0/c,...`	Port no. of the interface	
`all`	All ports will be disabled.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The selected ports will be disabled.

Additional notes

You enable the ports with the `ports` command.

You display the setting with the `show ip dhcp-server pools` command.

You enable the IPv4 address band with the `pool-enable` command.

8.4.3.12 relay-information

Description

With this command you define that devices with a certain remote ID and circuit ID are assigned the IPv4 addresses from a specific address band.

If you create such an entry for an address band, address pool only reacts to DHCP queries via a DHCP relay agent (option 82). You can create further address bands for the same IP interfaces so that the pools react to different requests.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
relay-information <remote-id> <circuit-id>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`remote-id`	Remote ID of the device	Enter the remote ID of the device.
`circuit-id`	Circuit ID of the device.	Enter the circuit ID of the device.

Result

Devices with a certain remote ID and circuit ID are assigned the IPv4 addresses from a specific address band. Before the IPv4 address band can be used, it still needs to be activated.

Further notes

You cancel the assignment with the `no relay-information` command.

You display the setting with the `show ip dhcp relay information` command.

You enable the IPv4 address band with the `pool-enable` command.

8.4.3.13 no relay-information

Description

With this command you cancel the assignment of devices with a certain remote ID and circuit ID to IPv4 addresses from a specific address band.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
no relay-information <remote-id> <circuit-id>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`remote-id`	Remote ID of the device	Enter the remote ID of the device.
`circuit-id`	Circuit ID of the device.	Enter the circuit ID of the device.

Result

The assignment is canceled.

Further notes

With the `relay-information` command, you assign devices with a certain remote ID and circuit IPv4 addresses from a specific address band.

You display the setting with the `show ip dhcp relay information` command.

You enable the IPv4 address band with the `pool-enable` command.

8.4.3.14 set-interface

Description

With this command, you specify the interface via which the IPv4 addresses are dynamically assigned.

Note

Assignment of IP addresses

When assigning IP addresses from a local address band, the IPv4 address of the interface must be located within the IPv4 address band. If this is not the case, the interface does not assign any IPv4 addresses.

The IP address does not need to be within the IPv4 address band if relay agent information is configured for the address band.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call the command with the following parameters:

```
set-interface {vlan <vlan-id (1-4094)> | <interface-type>
<interface-id> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The interface is assigned. Before the IPv4 address band can be used, it still needs to be activated.

Additional notes

You display the setting with the `show ip dhcp-server pools` command.

You enable the IPv4 address band with the `pool-enable` command.

8.4.3.15 static-lease

Description

With this command you specify that devices with a certain MAC address or client ID are assigned to the preset IPv4 address.

Requirement

- The assignment has not yet been created.
- You are in the DHCPPOOL configuration mode.
  The command prompt is as follows:
  `cli(config-dhcp-pool-<ID>)#`

Syntax

Call up the command with the following parameters:

```
static-lease {mac <mac-address> | client-id <string>} <ip-address>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mac`	Keyword for a MAC address	-
`mac-address`	Unicast MAC address	Specify the MAC address. aa:bb:cc:dd:ee:ff
`client-id`	Keyword for a DHCP client ID	-
`string`	Freely definable DHCP client ID	Enter the required designation. Maximum of 254 characters
`ip-address`	Unicast IPv4 address	Enter a valid IPv4 address. The IPv4 address must match the subnet of the IPv4 address band.

Result

The assignment is specified.

Further notes

You display the setting with the `show ip dhcp dhcp-server bindings` command.

You disable the IPv4 address band with the `no pool-enable` command.

You delete the assignment with the `no static-lease` command.

8.4.3.16 no static-lease

Description

With this command, you delete the assignment of an IPv4 address to a MAC address.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
no static-lease { mac <mac-address> | client-id <string> }
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`mac`	Keyword for a MAC address	-
`mac-address`	Unicast MAC address	Specify the MAC address. aa:bb:cc:dd:ee:ff
`client-id`	Keyword for a DHCP client ID	-
`string`	Freely definable DHCP client ID	Enter the required designation.

Result

The assignment is deleted.

Further notes

You configure the assignment with the `static-lease` command.

8.5 DHCP Relay

This section describes commands for the DHCP Relay Agent.

8.5.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.5.1.1 show dhcp server

Description

With this command, you display the IP addresses of the DHCP servers to which the device forwards the frames.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode or in the Global Configuration mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show dhcp server
```

Result

The IP addresses of the DHCP servers are displayed.

Further notes

With the "`ip dhcp server`" command, you specify the IP addresses.

8.5.1.2 show ip dhcp relay information

Description

This command displays the DHCP relay agent settings for all or for a selected VLAN.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode or in the Global configuration mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show ip dhcp relay information [vlan <vlan-id>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The configuration settings are displayed.

8.5.2 Commands in the Global Configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.5.2.1 ip dhcp server

Description

With this command, you specify the IP addresses of the DHCP servers to which the DHCP relay agent forwards the frames. You can specify up to four IP addresses for the DHCP relay agent.

Requirement

- You are in global configuration mode.
  The command prompt is:
  `cli(config)#`

Syntax

Call up the command with the following parameters:

```
ip dhcp server <ip address>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`ip address`	IPv4 address of the DHCP server	Enter a valid IP address

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The IP address is specified.

Additional notes

You remove the IP address with the `no ip dhcp server` command.

You enable the DHCP Relay Agent with the `service dhcp-relay` command.

You display the IP addresses with the `show dhcp server` command.

You display the settings with the `show ip dhcp relay information` command.

8.5.2.2 no ip dhcp server

Description

With this command, you delete the IP address of the DHCP server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no ip dhcp server <ip address>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`ip address`	IP address of the DHCP server	Enter the IP address to be deleted.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The IP address is removed.

Further notes

You enable the DHCP Relay Agent with the `service dhcp-relay` command.

You create the IP address with the `ip dhcp server` command.

You display the IP addresses with the `show dhcp server` command.

8.5.2.3 ip dhcp relay circuit-id option

Description

The Circuit ID is a sub option of the "DHCP Relay Information" option. The Circuit ID contains information about the origin of the DHCP packet.

With this command, you specify the information contained in the Circuit ID.

The Circuit ID is encoded in the DHCP packet if the "DHCP relay information" option is enabled.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

`ip dhcp relay circuit-id option [router-index] [vlanid] [recv-port]`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`router-index`	The router index is added to the Circuit ID.	Default setting
`vlanid`	The VLAN ID is added to the Circuit ID.	-
`recv-prot`	The Circuit ID is added to the receiving port.	-

Result

The content of the Circuit ID is specified.

Additional notes

You enable the DHCP Relay Information option with the `ip dhcp relay information option` command.

You display the information with the `show ip dhcp relay information` command.

8.5.2.4 ip dhcp relay common-agent-address

Description

With this command, you enable the use of a common agent address. When the function is enabled, in the DHCP request the relay agent replaces the address of the receiving port with the address of the interface that you define with the `ip dhcp relay common-agent-address-interface` command or the default value.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`ip dhcp relay common-agent-address`

Result

The relay agent uses a common agent address in DHCP requests.

Further notes

You disable the use of a common agent address with the `no ip dhcp relay common-agent-address` command.

You define a common agent address with the `ip dhcp relay common-agent-address-interface` command.

You reset the common agent address to the default value with the `no ip dhcp relay common-agent-address-interface` command.

8.5.2.5 no ip dhcp relay common-agent-address

Description

With this command, you disable the use of a common agent address. When the function is disabled, the relay uses the address of the receiving port in DHCP requests.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no ip dhcp relay common-agent-address
```

Result

The relay agent uses the address of the receiving port in DHCP requests.

Further notes

You enable the use of a common agent address with the `ip dhcp relay common-agent-address` command.

You define a common agent address with the `ip dhcp relay common-agent-address-interface` command.

You reset the common agent address to the default value with the `no ip dhcp relay common-agent-address-interface` command.

8.5.2.6 ip dhcp relay common-agent-address-interface

Description

With this command you define the interface whose IP address the relay agent uses as the source address (giaddr) in DHCP requests.

Requirement

You are in the Global configuration mode.
The command prompt is:
`cli(config)#`

Syntax

Call up the command with the following parameters:

```
ip dhcp relay common-agent-address-interface { vlan <vlan-id
(1-4094)> | <interface-type> <interface-id> }
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094 Default: vlan1
`interface-type`	Type or speed of the interface	Enter a valid interface name.
`interface-id`	Slot no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The IP address of the interface is used as a common agent address.

Further notes

You reset the common agent address to the default value with the `no ip dhcp relay common-agent-address-interface` command.

You enable the use of a common agent address with the `ip dhcp relay common-agent-address` command.

You disable the use of a common agent address with the `no ip dhcp relay common-agent-address` command.

8.5.2.7 no ip dhcp relay common-agent-address-interface

Description

With this command you reset the common agent address to the default value.

Requirement

You are in the Global configuration mode.
The command prompt is:
`cli(config)#`

Syntax

Call the command without parameter assignment:

```
no ip dhcp relay common-agent-address-interface
```

Result

The default value for the common agent address is used.

Further notes

You define a common agent address with the `ip dhcp relay common-agent-address-interface` command.

You enable the use of a common agent address with the `ip dhcp relay common-agent-address` command.

You disable the use of a common agent address with the `no ip dhcp relay common-agent-address` command.

8.5.2.8 ip dhcp relay information option

Description

With this command, you enable the DHCP option 82. If the option is enabled, prior to forwarding to the DHCP server, information about the origin of the DHCP query is encoded in the packet. If the DHCP server sends a response, the information is removed again before forwarding to the DHCP client.

This information is only encoded in the data packet if the DHCP relay agent is enabled.

Requirement

You are in the Global configuration mode or in the Interface configuration mode of VLAN.

The command prompt is as follows:

`cli(config)#` or `cli(config-if-$$)#`

Syntax

Call the command without parameter assignment:

```
ip dhcp relay information option
```

Result

The option is enabled.

Further notes

You disable the option with the `no ip dhcp relay information option` command.

You enable the DHCP Relay Agent with the `service dhcp-relay` command.

You configure the content of the information with the `ip dhcp relay circuit-id option` command.

You can display the status of this option and other information with the `show ip dhcp relay information` command.

8.5.2.9 no ip dhcp relay information option

Description

With this command, you disable the DHCP option 82.

Requirement

You are in the Global configuration mode or in the Interface configuration mode of VLAN.

The command prompt is as follows:

`cli(config)#` or `cli(config-if-$$)#`

Syntax

Call the command without parameter assignment:

```
no ip dhcp relay information option
```

Result

The option is disabled.

Further notes

You enable the option with the `ip dhcp relay information option` command.

You can display the status of this option and other information with the `show ip dhcp relay information` command.

8.5.2.10 service dhcp-relay

Description

With this command, you enable the DHCP relay agent on the device. The DHCP relay agent forwards DHCP queries to DHCP servers located in a different subnet.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
service dhcp-relay
```

Result

The DHCP Relay Agent is activated.

Further notes

You disable the DHCP Relay Agent with the `no service dhcp-relay` command.

You create the IP addresses of the DHCP server with the `ip dhcp server` command.

You can display the status of this function and other information with the `show ip dhcp relay information`command.

8.5.2.11 no service dhcp-relay

Description

This command disables the DHCP relay agent.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

`no service dhcp-relay`

Result

The DHCP Relay Agent is disabled.

Further notes

You enable the DHCP Relay Agent with the `service dhcp-relay` command.

You can display the status of this function and other information with the `show ip dhcp relay information`command.

8.5.3 Commands in the Interface Configuration mode

This section describes commands that you can call up in the Interface Configuration mode of VLAN.

In global configuration mode, enter the `interface vlan $$$` command to change to this mode. When doing this, you need to replace the `$$$` placeholders with the relevant VLAN ID.

Commands relating to other topics that can be called in the Interface Configuration mode of VLAN can be found in the relevant sections.

- If you exit the Interface Configuration mode of VLAN with the `exit` command, you return to the Interface Configuration mode.
- If you exit the Interface Configuration mode of VLAN with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode of VLAN.

To do this, you replace `[command]` with the command that you want to execute.

8.5.3.1 ip dhcp relay circuit-id

Description

With this command, you assign a Circuit ID to the interface.

Requirement

- The interface is an IP interface.
- You are in the Interface configuration mode of VLAN
  The command prompt is as follows:
  `cli(config-if-vlan-$$)#`

Syntax

Call up the command with the following parameters:

`ip dhcp relay circuit-id <circuit-id>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`circuit-id`	Circuit ID	1 ... 188

Result

The Circuit ID is assigned.

Further notes

You remove the Circuit ID with the `no ip dhcp relay circuit-id` command.

You display the IP addresses with the `show dhcp server` command.

You display the settings with the `show ip dhcp relay information` command.

8.5.3.2 no ip dhcp relay circuit-id

Description

With this command, you remove the Circuit ID.

Requirement

- The interface is an IP interface.
- You are in the Interface Configuration mode of VLAN. The command prompt is as follows:

  `cli(config-if-vlan-$$)#`

Syntax

Call the command without parameter assignment:

`no ip dhcp relay circuit-id`

Result

The Circuit ID is removed.

Further notes

You configure the Circuit ID with the `ip dhcp relay circuit-id` command.

You display the IP addresses with the `show dhcp server` command.

You display the settings with the `show ip dhcp relay information` command.

8.5.3.3 ip dhcp relay information option

Description

With this command, you enable the DHCP option 82. If the option is enabled, prior to forwarding to the DHCP server, information about the origin of the DHCP query is encoded in the packet. If the DHCP server sends a response, the information is removed again before forwarding to the DHCP client.

This information is only encoded in the data packet if the DHCP relay agent is enabled.

Requirement

You are in the Global configuration mode or in the Interface configuration mode of VLAN.

The command prompt is as follows:

`cli(config)#` or `cli(config-if-$$)#`

Syntax

Call the command without parameter assignment:

```
ip dhcp relay information option
```

Result

The option is enabled.

Further notes

You disable the option with the `no ip dhcp relay information option` command.

You enable the DHCP Relay Agent with the `service dhcp-relay` command.

You configure the content of the information with the `ip dhcp relay circuit-id option` command.

You can display the status of this option and other information with the `show ip dhcp relay information` command.

8.5.3.4 no ip dhcp relay information option

Description

With this command, you disable the DHCP option 82.

Requirement

You are in the Global configuration mode or in the Interface configuration mode of VLAN.

The command prompt is as follows:

`cli(config)#` or `cli(config-if-$$)#`

Syntax

Call the command without parameter assignment:

```
no ip dhcp relay information option
```

Result

The option is disabled.

Further notes

You enable the option with the `ip dhcp relay information option` command.

You can display the status of this option and other information with the `show ip dhcp relay information` command.

8.5.3.5 ip dhcp relay remote-id

Description

With this command, you specify the device ID.

Requirement

- The interface is an IP interface.
- You are in the Interface Configuration mode of VLAN. The command prompt is as follows:

  `cli(config-if-vlan-$$)#`

Syntax

Call up the command with the following parameters:

```
ip dhcp relay remote-id <remote-id name>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`remote-id name`	Device ID	max. 32 characters Default: XYZ

Result

The device ID is specified.

Further notes

You remove the device ID with the `no ip dhcp relay remote-id` command.

You display the IP addresses with the `show dhcp server` command.

You display the settings with the `show ip dhcp relay information` command.

8.5.3.6 no ip dhcp relay remote-id

Description

With this command, you remove the device identifier.

Requirement

- The interface is an IPv4 interface.
- You are in the Interface configuration mode
  The command prompt is as follows:
  `cli(config-if-$$)#`

Syntax

Call the command without parameter assignment:

```
no ip dhcp relay remote-id
```

Result

The device ID is removed.

Additional notes

You configure the device ID with the `ip dhcp relay remote-id` command.

You display the IP addresses with the `show dhcp server` command.

You display the settings with the `show ip dhcp relay information` command.

8.6 SNMP

This section describes commands of the Simple Network Management Protocol (SNMP).

Example of a configuration

IP configuration

Define the IP address of the device that is suitable for the SNMP trap receiver used.

Execute the following commands:

```
configure terminal
int vlan 1
no ip address
ip address 192.168.1.1 255.255.255.0
end
```

Trap configuration forr SNMPv2c notifications

To configure the sending of SNMP traps, an SBMP community is required.

This community is used along with other SNMP parameters to send traps to a trap recipient.

The selection of the traps recipient is made using tags that are set when SNMP notifications are called.

Execute the following commands:

```
configure terminal
snmp community index v2trapindex name public security v2secname
snmp targetaddr trapringer param pav2c ipv4 192.168.1.254 taglist
publictrapv2tag
snmp targetparams pav2c user v2secname security-model v2c message-
processing v2c
snmp notify testnotify tag publictrapv2tag type trap
end
```

Event configuration

Enable the sending of traps.

Execute the following commands:

```
configure terminal
events
client config trap
end
```

For system messages all configured SNMP notification are always called.

With RMOB events. the SNMP notifications to be called must be configured explicitly, see section "RMON (Page 748)".

8.6.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.6.1.1 show snmp

Description

This command shows the status information of SNMP.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp
```

Result

The status information is displayed.

8.6.1.2 show snmp community

Description

This command shows the details of the configured of SNMP communities.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp community
```

Result

The details of the configured SNMP communities are displayed.

8.6.1.3 show snmp engineID

Description

This command shows the SNMP identification number of the device.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp engineID
```

Result

The SNMP identification number of the device is displayed.

8.6.1.4 show snmp filter

Description

This command shows the configured SNMP filters.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp filter
```

Result

The configured SNMP filters are displayed.

8.6.1.5 show snmp group

Description

This command shows the configured SNMP groups.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp group
```

Result

The configured SNMP groups are displayed.

8.6.1.6 show snmp group access

Description

This command shows the rights of the configured SNMP groups.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp group access
```

Result

The rights of the configured SNMP groups are displayed.

8.6.1.7 show snmp inform statistics

Description

This command shows the statistics of the Inform Messages.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp inform statistics
```

Result

The statistics of the Inform Messages are displayed.

8.6.1.8 show snmp notif

Description

With this command, you display the configured SNMP notification types.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp notif
```

Result

The configured SNMP notification types are displayed.

8.6.1.9 show snmp targetaddr

Description

This command shows the configured SNMP target addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp targetaddr
```

Result

The configured SNMP target addresses are displayed.

8.6.1.10 show snmp targetparam

Description

This command shows the configured SNMP target parameters.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp targetparam
```

Result

The configured SNMP target parameters are displayed.

8.6.1.11 show snmp tcp

Description

This command shows the configuration for SNMP via TCP.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp tcp
```

Result

The configuration for SNMP via TCP is displayed.

8.6.1.12 show snmp user

Description

This command shows the settings for the SNMP users.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp user
```

Result

The settings for the SNMP users are displayed.

8.6.1.13 show snmp viewtree

Description

This command shows the settings for the SNMP tree view.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show snmp viewtree
```

Result

The settings for the SNMP tree view are displayed.

8.6.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.6.2.1 snmpagent

Description

With this command, you enable the SNMP agent function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`snmpagent`

Result

The SNMP agent function is enabled.

Further notes

You disable the SNMP agent function with the`no snmpagent` command.

8.6.2.2 no snmpagent

Description

With this command, you disable the SNMP agent function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no snmpagent`

Result

The SNMP agent function is disabled.

Further notes

You enable the SNMP agent function with the `snmpagent` command.

8.6.2.3 snmpagent port

Description

With this command, you specify the port at which the SNMP agent waits for the SNMP queries.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
snmpagent port <port-number(1024-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`port-number`	Port number	1024 ... 65535 Default: 161 (standard port)

Result

The port is defined.

Additional notes

You reset the port to the standard port with the `no snmpagent port` command.

8.6.2.4 no snmpagent port

Description

With this command, you reset the port to the standard port.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no snmpagent port
```

Result

The port is reset to the standard port 161.

Additional notes

You configure the port with the `snmpagent port` command.

8.6.2.5 snmp access

Description

With this command, you configure the access to an SNMP group.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}
  [read <ReadView | none>] [write <WriteView | none>]  [notify
<NotifyView | none>]
 [{volatile | nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`GroupName`	Name of the group to which access is configured	max. 32 characters
Version	Selects the version of the protocol used	• `v1` • `v2c` • `v3`
Authentication	Selects the authentication method.	• `auth` Enables MD5 or SHA as authentication method • `noauth` No authentication • `priv` Enables authentication and encryption
`read`	The data can be read. Keyword	• `ReadView` • `none`
`write`	The data can be read and written Keyword	• `WriteView` • `none`
`notify`	Changes can be sent as a tag. Keyword	• `NotifyView` • `none`
Storage Type	Specifies whether the settings remain following a restart.	• `volatile :` The settings are lost after a restart • `nonvolatile :` The settings are retained after a restart

The keywords need to be specified.

If optional parameters are not specified when configuring a group, the default value will be used.

Result

The settings for access to an SNMP group are configured.

Additional notes

You delete the access to an SNMP group with the `no snmp access` command.

You display the configured SNMP groups with the `show snmp group` command.

You display the access configurations for SNMP groups with the `show snmp group access` command.

You display the configured SNMP tree views with the `show snmp viewtree` command.

8.6.2.6 no snmp access

Description

With this command, you delete the access to an SNMP group.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`GroupName`	Name of the group to which access is deleted	max. 32 characters
Version	Selects the version of the protocol used	• `v1` • `v2c` • `v3`
Authentication	Selects the authentication method.	• `auth` • `noauth` • `priv`

Result

The access to an SNMP group is deleted.

Additional notes

You configure the setting with the `snmp access` command.

You display the configured SNMP groups with the `show snmp group` command.

You display the access configurations for SNMP groups with the `show snmp group access` command.

You display the configured SNMP tree views with the `show snmp viewtree` command.

8.6.2.7 snmp agent version

Description

With this command, you configure whether all SNMP queries or only SNMPv3 queries are processed.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
snmp agent version {v3only | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`v3only`	Only SNMPv3 queries are processed	-
`all`	All SNMP queries are processed	Default: all

Result

The setting is configured.

8.6.2.8 snmp community index

Description

With this command, you configure the details of an SNMP community.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
snmp community index <CommunityIndex> name <CommunityName>
  security <SecurityName> [context <name>] [{volatile | nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`CommunityIndex`	Index of the community	Max. 256 characters
`name`	Keyword for the name of the community	-
`CommunityName`	Name of the community	Max. 256 characters
`security`	Keyword for the security name	-
`SecurityName`	Security name	Max. 32 characters
`context`	Keyword for the context name	-
`name`	Context name	Max. 32 characters
Storage type	Specifies whether the settings remain following a restart.	• : The settings are lost after a restart • : The settings are retained after a restart

If optional parameters are not specified when configuring a community, the default values apply.

Note

Community string

For security reasons, do not use the standard values "public" or "private". Change the community strings following the initial installation.

The recommended minimum length for community strings is 6 characters.

Result

The settings are configured.

Additional notes

You delete the details of an SNMP community with the `no snmp community index` command.

You show the details of an SNMP community with the `show snmp community` command.

You show the status information of the SNMP communication with the `show snmp` command.

8.6.2.9 no snmp community index

Description

With this command, you delete the details of an SNMP community.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`no snmp community index <CommunityIndex>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`CommunityIndex`	Name of the community	max. 32 characters

Result

The details of an SNMP community are deleted.

Further notes

You configure the details of an SNMP community with the `snmp community index` command.

You show the details of an SNMP community with the `show snmp community` command.

You show the status information of the SNMP communication with the `show snmp` command.

8.6.2.10 snmp engineid migrate

Description

With this command, you enable the SNMPv3 user migration.

If the function is enabled, an SNMP engine ID is generated that can be migrated. You can transfer configured SNMPv3 users to a different device. If you enable this function and load the configuration of the device on another device, configured SNMPv3 users are retained.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`snmp engineid migrate`

Result

The SNMPv3 user migration is enabled.

Further notes

You disable the SNMPv3 user migration with the `no snmp engineid migrate` command.

8.6.2.11 no snmp engineid migrate

Description

With this command, you disable the SNMPv3 user migration.

If the function is disabled, a device-specific SNMP engine ID is generated. To generate the ID, the agent MAC address of the device is used. You cannot transfer this SNMP user configuration to other devices.

If you load the configuration of the device on another device, all configured SNMPv3 users are deleted.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no snmp engineid migrate`

Result

The SNMPv3 user migration is disabled.

Further notes

You enable the SNMPv3 user migration with the `snmp engineid migrate` command.

8.6.2.12 snmp group

Description

With this command, you configure the details of an SNMP group.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
snmp group <GroupName> user <UserName> security-model {v1|v2c|v3}
   [{volatile|nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`GroupName`	Name of the group	max. 32 characters
`user`	Keyword for the user name	-
`UserName`	Name of the user	max. 32 characters
`security-model`	Specifies which security settings will be used.	• `v1` • `v2c` • `v3`
Storage type	Specifies whether the settings remain following a restart.	• `volatile` : The settings are lost after a restart • `nonvolatile` : The settings are retained after a restart.

If optional parameters are not specified when configuring a group, the default values apply.

Result

The details of the group are configured.

Further notes

You delete the details of an SNMP group with the `no snmp group` command.

You display the created SNMP groups with the `show snmp group` command.

You display the created SNMP users with the `show snmp user` command.

8.6.2.13 no snmp group

Description

With this command, you delete the details of an SNMP group.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`no snmp group <GroupName> user <UserName> security-model {v1|v2c|v3}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`GroupName`	Name of the group	max. 32 characters
`user`	Keyword for the user name	-
`UserName`	Name of the user	max. 32 characters
`security-model`	Specifies which security settings are used for sending.	• `v1` • `v2c` • `v3`

Result

The details of the group are deleted.

Further notes

You change the details of an SNMP group with the `snmp group` command.

You display the created SNMP groups with the `show snmp group` command.

You display the created SNMP users with the `show snmp user` command.

8.6.2.14 snmp notify

Description

With this command, you configure the details of the SNMP notifications.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
snmp notify <NotifyName> tag <TagName> type {Trap|Inform}
   [{volatile|nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`NotifyName`	Name of the SNMP notification	max. 32 characters
`tag`	Keyword for a target key	-
`TagName`	Name of the target key	max. 32 characters
`Type`	Type of the SNMP notification	• `Trap` Generates a trap. • `Inform` Generates a log entry or sends an entry to the log server.
Storage type	Specifies whether the settings remain following a restart.	• : The settings are lost after a restart • : The settings are retained after a restart

Result

The details of the SNMP notifications are configured.

Further notes

You delete the details of an SNMP notification with the `no snmp notify` command.

You display the configured SNMP notifications with the `show snmp notif` command.

You display the configured SNMP target addresses with the `show snmp targetaddr` command.

8.6.2.15 no snmp notify

Description

With this command, you delete the details of the SNMP notifications.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`no snmp notify <NotifyName>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`NotifyName`	Name of the notification	max. 32 characters

Result

The details of the SNMP notifications are deleted.

Further notes

You change the details of an SNMP group with the `snmp notify` command.

You display the configured SNMP notifications with the `show snmp notif` command.

You display the configured SNMP target addresses with the `show snmp targetaddr` command.

8.6.2.16 snmp targetaddr

Description

With this command, you configure the SNMP target address.

Requirement

- The SNMP target parameters are configured.

You are in the Global configuration mode.
The command prompt is:
`cli(config)#`

Syntax

Call up the command with the following parameters:

```
snmp targetaddr <TargetAddressName> param <ParamName>
     {ipv4 <IPAddress> | fqdn-name <FQDN>}
     [timeout <Seconds(1-1500)] [retries <RetryCount(1-3)]
     [taglist <TagIdentifier | none>] [{volatile | nonvolatile}]
     [port <integer (1-65535)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`TargetAddressName`	Name of the target address	Maximum of 32 characters
`param`	Keyword for the parameter name	-
`ParamName`	Name of the parameter	Maximum of 32 characters
`ipv4`	Keyword for an IPv4 address	-
`IPAddress`	IPv4 address	Enter a valid IPv4 unicast address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters
`timeout`	Keyword for the time the SNMP agent waits for a response before it repeats the inform request message	-
`Seconds`	Time in seconds	1 ... 1500
`retries`	Keyword for the maximum number of attempts to obtain a response to an inform request message	-
`RetryCount`	Number of attempts	1 ... 3
`taglist`	Keyword for tag list	-
`TagIdentifier`	Tag identifier that selects the destination address for SNMP.	Specify the tag identifier.
`none`	No tag identifier	-
`volatile` `nonvolatile`	Specifies whether the settings remain following a restart.	• `volatile`: The default settings are used after a restart. • `nonvolatile`: The saved settings are used after a restart.
`port`	Keyword for the port number at which the SNMP manager receives traps and inform messages	-
`integer`	Port number	1 ... 65535

For information on addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If optional parameters are not specified when configuring, the default values apply.

Result

The SNMP target address is configured.

Further notes

You delete the SNMP target address with the `no snmp targetaddr` command.

You display the SNMP target address with the `show snmp targetaddr` command.

You configure the SNMP target parameters with the `snmp targetparams` command.

You display the SNMP target parameters with the `show snmp targetparam` command.

8.6.2.17 no snmp targetaddr

Description

With this command, you delete the SNMP target address.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no snmp targetaddr <TargetAddressName>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`TargetAddressName`	SNMP target address	max. 32 characters

Result

The SNMP target address is deleted.

Further notes

You change the SNMP target address with the `snmp targetaddr` command.

You display the SNMP target address with the `show snmp targetaddr` command.

8.6.2.18 snmp targetaddr remote-engine-id

Description

With this command, you configure the SNMP destination address.

Requirement

- The SNMP target parameters are configured.
- You are in the Global configuration mode.
  The command prompt is:
  `cli(config)#`

Syntax

Call up the command with the following parameters:

```
snmp targetaddr <TargetAddressName> remote-engine-id
<EngineIdentifier>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`TargetAddressName`	Name of the destination address	Maximum of 32 characters
`remote-engine-id`	Keyword for the Remote Engine ID	-
`EngineIdentifier`	The Remote Engine ID	An engine ID correspond to RFC 3411.

Result

The SNMP destination address is configured.

Further notes

You delete the SNMP destination address with the `no snmp targetaddr` command.

You display the SNMP destination address with the `show snmp targetaddr` command.

You display the SNMP target parameters with the `show snmp targetparam` command.

You store a domain name with the `ip domain name` or `domain name` command.

8.6.2.19 snmp targetparams

Description

With this command, you configure the SNMP target parameters.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
snmp targetparams <ParamName> user <UserName>  security-model {v1 |
v2c | v3 {auth | noauth | priv}}
  message-processing {v1 | v2c | v3} [{volatile | nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ParamName`	Name of the SNMP parameter	max. 32 characters
`user`	Keyword for the user name	-
`UserName`	Value for the user name	max. 32 characters
`security-model`	Specifies which SNMP version is used. With SNMPv3 a security level (authentication, encryption) can also be configured.	• SNMP version – `v1` – `v2c` – `v3` • Security level for v3 – `auth` Authentication enabled / no encryption enabled – `noauth` No authentication enabled, no encryption enabled – `priv` Authentication enabled / encryption enabled
`message-processing`	Specifies which SNMP version is used for processing the messages and whether the settings remain following a restart.	• SNMP version – `v1` – `v2c` – `v3` • Settings after the restart – `volatile`: The settings are lost after a restart. – `nonvolatile`: The settings are retained after a restart.

If optional parameters are not specified when configuring, the default values apply.

Result

The SNMP target parameters are configured.

Additional notes

You delete the SNMP target parameters with the `no snmp targetparams` command.

You display settings of this function with the `show snmp targetparam` command.

You configure the user profile with the `snmp user` command.

You display the list of users with the `show snmp user` command.

8.6.2.20 no snmp targetparams

Description

With this command, you delete the SNMP target parameters.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no snmp targetparams <ParamName>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`ParamName`	Name of the SNMP parameter	max. 32 characters

Result

The SNMP target parameters are deleted.

Further notes

You change the SNMP target parameters with the `snmp targetparams` command.

You display settings of this function with the `show targetparam` command.

8.6.2.21 snmp user

Description

With this command, you configure the details of an SNMP user.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
snmp user <UserName> [auth {md5 | sha} <passwd> [priv {DES |
AES128} <passwd>]] [{volatile | nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`UserName`	Name of the user	max. 32 characters
`auth`	Keyword for the authentication	Default: No authentication
`md5`	MD5 (Message Digest 5) is used as hash function.	-
`sha`	SHA (Secure Hash Algorithm) is used as hash function.	-
`passwd`	Password for authentication	max. 32 characters
`priv`	Specifies that there is encryption.	Default: No encryption
`DES`	DES is used as encryption algorithm.	-
`AES128`	AES128 is used as encryption algorithm.	-
`passwd`	Value for the password of the encryption	max. 32 characters
`volatile`	The default settings are used after a re-start.	-
`nonvolatile`	The saved settings are used after a re-start.	-

If optional parameters are not specified when configuring an SNMP user, the default values apply.

Result

The details of an SNMP user are configured.

Additional notes

You delete the settings with the `no snmp user` command.

You display the configured users with the `show snmp user` command.

8.6.2.22 no snmp user

Description

With this command, you delete the details of an SNMP user.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no snmp user <UserName>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`UserName`	Name of the user	max. 32 characters

Result

The details of an SNMP user are deleted.

Further notes

You change the settings with the `snmp user` command.

You display the configured users with the `show snmp user`command.

8.6.2.23 snmp v1-v2 readonly

Description

With this command, you block write access for SNMPv1 and SNMPv2 PDUs.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
snmp v1-v2 readonly
```

Result

Write access for SNMPv1 and SNMPv2 PDUs is blocked.

Further notes

You release write access for SNMPv1 and SNMPv2 PDUs with the `no snmp v1-v2 readonly` command.

8.6.2.24 no snmp v1-v2 readonly

Description

With this command, you enable write access for SNMPv1 and SNMPv2 PDUs.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no snmp v1-v2 readonly
```

Result

Write access for SNMPv1 and SNMPv2 PDUs is enabled.

Further notes

You block write access for SNMPv1 and SNMPv2 PDUs with the `snmp v1-v2 readonly` command.

8.6.2.25 snmp view

Description

With this command, you configure an SNMP view.

Requirement

- An SNMP group has been created
- The access to the group is configured with `snmp access`
- You are in the Global Configuration mode.
  The command prompt is:
  `cli(config)#`

Syntax

Call up the command with the following parameters:

```
snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included |
excluded}
   [{volatile | nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ViewName`	Name of the SNMP view	max. 32 characters
`OIDTree`	Object ID	Path information of the MIB tree
`mask`	Keyword for the OID mask	-
`OIDMask`	Mask that filters access to the elements of the MIB tree	A series of "`0`" and "`1`" separated by dots in keeping with the path information of the MIB tree
View type	Specifies whether the filtered elements are used or excluded.	• `included` (Default) • `excluded`
Storage type	Specifies whether the settings remain following a restart.	• `volatile`: The settings are lost after a restart • `nonvolatile`: The settings are retained after a restart (default).

If optional parameters are not specified when configuring, the default values apply.

Result

The SNMP view is configured.

Additional notes

You delete the view with the `no snmp view` command.

You display the configured SNMP tree views with the `show snmp viewtree` command.

You display the access rights of the SNMP groups with the `show snmp group access` command.

You configure the access rights of the SNMP groups with the `snmp access`command.

8.6.2.26 no snmp view

Description

With this command, you delete an SNMP view.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no snmp view <ViewName> <OIDTree>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ViewName`	Name of the view	max. 32 characters
`OIDTree`	Object ID	Path information of the MIB tree

Result

The SNMP view is deleted.

Further notes

You configure a view with the `snmp view` command.

You display the configured SNMP tree views with the `show snmp viewtree` command.

8.7 SMTP client

This section describes commands of the Simple Mail Transfer Protocol (SMTP).

8.7.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.7.1.1 show events smtp-server

Description

This command shows the configured e-mail servers.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show events smtp-server
```

Result

The configured e-mail servers are displayed.

8.7.2 Commands in the Events configuration mode

This section describes commands that you can call up in the EVENTS configuration mode.

In global configuration mode, enter the `events` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

- If you exit the EVENTS configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the EVENTS configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in EVENTS configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.7.2.1 smtp-server

Description

With this command, you change to the SMTP server configuration mode. There are two options to do this:

- Create new
  If there is no entry with this address yet, a new SMTP server entry is created and a switch to the SMTP server configuration mode takes place. In this mode, you configure the other settings of the SMTP server.
- Change configuration
  If the entry already exists, a switch to the SMTP configuration mode takes place. In this mode, you can change the settings of the SMTP server.

Requirement

You are in the EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
smtp-server { ipv4 <ucast_addr> | fqdn-name <FQDN>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	IPv4 address of the SMTP server	Enter a valid IPv4 unicast address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters

For information on addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

An entry for the SMTP server is created.

You are now in the SMTP server configuration mode.

The command prompt is as follows:

```
cli(events-smtp-server)#
```

Further notes

You delete the SMTP server entry with the `no smtp-server` command.

You display the configuration of the SMTP server with the `show events smtp-server` command.

8.7.2.2 no smtp-server

Description

With this command, you delete an SMTP server entry.

Requirement

You are in the EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
no smtp-server { ipv4 <ucast_addr> | fqdn-name <FQDN)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	IPv4 address of the SMTP server	Enter a valid IPv4 unicast address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters

For information on addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The SMTP server entry is deleted.

Further notes

You configure an SMTP server entry with the `smtp-server` command.

8.7.2.3 send test mail

Description

With this command, you send an e-mail according to the currently configured SMTP settings.

Requirement

You are in the EVENTS configuration mode.

The command prompt is as follows:

`cli(config-events)#`

Syntax

Call the command without parameters:

`send test mail`

Result

An e-mail according to the currently configured SMTP settings is sent.

Further notes

You can display the current SMTP settings with the `show events smtp-server` command.

8.7.3 Commands in SMTP server configuration mode

8.7.3.1 Introductory sentence for the SMTP server configuration mode

This section describes commands that you can call up in the SMTP server configuration mode.

In the Events configuration mode, enter the `smtp-server` command to change to this mode.

- If you exit the SMTP server configuration mode with the `exit` command, you return to the events configuration mode.
- If you exit the SMTP server configuration mode with the `end` command, you return to the Privileged EXEC mode.

8.7.3.2 auth username

Description

With this command, you configure the user data (user name and password) used for authentication on the SMTP server.

Requirement

You are in the SMTP server configuration mode.

The command prompt is as follows:

```
cli(events-smtp-server)#
```

Syntax

Call up the command with the following parameters:

```
auth username <username> password <password>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`username`	Keyword for a user name	-
`username`	User name	Enter the user name used for authentication on the SMTP server. Maximum length: 64 characters
`password`	Keyword for a password	-
`password`	Password	Enter the password used for authentication on the SMTP server. Maximum length: 64 characters

Result

The user data is configured.

Further notes

You delete the user data with the `no auth username` command.

You display this setting with the `show events smtp-server` command.

8.7.3.3 no auth username

Description

With this command, you delete the user data.

Requirement

You are in the SMTP server configuration mode.

The command prompt is as follows:

`cli(events-smtp-server)#`

Syntax

Call the command without parameters:

`no auth username`

Result

The SMTP port is reset to the default value.

Further notes

You configure the user data with the `auth username` command.

You display this setting with the `show events smtp-server` command.

8.7.3.4 port

Description

With this command, you configure the port via which the SMTP server can be reached.

Requirement

You are in SMTP server configuration mode

The command prompt is as follows:

`cli(events-smtp-server)#`

Syntax

Call up the command with the following parameters:

`port <smtp-port(1-65535)>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`smtp-port`	Value for the SMTP port	1 ... 65535 Default: • 25 (no security) • 465 (security)

Result

The SMTP port is configured.

Additional notes

You display this setting with the `show events smtp-server` command.

You reset the setting to the default with the `no port` command.

8.7.3.5 no port

Description

With this command, you reset the SMTP port to the default.

Requirement

You are in SMTP server configuration mode

The command prompt is as follows:

```
cli(events-smtp-server)#
```

Syntax

Call the command without parameters:

```
no port
```

Result

The SMTP port is reset to the default value.

- 25 (no security)
- 465 (security)

Additional notes

You configure the setting with the `port` command.

You display this setting with the `show events smtp-server` command.

8.7.3.6 sender address

Description

With this command, you configure the sender specified in the e-mail.

Requirement

You are in the SMTP server configuration mode.

The command prompt is as follows:

```
cli(events-smtp-server)#
```

Syntax

Call up the command with the following parameters:

```
sender-address <mail-address>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`mail-address`	Sender Email Address	Max. 100 characters

Result

The e-mail address of the sender is configured.

Further notes

You display this setting with the `show events smtp-server` command.

You delete the sender with the `no sender-address` command.

8.7.3.7 no sender address

Description

You delete the sender with this command.

Requirement

You are in the SMTP server configuration mode.

The command prompt is as follows:

```
cli(events-smtp-server)#
```

Syntax

Call the command without parameters:

```
no sender-address
```

Result

The e-mail name of the sender is deleted.

Further notes

You configure a sender with the `sender-address` command.

You display this setting with the `show events smtp-server` command.

8.7.3.8 receiver-address

Description

With this command, you specify who receives an e-mail when an event occurs.

Requirement

- "email" is activated for the event in question.
- You are in the SMTP server configuration mode.
  The command prompt is as follows:
  `cli(events-smtp-server)#`

Syntax

Call up the command with the following parameters:

`receiver-address <mail-address> [shutdown]`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mail-address`	Receiver Email Address	Max. 100 characters
`shutdown`	Disables sending of the e-mail. This recipient will not receive an e-mail when an event occurs.	-

Result

A recipient is configured.

Further notes

You delete the recipient with the `no receiver-address` command.

You display this setting with the `show events smtp-server` command.

You configure the setting "`email`" with the `event config` command.

8.7.3.9 no receiver-address

Description

With this command, you delete a recipient.

Requirement

You are in the SMTP server configuration mode.

The command prompt is as follows:

`cli(events-smtp-server)#`

Syntax

Call up the command with the following parameters:

`no receiver-address <mail-address>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`mail-address`	Receiver Email Address	Max. 100 characters

Result

The recipient is deleted.

Further notes

You create a recipient with the `receiver-address` command.

You display this setting with the `show events smtp-server` command.

8.7.3.10 security

Description

With this command, you configure the method for encrypted transfer of the e-mail from the device to the SMTP server.

Requirement

You are in the SMTP server configuration mode.

The command prompt is as follows:

`cli(events-smtp-server)#`

Syntax

Call up the command with the following parameters:

`security {ssltls | starttls}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ssltls`	Uses SSL/TLS	-
`starttls`	Uses STARTTLS	-

Result

The method for the transfer is configured.

Further notes

You disable the setting with the `no security` command.

You display this setting with the `show events smtp-server` command.

8.7.3.11 no security

Description

With this command, you specify that the e-mail is transferred unencrypted.

Requirement

You are in the SMTP server configuration mode.

The command prompt is as follows:

`cli(events-smtp-server)#`

Syntax

Call the command without parameters:

`no security`

Result

Transfer of the e-mail from the device to the SMTP server is unencrypted.

Further notes

You configure the setting with the `security` command.

You display this setting with the `show events smtp-server` command.

8.7.3.12 smtp-server-enable

Description

With this command, you enable the SMTP server.

Requirement

You are in SMTP server configuration mode

The command prompt is as follows:

`cli(events-smtp-server)#`

Syntax

Call the command without parameters:

`smtp-server-enable`

Result

The SMTP server is enabled.

Additional notes

You disable the SMTP server with the `no smtp-server-enable` command.

8.7.3.13 no smtp-server-enable

Description

You disable the SMTP server with this command.

Requirement

You are in SMTP server configuration mode

The command prompt is as follows:

`cli(events-smtp-server)#`

Syntax

Call the command without parameters:

`no smtp-server-enable`

Result

The SMTP server is disabled.

Additional notes

You activate the SMTP server with the `smtp-server-enable` command.

8.7.3.14 test

Description

You send a test e-mail to the configured recipients with this command.

Requirement

You are in the SMTP server configuration mode.

The command prompt is as follows:

```
cli(events-smtp-server)#
```

Syntax

Call the command without parameters:

```
test
```

Result

A test e-mail was sent to the configured recipients. The test result is shown in the console output. If sending was not successful, the message contains possible causes.

8.8 HTTP server

This section describes commands of the Hypertext Transfer Protocol (HTTP).

8.8.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.8.1.1 show ip http server status

Description

This command shows the status of the HTTP server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip http server status
```

Result

The status of the HTTP server is displayed.

8.8.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.8.2.1 ip http

Description

With this command, you enable HTTP access to the WBM.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`ip http`

As default the function is "enabled".

Result

HTTP access is enabled.

Additional notes

You can display the setting of this function and other information with the `show ip http server status`command.

You disable HTTP access with the `no ip http` command.

8.8.2.2 no ip http

Description

With this command, you disable HTTP access.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no ip http`

Result

Access to the WBM is now only possible with HTTPS.

Additional notes

You can display the setting of this function and other information with the `show ip http server status`command.

You enable HTTP access with the `ip http` command.

8.8.2.3 ip http port

Description

With this command you specify the port for HTTP access to the WBM.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip http port <port-number(1024-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`port-number`	Port number	1024 ... 65535 Default: 80 (standard port)

Note

Used ports

Some ports are permanently reserved. Make sure that the specified port is not already in use. You can find the ports used in the "List of available services".

Result

The port for HTTP access has been changed. Access the WBM with the changed port.

Additional notes

You reset the port to the standard port with the `no ip http port` command.

8.8.2.4 no ip http port

Description

With this command, you reset the port to the standard port.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no ip http port`

Result

The port is reset to the standard port 80.

Further notes

You configure the port for HTTP access with the ip http port command

8.9 HTTPS server

This section describes commands of the Hypertext Transfer Protocol Secure (HTTPS).

8.9.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.9.1.1 show ip http secure server status

Description

This command shows the status of the HTTPS server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

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

Result

The status, cipher suite and version of the HTTPS server are displayed.

8.9.1.2 show ssl server-cert

Description

This command shows the SSL server certificate.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ssl server-cert
```

Result

The SSL server certificate is displayed.

8.9.2 Commands in global configuration mode

8.9.2.1 ip http secure

Description

With this command, you enable HTTPS access to the WBM.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`ip http secure`

Result

HTTP is enabled on the device.

Additional notes

You disable HTTPS access with the `no ip http secure` command.

8.9.2.2 no ip http secure

Description

With this command, you disable HTTPS access to the WBM.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no ip http secure`

Result

Access to the WBM is now only possible with HTTP.

Additional notes

You enable HTTPS access with the `ip http secure` command.

8.9.2.3 ip http secure port

Description

With this command you specify the port for HTTPS access to the WBM.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip http secure port <port-number(1024-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`port-number`	Value for the HTTPS port	1024 ... 65535 Default: 443 (standard port)

Note

Used ports

Some ports are permanently reserved. Make sure that the specified port is not already in use. You can find the ports used in the "List of available services".

Result

The port for HTTPS access has been changed. Access the WBM with the changed port.

Additional notes

You reset the port to the standard port with the `no ip http port` command.

8.9.2.4 no ip http secure port

Description

With this command, you reset the HTTPS port to the standard port.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip http secure port
```

Result

The port is reset to the standard port 443.

Further notes

You configure the port for HTTPS access with the `ip http secure port` command

8.9.2.5 ip http secure minimum tls-version

Description

With this command, you define which version of TLS is used at least.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip http secure minimum tls-version {v10 | v11 | v12| v13}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`v10`	TLS as of version 1.0 can be used	-
`v11`	TLS as of version 1.1 can be used	-
`v12`	TLS as of version 1.2 can be used	Factory setting
`v13`	TLS as of version 1.3 can be used	-

Result

HTTP is enabled on the device.

Additional notes

You can display the setting of this function and other information with the `show ip http secure server status` command.

8.10 ARP

This section describes commands of the Address Resolution Protocol (ARP).

8.10.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.10.1.1 show ip arp

Description

With this command, you display the ARP table. The ARP table contains the clear assignment of MAC address to IPv4 address.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameterization:

```
show ip arp [ { vlan <vlan-id(1-4094)> | <interface-type>
<interface-id> | <ip-address> | <mac-address> | summary |
information }]
```

The parameters have the following meaning:

Parameter	Description	Value range / note
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	
`ip-address`	Shows the IPv4 addresses of the entries in the ARP table	-
`mac-address`	Shows the MAC addresses of the entries in the ARP table	-
`summary`	Shows a summary of the entries in the ARP table	-
`information`	Displays information on the ARP configuration	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, all parameters of the ARP table are displayed.

Result

The ARP table is displayed.

8.10.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.10.2.1 arp timeout

Description

With this command, you configure the timeout setting of the ARP cache.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`arp timeout <seconds(30-86400)>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`seconds`	Value for the timeout in seconds	30 ... 86400 Default: 300

Result

The setting for the timeout setting of the ARP cache is configured.

Further notes

You can reset the timeout setting to the default with the `no arp timeout` command.

You can display the status of this function and other information with the `show ip arp` command.

8.10.2.2 no arp timeout

Description

With this command, you reset the timeout setting of the ARP cache back to the default value.

The default value for the timeout setting is 300 seconds.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

`no arp timeout`

Result

The timeout setting for the ARP cache is reset to the default value.

Further notes

You change the timeout setting with the `arp timeout` command.

You can display the status of this function and other information with the `show ip arp` command.

8.11 SSH server

This section describes commands of the Secure Shell (SSH) Server.

8.11.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.11.1.1 show ip ssh

Description

This command shows the settings of the SSH server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

`show ip ssh`

Result

The settings for the SSH server are displayed.

8.11.1.2 show ssh-fingerprint

Description

This command shows the SSH fingerprint.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

`show ssh-fingerprint`

Result

The SSH fingerprint is displayed.

8.11.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

8.11.2.1 ssh-server

Description

With this command, you enable the SSH protocol on the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`ssh-server`

As default the function is "enabled".

Result

The SSH protocol is enabled on the device.

Further notes

You disable the SSH protocol with the `no ssh-server` command.

8.11.2.2 no ssh-server

Description

With this command, you disable the SSH protocol on the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no ssh-server`

Result

The SSH protocol is disabled on the device.

Further notes

You enable the SSH protocol with the `ssh-server` command.

8.11.2.3 ssh-server kex-algorithm-level

Description

With this command, you specify the level of the exchange algorithm for SSH keys.

After a factory reset, the SSH key exchange algorithm is set to the default value of "High".

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameter assignment:

```
ssh-server kex-algorithm-level {low | high}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`low`	Curve25519-sha256 Curve25519-sha256@libssh.org Ecdh-sha2-nistp256 Ecdh-sha2-nistp384 Ecdh-sha2-nistp521 Diffie-hellman-group16-sha512 Diffie-hellman-group18-sha512 Diffie-hellman-group14-sha256 Diffie-hellman-group14-sha1	-
`high`	Curve25519-sha256 Curve25519-sha256@libssh.org Ecdh-sha2-nistp256 Ecdh-sha2-nistp384 Ecdh-sha2-nistp521	Default If connection problems with SSH clients (TeraTerm, PuTTY, STS) occur with the setting "`high`", this may be because the SSH clients do not support the exchange algorithms of the setting "`high`". Make sure that you are using the current versions of the SSH clients.

Result

The level of the exchange algorithm for SSH keys has been specified.

Additional notes

The supported SSH key exchange algorithms are listed with the command `show ip ssh`.

8.11.2.4 ssh-server port

Description

With this command, you specify the port for SSH access to the CLI.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ssh-server port <port-number(1024-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
port-number	Value for SSH port	1024 ... 65535 Default: 22 (standard port)

Note

Used ports

Some ports are permanently reserved. Make sure that the specified port is not already in use. You can find the ports used in the "List of available services".

Result

The port for SSH access has been changed. Access the CLI with the changed port.

Additional notes

You reset the port to the standard port with the `no ssh-server port` command.

8.11.2.5 no ssh-server port

Description

With this command, you reset the port to the standard port.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ssh-server port
```

Result

The port is reset to the standard port 22.

Additional notes

You configure the port for SSH access with the `ssh-server port.` command

Layer 2 management protocols

9

This part contains the sections that cover the following topics:

- GARP
- IGMP Snooping and IGMP Querying
- Redundancy
  - Ring redundancy
  - Standby redundancy
  - Link Check
  - MRP Interconnection

9.1 GARP

This section describes commands of the following protocols:

- GARP - Generic Attribute Registration Protocol
- GMRP - GARP Multicast Registration Protocol
- GVRP - GARP VLAN Registration Protocol

Timer

The following timers are set in the protocols mentioned above. The timer values are not configurable.

Timer	Description	Factory setting
Join-time	Time in milliseconds that passes between the transfer of two PDUs (Protocol Data Unit)	200 ms
Leave-time	Time period of the timer in milliseconds before the device changes its GARP status The timer starts and runs backwards with the defined time as soon as the device sends or receives a "Leave-all-time" message. The timer is stopped when the device receives a Join message.	600 ms
Leave-all-time	Time period of the timer in milliseconds before all devices change their GARP status	10000 ms

In devices connected via Layer 2, the same values must be set for the GARP/GMRP timer. If different values are set with the GARP/GMRP timers, GARP applications such as GMRP and GVRP cannot be executed successfully.

9.1.1 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.1.1.1 gmrp

Description

With this command, you enable the GMRP function for all or individual interfaces on the device.

Requirement

You are in the Global configuration mode

or

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config)#
cli (config-if-$$$) #
```

Syntax

Call the command without parameters:

```
gmrp
```

Result

In the Global configuration mode: The GMRP function is enabled on the device.

In the Interface configuration mode: The GMRP function is enabled for this interface.

Further notes

You need to enable GMRP globally for this device before you enable GMRP for individual interfaces.

If you want to enable or disable the function for a specific interface on the device, use the `no gmrp` command in the Interface configuration mode.

You can display the status of this function and other information with the `show vlan device info` command.

9.1.1.2 no gmrp

Description

With this command, you disable the GMRP function for all or individual interfaces on the device.

Requirement

You are in the Global configuration mode

or

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config)#
cli (config-if-$$$) #
```

Syntax

Call the command without parameters:

```
no gmrp
```

Result

In the Global configuration mode: The GMRP function is disabled on the device.

In the Interface configuration mode: The GMRP function is disabled for this interface.

Further notes

If you want to enable the function for a specific interface on the device, use the `gmrp` command.

You can display the status of this function and other information with the `show vlan device info` command.

9.1.1.3 gvrp

Description

With this command, you enable the GVRP function for all or individual interfaces on the device.

Requirement

You are in the Global configuration mode

or

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config)#
cli (config-if-$$$) #
```

Syntax

Call the command without parameters:

```
gvrp
```

Result

In the Global configuration mode: The GVRP function is enabled on the device.

In the Interface configuration mode: The GVRP function is enabled for this interface.

Further notes

If you have enabled the GARP module, you start GVRP explicitly with this command.

If you want to disable the function for a specific interface on the device, use the `no gvrp` command.

You can display the status of this function and other information with the `show vlan device info` command.

9.1.1.4 no gvrp

Description

With this command, you disable the GVRP function for all or individual interfaces on the device.

Requirement

You are in the Global configuration mode

or

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config)#
cli (config-if-$$$) #
```

Syntax

Call the command without parameters:

`no gvrp`

Result

In the Global configuration mode: The GVRP function is disabled on the device.

In the Interface configuration mode: The GVRP function is disabled for this interface.

Further notes

If you want to enable the function for a specific interface on the device, use the `gvrp` command.

You can display the status of this function and other information with the `show vlan device info` command.

9.2 IGMP snooping

This section describes the snooping functionality of the Internet Group Management Protocol.

9.2.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.2.1.1 show ip igmp snooping

Description

This command shows information about IGMP snooping for all or a selected VLAN.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode or in the Global configuration mode.

The command prompt is as follows:

`cli>` or `cli#` or `cli(config)#`

Syntax

Call up the command with the following parameters:

```
show ip igmp snooping [vlan <vlan-id (1-4094)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The information about IGMP snooping is displayed.

9.2.1.2 show ip igmp snooping forwarding-database

Description

This command shows the multicast forwarding entries for all or a selected VLAN. Optionally, only statically configured or dynamically learned multicast groups can be displayed.

Requirement

- IGMP snooping is enabled on the device
- You are in the User EXEC mode or Privileged EXEC mode.
  The command prompt is:
  `cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show ip igmp snooping forwarding-database [vlan <vlan-id (1-4094)>]
[{static | dynamic}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094
static	Only the statically configured multicast groups are displayed.	-
dynamic	Only the groups learned dynamically over the IGMP configuration are displayed.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The multicast forwarding entries are displayed.

9.2.1.3 show ip igmp snooping globals

Description

This command shows an overview of the settings of IGMP snooping.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call the command without parameter assignment:

```
show ip igmp snooping globals
```

Result

The settings are displayed.

9.2.1.4 show ip igmp snooping groups

Description

This command shows information about IGMP snooping for all or a selected VLAN.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode or in the Global configuration mode.

The command prompt is as follows:

`cli>` or `cli#` or `cli(config)#`

Syntax

Call up the command with the following parameters:

```
show ip igmp snooping groups [vlan <vlan-id (1-4094)> [Group
<Address>]] [{static | dynamic}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094
Group		
Address		
-		• static • dynamic

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The information about IGMP snooping is displayed.

9.2.1.5 show ip igmp snooping mrouter

Description

This command shows the ports at which IGMP queriers are connected for all or a selected VLAN..

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
show ip igmp snooping mrouter [vlan <vlan-id (1-4094)>] [detail]
```

The parameters have the following meaning:

Parameters	Description	Range of values
vlan	Keyword for a VLAN or VLAN range	-
vlan-id	Number of the addressed VLAN or VLAN range	1 ... 4094
detail	Specifies that detailed information is displayed.	-

Result

A list of the active ports is displayed.

9.2.1.6 show ip igmp snooping statistics

Description

This command shows the statistical information about IGMP snooping for all or a selected VLAN.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show ip igmp snooping statistics [vlan <vlan-id (1-4094)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The statistical information is displayed.

9.2.1.7 show ip igmp snooping switch-ip

Description

This command shows the IP address of the source for IGMP snooping.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ip igmp snooping switch-ip
```

Result

The IP address is displayed.

9.2.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.2.2.1 ip igmp snooping clear counters

Description

With this command, you delete the counters for all or a selected VLAN.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip igmp snooping clear counters [vlan <vlanid (1-4094)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN connection	-
`vlanid`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select a VLAN, the counters of all VLANs will be deleted.

Result

The counters are deleted.

9.2.2.2 ip igmp snooping port-purge-interval

Description

The time after which a port is deleted from the list if no IGMP router control packets are received is known as the purge time.

With this command, you configure this purge time for a port for a VLAN in seconds.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip igmp snooping port-purge-interval <(130 - 1225) seconds>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
-	Value for the purge time in seconds	130 ... 1225 Default: 300

Result

The purge time is configured.

Additional notes

You can reset the setting to the default with the `no ip igmp snooping port-purge-interval` command.

You can display the status of this function and other information with the `show ip igmp snooping globals` command.

9.2.2.3 no ip igmp snooping port-purge-interval

Description

With this command, you reset the setting for the purge time to the default value.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip igmp snooping port-purge-interval
```

Result

The purge time is reset to the default value.

Further notes

You configure the setting with the `ip igmp snooping port-purge-interval` command.

You can display the status of this function and other information with the `show ip igmp snooping globals`command.

9.2.2.4 ip igmp snooping report-forward

Description

With this command, you configure the ports to which IGMP reports are forwarded.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip igmp snooping report-forward {all-ports | router-ports | non-
edge-ports}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`all-ports`	The device forwards IGMP reports to all ports.	-
`router-ports`	The device forwards IGMP reports only to router ports.	Default setting
`non-edge-ports`	The device forwards IGMP reports only to those ports that are not Edge ports.	-

Result

The forwarding of IGMP reports is configured.

Additional notes

You display the status of this function and other information with the `show ip igmp snooping globals` command.

You disable the forwarding of IGMP reports with the `no ip igmp snooping report-forward` command.

9.2.2.5 no ip igmp snooping report-forward

Description

With this command, you enable the default setting for forwarding of IGMP reports. The device forwards IGMP reports only to router ports.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip igmp snooping report-forward
```

Result

The forwarding of IGMP reports is disabled.

Additional notes

You display the status of this function and other information with the `show ip igmp snooping globals` command.

You configure the forwarding of IGMP reports with the `ip igmp snooping report-forward` command.

9.2.2.6 ip igmp snooping send-query

Description

With this command, you enable sending of additional IGMP queries on topology changes.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:
`ip igmp snooping send-query`

Result

Additional IGMP queries are sent on topology changes.

Additional notes

You disable the setting with the `no ip igmp snooping send-query` command.

9.2.2.7 no ip igmp snooping send-query

Description

With this command, you disable sending of additional IGMP queries on topology changes.

In large Spanning Tree topologies, the sending of additional IGMP queries can lead to an undesired flood of queries.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:
`no ip igmp snooping send-query`

Result

No additional IGMP queries are sent on topology changes.

Additional notes

You enable the setting with the `ip igmp snooping send-query` command.

9.2.2.8 ip igmp snooping switch-ip

Description

With this command, you configure the IP address of the source for IGMP snooping queries.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
ip igmp snooping switch-ip <switch-ipaddr>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`switch-ipaddr`	Address of the source	Specify a valid IP address. Default: 0.0.0.0

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The IP address is configured.

9.2.2.9 ip igmp snooping version

Description

This command specifies which version of IGMP snooping the device will use. When shipped, the device uses IGMPv3.

Note

There is no separate show command to display the version of IGMP used by the device. This information is shown when you enter the `show ip igmp snooping` command in the User EXEC mode or in the Privileged EXEC mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ip igmp snooping version {v1 | v2 | v3}
```

The parameters have the following meaning:

Parameter	Description
v1	IGMPv1
v2	IGMPv2
v3	IGMPv3

Result

The version of IGMP snooping used by the device is specified.

9.2.2.10 ip igmp vlan-snooping

Description

With this command, you enable IGMP snooping for all VLANs.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`ip igmp vlan-snooping`

Result

IGMP snooping is enabled for all VLANs.

Further notes

You disable IGMP snooping with the `no ip igmp vlan-snooping` command.

9.2.2.11 no ip igmp vlan-snooping

Description

With this command, you disable IGMP snooping for all VLANs.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no ip igmp vlan-snooping`

Result

IGMP snooping is disabled for all VLANs.

Further notes

You enable IGMP snooping with the `ip igmp vlan-snooping` command.

9.2.2.12 snooping report-process config-level

Description

With this command, you configure which IGMP reports the device processes.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`snooping report-process config-level {non-router-ports | all-ports}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`non-router-ports`	The device only processes IGMP reports that were received by non-multicast router ports.	Default
`all-ports`	The device processes all IGMP reports.	-

Result

The processing of IGMP reports is configured.

Additional notes

You display the status of this function and other information with the `show ip igmp snooping globals` command.

9.2.3 Commands in VLAN configuration mode

This section describes commands that you can call up in the VLAN Configuration mode.

In global configuration mode, enter the `vlan $$$` command to change to this mode. When doing this, you need to replace the `$$$` placeholders with the relevant VLAN ID.

Commands relating to other topics that can be called in the VLAN Configuration mode can be found in the relevant sections.

- If you exit the VLAN Configuration mode with the `exit` command, you return to the Global Configuration mode.
- If you exit the VLAN Configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in VLAN configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.2.3.1 ip igmp snooping

Description

With this command, you enable the function IGMP Snooping for a VLAN.

Requirement

You are in VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call the command without parameters:

```
ip igmp snooping
```

As default the function is "disabled".

Result

The IGMP Snooping function is enabled for the specified VLAN.

Additional notes

You disable the function IGMP Snooping for a VLAN with the `no ip igmp snooping` command.

You display the status of this function and other information with the `show ip igmp snooping` command.

9.2.3.2 no ip igmp snooping

Description

With this command, you disable the function IGMP Snooping for a VLAN.

Requirement

You are in VLAN configuration mode.

The command prompt is as follows:

`cli(config-vlan-$$$)#`

Syntax

Call the command without parameters:

`no ip igmp snooping`

As default the function is "disabled".

Result

The IGMP Snooping function is disabled for the specified VLAN.

Additional notes

You enable the function IGMP Snooping for a VLAN with the `ip igmp snooping` command.

You display the status of this function and other information with the `show ip igmp snooping` command.

9.3 IGMP querier

This section describes the commands for the query functionality of the Internet Group Management Protocol (IGMP).

9.3.1 Commands in the Global Configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.3.1.1 ip igmp snooping querier

Description

With this command, you configure the IGMP snooping switch as querier.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip igmp snooping querier
```

As default the function is "disabled".

Result

The IGMP snooping switch is configured as querier.

Further notes

You delete the setting with the `no ip igmp snooping querier` command.

You can display the status of this function and other information with the `show ip igmp snooping` command.

9.3.1.2 no ip igmp snooping querier

Description

With this command, you delete the configuration of an IGMP snooping switch as querier.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no ip igmp snooping querier`

Result

The configuration of the IGMP snooping switch as querier is deleted.

Further notes

You configure the setting with the `ip igmp snooping querier` command.

You can display the status of this function and other information with the `show ip igmp snooping` command.

9.3.2 Commands in VLAN configuration mode

9.3.2.1 Introductory sentence for the VLAN configuration mode

This section describes commands that you can call up in the VLAN Configuration mode.

In global configuration mode, enter the `vlan $$$` command to change to this mode. When doing this, you need to replace the `$$$` placeholders with the relevant VLAN ID.

Commands relating to other topics that can be called in the VLAN Configuration mode can be found in the relevant sections.

- If you exit the VLAN Configuration mode with the `exit` command, you return to the Global Configuration mode.
- If you exit the VLAN Configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in VLAN configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.3.2.2 ip igmp snooping querier

Description

With this command, you enable the function IGMP Snooping Querier for a VLAN.

Requirement

You are in VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call the command without parameters:

```
ip igmp snooping querier
```

As default the function is "disabled".

Result

The IGMP Snooping Querier function is enabled for the specified VLAN.

Additional notes

You disable the function IGMP Snooping Querier for a VLAN with the `no ip igmp snooping querier` command.

You display the status of this function and other information with the `show ip igmp snooping` command.

9.3.2.3 no ip igmp snooping querier

Description

With this command, you disable the function IGMP Snooping Querier for a VLAN.

Requirement

You are in VLAN configuration mode.

The command prompt is as follows:

```
cli(config-vlan-$$$)#
```

Syntax

Call the command without parameters:

```
no ip igmp snooping querier
```

Result

The IGMP Snooping Querier function is disabled for the specified VLAN.

Additional notes

You enable the function IGMP Snooping Querier for a VLAN with the `ip igmp snooping querier` command.

You display the status of this function and other information with the `show ip igmp snooping` command.

9.4 Ring redundancy and standby connection

Note

Avoiding bad configurations

When using the commands in this section, you should take particular care because a bad configuration of this function can have serious negative affects on the network.

Ring redundancy

The ring redundancy function allows several devices to be interconnected in a ring structure. Since such a topology is not supported in normal network operation, such rings are logically disconnected using the Media Redundancy Protocol (MRP) or the High Speed Redundancy Protocol (HRP). If one component fails, all other elements of the ring can still be reached.

The device that logically disconnects the ring is known as the redundancy manager (RM).

The simple structure of the individual rings allows shorter reaction times if disruptions occur:

- MRP approx. 200 ms
- HRP approx. 300 ms

Complex network topologies cannot be set up with this function.

Standby (HRP)

Two network segments can be connected redundantly in each case via two links (master, slave). This function is known as the standby connection.

With it, the links of the interfaces of the master device are active and the links of the interfaces of the slave device are inactive.

Note

Position of master and slave device

The master and slave device of a standby connection (link pair between different structures of the ring redundancy) must be located in the same ring.

Note

Restriction in redundant linking of multiple HRP network segments

When linking multiple network segments over standby redundancy, make sure that the standby master and standby slave are located in a closed network segment, a HRP ring.

Otherwise, in the event of an error, there may be circulating frames that cause a failure in the network.

Link Check

With the Link Check function, you can monitor the transmission quality of optical sections within an HRP or MRP ring, identify disturbed connections and under certain conditions turn them off. When the disturbed section is turned off, the redundancy manager can close the ring and restore communication.

NOTICE
Make sure that the frames used by Link Check for monitoring the optical connections are not supplanted by an overload of high-priority frames in the network. An overload of high priority frames can be caused by the following, for example: • Network loops that can cause duplication of the high-priority frames • Changing the priorities for forwarding frames

9.4.1 clear hrp counters

Description

With this command, you reset the HRP counters.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
clear hrp counters
```

Result

The HRP counters have been reset.

9.4.2 clear interconnection counters

Description

This command deletes the counters for the MRP Interconnection interruptions.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call the command without parameters:

```
clear interconnection counters
```

Result

The counters for the MRP Interconnection interruptions are reset.

9.4.3 clear ring-redundancy manager counters

Note

This command can only be executed when the ring redundancy mode "HRP Manager" is configured.

Description

With this command, you reset the following counters:

- How often the device as redundancy manager switched to the active status. With this status change, the redundancy manager opens its blocked port because it no longer receives its sent RM frames.
- The maximum delay time of the test frames of the redundancy manager.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
clear ring-redundancy manager counters
```

Result

The counters are reset.

9.4.4 clear standby counter

Description

With this command, you reset the counters of the standby function.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
clear standby counter
```

Result

The standby counter is reset.

9.4.5 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.4.5.1 show hrp counters

Description

With this command, you display the following information:

- How often the device as redundancy manager switched to the active status, i.e. opened its blocked port because it no longer receives its sent RM frames.
- The maximum delay time of the test frames of the redundancy manager.
- How often the IE switch has changed the standby status from "Passive" to "Active".

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show hrp counters
```

Result

The counters are displayed.

9.4.5.2 show linkcheck

Description

With this command you show the following information on the link check:

- The ring ports on which you can enable Link Check
- The current status
- The statistics of sent and received Link Check frames of the monitored connections.

Note

If you use Link Check together with a redundancy protocol (e.g. HRP), the values for the sent and received Link Check frames can be different.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show linkcheck
```

Result

The current information is displayed.

9.4.5.3 show ring-redundancy

Description

With this command, you show the current configuration of the ring redundancy and standby functions.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ring-redundancy
```

Result

The current configurations are displayed.

9.4.5.4 show ring-redundancy manager counters

Description

With this command, you display the following information:

- How often the device as redundancy manager switched to the active status, i.e. opened its blocked port because it no longer receives its sent RM frames.
- The maximum delay time of the test frames of the redundancy manager.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show ring-redundancy manager counters
```

Result

The counters are displayed.

9.4.6 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.4.6.1 ring-redundancy configuration

Description

With this command, you change to the Redundancy Configuration mode.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

```
ring-redundancy configuration
```

Result

You are now in the Redundancy Configuration mode.

The command prompt is as follows:

```
cli(config-red)#
```

Further notes

You exit the Redundancy Configuration mode with the `end` or `exit` command.

9.4.6.2 ring-redundancy restore-default

Description

This command resets the configuration of redundant rings to factory settings. The "Multi-redundancy manager" configuration option is disabled.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ring-redundancy restore-default
```

Result

The configuration of the ring redundancy corresponds to the factory settings.

Additional notes

You can display the status of this function and more information with the `show ring-redundancy` command.

9.4.6.3 ring-redundancy hrpobserver

Description

With this command, you enable the observer or restart it.

The “observer” function is only available in HRP rings. The observer monitors malfunctions of the redundancy manager or incorrect configurations of an HRP ring.

If the observer is enabled, it can interrupt the connected ring if errors are detected. To do this, the observer switches a ring port to the "blocking" status. When the error is resolved, the observer enables the port again.

If numerous errors occur in quick succession, the observer no longer enables its port automatically. The ring port remains permanently in the "blocking" status. This is signaled by the error LED and a message text. After the errors have been eliminated, you can enable the port again with this command and the parameter `restart`.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ring-redundancy hrpobserver [restart]
```

The parameters have the following meaning:

Parameter	Description
`restart`	Restarts the observer.

If you do not specify the optional parameter, the observer is enabled.

Result

The observer is enabled or restarted.

Further notes

You disable the observer with the `no ring-redundancy hrpobserver` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.6.4 no ring-redundancy hrpobserver

Description

With this command, you disable the observer.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`no ring-redundancy hrpobserver`

Result

The observer is disabled.

Further notes

You enable the observer with the `ring-redundancy hrpobserver` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.6.5 ring-redundancy mode

Description

With this command, you enable the ring redundancy function on a device.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command with the following parameters:

`ring-redundancy mode { ard | mrpauto | mrpclient | hrpclient | hrpmanager }`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ard`	Enables the automatic redundancy mode (Automatic Redundancy Detection).	• Default setting with PROFINET variants: enabled • Default setting with EtherNet/IP variants: disabled • Default setting with Industrial Ethernet variants: disabled
`mrpauto`	Enables the automatic MRP manager.	-
`mrpclient`	Enables ring redundancy with the MRP protocol as client.	-
`hrpclient`	Enables ring redundancy with the HRP protocol as client.	-
`hrpmanager`	Enables ring redundancy with the HRP protocol in redundancy manager mode.	-

Result

The ring redundancy function is enabled and the redundancy mode is selected.

Additional notes

You disable the ring redundancy function with the `no ring-redundancy` command.

9.4.6.6 no ring-redundancy

Description

With this command, you disable the ring redundancy function on a device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no ring-redundancy`

Result

The ring redundancy function is disabled.

Further notes

You enable the ring redundancy function with the `ring-redundancy mode` command.

9.4.6.7 ring-redundancy dna-redundancy

Description

With this command, you enable Dual Network Access redundancy (DNA redundancy) on the device.

Requirements

- You are in global configuration mode.
  The command prompt is:
  `cli(config)#`
- The device must be configured as MRP manager or MRP client. DNA redundancy is only possible with MRP.

Syntax

Call the command without parameters:

```
ring-redundancy dna-redundancy
```

Result

DNA Redundancy is enabled.

Additional notes

You disable DNA Redundancy with the `no ring-redundancy dna-redundancy` command.

You display the current configuration of the ring redundancy with the `show ring-redundancy` command.

9.4.6.8 no ring-redundancy dna-redundancy

Description

With this command, you disable Dual Network Access redundancy (DNA redundancy) on the device.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no ring-redundancy dna-redundancy`

Result

DNA Redundancy is disabled.

Additional notes

You enable DNA Redundancy with the `ring-redundancy dna-redundancy` command.

You display the current configuration of the ring redundancy with the `show ring-redundancy` command.

9.4.6.9 ring-redundancy standby

Description

With this command, you enable the standby function.

Requirement

- HRP is enabled
- You are in the Global configuration mode.
  The command prompt is:
  `cli(config)#`

Syntax

Call the command without parameters:

`ring-redundancy standby`

Result

The standby function is enabled.

Further notes

You disable the setting with the `no ring-redundancy standby` command.

You can display the status of this function and other information with the `show ring-redundancy`command.

9.4.6.10 no ring-redundancy standby

Description

With this command, you disable the standby function.

Requirement

- HRP is enabled
- You are in the Global configuration mode.
  The command prompt is:
  `cli(config)#`

Syntax

Call the command without parameters:

```
no ring-redundancy standby
```

Result

The standby function is disabled.

Further notes

You enable the setting with the `ring-redundancy standby` command.

You can display the status of this function and other information with the `show ring-redundancy`command.

9.4.6.11 ring-redundancy mrpinterconnection

Description

With this command, you enable MRP Interconnection for the device.

Requirement

You can only enable MRP Interconnection when the following requirements are met:

- Ring redundancy is enabled.
- "MRP Auto-Manager" or "MRP Client" is used as ring redundancy mode.
- There is an activated MRP Interconnection connection.

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ring-redundancy mrpinterconnection
```

Result

MRP Interconnection is enabled for the device.

Additional notes

You disable MRP Interconnection with the `no ring-redundancy mrpinterconnection` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.6.12 no ring-redundancy mrpinterconnection

Description

With this command, you disable MRP Interconnection for the device.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ring-redundancy mrpinterconnection
```

Result

MRP Interconnection is disabled for the device.

Additional notes

You enable MRP Interconnection with the `ring-redundancy mrpinterconnection` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.7 Commands in the redundancy configuration mode

This section describes commands that you can call up in the Redundancy Configuration mode.

In global configuration mode, enter the `ring-redundancy configuration` command to change to this mode.

- If you exit the Redundancy Configuration mode with the `exit` command, you return to the Global Configuration mode.
- If you exit the Redundancy Configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in redundancy configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.4.7.1 linkcheck

Description

With this command, you enable the Link Check function on a ring port and you can reset the function.

Note

Enable Link Check on only one of two connection partners. This can lead to incorrect behavior.

Note

If Link Check is enabled on all devices of a ring at the same time, and several connections within the ring have problems, this leads to fragmentation of the ring.

1. During commissioning enable the Link Check function for one connection section after the other by enabling Link Check for the two connection partners connected to a line.
2. To ensure an error-free connection, wait 1 min. before you enable Link Check for the next connection section.

Requirement

- You can only enable the Link Check function with optical ring ports of an HRP or MRP ring. For MRP rings, only the ring ID "1" is supported.
- You cannot enable Link Check for ports with a transmission speed of 10 Gbps.
- Link Check must be enabled on two neighboring devices (connection partners) within an HRP or MRP ring.
- The ring ports on which you enable Link Check must be connected together.
- You are in the Redundancy configuration mode.
  The command prompt is as follows:
  `cli(config-red)#`

Syntax

Call the command with the following parameters:

```
linkcheck {<interface-type> <interface-id>} [reset]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`reset`	After resetting Link Check, the function is restarted on the port and the statistics are reset. If you use the `reset` parameter, the reset must be performed on both connection partners within 30 s.	When you use the `reset` parameter, loops can form temporarily resulting in a loss of data traffic. The loop is automatically cleared again. If this is not acceptable for your application, reset Link Check by pulling the connecting cable and plugging it in again.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

Link Check is activated on the port.

Additional notes

You disable the function with the `no linkcheck` command.

You can display the status of this function and other information with the `show linkcheck` command.

With the `event config` command, you can configure so that you are informed of a status change by a message.

9.4.7.2 no linkcheck

Description

With this command, you disable the Link Check function on a port.

Requirement

You are in the Redundancy configuration mode.

The command prompt is as follows:

```
cli(config-red)#
```

Syntax

Call up the command with the following parameters:

```
no linkcheck {<interface-type> <interface-id>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

Link Check is deactivated on the port.

Further notes

You enable the function and reset the count with the `linkcheck` command.

You can display the status of this function and other information with the `show linkcheck` command.

9.4.7.3 ring ports

Description

With this command, you configure the ports of the ring redundancy manager or ring redundancy client on a device.

- **Redundancy manager**
  - In the normal status, the network structure is operated via port. The other port is only used by the ring redundancy manager for checking.
  - If there is a disruption, the two parts of the ring operate via both ports.
- **Redundancy client**
  - The client forwards all frames of the redundancy manager to the ring ports.

Requirement

- The ports are disabled in Spanning Tree.
- You are in Redundancy configuration mode.
  The command prompt is as follows:
  `cli(config-red)#`

Syntax

Call the command with the following parameters:

```
ring ports {<interface-type> <interface-id>} {<interface-type>
<interface-id>}
```

The parameters have the following meaning:

Parameter	Description
`interface-type`	Specifies the interface type for the first ring port.
`interface-id`	Specifies the number of the interface for the first ring port.
`interface-type`	Specifies the interface type for the second ring port.
`interface-id`	Specifies the number of the interface for the second ring port.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Note

Differing port addresses

The first and second port must be configured on different interfaces.

Port groups for devices with more than 8 ports

The ring ports of an MRP ring should belong to the same logical port group.

XB-200

Device	Article number	Port group
SCALANCE XB216	6GK5 216-0BA00-2AB2 6GK5 216-0BA00-2TB2	**Group 1** Port 1 ... Port 8 **Group 2** Port 9 ... Port 16
SCALANCE XB213-3 (SC)	6GK5 213-3BD00-2AB2 6GK5 213-3BD00-2TB2	
SCALANCE XB213-3 (ST/BFOC)	6GK5 213-3BB00-2AB2 6GK5 213-3BB00-2TB2	
SCALANCE XB213-3LD	6GK5 213-3BF00-2AB2 6GK5 213-3BF00-2TB2	

XC-200

Device	Article number	Port group
SCALANCE XC216	6GK5 216-0BA00-2AC2	**Group 1** Port 1 ... Port 4 Port 9 ... Port 12 **Group 2** Port 5 ... Port 8 Port 13 ... Port 16
SCALANCE XC216 EEC	6GK5 216-0BA00-2FC2	
SCALANCE XC224	6GK5 224-0BA00-2AC2	**Group 1** Port 1 ... Port 8 **Group 2** Port 9 ... Port 12 Port 17 ... Port 20 **Group 3** Port 13 ... Port 16 Port 21 ... Port 24

XP-200

Device	Article number	Port group
SCALANCE XP216	6GK5 216-0HA00-2AS6	**Group 1** Port 1 ... Port 5, Port 7 **Group 2** Port 6, Port 8, Port 9, Port 11, Port 13, Port 15 **Group 3** Port 10, Port 12 Port 14, Port 16
SCALANCE XP216	6GK5 216-0HA00-2TS6	
SCALANCE XP216 EEC	6GK5 216-0HA00-2ES6	
SCALANCE XP216 PoE EEC	6GK5 216-0UA00-5ES6	

XR-300WG

Device	Article number	Port group
SCALANCE XR324WG	6GK5 324-0BA00-2AR3	**Group 1** Port 1 ... Port 4 Port 13 ... Port 16 **Group 2** Port 5 ... Port 8 Port 17 ... Port 20 **Group 3** Port 9 ... Port 12 Port 21 ... Port 24
SCALANCE XR324WG	6GK5 324-0BA00-3AR3	
SCALANCE XR328-4C WG	6GK5 328-4FS00-2AR3	**Group 1** Port 1 ... Port 4 Port 13 ... Port 16 **Group 2** Port 5 ... Port 8 Port 17 ... Port 20 **Group 3** Port 9 ... Port 12 Port 21 ... Port 24 **Group 4** Port 25 ... Port 28
SCALANCE XR328-4C WG	6GK5 328-4FS00-2RR3	
SCALANCE XR328-4C WG	6GK5 328-4FS00-3AR3	
SCALANCE XR328-4C WG	6GK5 328-4FS00-3RR3	
SCALANCE XR328-4C WG	6GK5 328-4SS00-2AR3	
SCALANCE XR328-4C WG	6GK5 328-4SS00-3AR3	

Note

Forwarding RSPAN stream

If the device is to forward RSPAN streams, two requirements must be met:

- Input port and output port must belong to the same port group.
- The "Learning" function must be disabled for the input port. This is only possible with the CLI command **no unicast mac learning**.

H-Sync

H-Sync is a Layer 2 protocol with which process data is synchronized via PROFINET in systems with redundant control.

The two controllers are connected redundantly via an MRP ring. The controllers must be directly connected with one another on a path. Both controllers are configured as "MRP Auto-Manager", so one of the controllers becomes MRP manager. All other devices in the ring are MRP clients. The two controllers send H-Sync frames in both directions of the ring (Provider). H-Sync frames that they receive are not forwarded (Consumer). All other devices in the ring only forward the H-Sync frames between their ring ports in both directions (Forwarder). The H-Sync frames are filtered on all other ports.

H-Sync is a transparent protocol for the IE switches. For information on which IE switches can be used as H-Sync forwarder, refer to the section "System functions and hardware equipment".

You only configure H-Sync via STEP 7 Basic or Professional. However, note that settings deviating from the following rules can result in complications in configuration:

- Redundancy mode: MRP Client
- Ring ports:
  - Use the ring ports preset in the factory.
  - Use the first two optical interfaces.
  - Use the first two gigabit interfaces.
  - Use Port 1 and Port 2.

Result

The ports of the ring redundancy are configured.

9.4.7.4 standby connection-name

Description

With this command, you assign a name to the standby connection on the device.

Requirement

You are in the Redundancy configuration mode.

The command prompt is as follows:

```
cli(config-red)#
```

Syntax

Call up the command with the following parameters:

```
standby connection-name <string(32)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
<string(32)>	Name of the connection	max. 32 characters

Result

The standby connection is assigned a name.

9.4.7.5 no standby connection-name

Description

With this command, you delete the name of a standby connection.

Requirement

You are in the Redundancy Configuration mode.

The command prompt is as follows:

```
cli(config-red)#
```

Syntax

Call the command without parameters:

```
no standby connection-name
```

Result

The name of the standby connection is deleted.

9.4.7.6 standby force-master

Description

With this command, you assign the role of standby master to the device, if the standby partner has not already been configured as master.

Requirement

- HRPis enabed
- You are in the Redundancy configuration mode.
  The command prompt is as follows:
  `cli(config-red)#`

Syntax

Call the command without parameters:

```
standby force-master
```

Result

The standby force-master function is enabled.

Additional notes

You disable the setting with the `no standby force-master` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.7.7 no standby force-master

Description

With this command, you disable the standby force-master function.

Requirement

- HRPis enabed
- You are in the Redundancy configuration mode.
  The command prompt is as follows:
  `cli(config-red)#`

Syntax

Call the command without parameters:

```
no standby force-master
```

Result

The standby force-master function is disabled.

Additional notes

You enable the setting with the `standby force-master` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.7.8 standby port

Description

With this command, you configure and enable the port for a standby connection on a device.

Requirement

- The ports are disabled in spanning tree.
- You are in the Redundancy configuration mode.
  The command prompt is as follows:
  `cli(config-red)#`

Syntax

Call up the command with the following parameters:

```
standby port {<interface-type> <interface-id>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The port for a standby connection is configured and enabled.

Further notes

You disable the setting with the `no standby port` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.7.9 no standby port

Description

With this command, disable the port for a standby connection on a device.

Requirement

You are in the Redundancy configuration mode.

The command prompt is as follows:

`cli(config-red)#`

Syntax

Call up the command with the following parameters:

```
no standby port {<interface-type><interface-id>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The ports for a standby connection are disabled.

Further notes

You enable the setting with the `standby port` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.7.10 standby wait-for-partner

Description

With this command, you enable the "Wait for standby partner" function on the device. A standby connection is enabled only after the standby master and the standby slave as well as their standby partners have established a connection. This ensures that the redundant connection is really available before communication via a standby connection is enabled. As default, this function is enabled.

With an optional parameter, you can also define a specific period for the timeout. In this case, the standby connection is only enabled after the defined wait time.

Requirement

You are in the Redundancy configuration mode.

The command prompt is as follows:

```
cli(config-red)#
```

Syntax

Call up the command with the following parameters:

```
standby wait-for-partner [timeout <milliseconds(1-60000)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`timeout`	Keyword for the timeout	-
`milliseconds`	Duration of the timeout in milliseconds	1 ... 60000

Result

The "Wait for standby partner" function is enabled.

9.4.7.11 no standby wait-for-partner

Description

With this command, you disable the "Wait for standby partner" function on the device. A standby connection is enabled even if the standby master has not yet established a connection to the standby slave.

Requirement

You are in the Redundancy configuration mode.

The command prompt is as follows:

```
cli(config-red)#
```

Syntax

Call the command without parameters:

```
no standby wait-for-partner
```

Result

The "Wait for standby partner" function is disabled.

9.4.7.12 ringid

Description

With this command, you specify the ID of the ring you want to configure and switch to the configuration mode for MRP multiple rings.

Requirement

- You are in the Redundancy configuration mode.
  The command prompt is as follows:
  `cli(config-red)#`

Syntax

Call the command with the following parameters:

`ringid <table entry idx (1-4)>`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`table entry idx`	The ring ID	1 ... 4

Result

The ring ID is configured. You are in the configuration mode for MRP multiple rings. The command prompt is as follows:
`cli(config-red-ringid-<idx>)#`

The placeholder <idx> stands for the index of the table entry, for example, the command prompt for the index 2:
`cli(config-red-ringid-2)#`

9.4.7.13 mrpinterconnection

Description

With this command, you create or change an MRP Interconnection connection. At the same time, you switch to MRP Interconnection configuration mode.

Requirement

You are in the Redundancy configuration mode.

The command prompt is as follows:

`cli(config-red)#`

Syntax

Call up the command with the following parameters:

`mrpinterconnection <table entry idx (1-64)>`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`table entry idx`	Index of an existing connection or one that has to be newly created in the MRP Interconnection table.	1 ... 64

Result

A new MRP Interconnection connection was created if a connection with the specified index did not exist yet. You are in the MRP Interconnection configuration mode. The command prompt is as follows:

```
cli(config-red-mrpin-<idx>)#
```

The placeholder <idx> stands for the index of the table entry, for example, the command prompt for the index 2 is `cli(config-red-mrpin-2)#`.

9.4.7.14 no mrpinterconnection

Description

With this command, you delete an MRP Interconnection connection.

Requirement

You are in the Redundancy configuration mode.

The command prompt is as follows:

```
cli(config-red)#
```

Syntax

Call up the command with the following parameters:

```
no mrpinterconnection <table entry idx (1-64)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`table entry idx`	Index of an existing connection in the MRP Interconnection table.	1 ... 64

Result

The MRP Interconnection connection with the specified index was deleted.

9.4.8 Commands in the configuration mode for MRP multiple rings

This section describes commands that you can call up in the Configuration mode for MRP multiple rings.

In redundancy configuration mode, enter the `ringid <table entry idx (1-4)>` command to change to this mode. The parameter `table entry idx (1-4)` stands for the index of an existing MRP ring or one that has to be newly created.

- When you exit the Configuration mode for MRP multiple rings with the `exit` command, you return to the Redundancy configuration mode.
- When you exit the Redundancy configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC mode with the `do [command]` in the Configuration mode for MRP multiple rings. To do this, you replace `[command]` with the command that you want to execute.

9.4.8.1 mode

Description

With this command, you configure the operating mode "MRP Manager" for the ring redundancy.

Note

When you configure multiple redundant rings, you need to select the "MRP Manager" ring redundancy mode for each ring.

Requirement

- You are in the Configuration mode for MRP multiple rings.
  The command prompt is as follows:
  `cli(config-red-ringid-<idx>)#`
  The placeholder <idx> stands for the index of the table entry.

Syntax

Call the command with the following parameters:
`mode {off | mrpmanager}`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`off`	For the ring redundancy, the "MRP Manager" operating mode is disabled.	-
`mrpmanager`	For the ring redundancy, the "MRP Manager" operating mode is configured.	-

Result

For the ring redundancy, the "MRP Manager" operating mode is configured or disabled.

9.4.8.2 ring ports

Description

With this command, you configure the ring ports.

Requirement

- You are in the Configuration mode for MRP multiple rings.
  The command prompt is as follows:
  `cli(config-red-ringid-<idx>)#`
  The placeholder <idx> stands for the index of the table entry.

Syntax

Call the command with the following parameters:
`ring ports {<interface-type> <interface-id>} {<interface-type> <interface-id>}`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of first ring port.	Specify a valid interface.
`interface-id`	Module no. and port no. of the first ring port.	
`interface-type`	Type or speed of second ring port.	Specify a valid interface.
`interface-id`	Module no. and port no. of the second ring port.	

Result

The ring ports are configured.

9.4.8.3 domain-name

Description

With this command, you configure a domain name. Each name can only be assigned to one ring.

Note

If you configure multiple redundant rings, you cannot use the "default-mrpdomain" domain name for any of the rings.

Requirement

- You are in the Configuration mode for MRP multiple rings.
  The command prompt is as follows:
  `cli(config-red-ringid-<idx>)#`
  The placeholder <idx> stands for the index of the table entry.

Syntax

Call the command with the following parameters:

`domain-name <default-mrpdomain | mrpdomain-(1-4)>`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`default-mrpdomain`	A possible domain name when you only configure one redundant ring.	-
`mrpdomain-(1-4)`	The domain names when you configure multiple redundant rings.	mrpdomain-1 ... mrpdomain-4

Result

The domain name of the MRP ring is configured.

9.4.9 Commands in MRP Interconnection configuration mode

This section describes commands that you can call up in the MRP Interconnection configuration mode.

In redundancy configuration mode, enter the `mrpinterconnection <table entry index (1-64)>` command to change to this mode. The parameter `table entry index (1-64)` stands for the index of an existing connection or one that has to be newly created in the MRP Interconnection table .

- If you exit the MRP Interconnection configuration mode with the `exit` command, you return to the Redundancy configuration mode.
- If you exit the Redundancy configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in MRP Interconnection configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.4.9.1 domain-id

Description

With this command, you configure the ID of an MRP Interconnection connection. When specifying the ID, observe the following rules:

- The Interconnection domain ID cannot be 0.
- You need to configure the same Interconnection Domain ID for all four devices used for linking the rings.

Requirement

You are in the MRP Interconnection configuration mode.

The command prompt is as follows:

```
cli(config-red-mrpin-<idx>)#
```

The placeholder `<idx>` stands for the index of a connection in the MRP Interconnection table.

Syntax

Call up the command with the following parameters:

```
domain-id <interconnection-id (1-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`interconnection-id`	The ID of an MRP Interconnection connection.	1 ... 65535

Result

The MRP Interconnection connection was assigned the specified ID.

Additional notes

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.9.2 domain-name

Description

With this command, you configure the name of an MRP Interconnection connection. You can specify any name. The names of the devices used for linking the rings can also be different.

Requirement

You are in the MRP Interconnection configuration mode.

The command prompt is as follows:

```
cli(config-red-mrpin-<idx>)#
```

The placeholder `<idx>` stands for the index of a connection in the MRP Interconnection table.

Syntax

Call up the command with the following parameters:

```
domain-name <interconnection-domain-name (240)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`interconnection-domain-name`	The name of an MRP Interconnection connection.	Permitted characters: • 'A' ... 'Z' • 'a' ... 'z' • '0' ... '9' • The character '-', but not as first or last character. Length: 1 to 240 characters

Result

The MRP Interconnection connection was assigned the specified name.

Additional notes

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.9.3 Interface

Description

With this command, you configure the port for the MRP Interconnection connection. Be aware of the following restrictions:

- The port cannot be disabled or blocked. The "Unicast Blocking" function cannot be enabled for the port.
- The port cannot be used for a link aggregation.
- The port cannot be a monitor port of the "Mirroring" function.
- The port cannot be a Spanning Tree port.

- The port cannot be a ring port.
- The port cannot be a router port.
- The port cannot be an 802.1X Authenticator Port.
- The port cannot be an 802.1X Supplicant Port.

Requirement

You are in the MRP Interconnection configuration mode.

The command prompt is as follows:

```
cli(config-red-mrpin-<idx>)#
```

The placeholder `<idx>` stands for the index of a connection in the MRP Interconnection table.

Syntax

Call up the command with the following parameters:

```
interface {<interface-type> <interface-id>}
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The MRP Interconnection connection was assigned the specified interface.

Additional notes

You display the status of this function and other information with the `show ring-redundancy` command.

9.4.9.4 role

Description

With this command, you configure whether the device has the role of the client or the manager for an MRP Interconnection connection.

Requirement

You are in the MRP Interconnection configuration mode.

The command prompt is as follows:

```
cli(config-red-mrpin-<idx>)#
```

The placeholder `<idx>` stands for the index of a connection in the MRP Interconnection table.

Syntax

Call up the command with the following parameters:

```
role {manager | client}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`manager`	Keyword for the "Manager" role	-
`client`	Keyword for the "Client" role	-

Result

The MRP Interconnection connection was assigned the specified role.

Additional notes

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.9.5 client-position

Description

With this command, you configure the client position of an MRP Interconnection connection.

Requirement

You are in the MRP Interconnection configuration mode.

The command prompt is as follows:

```
cli(config-red-mrpin-<idx>)#
```

The placeholder `<idx>` stands for the index of a connection in the MRP Interconnection table.

Syntax

Call up the command with the following parameters:

`client-position {primary | secondary}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`primary`	Keyword for the "Primary" client position	In each ring, there is a client in the "Primary" position. The primary MRP Interconnection connection is established between these two clients.
`secondary`	Keyword for the "Secondary" client position	A device in the "Secondary" position is connected via an MRP Interconnection connection to the MRP Interconnection Manager.

Result

The MRP Interconnection connection was assigned the specified client position.

Additional notes

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.9.6 wait-manager

Description

With this command, you specify that the MRP Interconnection Manager waits with data transfer until the primary client for MRP Interconnection is ready.

Requirement

You are in the MRP Interconnection configuration mode.

The command prompt is as follows:

`cli(config-red-mrpin-<idx>)#`

The placeholder `<idx>` stands for the index of a connection in the MRP Interconnection table.

Syntax

Call the command without parameters:

`wait-manager`

Result

The waiting time for completion of the configuration is enabled.

Additional notes

You disable the waiting time for completion of the configuration with the `no wait-manager` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.9.7 no wait-manager

Description

With this command, you specify that the MRP Interconnection interface is put into the "Forwarding" state after 200 milliseconds regardless of the operating state of the primary client.

Requirement

You are in the MRP Interconnection configuration mode.

The command prompt is as follows:

```
cli(config-red-mrpin-<idx>)#
```

The placeholder `<idx>` stands for the index of a connection in the MRP Interconnection table.

Syntax

Call the command without parameters:

```
no wait-manager
```

Result

The waiting time for completion of the configuration is disabled.

Additional notes

You enable the waiting time for completion of the configuration with the `no wait-for-completion` command.

You can display the status of this function and other information with the `show ring-redundancy` command.

9.4.9.8 Interconnection

Description

With this command, you enable or disable the MRP Interconnection connection.

Requirement

You are in the MRP Interconnection configuration mode.

The command prompt is as follows:

```
cli(config-red-mrpin-<idx>)#
```

The placeholder `<idx>` stands for the index of a connection in the MRP Interconnection table.

Syntax

Call up the command with the following parameters:

```
interconnection {enable | disable}
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
`enable`	Enables the MRP Interconnection connection.	-
`disable`	Disables the MRP Interconnection connection.	-

Result

The MRP Interconnection connection was enabled or disabled.

Additional notes

You can display the status of this function and other information with the `show ring-redundancy` command.

9.5 Unicast

The commands in this section configure the procedures for handling Unicast frames.

The commands allow the following:

- Filtering of Unicast frames
- Blocking of ports
- Automatic learning of Unicast
- Blocking unknown Unicast frames.

With the "show" commands, you can display the configuration data.

With the following commands, note which "Base bridge mode" you are in. If you are in the "Transparent Bridge" mode, all settings relate to the management VLAN: VLAN 1.

You change the mode with the `base bridge-mode` command.

9.5.1 The "show" commands VLAN bridge)

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.5.1.1 show mac-address-table

Description

This command shows the table with the static and dynamic unicast MAC addresses and multicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table [vlan <vlan-range>] [address
<aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN or VLAN range	-
`vlan-range`	Number of the addressed VLAN or VLAN range	1 ... 4094 Enter the range limits with a hyphen or a space.
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The entries of the MAC addresses table are displayed.

9.5.1.2 show mac-address-table dynamic unicast

Description

This command shows the table with the dynamic unicast MAC addresses learned by the switch based on the MAC address of the sender of received frames on its Ethernet ports.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table dynamic unicast[vlan<vlan-range>]
     [address<aa:aa:aa:aa:aa:aa>][{interface<interface-type>
     <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN connection	-
`vlan-range`	Number of the addressed VLAN	1 ... 4094 Enter the range limits with a hyphen without spaces.
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The dynamic unicast MAC addresses are displayed.

9.5.1.3 show mac-address-table static unicast

Description

This command shows the table with the static unicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table static unicast[vlan<vlan-range>]
  [address<aa:aa:aa:aa:aa:aa>][{interface<interface-type><interface-
id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan`	Keyword for a VLAN connection	-
`vlan-range`	Number of the addressed VLAN	1 ... 4094 Enter the range limits with a hyphen without spaces.
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The static unicast MAC addresses are displayed.

9.5.1.4 show unicast-block config

Description

This command shows the unicast blocking settings for ports.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show unicast-block config [port <interface-type> <interface-id)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`port`	Keyword for a port description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

The unicast blocking settings for ports are displayed.

9.5.1.5 show unicast-mac flush config

Description

This command shows whether automatic deletion of the MAC address table in the event of a link-down is configured for a port. If you do not specify any interface name as parameter, the settings for all ports are displayed.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show unicast-mac flush config [port <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`port`	Keyword for a port description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

The settings of the ports for deleting the MAC address table are displayed.

9.5.1.6 show unicast-mac learning config

Description

This command indicates whether automatic unicast address learning is configured for a port. If you do not specify any interface name as parameter, the settings for all ports are displayed.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show unicast-mac learning config [port <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`port`	Keyword for a port description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

The port settings for unicast address learning are displayed.

9.5.2 Commands in the global configuration mode (VLAN bridge)

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.5.2.1 mac-address-table static unicast

Description

With this command, you generate a static unicast MAC address entry in the forwarding database.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
mac-address-table static  unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-
id(1-4094)>
interface ([<interface-type> <interface-list>] [<interface-type>
<interface-list>]
[port-channel <interface-list>])
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-list`	Module no. and port no. of the interface	

Parameter	Description	Range of values/note
`port-channel`	Keyword for a port-channel connection	Enter a valid port channel connection.
`interface-list`	Number of the addressed port channel	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry in the forwarding database is generated.

Additional notes

With the `show mac-address-table static unicast` command, you display the list of configured entries.

With the `no mac-address-table static unicast` command, you delete an entry.

9.5.2.2 no mac-address-table static unicast

Description

With this command, you delete a static unicast MAC address entry from the forwarding database.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no mac-address-table static unicast <aa:aa:aa:aa:aa:aa>
   vlan<vlan-id(1-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry is deleted from the forwarding database.

Further notes

With the `show mac-address-table static unicast` command, you display the list of configured entries.

With the `mac-address-table static unicast` command, you create an entry.

9.5.3 The "show" commands (Transparent Bridge)

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.5.3.1 show dot1d mac-address-table

Description

This command shows the table with the static and dynamic unicast entries and the dynamic multicast entries.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
show dot1d mac-address-table [address <aa:aa:aa:aa:aa:aa>]
     [{interface <interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	Specify a valid MAC address.
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The entries are displayed.

9.5.3.2 show dot1d mac-address-table static unicast

Description

This command shows the table with the static unicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show dot1d mac-address-table static unicast [address
<aa:aa:aa:aa:aa:aa>]
     [{interface <interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The static unicast MAC addresses are displayed.

9.5.3.3 show unicast-block config

Description

This command shows the unicast blocking settings for ports.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show unicast-block config [port <interface-type> <interface-id)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`port`	Keyword for a port description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

The unicast blocking settings for ports are displayed.

9.5.3.4 show unicast-mac flush config

Description

This command shows whether automatic deletion of the MAC address table in the event of a link-down is configured for a port. If you do not specify any interface name as parameter, the settings for all ports are displayed.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show unicast-mac flush config [port <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
port	Keyword for a port description	-
interface-type	Type or speed of the interface	Enter a valid interface
interface-id	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

The settings of the ports for deleting the MAC address table are displayed.

9.5.3.5 show unicast-mac learning config

Description

This command indicates whether automatic unicast address learning is configured for a port. If you do not specify any interface name as parameter, the settings for all ports are displayed.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show unicast-mac learning config [port <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
port	Keyword for a port description	-
interface-type	Type or speed of the interface	Enter a valid interface
interface-id	Module no. and port no. of the interface	

For information on names of interfaces and addresses, refer to the section "Addresses and interface names (Page 50)".

Result

The port settings for unicast address learning are displayed.

9.5.4 Commands in the global configuration mode (Transparent Bridge)

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.5.4.1 mac-address-table static unicast

Description

With this command, you generate a static unicast MAC address entry in the forwarding database.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
mac-address-table static unicast <aa:aa:aa:aa:aa:aa>  interface
([<interface-type>
<interface-list>]  [<interface-type> <interface-list>] [port-
channel <interface-list>])
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`interface`	Keyword for a an interface description	-

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-list`	Module no. and port no. of the interface	
`port-channel`	Keyword for a port-channel connection	Enter a valid port channel connection.
`interface-list`	Number of the addressed port channel	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry in the forwarding database is generated.

Additional notes

With the `show dot1d mac-address-table static unicast` command, you display the list of configured entries.

With the `no mac-address-table static unicast` command, you delete an entry.

9.5.4.2 no mac-address-table static unicast

Description

With this command, you delete a static unicast MAC address entry from the forwarding database.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no mac-address-table static unicast <aa:aa:aa:aa:aa:aa>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry is deleted from the forwarding database.

Further notes

With the `show dot1d mac-address-table static unicast` command, you display the list of configured entries.

With the `mac-address-table static unicast` command, you create an entry.

9.5.5 Commands in interface configuration mode

9.5.5.1 Introductory sentence for the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.5.5.2 unicast mac learning

Description

With this command, you enable the learning of unicast addresses for a port. These unicast addresses are entered in the FDB as dynamically learned addresses.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
unicast mac learning
```

Result

The automatic learning of unicast addresses is enabled.

Additional notes

You disable automatic learning of unicast addresses with the `no unicast mac learning` command.

You show the table with the dynamically learned unicast MAC addresses with the `show mac-address-table dynamic unicast` command.

9.5.5.3 no unicast mac learning

Description

With this command, you disable the automatic learning of unicast addresses.

Note

Forwarding RSPAN stream

If the device is to forward RSPAN streams, two requirements must be met:

- Input port and output port must belong to the same port group.
- The "Learning" function must be disabled for the input port. This is only possible with the CLI command **no unicast mac learning**.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no unicast mac learning
```

Result

The automatic learning of unicast addresses is disabled.

Additional notes

You enable automatic learning of unicast addresses with the `unicast mac learning` command.

You show the table with the dynamically learned unicast MAC addresses with the `show mac-address-table dynamic unicast` command.

9.6 Multicast

The commands in this section configure the procedures for handling Multicast frames.

The commands allow the following:

- Configuration of groups
- IGMP
- Blocking unknown Multicast frames.

With the "show" commands, you can display the configuration data.

With the following commands, note which "Base bridge mode" you are in. If you are in the "Transparent Bridge" mode, all settings relate to the management VLAN: VLAN 1.

You change the mode with the `base bridge-mode` command.

9.6.1 The "show" commands VLAN bridge)

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.6.1.1 show mac-address-table

Description

This command shows the table with the static and dynamic unicast MAC addresses and multicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table [vlan <vlan-range>] [address
<aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN or VLAN range	-
`vlan-range`	Number of the addressed VLAN or VLAN range	1 ... 4094 Enter the range limits with a hyphen or a space.
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The entries of the MAC addresses table are displayed.

9.6.1.2 show mac-address-table dynamic multicast

Description

This command shows the table with the dynamic multicast MAC addresses assigned by the device.

Note

The device does not learn any reserved multicast addresses, see also RFC 5771.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table dynamic multicast[vlan<vlan-range>]
     [address<aa:aa:aa:aa:aa:aa>]
     [{interface<interface-type><interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan`	Keyword for a VLAN connection	-
`vlan-range`	Number of the addressed VLAN	1 ... 4094 Enter the range limits with a hyphen without spaces.
`address`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The dynamic multicast MAC addresses are displayed.

9.6.1.3 show mac-address-table static multicast

Description

This command shows the table with the static multicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show mac-address-table static multicast[vlan<vlan-range>]
  [address<aa:aa:aa:aa:aa:aa>][{interface<interface-type><interface-
id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vlan	Keyword for a VLAN connection	-
vlan-range	Number of the addressed VLAN	1 ... 4094 Enter the range limits with a hyphen without spaces.
address	Keyword for a MAC address	-
aa:aa:aa:aa:aa:aa	MAC address	-
interface	Keyword for a an interface description	-
interface-type	Type or speed of the interface	Enter a valid interface
interface-id	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The static multicast MAC addresses are displayed.

9.6.1.4 show multicast-block config

Description

This command shows the multicast blocking settings for ports.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

cli> or cli#

Syntax

Call up the command with the following parameters:

```
show multicast-block config [port <interface-type> <interface-id)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`port`	Keyword for a port description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If no parameters are specified, the settings for all ports are displayed.

Result

The multicast blocking settings for ports are displayed.

9.6.2 Commands in the global configuration mode (VLAN bridge)

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.6.2.1 mac-address-table static multicast

Description

With this command, you generate a static multicast MAC address entry in the forwarding database.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
mac-address-table static  multicast <aa:aa:aa:aa:aa:aa>
vlan <vlan-id(1-4094)> [interface ([<interface-type> <interface-
list>]
[<interface-type> <interface-list>] [port-channel <interface-
list>])]
[forbidden-ports ([<interface-type> <interface-list>] [<interface-
type>
<interface-list>] [port-channel <interface-list>  ])]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface`	Keyword for a an interface description	-
`interface-type`	Type of interface	Specify a valid interface.
`interface-list`	Module no. and port no. of the interface	
`port-channel`	Specifies the name of a port channel	Enter a valid port channel connection.
`interface-list`	Number of the addressed port channel	
`forbidden-ports`	Keyword for the interface description of the blocked ports	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry in the forwarding database is generated.

Additional notes

With the `show mac-address-table static multicast` command, you display the list of configured entries.

With the `no mac-address-table static multicast` command, you delete an entry.

9.6.2.2 no mac-address-table static multicast

Description

With this command, you delete a static multicast address.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan
<vlan-id(1-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value is used.

Result

The "static multicast" function is disabled.

9.6.3 The "show" commands (Transparent Bridge)

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.6.3.1 show dot1d mac-address-table

Description

This command shows the table with the static and dynamic unicast entries and the dynamic multicast entries.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call up the command with the following parameters:

```
show dot1d mac-address-table [address <aa:aa:aa:aa:aa:aa>]
     [{interface <interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
address	Keyword for a MAC address	-
aa:aa:aa:aa:aa:aa	MAC address	Specify a valid MAC address.
interface	Keyword for a an interface description	-
interface-type	Type or speed of the interface	Enter a valid interface.
interface-id	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The entries are displayed.

9.6.3.2 show dot1d mac-address-table static multicast

Description

This command shows the table with the static multicast MAC addresses.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show dot1d mac-address-table static multicast [address
<aa:aa:aa:aa:aa:aa>]
     [{interface <interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
address	Keyword for a MAC address	-
aa:aa:aa:aa:aa:aa	MAC address	-
interface	Keyword for a an interface description	-
interface-type	Type or speed of the interface	Enter a valid interface
interface-id	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The static multicast MAC addresses are displayed.

9.6.3.3 show multicast-block config

Description

This command shows the multicast blocking settings for ports.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

cli> or cli#

Syntax

Call up the command with the following parameters:

```
show multicast-block config [port <interface-type> <interface-id)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
port	Keyword for a port description	-
interface-type	Type or speed of the interface	Enter a valid interface
interface-id	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If no parameters are specified, the settings for all ports are displayed.

Result

The multicast blocking settings for ports are displayed.

9.6.4 Commands in the global configuration mode (Transparent Bridge)

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

9.6.4.1 mac-address-table static multicast

Description

With this command, you generate a static multicast MAC address entry in the forwarding database.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
mac-address-table static multicast <aa:aa:aa:aa:aa:aa>
[interface ([<interface-type> <interface-list>]  [<interface-type>
<interface-list>] [port-channel <interface-list>])]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`interface`	Keyword for a an interface description	-

Parameter	Description	Range of values/note
`interface-type`	Type of interface	Specify a valid interface.
`interface-list`	Module no. and port no. of the interface	
`port-channel`	Specifies the name of a port channel	Enter a valid port channel connection.
`interface-list`	Number of the addressed port channel	
`forbidden-ports`	Keyword for the interface description of the blocked ports	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value is used.

Result

The entry in the forwarding database is generated.

Additional notes

With the `show dot1d mac-address-table static multicast` command, you display the list of configured entries.

With the `no mac-address-table static multicast` command, you delete an entry.

9.6.4.2 no mac-address-table static multicast

Description

With this command, you delete a static multicast MAC address entry from the forwarding database.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no mac-address-table static multicast <aa:aa:aa:aa:aa:aa>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value is used.

Result

The entry is deleted from the forwarding database.

Further notes

With the `show dot1d mac-address-table static multicast` command, you display the list of configured entries.

With the `mac-address-table static multicast` command, you create an entry.

Layer 3 functions 10

10.1 NAT

Note

NAT/NATP is a layer 3 function and can only be used with IPv4.

When using the ISO protocol that operates at layer 2, it is not possible to use NAT.

With Network Address Translation (NAT), IP subnets are divided into "Inside" and "Outside". The division is from the perspective of a NAT interface. All networks that can be reached via the NAT interface itself count as "Outside" for this interface. All networks that csn be reached via IP interfaces of the same device count as being "Inside" for the NAT interface.

if there is routing via a NAT interface, the source or destination IP addresses of the transferred data packets are changed at the transition between "Inside" and "Outside". Whether the source or destination IP address is changed depends on the communication direction. It is always the IP address of the communications node that is located "Inside" that is adapted. Depending on the perspective, the IP address of a communications node is always designated as "Local" or "Global".

		Perspective	
		Local	**Global**
Position	**Inside**	An actual IP address that is assigned to a device in the internal network. This address cannot be reached from the external network.	An IP address at which an internal device can be reached from the external network.
	Outside	An actual IP address that is assigned to a device in the external network. Since only "Inside" addresses are converted, there is no distinction made between outside local and outside global.	

Computing capacity

Due to the load limitation of the CPU packet receipt of the device is limited to 300 packets a second. This corresponds to a maximum data through of 1.7 Mbps. This load limitation does not apply per interface but generally for all packets going the CPU.

The entire NAT communication runs via the CPU and therefore represents competition for IP communication going to the CPU, e.g. WBM and Telnet.

Note that a large part of the computing capacity is occupied if you use NAT.

NAT

With Network Address Translation (NAT), the IP address in a data packet is replaced by another. NAT is normally used on a gateway between an internal network ("Inside") and an external network ("Outside").

With source NAT, the inside local source address of an IP packet from a device in the internal network is rewritten by a NAT device to an inside global address at the gateway.

With destination NAT, the inside global destination address of an IP packet from a device in the external network is rewritten by a NAT device to an inside local address at the gateway.

To translate the internal into the external IP address and back, the NAT device maintains a translation list. The address assignment can be dynamic or static.

NAPT

In "Network Address Port Translation" (NAPT), several internal IP addresses are translated into the same external IP address. To identify the individual nodes, the port of the internal device is also stored in the translation list of the NAT device and translated for the external address.

If several internal devices send a query to the same external destination IP address via the NAT device, the NAT device enters its own external source IP address in the header of these forwarded frames. Since the forwarded frames have the same external source IP address, the NAT device assigns the frames to the devices using a different port number. These are logical port numbers and not physical Ethernet port numbers.

If a device from the external network wants to use a service in the internal network, the translation list for the static address assignment needs to be configured.

NAT/NAPT and IP routing

You can enable NAT/NAPT and IP routing at the same time. In this case, you need to regulate the reachability of internal addresses from external networks with IP access lists (ACL).

10.1.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

10.1.1.1 show ip nat

Description

This command shows address translations or active connections depending on the selected parameter.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

`show ip nat { interface | static | translations}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface`	Shows the configuration of the dynamic address translations.	-
`static`	Shows the configuration of the static 1:1 address translations.	-
`translations`	Displays the active NAT connections.	-

Result

The configured address translations or active connections are displayed.

Further notes

You configure a static address translation with the `ip nat static` command.

You delete a static address translation with the `no ip nat static` command.

You configure a dynamic address translation with the `ip nat pool` command.

You delete a dynamic address translation with the `no ip nat pool` command.

10.1.1.2 show ip nat config

Description

This command shows the global NAT/NAPT configuration.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameter assignment:

`show ip nat config`

Result

The global NAT configuration is displayed.

Further notes

You enable NAT/NAPT for the entire device with the `ip nat` command in the Global configuration mode.

You disable NAT/NAPT for the entire device with the `no ip nat` command in the Global configuration mode.

You delete the periods of time with the `ip nat timeout` command.

You can reset the time periods to the default with the `ip nat timeout` command.

10.1.1.3 show ip nat service

Description

This command shows static port translations (NAPT) for an interface with a service.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameter assignment:

```
show ip nat service
```

Result

The information is displayed.

Further notes

You configure static port translations for an interface with the `ip nat service` command.

You delete a configuration with the `no ip nat service` command.

10.1.1.4 show ip nat service portrange

Description

This command shows static port translations (NAPT) for an interface with a port range.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameter assignment:

```
show ip nat service portrange
```

Result

The selected service, start and end port of an interface are displayed.

Further notes

You configure static port translations for an interface with a port range with the `ip nat service portrange` command.

You delete a configuration with the `no ip nat service portrange` command.

10.1.1.5 show ip nat statistics

Description

This command shows statistical information on NAT, e.g. the number of active address assignments, NAT translations, etc.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameter assignment:

```
show ip nat statistics
```

Result

The statistical information is displayed.

10.1.1.6 show ip nat summary

Description

This command shows the NAT/NAPT configuration of the interfaces.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameter assignment:

```
show ip nat summary
```

Result

The current NAT/NAPT configuration of the interfaces is displayed.

Further notes

You enable NAT for the selected IP interface with the `ip nat` command in the Interface configuration mode.

You disable NAT for the selected IP interface with the `no ip nat` command in the Interface configuration mode.

You enable NAPT for the selected IP interface with the `ip nat napt` command in the Interface configuration mode.

You disable NAPT for the selected IP interface with the `no ip nat napt` command in the Interface configuration mode.

10.1.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

10.1.2.1 ip nat

Description

With this command you enable NAT/NAPT for the entire device.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip nat
```

Result

NAT/NAPT is enabled globally for the entire device. The device operates as a NAT router.

Further notes

You disable NAT/NAPT for the entire device with the `no ip nat` command.

You display the current configuration with the command.

10.1.2.2 no ip nat

Description

With this command you disable NAT/NAPT for the entire device.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip nat
```

Result

NAT/NAPT is disabled globally for the entire device.

Further notes

You enable NAT/NAPT for the entire device with the `ip nat` command.

You display the current configuration with the command.

10.1.2.3 ip nat timeout

Description

With this command you define periods of time after which existing connections are deleted if there is no data exchange.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ip nat {idle timeout <seconds (60-86400)> | {tcp | udp } timeout
<seconds (300-86400)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`idle timeout`	Keyword for the time after which a xxxx connection is deleted	-
`seconds`	Value for the time in seconds	For the parameter `idle`: • 60 ... 86400 For the parameter `udp`: • 300 ... 86400
`tcp`	Keyword for the time after which a TCP connection is deleted	-
`udp`	Keyword for the time after which a UDP connection is deleted	-

Result

The time periods are defined.

Further notes

You can reset the time periods to the default with the `ip nat timeout` command.

You display the current configuration with the command.

10.1.2.4 no ip nat timeout

Description

With this command you reset periods of time after which existing connections are deleted back to the default value.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no ip nat {idle | {tcp | udp } timeout
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`idle`	Keyword for the time period of a xxxx connection	-
`tcp`	Keyword for the time period of a TCP connection	-
`udp`	Keyword for the time period of a UDP connection	-

Result

The time periods are reset.

Further notes

You delete the periods of time with the `ip nat timeout` command.

You display the current configuration with the command.

10.1.3 Commands in the Interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

10.1.3.1 ip nat

Description

With this command, you enable NAT for the IP interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call the command without parameter assignment:

```
ip nat
```

Result

NAT is activated for the IP interface.

Further notes

You disable NAT for the selected IP interface with the `no ip nat` command.

You display the current configuration with the `show ip nat summary` command.

10.1.3.2 no ip nat

Description

With this command, you disable NAT for the selected IP interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call the command without parameter assignment:

```
no ip nat
```

Result

NAT is deactivated for the selected IP interface.

Further notes

You enable NAT for the selected IP interface with the `ip nat` command.

You display the current configuration with the `show ip nat summary` command.

10.1.3.3 ip nat napt

Description

With this command, you enable NAPT for the selected IP interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

`cli(config-if-$$)#`

Syntax

Call the command without parameter assignment:

`ip nat napt`

Result

NAPT is activated for the selected IP interface.

Further notes

You disable NAPT for the selected IP interface with the `no ip nat napt` command.

You display the current configuration with the `show ip nat summary` command.

10.1.3.4 no ip nat napt

Description

With this command, you disable NAPT for the selected IP interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

`cli(config-if-$$)#`

Syntax

Call the command without parameter assignment:

`no ip nat napt`

Result

NAPT is deactivated for the selected IP interface.

Further notes

You enable NAPT for the selected IP interface with the `ip nat napt` command.

You display the current configuration with the `show ip nat summary` command.

10.1.3.5 ip nat pool

Description

With this command, you configure a pool for dynamic address translations.

As default, the device cannot be reached from an external network. If the device wants to communicate in an external network, an inside global address is assigned to it dynamically. Using this inside global address, the device can be reached from the external network until the timer of the connection elapses.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call up the command with the following parameters:

```
ip nat pool <inside global ip> <mask>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`inside global ip`	Start address for the dynamic assignment of addresses at which devices will be reachable from external.	Enter a valid IPv4 address.
`mask`	Address mask of the external subnet	Enter a valid subnet mask.

Result

A pool is defined.

Further notes

You delete a dynamic address translation with the `no ip nat pool` command.

You display the current configuration with the `show ip nat` command.

10.1.3.6 no ip nat pool

Description

With this command, you delete a pool for dynamic address translations.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call up the command with the following parameters:

```
no ip nat pool <inside global ip>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`inside global ip`	Start address for the dynamic assignment of addresses at which devices are reachable from external.	Enter a valid IPv4 address.

Result

A pool is deleted.

Further notes

You configure a dynamic address translation with the `ip nat pool` command.

You display the current configuration with the `show ip nat` command.

10.1.3.7 ip nat service

Description

With this command, you configure static port translations (NAPT) for individual services for an interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call the command with the following parameters:

```
ip nat service <inside local ip> [<inside local port number>]
     { auth | dns | ftp | pop3 | pptp | smtp | telnet | http | nntp
| snmp | other [<inside global port number>]}
     [{ tcp | udp | any }] [<description>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`inside local ip`	Actual address of the device that should be reachable from external.	Enter a valid IPv4 address.
`inside local port number`	Port that will be assigned to the inside local address.	If you do not specify any ports, the port that you assign for the `inside global port number` parameter will be entered.
Service	Service for which the port translation is valid.	• `auth` • `dns` • `ftp` • `pop3` • `pptp` • `smtp` • `telnet` [1)] • `http` • `nntp` • `snmp` • `other`
`inside global port number`	Port that will be assigned to the inside global address.	If you have selected the `other` service, you can enter a port. If you have selected another service, a port will be specified.
Protocol	Protocol for which the port translation is valid.	• `tcp` • `udp` • `any`
`description`	Description for the port translation	-

1) Not available for SCALANCE XC-300/XR-300/XC-400/XR-500.

Result

The static port translation for a service has been configured.

Additional notes

You delete a configuration with the `no ip nat service` command.

You configure static port translations for an interface with a port range with the `ip nat service portrange` command.

You display the current configuration with the `show ip nat service` command.

10.1.3.8 no ip nat service

Description

With this command, you delete static port translations (NAPT) for a service for an interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call the command with the following parameters:

```
no ip nat service {{<inside local ip> <inside local port number>
[{ tcp | udp | any }]} | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`inside local ip`	Actual address of the device that is reachable from external.	Enter a valid IPv4 address.
`inside local port number`	Port that is assigned to the inside local address.	-
Protocol	Protocol for which the port translation is valid.	• `tcp` • `udp` • `any`
`all`	Deletes all port translations	-

Result

The static port translation for a service has been deleted.

Additional notes

You configure static port translations for a service for an interface with the `ip nat service` command.

You configure static port translations for a port range for an interface with the `ip nat service portrange` command.

You display the current configuration with the `show ip nat service` command.

10.1.3.9 ip nat service portrange

Description

With this command, you configure static port translations (NAPT) for a port range for an interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call the command with the following parameters:

```
ip nat service portrange <inside local ip> {tcp|udp|any} <inside
local start port no> <inside local end port no> [<description>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`inside local ip`	Actual address of the device that should be reachable from external.	Enter a valid IPv4 address.
Protocol	Protocol for which the port translation is valid.	• `tcp` • `udp` • `any`
`inside local start port no`	Start port that will be assigned to the inside local address.	The port range you define will also be used for the port of the inside global address. A port range can only be translated to the same port range.
`inside local end port no`	End port that will be assigned to the inside local address.	
`description`	Description for the port translation	-

Result

The static port translation for a port range has been configured.

Additional notes

You delete a configuration with the `no ip nat service portrange` command.

You configure static port translations for a service for an interface with the `ip nat service` command.

You display the current configuration with the `show ip nat service portrange` command.

10.1.3.10 no ip nat service portrange

Description

With this command, you delete static port translations (NAPT) for a port range for an interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call the command with the following parameters:

```
no ip nat service portrange <inside local ip> {tcp|udp|any} <inside
local start port no> <inside local end port no>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`inside local ip`	Actual address of the device that is reachable from external.	Enter a valid IPv4 address.
Protocol	Protocol for which the port translation is valid.	• `tcp` • `udp` • `any`
`inside local start port no`	Start port that is assigned to the inside local address.	-
`inside local end port no`	End port that is assigned to the inside local address.	-

Result

The static port translation for a port range has been deleted.

Additional notes

You configure static port translations for an interface with a port range with the `ip nat service portrange` command.

You configure static port translations with a service for an interface with the `ip nat service` command.

You display the current configuration with the `show ip nat service portrange` command.

10.1.3.11 ip nat static

Description

With this command, you configure static 1:1 address translations.

You specify which inside global address the inside local address of a device will be converted to and vice versa. This variant allows connection establishment in both directions. The device in the internal network can be reached from the external network.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call up the command with the following parameters:

```
ip nat static <inside local ip> <inside global ip>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`inside local ip`	Actual address of the device that should be reachable from external.	Enter a valid IPv4 address.
`inside global ip`	Address at which the device will be reachable from external	Enter a valid IPv4 address.

Result

A static address translation is defined.

Further notes

You delete a static address translation with the `no ip nat static` command.

You display the current configuration with the `show ip nat` command.

10.1.3.12 no ip nat static

Description

With this command, you delete static 1:1 address translations.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-if-$$)#
```

Syntax

Call up the command with the following parameters:

```
no ip nat static <inside local ip>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`inside local ip`	Actual address of the device that is reachable from external.	Enter a valid IPv4 address.

Result

A static address translation is deleted.

Further notes

You configure a static address translation with the `ip nat static` command.

You display the current configuration with the `show ip nat` command.

10.2 Single-Hop Inter-VLAN-Routing

Introduction

A physical network is divided into broadcast domains and subnets by VLANs.

Devices (hosts) within a VLAN can communicate with each other directly via layer 2. The frames are forwarded to the relevant device based on the MAC address.

Devices from different VLANs cannot communicate with each other directly via layer 2. The data traffic must be routed based on the IP address.

With the Single-Hop Inter-VLAN-Routing function it is possible that devices from different VLANs communicate with each other without a router being necessary.

Requirements

- The IE switch can manage several IP interfaces.
- The switch is a member in the VLANs to be routed.
- With the hosts, the IP address of the VLAN is entered as default gateway.

Single-Hop Inter-VLAN-Routing

The IE switch receives a frame and recognizes that it is addressed to a device in another VLAN. It forwards the frame to the corresponding port in the VLAN.

The IE switch only knows VLANs with which it is directly connected (Connected). With Single-Hop Inter-VLAN-Routing it is therefore only possible to route between two local IP interfaces.

10.2.1 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

10.2.1.1 ip single-hop inter-vlan-routing

Description

With this command, you enable the Single-Hop Inter-VLAN-Routing function.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip single-hop inter-vlan-routing
```

Result

The function is enabled. The device can route between two local IP interfaces.

Further notes

You disable the Single-Hop Inter-VLAN-Routing function with the `no ip single-hop inter-vlan-routing` command.

10.2.1.2 no ip single-hop inter-vlan-routing

Description

With this command, you enable the Single-Hop Inter-VLAN-Routing function.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip single-hop inter-vlan-routing
```

Result

The function is disabled.

Further notes

You enable the Single-Hop Inter-VLAN-Routing function with the `ip single-hop inter-vlan-routing` command.

Load control 11

This part contains the sections describing the functions for controlling and balancing network load.

11.1 Rate control

This section describes commands for controlling and restricting the data transmission rate of an interface.

11.1.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.1.1.1 show rate-limit output

Description

This command shows the packet rate for limiting the outgoing data stream of one or all interfaces.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show rate-limit output [interface <interface-type> <interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameter from the parameter list, the entries are displayed for all available interfaces.

Result

The entries are displayed.

11.1.2 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.1.2.1 rate-limit output

Description

With this command, you configure and enable the data rate in Kbps for limiting the outgoing data stream of the interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
rate-limit output <rate-value>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`rate-value`	Value for the data rate in Kbps	Default: The data rate is set to 0. The outgoing data stream is not limited.

If you do not select any parameters from the parameter list, the default value is used.

Result

The limitation of the outgoing data stream of the interface with the data rate is enabled.

Additional notes

You disable the function with the `no rate-limit output` command.

11.1.2.2 no rate-limit output

Description

With this command, you disable the data rate for limiting the outgoing data stream of the interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no rate-limit output
```

Result

The limitation of the outgoing data stream of the interface with the data rate is disabled.

Further notes

You enable the function with the `rate-limit output` command.

11.1.2.3 storm-control

Description

With this command, you enable data rate for limiting the incoming data stream of the interface for broadcast, multicast or unknown unicast packets.

Note

Applications

Storm control is only supported on physical interfaces.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`storm-control{broadcast | multicast | dlf | unicast}`

The parameters have the following meaning:

Parameter	Description
`broadcast`	Limits broadcast packets
`multicast`	Limits multicast packets
`dlf`	Limits unicast packets with unresolvable addresses (dfl = destination lookup fail)
`unicast`	Limits unicast packets with resolvable addresses

As default the function is "disabled" for all transfer types.

Note

Configuration of the threshold value

The default value for the storm control level is 0 Kbps. The incoming data stream is not limited.

To have the incoming data stream limited, configure the threshold value with the `storm-control level` command.

Result

The storm control function is enabled.

Additional notes

You disable the function with the `no storm-control` command.

You configure the threshold value for the storm control function with the `storm-control level` command.

11.1.2.4 no storm-control

Description

With this command, you disable the storm control function for broadcast, multicast or unknown unicast packets.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no storm-control{broadcast | multicast | dlf | unicast}
```

The parameters have the following meaning:

Parameter	Description
`broadcast`	Disables broadcast storm control
`multicast`	Disables multicast storm control
`dlf`	Disables unknown unicast storm control
`unicast`	Disables unicast storm control

if you call up the function without parameters, it is disabled for all types of transmission.

Result

The storm control function is disabled.

Additional notes

You enable the function with the `storm-control` command.

11.1.2.5 storm-control level

Description

With this command, you configure the value for the storm control function in Kbps.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
storm-control level <rate-value>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`rate-value`	Value for the data rate in Kbps	The value range depends on the port speed. The entry is rounded down to the next valid value. If small values are entered, the value is rounded up to the next valid value. Default: The data rate is set to 0. The incoming data stream is not limited.

Result

The value for the storm control function is configured.

Additional notes

You can reset the setting to the default with the `no storm-control level` command.

11.1.2.6 no storm-control level

Description

With this command, you reset the value for the storm control function to the default value.

The default value for the storm control level is 0 Kbps. The incoming data stream is not limited.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

`no storm-control level`

Result

The value for the storm control function is reset to the default.

Additional notes

You configure the value for the storm control function with the `storm-control level` command.

11.2 Static MAC filtering

11.2.1 Commands in the global configuration mode (VLAN bridge)

With the following commands, note which "Base bridge mode" you are in. If you are in the "Transparent Bridge" mode, all settings relate to the management VLAN: VLAN 1.

You change the mode with the `base bridge-mode` command.

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.2.1.1 mac-address-table static multicast

Description

With this command, you generate a static multicast MAC address entry in the forwarding database.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
mac-address-table static  multicast <aa:aa:aa:aa:aa:aa>
vlan <vlan-id(1-4094)> [interface ([<interface-type> <interface-
list>]
[<interface-type> <interface-list>] [port-channel <interface-
list>])]
[forbidden-ports ([<interface-type> <interface-list>] [<interface-
type>
<interface-list>] [port-channel <interface-list>  ])]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface`	Keyword for a an interface description	-
`interface-type`	Type of interface	Specify a valid interface.
`interface-list`	Module no. and port no. of the interface	
`port-channel`	Specifies the name of a port channel	Enter a valid port channel connection.
`interface-list`	Number of the addressed port channel	
`forbidden-ports`	Keyword for the interface description of the blocked ports	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry in the forwarding database is generated.

Additional notes

With the `show mac-address-table static multicast` command, you display the list of configured entries.

With the `no mac-address-table static multicast` command, you delete an entry.

11.2.1.2 no mac-address-table static multicast

Description

With this command, you delete a static multicast MAC address entry from the forwarding database.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no mac-address-table static multicast<aa:aa:aa:aa:aa:aa>
      vlan<vlan-id(1-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`vlan`	Keyword for the number of a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry is deleted from the forwarding database.

Further notes

With the `show mac-address-table static multicast` command, you display the list of configured entries.

With the `mac-address-table static multicast` command, you create an entry.

11.2.1.3 mac-address-table static unicast

Description

With this command, you generate a static unicast MAC address entry in the forwarding database.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
mac-address-table static  unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-
id(1-4094)>
interface ([<interface-type> <interface-list>] [<interface-type>
<interface-list>]
[port-channel <interface-list>])
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-list`	Module no. and port no. of the interface	
`port-channel`	Keyword for a port-channel connection	Enter a valid port channel connection.
`interface-list`	Number of the addressed port channel	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry in the forwarding database is generated.

Additional notes

With the `show mac-address-table static unicast` command, you display the list of configured entries.

With the `no mac-address-table static unicast` command, you delete an entry.

11.2.1.4 no mac-address-table static unicast

Description

With this command, you delete a static unicast MAC address entry from the forwarding database.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no mac-address-table static unicast <aa:aa:aa:aa:aa:aa>
   vlan<vlan-id(1-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry is deleted from the forwarding database.

Further notes

With the `show mac-address-table static unicast` command, you display the list of configured entries.

With the `mac-address-table static unicast` command, you create an entry.

11.2.2 Commands in the global configuration mode (Transparent Bridge)

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.2.2.1 mac-address-table static multicast

Description

With this command, you generate a static multicast MAC address entry in the forwarding database.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
mac-address-table static multicast <aa:aa:aa:aa:aa:aa>
[interface ([<interface-type> <interface-list>]  [<interface-type>
<interface-list>] [port-channel <interface-list>])]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type of interface	Specify a valid interface.
`interface-list`	Module no. and port no. of the interface	
`port-channel`	Specifies the name of a port channel	Enter a valid port channel connection.
`interface-list`	Number of the addressed port channel	
`forbidden-ports`	Keyword for the interface description of the blocked ports	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value is used.

Result

The entry in the forwarding database is generated.

Additional notes

With the `show dot1d mac-address-table static multicast` command, you display the list of configured entries.

With the `no mac-address-table static multicast` command, you delete an entry.

11.2.2.2 no mac-address-table static multicast

Description

With this command, you delete a static multicast MAC address entry from the forwarding database.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no mac-address-table static multicast <aa:aa:aa:aa:aa:aa>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value is used.

Result

The entry is deleted from the forwarding database.

Further notes

With the `show dot1d mac-address-table static multicast` command, you display the list of configured entries.

With the `mac-address-table static multicast` command, you create an entry.

11.2.2.3 mac-address-table static unicast

Description

With this command, you generate a static unicast MAC address entry in the forwarding database.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
mac-address-table static unicast <aa:aa:aa:aa:aa:aa>  interface
([<interface-type>
<interface-list>]  [<interface-type> <interface-list>] [port-
channel <interface-list>])
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-list`	Module no. and port no. of the interface	
`port-channel`	Keyword for a port-channel connection	Enter a valid port channel connection.
`interface-list`	Number of the addressed port channel	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry in the forwarding database is generated.

Additional notes

With the `show dot1d mac-address-table static unicast` command, you display the list of configured entries.

With the `no mac-address-table static unicast` command, you delete an entry.

11.2.2.4 no mac-address-table static unicast

Description

With this command, you delete a static unicast MAC address entry from the forwarding database.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no mac-address-table static unicast <aa:aa:aa:aa:aa:aa>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry is deleted from the forwarding database.

Further notes

With the `show dot1d mac-address-table static unicast` command, you display the list of configured entries.

With the `mac-address-table static unicast` command, you create an entry.

11.2.3 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.2.3.1 switchport ingress-filter

Description

With incoming packets, the ingress filter checks whether the port on which the packet was received belongs to the sending VLAN. If this is not the case, the packet is not processed.

With this command, you enable the ingress filter.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
switchport ingress-filter
```

Result

The ingress filter is activated.

Further notes

You disable the filter with the `no switchport ingress-filter` command.

You can display the status of the ingress filter and other settings with the `show vlan port config` command.

11.2.3.2 no switchport ingress-filter

Description

With this command, you disable the ingress filter.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

`no switchport ingress-filter`

Result

The ingress filter is deactivated.

Further notes

You enable the filter with the `switchport ingress-filter` command.

You can display the status of the ingress filter and other settings with the `show vlan port config` command.

11.3 Dynamic MAC aging

The section describes commands with which the aging of dynamically learned entries is configured in a MAC address list.

11.3.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.3.1.1 show mac-address-table aging-time

Description

To ensure that the address entries are up-to-date, MAC addresses are only kept in the address table for a specified time.

This command shows the time after which the MAC addresses are removed from the address table.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show mac-address-table aging-time
```

Result

The time is displayed.

11.3.1.2 show mac-address-table aging-status

Description

This command shows whether or not MAC aging is enabled.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show mac-address-table aging-status
```

Result

The status of the MAC aging is displayed.

11.3.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.3.2.1 mac-address-table aging-time

Description

With this command, you configure the aging of a dynamically learned entry in the MAC address list.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
mac-address-table aging-time <seconds(15-630)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`seconds`	Life of the entry in seconds	15 ... 630 Default: 30 Enter the period of time in seconds in steps of 15. When you input the Aging Time, note that the WBM rounds to correct values. If you enter a value that cannot be divided by 15, the value is automatically rounded down.

Result

The value of the aging of a dynamically learned entry is configured.

Additional notes

You can reset the setting to the default with the `no mac-address-table aging-time` command.

You display the setting with the `show mac-address-table aging-time` command.

11.3.2.2 no mac-address-table aging-time

Description

With this command, you reset the value for the aging of a dynamically learned entry in the MAC address list to the default value.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

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

Result

The value of the aging of a dynamically learned entry is reset to the default value.

Further notes

You configure the setting with the `mac-address-table aging-time` command.

You display the setting with the `show mac-address-table aging-time` command.

11.3.2.3 mac-address-table aging

Description

With this command, you enable the "Aging" function. The "Aging" function ensures that an entry in the MAC address list that was learned dynamically is deleted again after a certain time.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
mac-address-table aging
```

Result

The "Aging" function is enabled.

Further notes

You configure the time with the `mac-address-table aging-time` command.

You disable the "Aging" function with the `no mac-address-table aging` command.

11.3.2.4 no mac-address-table aging

Description

With this command, you disable the "Aging" function.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

`no mac-address-table aging`

Result

The "Aging" function is disabled.

Further notes

You enable the "Aging" function with the `mac-address-table aging` command.

11.4 Flow control

The flow control function monitors the incoming data traffic of a port. If there is overload ("Congestion", "Overflow") it sends a signal to the connection partner. If the flow control function receives a signal at the sending end, it stops the data transmission to avoid loss of data.

This section describes commands of the flow control function.

11.4.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.4.1.1 show flow-control

Description

This command shows the settings of the flow control function.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the information for the router will be displayed.

Result

The settings of the flow control function are displayed.

11.4.2 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.4.2.1 flowcontrol

Description

The flow control function monitors a connection at the receiving end to make sure that not more data is received than can be processed. If flow control detects a threat of data overflow, the partner at the sending end is sent a signal to stop transmitting.

With this command, you configure the flow control function for an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`flowcontrol {on|off}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`on`	Enables the function	You can only enable or disable flow control when the "Auto negotiation" function is turned off. Afterwards you can enable "Auto negotiation" again. To use the flow control function, enable flow control at the appropriate input and output ports. If a packet is sent from an input port with flow control enabled to an output port with flow control enabled, the packet is not discarded if there is overflow. If flow control is enabled only on the input port, the packet can be discarded if there is overload.
`off`	Disables the function	-

Result

The settings for the flow control function are configured.

Further notes

You can display the status of this function with the `show flow-control` command.

You disable "Auto negotiation" with the `no negotiation` command.

You enable "Auto negotiation" with the `negotiation` command.

11.5 Service classes

This section describes commands for configuring the assignment tables for service classes and the Differentiated Services Code Point (DSCP).

11.5.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.5.1.1 show qos agent-priority

Description

This command shows the current priority of agent frames.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show qos agent-priority
```

Result

The current priority of the agent frames is displayed.

Further notes

You configure the priority of agent frames with the `agent-priority` command.

11.5.1.2 show qos broadcast-priority

Description

This command shows the current priority of broadcast frames.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

`show qos broadcast-priority`

Result

The current priority of the broadcast frames is displayed.

Further notes

You configure the priority of broadcast frames with the `broadcast-priority` command.

11.5.1.3 show qos cos-map

Description

This command shows the assignment table of CoS priorities to queues.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

`show qos cos-map`

Result

The assignment table of CoS priorities to queues is displayed.

Further notes

You configure the assignment of the CoS priority to a queue with the `cos-map` command.

11.5.1.4 show qos cos-remap

Description

For individual ports, this command shows the priority with which frames are sent.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show qos cos-remap
```

Result

The assignment table for send priority is displayed.

Further notes

You enable the the Cos reassignment with the `cos-remap-enable` command.

You change the priority with which frames are sent `cos-remap`command.

11.5.1.5 show qos dscp-map

Description

This command shows the assignment table of DSCP priorities to queues.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show qos dscp-map
```

Result

The assignment table of DSCP priorities to queues is displayed.

Further notes

You configure the assignment of the DSCP priority to a queue with the `dscp-map` command.

11.5.1.6 show qos scheduling mode

Description

This command shows the method with which the processing order of the frames is decided.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show qos scheduling mode
```

Result

The method with which the frames are processed is displayed.

Further notes

You configure the method for deciding the processing order with the `scheduling mode` command.

11.5.1.7 show qos-trust-mode

Description

This command shows port by port the method according to which packets to be forwarded are prioritized.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show qos-trust-mode
```

Result

The list for all ports with the corresponding Trust mode is displayed.

11.5.2 Commands in the Global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.5.2.1 qos

Description

With this command, you change to the QOS configuration mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
qos
```

Result

You are now in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Further notes

You exit the QOS configuration modewith the command `end` or `exit`.

11.5.3 Commands in the QOS configuration mode

Quality of Service (QoS)

Quality of Service (QoS) is a method to allow efficient use of the existing bandwidth in a network.

QoS is implemented by prioritization of the data traffic. Incoming frames are sorted into a Queue according to a certain prioritization and further processed. This gives certain frames priority.

The different QoS methods influence each other and are therefore taken into account in the following order:

1. The switch first checks whether the incoming frame is a broadcast or agent frame.
   → When the first condition is met, the switch takes into account the set priority with the `agent-priority` or `broadcast-priority` command..
   The switch sorts the frame into a queue according to the the `cos-map` command.
2. If the first condition is not met the switch checks whether the frame contains a VLAN tag.
   → If the second condition is met, the switch checks whether the priority is enabled (`priority-enable`).
   If priority is enabled, the switch sorts the frame into a queue according to the the `cos-map` command.
3. If the second condition is also not met the frames are further processed according to the Trust mode. You configure the trust mode with the `qos-trust-mode` command.

Commands in this section

This section describes commands that you can call up in the QOS configuration mode.

In global configuration mode, enter the `qos` command to change to this mode.

- If you exit the QOS configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the QOS configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in QOS configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

11.5.3.1 agent-priority

Description

With this command you specify the priority of agent frames. The switch sorts incoming frames into a queue according to this prioritization .

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call up the command with the following parameters:

```
agent-priority <integer (0-7)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`integer`	Value of the priority	0 ... 7

Result

The priority of agent frames is configured.

Further notes

You reset the priority of agent frames to the default value with the `no agent-priority` command.

You display the current priority of agent frames with the `show qos agent-priority` command.

You configure the assignment of the CoS priority to a queue with the `cos-map` command.

11.5.3.2 no agent-priority

Description

With this command, you reset the priority of agent frames back to the default value.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call the command without parameters:

```
no agent-priority
```

Result

The priority of agent frames has been reset to the default value.

Further notes

You change the priority of agent frames with the `agent-priority` command.

You display the current priority of agent frames with the `show qos agent-priority` command.

You configure the assignment of the CoS priority to a queue with the `cos-map` command.

11.5.3.3 broadcast-priority

Description

With this command you specify the priority of broadcast frames. The switch sorts incoming frames into a queue according to this prioritization .

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call up the command with the following parameters:

```
broadcast-priority <integer (0-7)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`integer`	Value of the priority	0 ... 7

Result

The priority of broadcast frames is configured.

Further notes

You reset the priority of broadcast frames to the default value with the `no broadcast-priority` command.

You display the current priority of broadcast frames with the `show qos broadcast-priority` command.

You configure the assignment of the CoS priority to a queue with the `cos-map` command.

11.5.3.4 no broadcast-priority

Description

With this command, you reset the priority of broadcast frames back to the default value.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call the command without parameters:

```
broadcast-priority
```

Result

The priority of broadcast frames has been reset to the default value.

Further notes

You change the priority of broadcast frames with the `broadcast-priority` command.

You display the current priority of broadcast frames with the `show qos broadcast-priority` command.

You configure the assignment of the CoS priority to a queue with the `cos-map` command.

11.5.3.5 cos-map

Description

With this command, you configure the assignment of CoS priorities to queues.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call up the command with the following parameters:

```
cos-map <cos(0-7)> queue <queue(1-4)>
```

or

```
cos-map <cos(0-7)> queue <queue(1-8)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`cos`	Priority	0 ... 7 Default: 1
`queue`	Keyword for a queue	-
`queue`	Queue to which this priority is assigned	1 ... 4/8 *) Default: 2

*) Depending on the device.

The CoS priorities are assigned to the queues as follows in the default setting:

COS	Devices with 4 queues	Devices with 8 queues
0	Queue 2	Queue 2
1	Queue 1	Queue 1
2	Queue 1	Queue 3
3	Queue 2	Queue 4
4	Queue 3	Queue 5
5	Queue 3	Queue 6
6	Queue 4	Queue 7
7	Queue 4	Queue 8

The higher the number of the queue, the higher the processing priority.

Result

The assignment table for service classes is configured.

Additional notes

You display the current assignment table of CoS priorities to queues with the `show qos cos-map` command.

11.5.3.6 cos-remap

Description

With this command depending on the priority when receiving a frame, you can change the priority with which it is sent.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call up the command with the following parameters:

```
cos-remap interface <interface-type><interface-id> <prio (0-7)>
<remapped prio (0-7)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface
`interface-id`	Module no. and port no. of the interface	
`prio`	Priority with which a frame is received.	0 ... 7
`remapped prio`	Priority with which a frame will be sent	0 ... 7

Result

The send priority has been changed.

Further notes

You reset the send priority to the default value with the `no cos-remap` command.

You enable the CoS reassignment with the `cos-remap-enable` command.

You disable the the CoS reassignment with the `no cos-remap-enable` command.

You display the assignment table for the send priority with the `show qos cos-remap` command.

11.5.3.7 no cos-remap

Description

With this command, you reset the send priority back to the default value.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call the command without parameters:

```
no cos-remap
```

Result

The send priorities are reset to the default value.

Further notes

You change the send priority depending on the priority when receiving a frame with the `cos-remap` command.

You enable the the CoS reassignment with the `cos-remap-enable` command.

You disable the the CoS reassignment with the `no cos-remap-enable` command.

You display the assignment table for the send priority with the `show qos cos-remap` command.

11.5.3.8 cos-remap-enable

Description

With this command, you enable the CoS reassignment function. Depending on the priority when receiving a frame, you can change the priority with which it is sent.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call the command without parameters:

`cos-remap-enable`

Result

The CoS reassignment function is enabled.

Further notes

You disable the function with the `no cos-remap-enable` command.

You change the priority with which frames are sent with the `cos-remap` command.

You reset the send priority to the default value with the `no cos-remap` command.

You display the assignment table for the send priority with the `show qos cos-remap` command.

11.5.3.9 no cos-remap-enable

Description

With this command, you disable the CoS reassignment function.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

`cli(config-qos)#`

Syntax

Call the command without parameters:

`no cos-remap-enable`

Result

The CoS reassignment function is disabled.

Further notes

You enable the function with the `cos-remap-enable` command.

You change the priority with which frames are sent with the `cos-remap` command.

You reset the send priority to the default value with the `no cos-remap` command.

You display the assignment table for the send priority with the `show qos cos-remap` command.

11.5.3.10 dscp-map

Description

With this command, you configure the assignment of DSCP priorities to queues.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call up the command with the following parameters:

```
dscp-map {<dscp (0-63)> | range <dscp (0-63)> - <dscp (0-63)>}
queue <queue(1-8)>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`dscp`	Priority	0 ... 63
`range`	Keyword for a range of DSCP codes	-
`queue`	Keyword for a queue	-
`queue`	Queue to which this priority is assigned	1 ... 4/8 *)

*) Depending on the device.

The DSCP priorities are assigned to the queues as follows in the default setting:

DSCP codes	Devices with 4 queues
0 - 15	Queue 1
16 - 31	Queue 2
32 - 47	Queue 3
48 - 63	Queue 4

DSCP codes	Devices with 8 queues
0 - 7	Queue 2
8 - 15	Queue 1
16 - 23	Queue 3
24 - 31	Queue 4
32 - 39	Queue 5

DSCP codes	Devices with 8 queues
40 - 47	Queue 6
48 - 55	Queue 7
56 - 63	Queue 8

Result

The assignment table for DSCP codes is configured.

Further notes

You display the current assignment table of DSCP priorities to queues with the `show qos dscp-map` command.

11.5.3.11 qos-trust-mode

Description

With this command you can set the method according to which frames to be forwarded are prioritized port by port.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call up the command with the following parameters:

```
qos-trust-mode interface {<interface-type> <interface-id > | range
<interface-type> <interface-id > - <interface-type> <interface-id
>} {untrust | cos | dscp | cos-dscp}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	
`range`	Keyword for a range of interfaces	-
`untrust`	The switch sorts the incoming frames into a queue according to the prioritization of the receiving port. If there is a DSCP value in the IP header, this is ignored. If a VLAN tag exists, it is replaced by the priority value of the receiving port.	-

Parameter	Description	Range of values/note
`cos`	If an incoming frame contains a VLAN tag, the switch sorts it into a queue according to this prioritization. If the frame does not contain a VLAN tag, the switch sorts the frame into a queue according to the prioritization of the receiving port. If there is a DSCP value in the IP header, this is ignored.	Default setting with PROFINET variants
`dscp`	If an incoming frame contains a DSCP prioritization, the switch sorts it into a queue according to this prioritization. If the frame does not contain a DSCP prioritization, the switch sorts the frame into a queue according to the prioritization of the receiving port. If the frame contains a VLAN tag, this is ignored.	Default setting with EtherNet/IP variants
`cos-dscp`	With an incoming frame, there is a sequential check of which prioritization it contains. If it contains a DSCP prioritization, it is handled as in the "Trust DSCP" mode. If it contains no DSCP prioritization, the switch checks whether it contains a VLAN tag. If it contains a VLAN tag, the switch sorts it into a queue according to this prioritization. If the frame contains neither a DSCP prioritization nor a VLAN tag, the switch sorts the frame into a queue according to the prioritization of the receiving port.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The prioritization for forwarding frames is configured.

Further notes

You configure the assignment of the CoS priority to a queue with the `cos-map` command.

You configure the assignment of the DSCP priority to a queue with the `dscp-map` command.

You configure the prioritization of the receiving port with the `switchport priority default` command.

11.5.3.12 scheduling mode

Description

With this command, you can specify the order in which the frames in the forwarding queues are sent. The higher the queue number, the higher the send priority.

Requirement

You are in the QOS configuration mode.

The command prompt is as follows:

```
cli(config-qos)#
```

Syntax

Call up the command with the following parameters:

`scheduling mode { strict | weighted }`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`strict`	As long as there are frames with high priority in the queue, only these high-priority frames are processed.	-
`weighted`	Even if there are frames with high priority in the queue, frames with a lower priority will be processed occasionally.	-

Result

The method for the processing order of the frames is specified.

Additional notes

You display the method for the processing order of the frames with the `show qos scheduling mode` command.

Security and authentication 12

This part contains the sections that describe the access rights and authentication methods.

12.1 User management

This section describes commands for access as administrator and the configuration of the authentication methods.

12.1.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.1.1.1 show function-rights

Description

With this command, you list the available function rights in a table.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show function-rights
```

Result

The available function rights are displayed.

12.1.1.2 show password-policy

Description

This command shows which password policy is currently being used.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call the command without parameters:

`show password-policy`

Result

The currently valid password policy is displayed.

Additional notes

You configure the password policy with the `password-policy` command.

12.1.1.3 show roles

Description

This command shows the created roles.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call the command without parameters:

`show roles`

Result

The created roles are shown.

Additional notes

You create a role with the `role` command.

You delete a role with the `no role` command.

12.1.1.4 show user-accounts

Description

This command shows the created users.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call up the command with the following parameters:

`show user-accounts [external]`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`external`	Keyword for the table "External User Accounts"	-

If you do not specify the optional parameters, the local users are shown.

Result

The created users are shown.

Further notes

You create a new local user and create an entry in the table "External User Accounts" with the `user-account` command.

You link a user created on an external server with a role on the device in the table External User Accounts" with the `user-account-ext` command.

You delete a local user and the corresponding entry in the table "External User Accounts" with the `no user-account` command.

You delete a link in the table "External User Accounts" with the `no user-account-ext` command.

12.1.1.5 show user-groups

Description

This command shows the links between groups and roles.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call the command without parameters:

`show user-groups`

Result

The links are shown.

Further notes

You link a group with a role with the `user-group` command.

You delete a link with the `no user-group` command.

12.1.1.6 show users

Description

This command shows the logged-in CLI users.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show users
```

Result

The logged-in CLI users are displayed.

12.1.2 change password

Description

With this command, you change the password of the logged in user.

Requirement

- You are logged into the device with a local user account
- You are in the User EXEC mode or in the Privileged EXEC mode.
  The command prompt is as follows:
  `cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
change password <passwd>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`passwd`	Value for the password	Enter the password. The entry depends on the password policy. The `show password-policy` command shows which password policy is currently being used.

Result

The password is changed.

Note

Changing the password in Trial mode

Even if you change the password in Trial mode, this change is saved immediately.

Further notes

You create a user with the `user-account` command.

You delete a user with the `no user-account` command.

You show the created users with the `show user-accounts` command.

You configure the password policy with the `password-policy` command.

12.1.3 whoami

Description

This command shows the user name of the logged in user.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

`whoami`

Result

The user name of the logged in user is displayed.

12.1.4 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.1.4.1 password-policy

Description

With this command, you specify which password policy will be used when assigning new passwords.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`password-policy {low | high | custom}`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`low`	Password policy: Low	Password length: at least 6 characters
`high`	Password policy: High	Password length: at least 8 characters: At least 1 uppercase letter At least 1 special character At least 1 number
`custom`	User-defined password policy	The password requirements can be configured.

Result

The password policy is specified.

Additional notes

You assign a new password with the `user-account` command.

You display the setting with the `show password-policy` command.

You configure user-defined password policies with the `password-policy` command. This command has different parameters to the `password-policy` command described here

12.1.4.2 password-policy min-length

Description

With this command, you configure the minimum length of passwords that are assigned according to the user-defined password policy.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
password-policy min-length {<integer(8-32)>}
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`min-length`	The minimum length of the password	8 ... 32

Result

The minimum length of the password is set.

Additional notes

You assign a new password with the `user-account` command.

You display the setting with the `show password-policy` command.

With the `password-policy` command, you specify which password policy will be used when assigning new passwords. This command has different parameters to the `password-policy` command described here.

12.1.4.3 password-policy (parameter)

Description

With this command, you configure the password policy.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
password-policy {min-numeric | min-special | min-uppercase | min-
lowercase} {<integer(0-32)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`min-numeric`	The minimum number of numeric characters	0 ... 32
`min-special`	The minimum number of special characters	0 ... 32
`min-uppercase`	The minimum number of uppercase letters	0 ... 32
`min-lowercase`	The minimum number of lowercase letters	0 ... 32

Result

The minimum password requirements have been set.

Additional notes

You assign a new password with the `user-account` command.

You display the setting with the `show password-policy` command.

With the `password-policy` command, you specify which password policy will be used when assigning new passwords. This command has different parameters to the `password-policy` command described here.

12.1.4.4 role

Description

With this command, you create roles that are valid locally on the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
role <role-name> function-rights <function-rights-value(1-15)>
[description <role-description>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`role-name`	Role name	Enter a name for the role. The name must meet the following conditions: • It must be unique. • It must be between 1 and 64 characters long. • The following characters must not be included: § ? " ;
`function-rights`	Keyword for the function rights	-
`function-rights-value`	Value of the function rights	Select the function rights of the role. • 1 Users with this role can read device parameters but cannot change them. • 15 Users with this role can both read and change device parameters.
`description`	Keyword for the description	-
`role-description`	Content of the description	Enter a description for the role. The description text can be up to 100 characters long.

Result

The role is created.

Note

Role name cannot be changed

After creating a role, the name of the role can no longer be changed.

If a name of a role needs to be changed, the role must be deleted and a new role created.

Note

Function rights changeable with restrictions

You can only change the function rights of a role when the role is no longer linked to a user.

Further notes

You delete a role with the `no role` command.

You show the created roles with the `show roles` command.

12.1.4.5 no role

Description

With this command, you delete a role.

Note

You can only delete a role when the role is not linked to a user.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`no role <role-name>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`role-name`	Role name	Enter the name of a role.

Result

The role is deleted.

Further notes

You create a role with the `role` command.

You show the created roles with the `show roles` command.

12.1.4.6 user-account

Description

With this command, you specify a new user. You can also change the password and the role of an already created user.

Requirement

The user is logged in with the "admin" role.

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
user-account <user-name> password <user-password> role {user-role}
[description <user-description>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`user-name`	User name	Enter a user name. The name must meet the following conditions: • It must be unique. • It must be between 1 and 32 characters long. • The following characters must not be included: § ? " ; : < =
`password`	Keyword for a password	-
`user-password`	Value for the password	Enter the password. The strength of the password depends on the set password policy: • `low`: Password length: at least 6 characters, maximum 32 characters • `high`: The password must meet the following conditions: – Password length: at least 8 characters, maximum 32 characters – At least 1 uppercase letter – At least 1 special character – At least 1 number
`role`	Keyword for the role of the user	-
`user-role`	The user role	The following user roles exist: • `user` The user only has read rights. • `admin` The user can create, edit or delete entries.
`description`	Keyword for information on the user.	-
`user-description`	Information on the user.	Maximum of 100 characters.

Result

The new user has been created or the password/role has been changed.

Note

Changes in "Trial" mode

Even if the device is in "Trial" mode, changes that you carry out with this command are saved immediately.

Note

User name cannot be changed

After creating a user, the user name can no longer be modified because the user name is used for encryption of the password. If a user name needs to be changed, the user must be deleted and a new user created.

Additional notes

You delete a user with the `no user-account` command.

You show the created users with the `show user-accounts` command.

12.1.4.7 no user-account

Description

With this command, you delete a user.

Note

Default users "admin" as well as logged in users cannot be deleted.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no user-account <user-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
user-name	User name	Enter a valid user name.

Result

The user has been deleted.

Further notes

You create a user with the `user-account` command.

You show the created users with the `show user-accounts` command.

12.1.4.8 user-account-ext

Description

With this command you link a user with a role in the table "External User Accounts". The user is defined on RADIUS server. The roll is defined locally on the device.

When a RADIUS server authenticates a user, the corresponding group however is unknown or does not exist, the device checks whether or not there is an entry for the user in the table "External User Accounts". If an entry exists, the user is logged in with the rights of the associated role. If the corresponding group is known on the device, both tables are evaluated. The user is assigned the role with the higher rights.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
user-account-ext <user-name-ext> role <user-role-ext> [description
<user-ext-description>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`user-account-ext`	Keyword for a user in the table "External User Accounts"	-
`user-name-ext`	User name	Enter the name for the user. The name must meet the following conditions: • It must be unique. • It must be between 1 and 250 characters long.
`role`	Keyword for the role name	-
`user-role-ext`	Role name	Enter a role. You can choose between system-defined and self-defined roles.
`description`	Keyword for the description	-
`user-ext-description`	Content of the description	Enter a description for the user in the table "External User Accounts". The description text can be up to 100 characters long.

Result

A link in the table "External User Accounts" has been created.

Note

User name cannot be changed

After creating a user, the user name can no longer be modified. If a user name needs to be changed, the user must be deleted and a new user created.

Further notes

You delete a link with the `no user-account-ext` command.

You show the links in the table "External User Accounts" with the `show user-accounts external` command.

12.1.4.9 no user-account-ext

Description

With this command, you delete the link between a user and a role in the table "External User Accounts".

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`no user-account-ext <user-name-ext>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`user-name-ext`	User name	Enter the name of a user.

Result

The link in the table "External User Accounts" has been deleted.

Further notes

You link a user with a role in the table "External User Accounts" with the `user-account-ext` command.

You show the links in the table "External User Accounts" with the `show user-accounts external` command.

12.1.4.10 user-name case-insensitive

Description

With this command, you specify that no distinction is made between upper- and lower-case for the user name. If user names that differ only in case have already been created, this command is not permissible. The device outputs an error message in this case.

Requirement

- The user is logged in with the "admin" role.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call the command without parameters:

`user-name case-insensitive`

Result

User names are not case-sensitive.

Additional notes

You enable the distinction between upper- and lower-case in user names with the `no user-name case-insensitive` command.

You show the created users with the `show user-accounts` command.

12.1.4.11 no user-name case-insensitive

Description

With this command, you specify that a distinction is made between upper- and lower-case for the user name.

Requirement

- The user is logged in with the "admin" role.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call the command without parameters:

```
no user-name case-insensitive
```

Result

User names are case-sensitive.

Additional notes

You disable the distinction between upper- and lower-case in user names with the `user-name case-insensitive` command.

You show the created users with the `show user-accounts` command.

12.1.4.12 user-group

Description

With this command you link a group with a role.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
user-group <user-group-name> role <role-name> [description <user-group-description>]
```

Note

The character strings for `user-group-name`, `role-name` and `user-group-description` must meet the following conditions:

- The character string must be unique.
- The character string must not include the following characters: | § ? " ; :
- The character string must not include Extended ASCII Codes (characters > 0x7F).
- When the character string contains spaces, the entire characters string must be set in quotation marks.

The parameters have the following meaning:

Parameter	Description	Range of values / note
`user-group`	Keyword for a group name	-
`user-group-name`	Group name	Enter the name of the group. The name must match the group on the RADIUS server. The name must meet the following conditions: • It must be unique. • It must be between 1 and 64 characters long.
`role`	Keyword for the role name	-
`role-name`	Role name	Enter a role name. Users who are authorized with the linked group on the RADIUS server receive the rights of this role locally on the device. You can choose between system-defined and self-defined roles.
`description`	Keyword for the description	-
`user-group-description`	Content of the description	Enter a description for the link. The description text can be up to 100 characters long.

Result

The group is linked to a role.

Further notes

You delete a link with the `no user-group` command.

You show the created links with the `show user-groups` command.

12.1.4.13 no user-group

Description

With this command, you delete the link between a group and a role.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no user-group <user-group-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`user-group-name`	Group name	Enter the name of a group.

Result

The link is deleted.

Further notes

You link a group with a role with the `user-group` command.

You show the created links with the `show user-groups` command.

12.1.4.14 username

Note

User "user" preset in the factory

As of firmware version 2.1, the default user set in the factory "user" is no longer available when the product ships.

If you update a device to firmware V2.1, the user "user" is initially still available. If you reset the device to the factory settings ("Restore Factory Defaults and Restart"), the user "user" is deleted.

You can create users with the role "user".

Description

With this command, you change the password for users with the user name "`user`" or "`admin`".

Requirement

- The user is logged in with the "admin" role.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call up the command with the following parameters:

```
username {user|admin} password <passwd>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`user`	User with the "`user`" user name.	If you have created a user with the user name "`user`", you can change the password for this user with this command.
`admin`	User with the "`admin`" user name.	If you have not renamed the "`admin`" user preset in the factory, you can change the password for this user with this command.

Parameter	Description	Range of values/note
`password`	Keyword for a password	-
`passwd`	Value for the password	Enter the password. The password must meet the following conditions: • It must be unique. • The following characters must not be included: | § ? " ; : • It must not include Extended ASCII Codes (characters > 0x7F). • When the password contains spaces, the entire character string must be set in quotation marks. The strength of the password depends on the set password policy: • `low`: Password length: at least 6 characters • `high`: The password must meet the following conditions: – Password length: at least 8 characters – at least 1 uppercase letter – at least 1 special character – at least 1 number

Result

The password is changed.

Note

Changing the password in Trial mode

Even if you change the password in Trial mode, this change is saved immediately.

Further notes

You show the created users with the `show user-accounts` command.

You can also change the passwords with the `user-account` command.

You display the currently valid password policy with the `show password-policy` command.

12.2 RADIUS client

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol that allows the centralized login of users logging in in a physical or virtual network. This makes central administration of user data possible.

This section describes commands relevant for the configuration of this service.

12.2.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.2.1.1 show radius statistics

Description

This command shows the connection statistics from the RADIUS client to the RADIUS server.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show radius statistics
```

Result

The connection statistics are displayed.

12.2.1.2 show radius server

Description

This command shows the RADIUS server configuration.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
show radius server [<ucast_addr>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ucast_addr`	Value for an IPv4 unicast address	Enter a valid unicast address

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If no parameters are specified, all configured RADIUS servers are displayed.

Result

The RADIUS server configuration is displayed.

12.2.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.2.2.1 login authentication

Description

With this command, you enable authentication via a RADIUS server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

`login authentication {radius | local-and-radius | radius-fallback-local}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`radius`	The login is via a RADIUS server.	-
`local-and-radius`	The login is possible both with the users that exist in the firmware (user name and password) and via a RADIUS server.	The local users have priority. The user is first searched for in the local database. If the user does not exist there, a RADIUS query is sent.
`radius-fallback-local`	The authentication must be handled via a RADIUS server.	A local authentication is performed only when the RADIUS server cannot be reached in the network.

Result

The authentication is made according to the selected parameter.

Further notes

You disable the authentication via a RADIUS server with the `no login authentication` command.

You can display the status of this function and other information with the `show device information` command.

12.2.2.2 no login authentication

Description

With this command, you disable authentication via a RADIUS server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

```
no login authentication
```

Result

The RADIUS authentication is deactivated.

Note

The login is possible only with a local user name and password. If the local logon fails, there is no authentication via a RADIUS server.

Further notes

You enable the authentication via a RADIUS server with the `login authentication` command.

12.2.2.3 radius authorization-mode

Description

With this command you specify for the login authentication how the rights are assigned to the user with a successful authentication.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
radius authorization-mode { standard | vendor-specific }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`standard`	In this mode the user is logged in with administrator rights if the server returns the value "Administrative User" to the device for the attribute "Service Type". In all other cases the user is logged in with read rights.	Default
`vendor-specific`	In this mode, the assignment of rights depends on whether and which group the server returns for the user and whether or not there is an entry for the user in the table "External User Accounts".	-

Result

The assignment of rights during the login authentication is defined.

Further notes

You can display the status of this function and other information with the `show device information` command.

12.2.2.4 radius disconnect-packet

Description

With this command, you enable the evaluation of Disconnect messages of the RADIUS server.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
radius disconnect-packet
```

Result

The device evaluates the Disconnect messages of the RADIUS server.

Additional notes

You show the configuration of a RADIUS server on the client with the `show radius server` command.

12.2.2.5 no radius disconnect-packet

Description

With this command, you disable the evaluation of Disconnect messages of the RADIUS server.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no radius disconnect-packet
```

Result

The device does not evaluate Disconnect messages of the RADIUS server.

Additional notes

You show the configuration of a RADIUS server on the client with the `show radius server` command.

12.2.2.6 radius-server

Description

With this command, you configure a RADIUS server entry on the RADIUS client.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
radius-server { ipv4 <ipv4-address> | fqdn-name <FQDN> } [auth-port
<portno(1-65535)>] [retransmit <1-5>]
```

```
[key <secret-key-string>] [primary] [{login | dot1x  | login-
dot1x}] [test] [timeout <1-120>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
ipv4	Keyword for an IPv4 address.	-
ipv4-address	Value for the IPv4 address of the RADIUS server	Enter a valid IPv4 address.
fqdn-name	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name) of the RADIUS server	Maximum of 100 characters
auth-port	Keyword for the UDP port number for authentication	-
portno	Number of the port	1 ... 65535 Default: 1812
retransmit	Keyword for the number of connection retries	-
<1-5>	Enter the maximum number of retries for an attempted query. The initial connection attempt is repeated the number of times specified here before another configured RADIUS server is queried or the login counts as having failed.	1 ... 5 Default: 3 retries. This means 4 connection attempts
key	Keyword for the key for communication between the authenticator and the server	-
secret-key-string	Value for the key	46 characters Default: "default"
primary	Identifies the RADIUS server as primary server	-
login	The server is used only for the login authentication.	-
dot1x	The server is used only for the 802.1X authentication.	-
login-dot1x	The server is used for both authentication procedures.	Default setting
test	Tests whether or not the specified RADIUS server is available. At the same time you can create a new RADIUS server and run the test.	-
timeout	Keyword for the response wait time. If this time expires, the request is reported as "timed out".	Time until timeout 1 ... 120

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If optional parameters are not specified when configuring, the default values apply.

Note

Primary server

In a network, only one RADIUS server can be selected as the primary server.

If you select a RADIUS server as the primary server, this replaces the server that previously had the role of primary server.

Result

The entry for a connection between the RADIUS client and a server or the identification as primary server is configured.

Additional notes

You delete a RADIUS server entry with the `no radius-server` command.

You show the configuration of a RADIUS server on the client with the `show radius server` command.

You show the statistical information of this function with the `show radius statistics` command.

12.2.2.7 no radius-server

Description

With this command, you delete a RADIUS server entry on the client.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no radius-server { ipv4 <ipv4-address> | fqdn-name <FQDN> }
[primary]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ipv4`	Keyword for an IPv4 address.	-
`ipv4-address`	Value for the IPv4 address of the RADIUS server	Enter a valid IPv4 address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name) of the RADIUS server	Maximum of 100 characters
`primary`	Identifies the RADIUS server as primary server	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The entry for a connection between the RADIUS client and a server or the identification as primary server is deleted.

Additional notes

You configure the connection of a RADIUS client to a server with the `radius-server` command.

You show the configuration of a RADIUS server on the client with the `show radius server` command.

You show the statistical information of this function with the `show radius statistics` command.

12.3 Management Access Control List

This section describes the commands relevant for working with the management access control list.

12.3.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.3.1.1 show authorized-managers

Description

This command shows the information about the configuration of the authorized managers.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ip-source`	Keyword for the network or host address	-
`ip-address`	Value for an IP address	specify a valid IP address

For information on identifiers of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The information about the configuration of the authorized managers is displayed.

12.3.2 Commands in the Global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.3.2.1 authorized-manager

Description

With this command, the Management ACL is enabled.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`authorized-manager`

Result

The Management ACL is enabled.

Additional notes

You disable the function with the `no authorized-manager` command.

12.3.2.2 no authorized-manager

Description

With this command, the Management ACL is disabled.

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`no authorized-manager`

Result

The Management ACL is disabled.

Additional notes

You enable the function with the `authorized-manager` command.

12.3.2.3 authorized-manager ip-source

Description

With this command, you configure the interfaces and protocols via which an authorized manager is allowed to access the device.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameter assignment:

```
authorized-manager ip-source <ip-address> [{<subnet-mask> | /
<prefix-length(0-32)>}]
[interface [<interface-type <0/a-b, 0/c, ...>]
[<interface-type <0/a-b, 0/c, ...>]
[<interface-type <0/a-b, 0/c, ...>]
[<interface-type <0/a-b, 0/c, ...>]]
[vlan <a,b or a-b or a,b,c-d>] [service [snmp] [telnet] [http]
[https] [ssh]]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ip-address`	Specifies the network or the IP address for which the IP manager is authorized	Enter a valid IPv4 address or a network.
`subnet-mask`	Subnet mask that restricts the authorization	Enter a valid mask.
`prefix-length`	Decimal representation of the mask as a number of "1" bits	0 ... 32
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`0/a-b,0/c,...`	Module no. and port no. of the interface	

Parameter	Description	Range of values/note
`vlan`	Keyword for a VLAN connection	• In the "VLAN Bridge" mode Enter a valid VLAN or VLAN range. • In the "Transparent Bridge" mode: The configurations relating to VLANs are ignored. The rules apply to all VLANs. If you have defined certain VLANs with a firmware version < 1.2, the configuration of the VLANs will be replaced during a firmware update with the default value "1-4094".
`a,b or a-b or a,b,c-d`	Number of a VLAN or VLAN range	
`service`	Specifies the services for which the manager is authorized. You can select several options.	• `snmp` • `telnet` • `http` • `https` • `ssh`

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

The IP address 0.0.0.0 means "any manager".

If optional parameters are not specified when configuring, the manager is authorized for all services.

Note

Configuration of the first entry

As long as the list of authorized managers is empty, access to the system is not restricted.

As soon as the list contains an entry and the "authorized-manager" command is executed, access to the system is blocked for all others.

You should therefore configure the interface via which you access the system first because your access is otherwise blocked.

Result

The interfaces and protocols via which an authorized manager is allowed to access the device are configured.

Note

No restrictions for console port

The restrictions do not apply to the serial console (console port).

Additional notes

You delete an interface for access of an authorized manager with the `no authorized-manager ip-source` command.

You show the information about the configuration of the authorized managers with the `show authorized-manager` command.

You change the mode with the `base bridge-mode` command.

12.3.2.4 no authorized-manager ip-source

Description

With this command, you delete an interface via which an authorized manager is allowed to access the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no authorized-manager ip-source <ip-address>
   [{<subnet-mask>|/<prefix-length(0-32)>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ip-address`	Specifies the network or the IP address for which the IP manager is authorized	Enter a valid IP address or a network
`subnet-mask`	Subnet mask that restricts the authorization	Enter a valid mask
`prefix-length`	Decimal representation of the mask as a number of "1" bits	0 ... 32

For information on identifiers of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

An authorized manager is deleted from the list.

Further notes

You configure the interfaces and protocols via which an authorized manager is allowed to access the device with the `authorized-manager ip-source` command.

You show the information about the configuration of the authorized managers with the `show authorized-manager` command.

12.4 Port Access Control List Locked Ports

With the Port Access Control List Locked Ports functionality, MAC addresses that do not age are collected on a port after the `start` command. With the `stop` command, these addresses are converted to static entries in the address list and the aging is reactivated for all the addresses that follow.

If the learning of addresses on this port is then disabled, data packets are only forwarded to the static addresses entered in the table.

This section describes commands relevant for the configuration of this function.

12.4.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.4.1.1 show lock port

Description

This command shows whether or not the learning of MAC entries is enabled or locked on an interface.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show lock port [<interface-type><interface-id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select an interface, the configuration of all interfaces is displayed.

Result

The configuration of the interface for the learning of MAC entries is displayed.

12.4.2 Commands in the Global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.4.2.1 clear-all-static-unicast

Description

With this command, you delete all static unicast MAC address entries from the MAC address table.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
clear-all-static-unicast
```

Result

The static unicast MAC address entries are deleted from the MAC address table.

12.4.2.2 auto-learn

Description

With this command, you change to the AUTOLEARN mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
auto-learn
```

Result

You are now in the AUTOLEARN mode.

The command prompt is as follows:

```
cli(config-auto-learn)#
```

Further notes

You exit the AUTOLEARN configuration modewith the command `end` or `exit`.

12.4.3 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.4.3.1 switchport lock

Description

With this command, you block the learning of MAC entries. Only the static address entries of the MAC address list are used on the port.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
switchport lock
```

Result

The learning of MAC addresses is blocked.

Further notes

You enable the learning of MAC addresses with the `no switchport lock` command.

You display the configuration with the `show lock port` command.

12.4.3.2 no switchport lock

Description

With this command, you enable the learning of MAC addresses.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call the command without parameters:

`no switchport lock`

Result

The learning of MAC addresses is enabled.

Further notes

You block the learning of MAC addresses with the `switchport lock` command.

You display the configuration with the `show lock port` command.

12.4.4 Commands in the AUTOLEARN mode

This section describes commands that you can call up in the AUTOLEARN mode.

In global configuration mode, enter the `auto-learn` command to change to this mode.

- If you exit the AUTOLEARN mode with the `exit` command, you return to the Global configuration mode.
- If you exit the AUTOLEARN mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in AUTOLEARN mode.

To do this, you replace `[command]` with the command that you want to execute.

12.4.4.1 start

Description

With this command, you start automatic learning. During automatic learning, the aging timer is disabled for all learned addresses.

Requirement

You are in the AUTOLEARN mode.

The command prompt is as follows:

```
cli(config-auto-learn)#
```

Syntax

Call the command without parameters:

```
start
```

Result

The learned MAC addresses are entered in the "port database" with the aging time 0. (The entries are NOT deleted when the "MAC Address Aging Time" expires).

Further notes

You stop automatic learning with the `stop` command.

12.4.4.2 stop

Description

With this command, you stop automatic learning and convert all learned MAC addresses to static entries.

Requirement

You are in the AUTOLEARN mode.

The command prompt is as follows:

```
cli(config-auto-learn)#
```

Syntax

Call the command without parameters:

```
stop
```

Result

Automatic learning is stopped and all learned entries are converted to static entries.

Further notes

You start automatic learning with the `start` command.

12.5 Port Based Network Access Control

This section describes commands for working with port-based network access control (PNAC).

12.5.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.5.1.1 show dot1x

Description

This command shows information about port-based network access control (PNAC).

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show dot1x [{ interface <interface-type> <interface-id> |
statistics interface <interface-type> <interface-id> }]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	
`statistics interface`	Keyword for the display of the statistical data of the dot1x Authenticator for an interface	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The dot1x information is displayed.

12.5.1.2 show dot1x guest-vlan mac-info

Description

This command displays which MAC address and which port are assigned to a guest VLAN.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show dot1x guest-vlan mac-info
```

Result

A list with guest VLAN, MAC address and port is displayed.

12.5.1.3 show dot1x mac-auth mac-info

Description

This command shows the MAC addresses for which MAC authentication is enabled.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show dot1x mac-auth mac-info
```

Result

A list of the MAC addresses is displayed.

12.5.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.5.2.1 dot1x guest-vlan

Description

With this command, you enable the guest VLAN function for the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
dot1x guest-vlan
```

Result

The guest VLAN function is enabled for the device.

Further notes

You also still need to enable the guest VLAN function for every port intended to use this function. You do this with the `dot1x guest-vlan` command in the Interface configuration mode.

You disable the function with the `no dot1x guest-vlan.` command

You display this setting and other information with the `show dot1x` command.

12.5.2.2 no dot1x guest-vlan

Description

With this command, you disable the guest VLAN function for the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no dot1x guest-vlan
```

Result

The guest VLAN function is disabled for the device.

Further notes

You enable the function with the `dot1x guest-vlan.` command

You display this setting and other information with the `show dot1x` command.

12.5.2.3 dot1x fallback timeout

Description

With this command, you specify the time interval in seconds after which the device is reinitialized for 802.1X authentication at the relevant port after MAC authentication fails. The default value is 0 seconds, i.e. there is no fallback timeout and no reinitialization for the 802.1X authentication.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameter:

```
dot1x fallback timeout <seconds(0-3600)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`seconds`	The length of the time interval in seconds after which the port is reinitialized for 802.1X authentication.	0 ... 3600 Default: 0

Result

The time interval for the 802.1X Fallback Timeout is configured.

Additional notes

You display this setting and other information with the `show dot1x` command.

You configure the maximum number of reinitializations for 802.1X authentication with the `dot1x fallback retry count` command.

12.5.2.4 dot1x fallback retry count

Description

With this command, you specify how often the port is reinitialized for 802.1X authentication after MAC authentication fails.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameter:

```
dot1x fallback retry count <count(1-100)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`count`	The maximum number of reinitializations for 802.1X authentication.	1 ... 100 Default: 3

Result

The maximum number of reinitializations for 802.1X authentication is configured.

Additional notes

You display this setting and other information with the `show dot1x` command.

You configure the length of the time interval after which the port is reinitialized for 802.1X authentication with the `dot1x fallback timeout` command.

12.5.2.5 dot1x mac-auth

Description

With this command, you enable MAC authentication for the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
dot1x mac-auth
```

Result

MAC authentication is enabled for the device.

Further notes

You also still need to enable MAC authentication for every port intended to use this function. You do this with the `dot1x mac-auth` command in the Interface configuration mode.

You disable the function with the `no dot1x mac-auth` command.

You display this setting and other information with the `show dot1x` command.

12.5.2.6 no dot1x mac-auth

Description

With this command, you disable MAC authentication for the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no dot1x mac-auth
```

Result

MAC authentication is disabled for the device.

Further notes

You enable the function with the `dot1x mac-auth` command.

You display this setting and other information with the `show dot1x` command.

12.5.2.7 dot1x nas-id

Description

With this command, you configure the NAS ID for the device that is sent to the server with an authentication request.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameter:

```
dot1x nas-id <identifier>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`identifier`	The NAS ID that the device uses for authentication.	NAS identifier according to RFC 2865 (>= 3 bytes)

Result

The NAS ID of the device is configured.

12.5.3 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.5.3.1 dot1x guest-vlan

Description

With this command, you enable the guest VLAN function for a port.

This function is also known as "Authentication failed VLAN".

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
dot1x guest-vlan
```

Result

The guest VLAN function is enabled for a port.

Further notes

You also need to enable the guest VLAN function for the device. You do this with the `dot1x guest-vlan` command in the Global configuration mode.

You disable the function with the `no dot1x guest-vlan` command.

You display this setting and other information with the `show dot1x` command.

12.5.3.2 no dot1x guest-vlan

Description

With this command, you disable the guest VLAN function for a port.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no dot1x guest-vlan
```

Result

The guest VLAN function is disabled for a port.

Further notes

You enable the function with the `dot1x guest-vlan` command.

You display this setting and other information with the `show dot1x` command.

12.5.3.3 dot1x guest-vlan vlan-id

Description

With this command, you configure a guest VLAN for a port.

The port can only be assigned to the VLAN, if the VLAN has been created on the device. Otherwise Authentication is rejected.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
dot1x guest-vlan vlan-id <vlan-id (1 - 4096)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vlan-id`	Keyword for the VLAN ID	-
-	VLAN ID	1 - 4096

Result

The guest VLAN ID is assigned to the port.

Further notes

You reset the guest VLAN ID to the default value with the `no dot1x guest-vlan vlan-id`command.

You display this setting and other information with the `show dot1x` command.

12.5.3.4 no dot1x guest-vlan vlan-id

Description

With this command, the guest VLAN ID is reset to the default value 1.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no dot1x guest-vlan vlan-id
```

Result

The ID of the guest VLAN has the value 1.

Further notes

You configure the guest VLAN ID with the `dot1x guest-vlan vlan-id` command.

You display this setting and other information with the `show dot1x` command.

12.5.3.5 dot1x guest-vlan reset

Description

This command removes MAC addresses from the guest VLAN. If you specify a MAC address, only this MAC address is removed from the guest VLAN. If you use this command without parameters, all MAC addresses are removed from the guest VLAN.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
dot1x guest-vlan reset [mac <aa:aa:aa:aa:aa:aa>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`mac`	Keyword for the MAC address	-
	MAC address to be removed from the guest VLAN.	`aa:aa:aa:aa:aa:aa`

Result

The specified MAC address or all MAC addresses are no longer assigned to the guest VLAN.

12.5.3.6 set dot1x guest-vlan mac-addr count

Description

With this command, you specify how many MAC addresses can be authenticated on the port at the same time.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
set dot1x guest-vlan mac-addr count <num-of-addresses (1-100)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
num-of-addresses	Maximum number of MAC addresses	1 ... 100

Result

The maximum number of MAC addresses for the port has been specified.

Further notes

You display this setting and other information with the `show dot1x` command.

12.5.3.7 dot1x mac-auth

Description

With this command, you enable MAC authentication for a port.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
dot1x mac-auth [{timeout | sticky}]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`timeout`	Keyword for the 802.1X timeout with which the conditions for the MAC authentication are defined. When you specify this keyword, MAC authentication is only possible after a 802.1X timeout, but not after a failed 802.1X authentication.	-
`sticky`	If this parameter is configured, new MAC addresses are automatically authenticated or rejected depending on the number of currently authenticated MAC addresses on a port (MAC Auth. Max Allowed Addresses): • If a new MAC address requests on a port and the number of currently authenticated MAC addresses on the port is < the number of maximum permitted MAC addresses, the request is automatically successful. • If a new MAC address requests on a port and the number of currently authenticated MAC addresses on the port is ≥ the number of maximum permitted MAC addresses, the request automatically fails. MAC addresses authenticated through this mechanism are subject to the following: • They are stored as static MAC addresses. • The authentication status is retained during link change events and restart of the device. You must delete the MAC addresses manually. Prerequisites: • The parameter is only active if MAC Authentication is globally enabled for the device. • The "802.1X Auth. Control" is configured to "Force Authorized". • A value ≥ 1 and ≤ 5 is configured for "MAC Auth. Max Allowed Addresses". • The number of statically configured MAC addresses on a port is ≤ the maximum number of permitted addresses.	No RADIUS server configuration is required for this parameter. If the parameter is configured, the following applies to the corresponding port: • Only values ≤ 5 can be configured for "MAC Auth. Max Allowed Addresses". • New static MAC addresses can only be configured on the port as long as their number is < the number of maximum permitted MAC addresses ("MAC Auth. Max Allowed Addresses").

If you call the command without parameters, MAC authentication is possible both after a 802.1X timeout and after a failed 802.1X authentication.

Result

MAC authentication is enabled for a port.

Further notes

In addition, you must enable MAC authentication globally for the device. You do this with the `dot1x mac-auth` command in the Global configuration mode.

You configure the port control parameter with the `dot1x port-control` command.

You specify how many MAC addresses can be authenticated on the port at the same time with the `set dot1x mac-auth mac-addr count` command.

You disable the function with the `no dot1x mac-auth` command.

You display this setting and other information with the `show dot1x` command.

12.5.3.8 no dot1x mac-auth

Description

With this command, you disable MAC authentication for a port. You can also define the conditions for a MAC authentication with a parameter.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no dot1x mac-auth [timeout]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`timeout`	Keyword for the 802.1X timeout with which the conditions for the MAC authentication are defined. When you specify this keyword, MAC authentication is also possible after a failed 802.1X authentication. If you call the command without the `timeout` parameters, you disable the MAC authentication for a port.	-

Result

MAC authentication is disabled for a port or the conditions for MAC authentication are defined.

Further notes

You enable the function with the `dot1x mac-auth` command.

You display this setting and other information with the `show dot1x` command.

12.5.3.9 dot1x mac-auth default-value

Description

If the RADIUS server specifies a VLAN ID during a successful authentication, the current PVID of the port is changed to the value transmitted by the RADIUS server. The prerequisite is that the assignment of the VLAN ID was enabled by the RADIUS server in the WBM or with the `dot1x mac-auth vlan-assign` command. An "Untagged membership" of the port may be set up in the relevant VLAN to enable communication in the respective VLAN.

The Default VLAN ID determines the assignment of the VLAN ID when the provision of the VLAN ID by the RADIUS server is enabled, but the RADIUS server does not send a VLAN ID after successful authentication. You have two options:

- **The value "0" is configured for the default VLAN ID**
  The PVID currently configured for the port continues to be used.
- **A value in the range from "1 ... 4094" is configured for the Default VLAN ID**
  The PVID of the port is changed to the "Default VLAN ID" configured in this column as if it had been transmitted by the RADIUS server.

In all cases, a changed PVID is reset to the originally configured value after the device logs out. Any "Port membership" that has been set up is deleted again. This applies to both 802.1X authentication and MAC authentication.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:

```
dot1x mac-auth default-vlan <vlan-id(1-4094)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`vlan-id`	The default VLAN ID	1 ... 4094

Result

The value for the default VLAN ID is configured.

Additional notes

You display this setting and other information with the `show dot1x interface` command.

You reset the default VLAN ID to the value "0" with the `no dot1x mac-auth default-vlan` command.

12.5.3.10 no dot1x mac-auth default-vlan

Description

With this command, you set the default VLAN ID to the value "0".

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no dot1x mac-auth default-vlan
```

Result

The value for the default VLAN ID is set to the value "0".

Additional notes

You display this setting and other information with the `show dot1x interface` command.

You configure the default VLAN ID with the `dot1x mac-auth default-vlan` command.

12.5.3.11 dot1x mac-auth port reset

Description

With this command, you reset MAC authentication for a port.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
dot1x mac-auth port [mac <aa:aa:aa:aa:aa:aa>] reset
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mac`	Keyword for a MAC address	-
`aa:aa:aa:aa:aa:aa`	MAC address of the interface	aa:aa:aa:aa:aa:aa

Result

MAC authentication is reset for the port.

12.5.3.12 dot1x mac-auth vlan-assign

Description

With this command you enable the assignment of the VLAN ID for a MAC address by the RADIUS server.

The port can only be assigned to the VLAN, if the VLAN has been created on the device. Otherwise Authentication is rejected.

If during authentication a port is assigned to a VLAN dynamically using this function, assignment using the VLAN ID or the VLAN name is possible. Configure the following values on the RADIUS server:

- Tunnel-Type = VLAN
- Tunnel-Medium-Type = IEEE-802
- Tunnel-Private-Group-Id = VLAN ID or VLAN name

The IE switch distinguishes as follows:

- VLAN ID: The RADIUS server transfers a numeric string for the parameter "Tunnel-Private-Group-Id".
- VLAN name: The RADIUS server transfers an alphanumeric string for the parameter "Tunnel-Private-Group-Id".

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
dot1x mac-auth vlan-assign
```

Result

The VLAN ID for a MAC address is assigned by the RADIUS server.

Additional notes

You disable the assignment of the VLAN ID for a MAC address by the RADIUS server with the `no dot1x mac-auth vlan-assign` command.

You display this setting and other information with the `show dot1x` command.

12.5.3.13 no dot1x mac-auth vlan-assign

Description

With this command you disable the assignment of the VLAN ID for a MAC address by the RADIUS server.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no dot1x mac-auth vlan-assign
```

Result

The VLAN ID for a MAC address is no longer assigned by the RADIUS server.

Further notes

You enable the assignment of the VLAN ID for a MAC address by the RADIUS server with the `dot1x mac-auth vlan-assign` command.

You display this setting and other information with the `show dot1x` command.

12.5.3.14 dot1x port-control

Description

With this command, you configure port control parameter of the authenticator.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`dot1x port-control {auto|force-authorized|force-unauthorized}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`auto`	Authentication according to IEEE 802.1x is enabled for the interface. The data traffic via the interface is permitted or blocked depending on the authentication result.	-
`force-authorized`	data traffic via the interface is permitted without restrictions	Default: `force-authorized` enabled
`force-unauthorized`	data traffic via the interface is blocked	-

Result

The port control parameter is configured.

Further notes

You can reset the port control parameter to the default with the `no dot1x port-control` command.

You can display the status of this function and other information with the `show dot1x`command.

12.5.3.15 no dot1x port-control

Description

With this command, you reset the port control parameter of the authenticator to the default value.

The default value is `force-authorized`.

With this, data traffic is permitted without restrictions.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no dot1x port-control
```

Result

The port control parameter of the authenticator is reset to the default value.

Further notes

You configure the port control parameter with the `dot1x port-control` command.

You can display the status of this function and other information with the `show dot1x`command.

12.5.3.16 set dot1x mac-auth mac-addr count

Description

With this command, you specify how many MAC addresses can be authenticated on the port at the same time.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
set dot1x mac-auth mac-addr count <num-of-addresses (1-200)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
num-of-addresses	Maximum number of MAC addresses	1 ... 200

Result

The maximum number of MAC addresses for the port has been specified.

Additional notes

You display this setting and other information with the `show dot1x` command.

You configure so that after the first successful authentication of a MAC address, the port is released for all MAC addresses with the command `no dot1x mac-auth mac-addr count`.

12.5.3.17 dot1x reauthentication

Description

With this command, you enable the 802.1X Re-Authentication function for the selected interface. When the function is enabled, the authenticator repeats authentication of the client periodically,

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
dot1x reauthentication
```

Result

Periodic authentication is enabled for the selected interface.

Further notes

You disable the function with the `no dot1x reauthentication` command.

You can display the status of this function and other information with the `show dot1x`command.

12.5.3.18 no dot1x reauthentication

Description

With this command, you disable the function that repeats the authentication of the client by the authenticator periodically.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no dot1x reauthentication
```

Result

Periodic authentication is disabled.

Further notes

You enable the function with the `dot1x reauthentication` command.

You can display the status of this function and other information with the `show dot1x`command.

12.5.3.19 dot1x timeout reauth-period

Description

With this command, you specify the time interval for reauthentication.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:

```
dot1x timeout reauth-period <seconds(300-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
seconds	Time interval in seconds after which the device is reauthenticated at the relevant port. Default: 3600 seconds	300 ... 65535

Result

The reauthentication interval for the port has been specified.

Additional notes

You display this setting and other information with the `show dot1x` command.

You reset the reauthentication interval to the default value with the `no dot1x timeout reauth-period` command.

12.5.3.20 no dot1x timeout reauth-period

Description

With this command, you reset the time interval for reauthentication to the default value.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command without parameters:

```
no dot1x timeout reauth-period
```

Result

The reauthentication interval for the port has been reset to the default value.

Additional notes

You display this setting and other information with the `show dot1x` command.

You define the time interval for reauthentication with the `dot1x timeout reauth-period` command.

12.5.3.21 dot1x timeout tx-period

Description

With this command, you specify the time interval in seconds after which an EAP request packet is sent if no client responds. If MAC authentication is enabled, a switch is made from 802.1X authentication to MAC authentication after the third EAP request packet. The default value is 5 seconds.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:

```
dot1x timeout tx-period <seconds(1-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`seconds`	Time interval in seconds.	1 ... 65535 Default: 5 seconds

Result

The wait time for sending EAP request packets is set.

Additional notes

You display this setting and other information with the `show dot1x` command.

12.6 Brute Force Prevention

12.6.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.6.1.1 show brute-force-prevention config

Description

This command shows the configuration of the "Brute Force Prevention" function.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:
`show brute-force-prevention config`

Result

The parameters of the "Brute Force Prevention" function are displayed.

Additional notes

You display the status of the "Brute Force Prevention" function with the `show brute-force-prevention status` command.

You configure the maximum number of invalid login attempts with the `brute-force-prevention ip-specific-login-attempts` command or the `brute-force-prevention user-specific-login-attempts` command.

You configure the duration for recording invalid login attempts with the `brute-force-prevention trigger-interval` command.

You configure the duration for blocking further invalid login attempts with the `brute-force-prevention auto-reset-timer` command.

You stop the blocking of further invalid login attempts with the `brute-force-prevention reset` command.

12.6.1.2 show brute-force-prevention status

Description

This command shows the number of invalid login attempts. It is also specified whether further login attempts are temporarily blocked by the "Brute Force Prevention" function.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:
`show brute-force-prevention status`

Result

The number of invalid login attempts and a blocking of the login are displayed.

Additional notes

You display the parameters of the function "Brute Force Prevention" with the `show brute-force-prevention config` command.

You configure the maximum number of invalid login attempts with the `brute-force-prevention ip-specific-login-attempts` command or the `brute-force-prevention user-specific-login-attempts` command.

You configure the duration for recording invalid login attempts with the `brute-force-prevention trigger-interval` command.

You configure the duration for blocking further invalid login attempts with the `brute-force-prevention auto-reset-timer` command.

You stop the blocking of further invalid login attempts with the `brute-force-prevention reset` command.

12.6.2 Commands in global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

12.6.2.1 brute-force-prevention auto-reset-timer

Description

With this command, you specify the time in minutes for which the device blocks login because the maximum number of invalid login attempts was exceeded.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:
`brute-force-prevention auto-reset-timer <minutes (0-255)>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`minutes`	Time in minutes for which the device blocks login.	0 ... 255 0: Disabled Default: 12

Result

Login is possible again after the configured time period.

Further notes

You show the configuration of the Brute Force Prevention with the `show brute-force-prevention config` command.

You display the status of the Brute Force Prevention with the `show brute-force-prevention status` command.

You disable the BFP timer with the `no brute-force-prevention auto-reset-timer` command.

12.6.2.2 no brute-force-prevention auto-reset-timer

Description

With this command, you reset the timer to the default value.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:
`brute-force-prevention auto-reset-timer`

Result

The timer is reset to the default value.

Further notes

You show the configuration of the Brute Force Prevention with the `show brute-force-prevention config` command.

You display the status of the Brute Force Prevention with the `show brute-force-prevention status` command.

You enable the BFP timer with the `brute-force-prevention auto-reset-timer` command.

12.6.2.3 brute-force-prevention ip-specific-login-attempts

Description

With this command, you specify the maximum number of invalid login attempts for an IP address. Further login attempts for this IP address are blocked for a specific time.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:
`brute-force-prevention ip-specific-login-attempts <number-of-login-attempts (0-255)>`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`number-of-login-attempts`	The maximum number of invalid login attempts for an IP address.	0 ... 255 0: Disabled Default: 10

Result

The maximum number of invalid login attempts for an IP address is set.

Additional notes

You show the configuration of the Brute Force Prevention with the `show brute-force-prevention config` command.

You display the status of the Brute Force Prevention with the `show brute-force-prevention status` command.

You disable the IP-specific BFP with the `no brute-force-prevention ip-specific-login-attempts` command.

12.6.2.4 no brute-force-prevention ip-specific-login-attempts

Description

With this command, you reset the function to the default value.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:
`no brute-force-prevention ip-specific-login-attempts`

Result

The function is reset to the default value.

Additional notes

You show the configuration of the Brute Force Prevention with the `show brute-force-prevention config` command.

You display the status of the Brute Force Prevention with the `show brute-force-prevention status` command.

You enable the IP-specific BFP with the `brute-force-prevention ip-specific-login-attempts` command.

12.6.2.5 brute-force-prevention user-specific-login-attempts

Description

With this command, you specify the maximum number of invalid login attempts for a user. Further login attempts for this user are blocked for a specific time. All users that are not configured as local users for the device are summarized under the user name "UnknownUser".

Requirement

- With login authentication, the "Local" or "Local and RADIUS" mode is set.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call up the command with the following parameters:
`brute-force-prevention user-specific-login-attempts <number-of-login-attempts (0-255)>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`number-of-login-attempts`	The maximum number of invalid login attempts for a user.	0 ... 255 0: Disabled Default: 12

Result

The maximum number of invalid login attempts for a user is set.

Further notes

You show the configuration of the Brute Force Prevention with the `show brute-force-prevention config` command.

You display the status of the Brute Force Prevention with the `show brute-force-prevention status` command.

You disable the user-specific BFP with the `no brute-force-prevention user-specific-login-attempts` command.

You configure login authentication with the `login authentication` command.

12.6.2.6 no brute-force-prevention user-specific-login-attempts

Description

With this command, you reset the function to the default value.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:
`no brute-force-prevention user-specific-login-attempts`

Result

The function is reset to the default value.

Further notes

You show the configuration of the Brute Force Prevention with the `show brute-force-prevention config` command.

You display the status of the Brute Force Prevention with the `show brute-force-prevention status` command.

You enable the user-specific BFP with the `brute-force-prevention user-specific-login-attempts` command.

12.6.2.7 brute-force-prevention trigger-interval

Description

With this command, you specify the time in minutes for which counting of invalid login attempts is relevant. When the permissible number of invalid login attempts (per user or per IP) is reached during this time, the device blocks login for a specific period of time. Invalid login attempts per user and per IP address are handled independently of one another.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:
`brute-force-prevention trigger-interval <minutes (5-255)>`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`minutes`	The duration for counting invalid login attempts.	5 ... 255 Default: 5

Result

The duration for counting invalid login attempts is set.

Additional notes

You show the configuration of the Brute Force Prevention with the `show brute-force-prevention config` command.

You display the status of the Brute Force Prevention with the `show brute-force-prevention status` command.

12.6.2.8 brute-force-prevention reset

Description

With this command, you end blocking of login for a user or an IP address and set the following counters and time measurements back to the value "0":

- Number of failed login attempts
- Time since the last failed login attempt
- Remaining time until login is possible again

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:
```
brute-force-prevention reset {user <user-name> | ipv4 <ipv4-address> | ipv6 <ipv6-address>}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`user`	Keyword for a user name.	-
`user-name`	The user name for which login is possible again.	Enter a valid user name.
`ipv4`	Keyword for an IPv4 address.	-
`ipv4-address`	The IPv4 address for which login is possible again.	Specify a valid IPv4 address.
`ipv6`	Keyword for an IPv6 address.	-
`ipv6-address`	The IPv6 address for which login is possible again.	Specify a valid IPv6 address.

Result

Blocking of the login has been removed.

Additional notes

You show the configuration of the Brute Force Prevention with the `show brute-force-prevention config` command.

You display the status of the Brute Force Prevention with the `show brute-force-prevention status` command.

Diagnostics 13

The monitoring of the system and error diagnostics are handled in different ways:

- Events and faults handling:
  Predefined events generate a message. These messages can be distributed in different ways:
  - Entry in the local log
  - Transfer to the Syslog server
  - Sending as e-mail
  - Sending as SNMP trap
- Syslog:
  Configures the transfer to the Syslog server
- Remote Monitoring (RMON):
  Variables of the Management Information Base are monitored for the violation of limit values and messages are generated if they do. These messages are collected and can be distributed in the following ways:
  - Entry in the local log
  - Sending as SNMP trap
  - Transfer to the Syslog server
  - Transfer to a network management station using SNMP
- Port mirroring:
  Mirroring of ports to analyze the data stream without disturbing operation
- Loop Detection:
  Detection and monitoring of parallel connections or loops in an Ethernet network. Loops in the network can cause total failure of the transfer and must be detected and eliminated.

13.1 Event and fault handling

In events and faults handling, you set the events whose messages will be distributed in one of the available ways.

You configure the monitoring of certain system events and power supply and physical interfaces in the Events configuration mode.

13.1.1 logging console

Description

With this command, you display the log messages in the console. The function can only be active on one connection at a time.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
logging console
```

Result

The output of the log messages in the console is activated.

Further notes

You disable the function with the `no logging console` command.

As default the function is "disabled".

13.1.2 no logging console

Description

With this command, you disable the output of log messages in the console.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
no logging console
```

Result

The function is disabled.

Further notes

You enable the function with the `logging console` command.

As default the function is "disabled".

13.1.3 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.1.3.1 show counter log-events

Description

This command displays the sum of all events with "Critical" severity as well as "Warning" severity within the last 24 hours.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

This`cli>` or `cli#`

Syntax

Call the command without parameters:
`show counter log-events`

Result

The sum of all events is displayed per severity.

13.1.3.2 show events config

Description

This command shows the current configuration for forwarding the messages of the various event types.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show events config
```

Result

The current configuration of the events display is displayed.

13.1.3.3 show events severity

Description

This command shows the degree of severity of an event ("Info", "Warning" or "Critical") starting at which a notification (sending of an e-mail, entry in the Syslog table, entry in the Syslog file) is generated.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show events severity
```

Result

The corresponding degree of severity is shown for each type of notification.

Further notes

You configure the assignment of the degree of severity of an event and the type of notification with the `severity` command.

13.1.3.4 show events faults config

Description

This command shows the current configuration of the following error monitoring functions:

- Monitoring of the power supply for power outage
- Monitoring of the network connections for a change in the connection status

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show events faults config [{power|link}]
```

The parameters have the following meaning:

Parameter	Description
`power`	Monitoring of the power supply for power outage
`link`	Monitoring of the network connections for a change in the connection status

If no parameters are specified, the settings for both error monitoring functions are displayed.

Result

The current configuration of the selected error monitoring function is displayed.

13.1.3.5 show events faults status

Description

This command shows the status messages of fault monitoring of the power supply and network connections.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show events faults status
```

Result

A table with the status messages of the error monitoring functions is displayed.

13.1.3.6 show startup-information

Description

This command shows the startup information.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show startup-information
```

Result

The startup information is displayed.

13.1.3.7 show logbook

Description

With this command, you display the content of the logbook. The log entries are categorized differently.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show logbook
```

or

Call up the command with the following parameters:

```
show logbook [{ info | warning | critical }]
```

The parameters have the following meaning:

Parameter	Description
`info`	All log entries of the category "Information" are displayed.
`warning`	All log entries of the category "Warning" are displayed.
`critical`	All log entries of the category "Critical" are displayed.

Result

The content of the logbook is displayed.

13.1.3.8 show fault counter

Description

This command shows the number of errors since the last startup.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show fault counter
```

Result

The number of faults is displayed.

Further notes

You reset the counter for the errors with the `clear fault counter` command.

13.1.3.9 show cabletest interface

Description

This command shows the result of the cable test of the interface.

Requirement

- The interface has no active data traffic.
- The `cabletest interface` function was used on the specified interface in the Global configuration mode.
- You are in User EXEC mode or in Privileged EXEC mode.
  The command prompt is:
  `cli>` or `cli#`

Syntax

Call the command with the following parameter assignment:

```
show cabletest interface <interface-type> <interface-id>
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type of interface	Enter a valid interface.
`interface-id`	Interface identifier	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The result is displayed.

Additional notes

You enable the cable test function with the `cabletest interface` command in the Global configuration mode.

13.1.3.10 show interface transceiver details

Description

This command runs error diagnostics for an SFP port.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameter assignment:

```
show interface transceiver details
```

Result

Hardware information (model, serial number) and operating parameters (data transmission rate, voltage and current consumption as well as the transmit and receive power) for SFP port are displayed.

13.1.3.11 show power-line-state

Description

This command shows the status of the power supply.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show power-line-state
```

Result

The status of the power supply is displayed.

13.1.4 clear logbook

Description

With this command, you delete the content of the logbook.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
clear logbook
```

Result

The content of the logbook is deleted.

13.1.5 clear fault counter

Description

With this command you reset the counter that shows the number of faults since the last startup.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
clear fault counter
```

Result

The counter is set to "0".

Further notes

You shows the number of faults since the last startup with the `show fault counter` command.

13.1.6 fault report ack

Description

Some errors can be acknowledged and thus removed from the error list, e.g. an error of the event "Cold/warm restart".

With this command, you can acknowledge these errors or remove them from the error list.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameter:

```
fault report ack <fault-state-id>
```

The parameter has the following meaning:

Parameters	Description	Range of values/note
`fault-state-id`	Error ID	Enter the ID of the error. You determine the ID with the "`show events faults status`" command.

Result

The error is acknowledged and removed from the error list.

13.1.7 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.1.7.1 events

Description

With this command, you change to the EVENTS configuration mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
events
```

Result

You are now in the EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Further notes

You exit the EVENTS configuration mode with the command `end` or `exit`.

13.1.7.2 cabletest interface

Description

With this command, you enable the cable test for the specified interface.

Note

Wire pairs

Wire pairs 4-5 and 7-8 of 10/100 Mbps network cables are not used.

The wire pair assignment - pin assignment is as follows (DIN 50173):

Pair 1 = pin 1-2

Pair 2 = pin 3-6

Pair 3 = pin 4-5

Pair 4 = pin 7-8

Requirement

- The interface has no active data traffic.
- You are in the Global configuration mode.
  The command prompt is:
  `cli(config)#`

Syntax

Call up the command without parameters or with the following parameter assignment:

```
cabletest interface <interface-type> <interface-id> [force]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface-type`	Type of interface	Enter a valid interface.
`interface-id`	Interface identifier	
`force`	Forces a `link down` during the test	Necessary parameter if there is a `link up` on the interface.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value is used.

Result

Following the test phase, the result is displayed.

The value for the distance has a tolerance of +/- 1 m.

13.1.7.3 link flap count

Description

Use this command to configure the maximum number of allowed changes between "Link up" and "Link down" within the flap time.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:
`link flap count <integer (1-60)>`

The parameters have the following meaning:

Parameter	Description	Range of values / note
-	Configure the maximum number.	1 ... 60

Result

The Flap Count is configured.

Additional notes

You configure the flap time with the command `link flap time`.

You configure the flap reaction with the `link flap reaction` command.

13.1.7.4 link flap reaction

Description

Use this command to configure what happens when the fault occurs.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:
`link flap reaction { notify | notify-powerdown }`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`notify`	If the error occurs, a persistent error message is triggered that needs to be acknowledged by the user.	-
`notify-powerdown`	If the error occurs, a persistent error message is triggered that needs to be acknowledged by the user and the port is disabled.	-

Result

The Flap Reaction is configured.

Additional notes

You configure the flap time with the command `link flap time`.

You configure the flap count with the `link flap count` command.

You acknowledge the error message with the command `fault report ack`.

You manually enable a port with the command `power`.

13.1.7.5 link flap time

Description

You use this command to configure the time interval in which the maximum number of allowed changes between "Link up" and "Link down" is monitored.

If a port changes between "Link up" and "Link down" within the flap time more often than the value of the flap count, the fault is triggered.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:
`link flap time <seconds (1-60)>`

The parameters have the following meaning:

Parameter	Description	Range of values / note
-	Configure the time interval in seconds.	1 ... 60

Result

The Flap Time is configured.

Additional notes

You configure the flap count with the `link flap count` command.

You configure the flap reaction with the `link flap reaction` command.

13.1.8 Commands in the Events configuration mode

This section describes commands that you can call up in the EVENTS configuration mode.

In global configuration mode, enter the `events` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

- If you exit the EVENTS configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the EVENTS configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in EVENTS configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.1.8.1 add log

Description

This command is used to create a log message with the desired severity in the event log.

Requirement

You are in the EVENTS Configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call the command without parameters:

```
add log <log-entry> [{ emergency | alert | critical | error |
warning | notice | informational }]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`log-entry`	Entry in the logbook	max. 150 characters
-	Severity level	Specify the desired severity. • `emergency` • `alert` • `critical` • `error` • `warning` • `notice` • `informational`

Result

The entry has been made in the event log.

13.1.8.2 client config

Description

With this command, you enable one of the clients that processes or forwards the messages of the device.

The following clients are available:

- `syslog`: sends the messages to the Syslog server
- `trap`: sends the messages as SNMP trap to a configured recipient
- `email`: sends the messages as e-mails

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
client config {syslog | trap | email | all}
```

The parameters have the following meaning:

Parameter	Description
`syslog`	Enables the client that sends the messages to the Syslog server
`trap`	Enables the client that sends the SNMP traps
`email`	Enables the client that sends the e-mails
`all`	Enables all clients at once

Result

The client selected for the transmission is enabled.

Additional notes

You display the status of the events and the clients with the `show events config` command.

You disable a client with the `no client config` command.

13.1.8.3 no client config

Description

With this command, you disable one of the clients that processes or forwards the messages of the device.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
no client config {syslog | trap | email | all}
```

The parameters have the following meaning:

Parameter	Description
`syslog`	Disables the client that sends the messages to the Syslog server
`trap`	Disables the client that sends the SNMP traps
`email`	Disables the client that sends the e-mails
`all`	Disables all clients at once

Result

The client selected for the transmission is disabled.

Additional notes

You display the status of the events and the clients with the `show events config` command.

You enable the function with the `client config` command.

13.1.8.4 event config

Note

Depending on the device type, the IE switch does not support all described parameters; see section "Features not supported (Page 40)".

Description

With this command, you configure which of the various message types of the device will be stored or forwarded.

The following events or message types are available:

- Message if there is cold or warm restart
- Message when there is a status change on a physical interface
- Message if there is an incorrect login
- Message when there is a Remote Monitoring alarm (RMON alarm)
- Message when there is a status change in the power supply
- Message when there is a status change in the redundancy manager (RM)
- Message when there is a status change on a standby connection
- Message when there is a status change in the error monitoring
- Message when there is a change in the spanning tree
- Message when there is a status change of the VRRP routers
- Message if there is a status change in the detection of network loops
- Message on status change of OSPF
- Message when there is a status change in the 802.1X authentication
- Message on status change of PoE
- Message on status change of FMP
- Message when there is a status change in the diagnostics data
- Message on status change of Link Check
- Message when an error was detected in the CLI script file

- Message on error in connection with secure NTP
- Message on persistent saving of configuration
- Message when there is a status change of the MRP Interconnection connection
- Message on non-configurable entry in the log table
- Message relating to the DHCP server

These messages can be processed by the clients in different ways:

- Entry in the logbook of the device
- Sending the message to the Syslog server
- Sending an e-mail
- Sending an SNMP trap

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
event config
{cold-warmstart|linkchange|authentication-failure|rmon-alarm|power-
change|
rm-state-change|standby-state-change|faultstate-change|stp-change|
vrrp-state-change|loopd-state-change|ospf-state-change|dot1x-port-
auth-state-change|
poe-state-change|fmp-state-change|env-data-change|linkcheck-change|
cli-script-file-status|secure-ntp|config-change|mrp-interconnection-
state-change|
service-information|dhcp-server|all} {logtable|syslog|email|trap|
faults|all}
```

The parameters have the following meaning:

Parameter	Description
`cold-warmstart`	Message if there is cold or warm restart
`linkchange`	Message when there is a status change on a physical interface
`authentication-failure`	Message if there is an incorrect login
`rmon-alarm`	Message when there is a RMON alarm
`power-change`	Message when there is a status change in the power supply
`rm-state-change`	Message when there is a status change in the redundancy manager
`standby-state-change`	Message when there is a status change on a standby connection
`faultstate-change`	Message when there is a status change in the error monitoring

Parameter	Description
`stp-change`	Message when there is a change in the spanning tree
`vrrp-state-change`	Message on status change of VRRP routers
`loopd-state-change`	Message if there is a status change in the detection of network loops
`ospf-state-change`	Message on status change of OSPF
`dot1x-port-auth-state-change`	Message when there is a status change in the 802.1X authentication
`poe-state-change`	Message on status change of PoE
`fmp-state-change`	Message on status change of FMP
`env-data-change`	Message when there is a status change in the diagnostics data
`linkcheck-change`	Message on status change of Link Check
`cli-script-file-status`	Message when an error was detected in the CLI script file
`secure-ntp`	Message on error in connection with secure NTP
`config-change`	Message on persistent saving of configuration
`mrp-interconnection-state-change`	Message when there is a status change of the MRP Interconnection connection
`service-information`	Message on non-configurable entry in the log table
`dhcp-server`	Message relating to the DHCP server
`all`	All messages
`logtable`	Client that processes the logbook entries
`syslog`	Client that sends the messages to the Syslog server
`email`	Client that sends the e-mails
`trap`	Client that sends the SNMP traps
`faults`	Error LED lights up. The setting is possible only for a cold or warm restart.
`all`	All clients at once

Result

The setting deciding which message of the device is stored or forwarded is configured.

Additional notes

You display the status of the events and the clients with the `show events config` command.

You delete the settings with the `no event config` command.

With this command, the clients are not enabled.

To enable the clients, use the `client config` command.

Note

Changing several message types or clients

With each command call, you can only select one message type and one client.

If you want to process several message types or clients, it may be more efficient to first select the `all` option and then disable individual elements.

13.1.8.5 no event config

Note

Depending on the device type, the IE switch does not support all described parameters; see section "Features not supported (Page 40)".

Description

With this command, you configure which of the various message types of the device will no longer be stored or forwarded.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
event config
{cold-warmstart|linkchange|authentication-failure|rmon-alarm|power-
change|
rm-state-change|standby-state-change|faultstate-change|stp-change|
vrrp-state-change|loopd-state-change|ospf-state-change|dot1x-port-
auth-state-change|
poe-state-change|fmp-state-change|env-data-change|linkcheck-change|
cli-script-file-status|secure-ntp|config-change|mrp-interconnection-
state-change|
service-information|dhcp-server|all} {logtable|syslog|email|trap|
faults|all}
```

The parameters have the following meaning:

Parameter	Description
`cold-warmstart`	Message if there is cold or warm restart
`linkchange`	Message when there is a status change on a physical interface
`authentication-failure`	Message if there is an incorrect login
`rmon-alarm`	Message when there is a RMON alarm
`power-change`	Message when there is a status change in the power supply
`rm-state-change`	Message when there is a status change in the redundancy manager
`standby-state-change`	Message when there is a status change on a standby connection
`faultstate-change`	Message when there is a status change in the error monitoring
`stp-change`	Message when there is a change in the spanning tree
`vrrp-state-change`	Message on status change of VRRP routers
`loopd-state-change`	Message if there is a status change in the detection of network loops
`ospf-state-change`	Message on status change of OSPF
`dot1x-port-auth-state-change`	Message when there is a status change in the 802.1X authentication
`poe-state-change`	Message on status change of PoE
`fmp-state-change`	Message on status change of FMP
`env-data-change`	Message when there is a status change in the diagnostics data
`linkcheck-change`	Message on status change of Link Check
`cli-script-file-status`	Message when an error was detected in the CLI script file
`secure-ntp`	Message on error in connection with secure NTP
`config-change`	Message on persistent saving of configuration
`mrp-interconnection-state-change`	Message when there is a status change of the MRP Interconnection connection
`service-information`	Message on non-configurable entry in the log table
`dhcp-server`	Message relating to the DHCP server
`all`	All messages
`logtable`	Client that processes the logbook entries
`syslog`	Client that sends the messages to the Syslog server
`email`	Client that sends the e-mails
`trap`	Client that sends the SNMP traps
`faults`	Error LED lights up. The setting is possible only for a cold or warm restart.
`all`	All clients at once

Result

The setting deciding which messages of the device are not stored or forwarded is configured.

Additional notes

You display the status of the events and the clients with the `show events config` command.

You configure which of the various message types of the device will be stored or forwarded with the `event config` command.

13.1.8.6 hrp-redundancy-loss

Description

With this command, you activate the monitoring of HRP and MRP redundancy.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call the command without parameter assignment:

```
hrp-redundancy-loss
```

Result

Redundancy monitoring is enabled.

Additional notes

You can display the current setting with the `show events faults config` command.

You disable the function with the `no hrp-redundancy-loss` command.

13.1.8.7 no hrp-redundancy-loss

Description

With this command, you disable the monitoring of HRP and MRP redundancy.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call the command without parameter assignment:

```
no hrp-redundancy-loss
```

Result

Redundancy monitoring is disabled.

Additional notes

You can display the current setting with the `show events faults config` command.

You enable the function with the `hrp-redundancy-loss` command.

13.1.8.8 link

Description

With this command, you configure and enable the monitoring of the physical network connections for cable breaks or for pulling of the connector.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
link {up | down | flap} [{<interface-type> <iface_list>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`up`	Only the establishment of a connection is signaled	-
`down`	Only the termination of a connection is signaled	-
`flap`	Frequent switches between "Link up" and "Link down" are reported: If the port switches between "Link up" and "Link down" more frequently than the value of the flap count within the flap time.	-
`interface-type`	Type or speed of the interface	Specify a valid interface.
`iface_list`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select an interface, the function is enabled for all available interfaces.

Result

The settings for monitoring the physical network connections have been configured.

Additional notes

You display the setting with the `show events faults config` command.

You display the current error state with the `show events faults status` command.

You disable the function with the `no link` command.

You configure the flap time with the command `link flap time`.

You configure the flap reaction with the `link flap reaction` command.

You configure the flap count with the `link flap count` command.

13.1.8.9 no link

Description

With this command, you disable the monitoring of the physical network connections for cable breaks or for pulling of the connector.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
no link [{up | down | flap}] [{<interface-type> <iface_list>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`up`	The message when establishing a connection is disabled	-
`down`	The message when a connection is down is disabled	-

Parameter	Description	Range of values/note
`flap`	Frequent switches between "Link up" and "Link down" are reported: If the port switches between "Link up" and "Link down" more frequently than the value of the flap count within the flap time.	
`interface-type`	Type or speed of the interface	Specify a valid interface.
`iface_list`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select an interface, the function is disabled for all available interfaces.

Result

The settings for monitoring the physical network connections have been configured.

Additional notes

You display this setting and other information with the `show events faults config` command.

You display the current error state with the `show events faults status` command.

You enable the function with the `link` command.

13.1.8.10 logbook alarm threshold_X

Description

With this command, you configure the threshold value for the entries in the log table. When the threshold value of entries is reached, a message is output in the log table.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:
`logbook alarm threshold <integer(50-350)>`

The parameters have the following meaning:

Parameter	Description	Range of values / note
-	Threshold value for the logbook entries	50 ... 350

Result

The threshold value is specified.

13.1.8.11 power

Description

With this command, you configure and activate the monitoring of the power supplies.

Requirement

You are in the EVENTS configuration mode.

The command prompt is as follows:

`cli(config-events)#`

Syntax

Call the command with the following parameters:

`power [{l1 | l2}]`

The parameters have the following meaning:

Parameter	Description
`l1`	Monitoring of power supply 1
`l2`	Monitoring of power supply 2

If you do not select any parameters from the parameter list, the default value "L1 and L2" is used.

Result

The setting for monitoring the power supplies is configured.

Additional notes

You can display the current setting with the `show events faults config` command.

You disable the function with the `no power` command.

13.1.8.12 no power

Description

With this command, you disable the monitoring of the power supplies.

Requirement

You are in the EVENTS configuration mode.

The command prompt is as follows:

`cli(config-events)#`

Syntax

Call the command with the following parameters:

`no power [{l1 | l2}]`

The parameters have the following meaning:

Parameter	Description
`l1`	No monitoring of power supply 1
`l2`	No monitoring of power supply 2

If you do not select any parameters from the parameter list, the default value "L1 and L2" is used.

Result

The setting for monitoring the power supplies is configured.

Additional notes

You can display the current setting with the `show events faults config` command.

You enable the function with the `power` command.

13.1.8.13 severity

Description

With this command, you configure the threshold values for the sending of system event notifications.

Requirement

You are in the EVENTS Configuration mode.

The command prompt is as follows:

`cli (config-events) #`

Syntax

Call up the command with the following parameters:

`severity { mail | log | syslog } { info | warning | critical }`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mail`	Specifies the threshold value for sending system event messages by e-mail.	-
`log`	Specifies the threshold value for entering system event messages in the log table.	-
`syslog`	Specifies the threshold value for entering system event messages in the Syslog file.	-
`info`	System events are processed as of the severity level "`Information`".	-
`warning`	System events are processed as of the severity level "`Warning`".	-
`critical`	System events are processed as of the severity level "`Critical`".	-

Result

The settings for sending system event messages are configured.

The "severity" function is enabled.

Further notes

You disable the setting with the `no severity` command.

You display the status of this function and other information `show events severity`

13.1.8.14 no severity

Description

With this command, you disable the setting for the threshold values for the sending of system event notifications.

Requirement

You are in the EVENTS Configuration mode.

The command prompt is as follows:

```
cli (config-events) #
```

Syntax

Call up the command with the following parameters:

```
no severity { mail | log | syslog }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mail`	The setting of the threshold value for sending system event messages by e-mail is disabled.	-
`log`	The setting of the threshold value for entering system event messages in the log table disabled.	-
`syslog`	The setting of the threshold value the entering event messages in the Syslog file is disabled.	-

If you do not select any parameters from the parameter list, the default value is used.

Result

The settings for sending system event messages are configured.

Further notes

You enable the setting with the `severity` command.

You display the status of this function and other information `show events severity`.

13.1.8.15 syslogserver

Description

With this command, you configure the Syslog server address.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli (config-events) #
```

Syntax

Call up the command with the following parameters:

```
syslogserver { ipv4 <ucast_addr> | fqdn-name <FQDN> }
[<port(1-65535)>] [ tls ]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ipv4`	Keyword for an IP address	-
`ucast_addr`	Syslog server IPv4 address	Enter a valid IPv4 address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters
`port`	Serverport	1 .. 65535 Default: 514
`tls`	Communication with the Syslog server is encrypted.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value is used.

Result

The settings for the Syslog server are configured.

Additional notes

You disable the setting with the `no syslogserver` command.

You display the status of this function and other information with the `show events syslogserver` command.

13.1.8.16 no syslogserver

Description

With this command, you delete a Syslog server.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli (config-events) #
```

Syntax

Call up the command with the following parameters:

```
no syslogserver { ipv4 <ucast_addr> | fqdn-name <FQDN> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ipv4`	Keyword for an IP address	-
`ucast_addr`	Syslog server IPv4 address	Enter a valid IPv4 address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The Syslog server is deleted.

Additional notes

You add a Syslog server `syslogserver`.

13.2 FMP

With Fiber Monitoring, you can monitor the received power and the loss of power on optical links between two switches.

If you enable fiber monitoring on an optical port, the device sends the current transmit power of the port to its connection partner using LLDP packets. In addition to sending, the device also checks whether corresponding information is received from the connection partner.

Regardless of whether the IE switch receives diagnostics information from its connection partner, it monitors the received power measured at the optical port for the set limit values.

If fiber monitoring is enabled on the connection partner, the connection partner transfers the current value for the transmit power of the port to the device. The device compares the value it has received for the transmit power with the actually received power. The difference between the received power and the transmit power represents the power loss on the link. The calculated power loss is also monitored for the set limit values.

If the value of the received power or the power loss falls below or exceeds the set limit values, an event is triggered. You can set limit values in two stages for messages with the severity levels "Warning" and "Critical".

13.2.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.2.1.1 show fmp limit

Description

This command shows the limit values for the received power and the power loss that you set for monitoring optical ports or connections with fiber monitoring.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show fmp limit [port {<interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`port`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If no parameters are specified, the settings for all interfaces are displayed.

Result

The limits set for the received power and the power loss are displayed.

13.2.1.2 show fmp status

Description

This command shows the current status and the current values of the optical ports or connections that you monitor with fiber monitoring.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:

```
show fmp status [port {<interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`port`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If no parameters are specified, the settings for all interfaces are displayed.

Result

The status of the optical ports is displayed.

13.2.2 Commands in the Interface Configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.2.2.1 fmp

Description

With this command, you enable fiber monitoring.

Requirement

- To be able to use the fiber monitoring function, enable LLDP. The fiber monitoring information is appended to the LLDP packets.
- You can only use fiber monitoring with transceivers capable of diagnostics. Note the documentation of the devices.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

`fmp`

Default: Disabled

Result

Fiber monitoring is enabled.

Additional notes

You disable this function with the `no fmp` command.

You display the status of this function and other information with the `show fmp status` and `show fmp limit` commands.

You define the limit values with the `fmp power-loss` and `fmp rx-power` commands.

13.2.2.2 no fmp

Description

With this command, you disable fiber monitoring.

Requirement

You are in the Interface configuration mode.
The command prompt is:
`cli(config-if-$$$)#`

Syntax

Call the command without parameter assignment:

`no fmp`

Default: enabled

Result

Fiber monitoring is disabled.

Further notes

You enable this function with the `fmp` command.

You display the status of this function and other information with the and `show fmp limit` commands.

You define the limit values with the `fmp power-loss` and `fmp rx-power` commands.

13.2.2.3 fmp power-loss

Description

With this command, you specify the limit values for monitoring the power loss per port.

Requirement

You are in the Interface configuration mode.
The command prompt is:
`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

```
fmp power-loss [req { <integer(0-0)> | - <integer(1-55)>}] [dem
{ <integer(0-0)> | - <integer(1-55)>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`req`	Specify the value at which you are informed of the power loss of the connection by a message of the severity level "Warning"	0 ... -55 dB Default: -50 dB If you enter the value "0", the power loss is not monitored.
`dem`	Specify the value at which you are informed of the power loss of the connection by a message of the severity level "Critical"	0 ... -55 dB Default: -55 dB If you enter the value "0", the power loss is not monitored.

Result

The limits for monitoring the power loss are defined.

Further notes

You enable this function with the `fmp` command.

You disable this function with the `no fmp` command.

You display the status of this function and other information with the and `show fmp limit` commands.

You define the limit values for the received power with the command `fmp rx-power`.

13.2.2.4 fmp rx-power

Description

With this command, you specify the limit values for monitoring the received power per port.

Requirement

You are in the Interface configuration mode.
The command prompt is:
`cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

```
fmp rx-power [req { <integer(0-0)> | - <integer(1-40)>}] [dem
{ <integer(0-0)> | - <integer(1-40)>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`req`	Specify the value at which you are informed of the deterioration of the received power by a message of the severity level "Warning"	0 ... -40 dBm The default value depends on the relevant pluggable transceiver. If you enter the value "0", the received power is not monitored.
`dem`	Specify the value at which you are informed of the deterioration of the received power by a message of the severity level "Critical"	0 ... -40 dBm The default value depends on the relevant pluggable transceiver. If you enter the value "0", the received power is not monitored.

Result

The limits for monitoring the received power are defined.

Additional notes

You enable this function with the `fmp` command.

You disable this function with the `no fmp` command.

You display the status of this function and other information with the and `show fmp limit` commands.

You define the limit values for the power loss with the command `fmp power-loss`.

13.3 Syslog client

With the commands in this section, the following settings are configured:

- Transfer of the messages to the Syslog server
- Local buffering and storage of messages
- Receipt and forwarding of messages from other devices (relay mode)

13.3.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.3.1.1 show events syslogserver

Description

This command shows the entries of the configured Syslog server.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show events syslogserver
```

Result

The entries of the configured Syslog server are displayed.

13.3.2 Commands in the Events configuration mode

This section describes commands that you can call up in the EVENTS configuration mode.

In global configuration mode, enter the `events` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

- If you exit the EVENTS configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the EVENTS configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in EVENTS configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.3.2.1 syslogserver

Description

With this command, you configure the Syslog server address.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli (config-events) #
```

Syntax

Call up the command with the following parameters:

```
syslogserver { ipv4 <ucast_addr> | fqdn-name <FQDN> }
[<port(1-65535)>] [ tls ]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ipv4`	Keyword for an IP address	-
`ucast_addr`	Syslog server IPv4 address	Enter a valid IPv4 address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters
`port`	Serverport	1 .. 65535 Default: 514
`tls`	Communication with the Syslog server is encrypted.	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value is used.

Result

The settings for the Syslog server are configured.

Additional notes

You disable the setting with the `no syslogserver` command.

You display the status of this function and other information with the `show events syslogserver` command.

13.3.2.2 no syslogserver

Description

With this command, you delete a Syslog server.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli (config-events) #
```

Syntax

Call up the command with the following parameters:

```
no syslogserver { ipv4 <ucast_addr> | fqdn-name <FQDN> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ipv4`	Keyword for an IP address	-
`ucast_addr`	Syslog server IPv4 address	Enter a valid IPv4 address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The Syslog server is deleted.

Additional notes

You add a Syslog server `syslogserver`.

13.4 RMON

The RMON function provides commands with which variables of the Management Information Base (MIB) can be monitored for violation of limit values and to store or forward these events in the following ways:

- Entry in the local log
- Sending as SNMP trap
- Transfer to the Syslog server
- Transfer to a network management station using SNMP

Example of a configuration

Calls the SNMP notification configured in the section "SNMP (Page 416)" ("`testnotify`") for sending SNMP traps.

As soon as the threshold of 10 entries is exceeded in the log table, event 1 is triggered.

As soon as the threshold of 9 entries is exceeded in the log table, event 2 is triggered.

Execute the following commands:

```
configure terminal
rmon event 1 description "More than 10 log entries" trap testnotify
rmon event 2 description "Less than 9 log entries" trap testnotify
rmon alarm 1 1.3.6.1.4.1.4329.20.1.1.1.1.31.2.0 1 absolute rising-
threshold 10 1 falling-threshold 9 2
end
```

13.4.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.4.1.1 show rmon

Description

This command shows the settings of the remote monitoring function.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command with the following parameters:
`show rmon [statistics [<stats-index (1-52)>]] [alarms] [events] [history [history-index (1-52)] [overview]]`

The parameters have the following meaning:

Parameter	Description	Range of values/note
`statistics`	Shows counts for various packet characteristics and sizes.	-
`stats-index`	Index number of the port for which statistical information is displayed.	1 ... maximum number of ports of the device
`alarms`	Shows the threshold values and event assignments for alarms.	-
`events`	Shows the status and the actions that are triggered.	-
`history`	Shows the stored statistical values for earlier transmission periods.	-
`history-index`	Index number of the port for which earlier statistical information is displayed.	1 ... maximum number of ports of the device
`overview`	Displays an overview.	-

With this command, you can display several parameters with one call.

If you do not select any parameters from the parameter list, only the `enabled` or `disabled` status is shown.

Result

The settings of the remote monitoring function are displayed.

13.4.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.4.2.1 rmon

Description

With this command, you enable the Remote Monitoring function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
rmon
```

Default: disabled

Result

The Remote Monitoring function is enabled.

Further notes

You disable this function with the `no rmon` command.

You can display the status of this function and other information with the `show rmon` command.

13.4.2.2 no rmon

Description

With this command, you disable the Remote Monitoring function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameter assignment:

`no rmon`

Default: disabled

Result

The Remote Monitoring function is disabled.

Further notes

You enable this function with the `rmon` command.

You can display the status of this function and other information with the `show rmon` command.

13.4.2.3 rmon alarm

Description

With this command, you configure an alarm for monitoring a MIB variable. The variable is checked at specific intervals to determine whether or not it has exceeded or fallen below threshold values. Events are assigned to these occurrences.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

Parameter	Description	Range of values / note
alarm-number	Number of the alarm	1 ... 250
mib-object-id	OID of the MIB variable to be monitored.	max. 255 characters
sample-interval-time	Interval for the check [s]	1 ... 65535
absolute	The current absolute value of the monitored MIB is evaluated.	-
delta	The difference between the current and previous value of the monitored MIB is evaluated.	-
rising-threshold	Keyword for threshold value for rising or high variable values	-
value	Respective threshold	0 ... 2147483647
rising-event-number	Event number for this	1 ... 65535
falling-threshold	Keyword for threshold value for falling or low variable values	-
value	Respective threshold	0 ... 2147483647
falling-event-number	Event number for this	1 ... 65535
owner	User to which the alarm is assigned	-
ownername	User name of the user	max. 127 characters

If you do not select a parameter from the parameter list, the events for high and low threshold values are assigned the lowest event number available in the event table.

Note

MIB variables that can be monitored

With the RMON function, only MIB variables of the Ethernet interfaces can be monitored.

Note

Magnitude of the threshold values

The threshold value for falling or low variable values should be less than the threshold value for rising or high variable values.

Note

Conditions for working with alarms

The events assigned to the alarms are configured.

The Remote monitoring function is started with the `rmon` command.

Result

The alarm for monitoring a MIB variable is configured.

Further notes

You delete an alarm with the `no rmon alarm` command.

You display the list of configured RMON alarms with the `show rmon alarms` command.

13.4.2.4 no rmon alarm

Description

With this command, you delete an alarm for monitoring a MIB variable.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no rmon alarm <number (1-250)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`number`	Number of the alarm to be deleted	1 ... 250

Result

The entry for monitoring a MIB variable is deleted.

13.4.2.5 rmon collection history preset

Description

You enable the following presets for the RMON history with this command:

- Setting: Enabled
- Entries: 24
- Interval[s]: 3600

After the presets have been enabled, all user-defined settings for the RMON history are deleted and the values are locked against individual configuration. If you disable the option, the settings are retained, but are individually configurable again.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
rmon collection history preset
```

Result

The presets for the RMON history have been enabled.

Further notes

You disable this function with the `no rmon collection history preset` command.

You can display the status of this function and other information with the `show rmon` command.

13.4.2.6 no rmon collection history preset

Description

You disable the following presets for the RMON history with this command:

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no rmon collection history preset
```

Result

The presets for the RMON history have been disabled.

Further notes

You enable this function with the `rmon collection history preset` command.

You can display the status of this function and other information with the `show rmon` command.

13.4.2.7 rmon event

Description

With this command, you configure an event in the RMON Event Table.

You specify a description and the person responsible and specify which SNMP notification is generated. You can configure the sending of traps globally with the command `snmp notify`.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
rmon event <number (1-500)> [description <event-description (127)>]
[owner <ownername (127)>] [trap <notify (127)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`number`	Number of the event	1 ... 500
`description`	Keyword for a description	-
`event-description`	Description of the event that is output in the message.	max. 127 characters

Parameter	Description	Range of values / note
`owner`	Keyword for the person responsible	-
`ownername`	Name of the person responsible	max. 127 characters
`trap`	Keyword for selecting an SNMP notification	-
`notify`	Name of the SNMP notification to be triggered.	The only valid entry allowed is "SNMPv1Traps". You can configure the sending of traps globally with the command `snmp notify`.

Result

The event is configured.

Further notes

You delete an entry with the `no rmon event` command.

You display the RMON Event Table with the `show rmon events` command.

You show the details of the SNMP community with the `show snmp community` command.

13.4.2.8 no rmon event

Description

With this command, you delete an entry from the RMON event table.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no rmon event <number (1-500)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`number`	Number of the event entry to be deleted	1 ... 500

Result

The entry is deleted from the RMON event table.

13.4.3 Commands in the interface configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.4.3.1 rmon collection stats

Description

With this command, you start the recording of statistical data of an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
rmon collection stats <index (1-52)>[owner<ownername(127)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`index`	Number of the recording	1 ... 52
`owner`	User to which the event is assigned	-
`ownername`	User name of the user	max. 127 characters

Result

The recording of statistical data is started.

Further notes

You can display the content of a recording with the `show rmon statistics` command.

13.4.3.2 no rmon collection stats

Description

With this command, you end the recording of statistical data of an interface.

Requirement

You are in interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call the command with the following parameters:

```
no rmon collection stats [index (1-52)]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`index`	Number of the recording	1 ... 52

Result

The recording of statistical data is ended.

13.4.3.3 rmon collection history

Description

With this command you configure whether or not samples of the statistics are saved for a port. You can specify how many entries ("Buckets") should be saved and at which intervals samples should be taken.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
rmon collection history<index(1-52)>
   [buckets<bucket-number(1-65535)>]
   [interval<seconds(1-3600)>]
   [owner<ownername(127)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`index`	Number of the recording	1 ... 65535
`buckets`	Keyword for entries	-
`bucket-number`	Maximum number of entries (recordings)	1 ... 65535 The maximum number of entries can be restricted by the capacity of the device. Default: 50
`interval`	Keyword for recording intervals	-
`seconds`	Duration of the recording intervals in seconds	1 ... 3600 Default: 1800
`owner`	User to which the event is assigned	-
`ownername`	User name of the user	max. 127 characters Default: monitor

If you do not select any parameter from the parameter list, the default values are used.

Result

The data is recorded.

Further notes

You can display the content of a recording with the `show rmon history` command.

13.4.3.4 no rmon collection history

Description

With this command, you end the recording of statistical data of the interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

```
cli(config-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no rmon collection history <index(1-52)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
index	Number of the recording	1 ... 52

Result

The data recording is ended.

13.5 Port Mirroring

Note

It cannot be guaranteed when mirroring the data traffic that all packets are mirrored.

With the port mirroring function, you copy the data stream of one or more ports to another interface to be able to analyze this data stream without disturbing operation.

Note

You need to disable port mirroring if you want to connect a normal end device to the monitor port.

Note the data rate

If the maximum data rate of the mirrored port is higher than that of the monitor port, data may be lost and the monitor port no longer reflects the data traffic at the mirrored port. Several ports can be mirrored to one monitor port at the same time.

Several source ports from the same VLAN

If in a VLAN you select more than one source port for the port-based egress mirroring, unknown unicast and multicast frames as well as broadcast frames are forwarded only once to the destination port.

13.5.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.5.1.1 show monitor

Description

This command shows the status of the port mirroring function.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show monitor
```

Result

The status of the port mirroring function is displayed.

13.5.1.2 show monitor barrier

Description

This command shows the status of the communication via the monitor port. If you enable this option, management of the switch via the monitor port is no longer reachable.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameter assignment:

```
show monitor barrier
```

Result

The settings are displayed.

13.5.1.3 show monitor session

Description

This command shows the settings used for mirroring ports.

You obtain information about the ports from which incoming and/or outgoing data traffic is mirrored and the port at which the mirrored data is output.

Requirement

You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command with the following parameters:

```
show monitor {session <session-id(1-1)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`session`	Keyword for a session whose settings are displayed	-
`session-id`	Number of the session	1

Result

The settings for mirroring ports are displayed.

13.5.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.5.2.1 monitor

Description

With this command, you enable the port mirroring function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
monitor
```

As default the function is "disabled".

Result

The port mirroring function is enabled.

Further notes

You can display the status of this function with the `show monitor`command.

You disable the function with the `no monitor` command.

13.5.2.2 no monitor

Description

With this command, you disable the port mirroring function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no monitor`

Result

The port mirroring function is disabled.

Further notes

You can display the status of this function with the `show monitor`command.

You enable the function with the `monitor` command.

13.5.2.3 monitor barrier enabled

Description

With this command, you disable the communication via the monitor port.

Note

Effects of monitor barrier enabled

If you enable this option, management of the switch via the monitor port is no longer reachable. The following port-specific functions are changed:

- DCP forwarding is turned off
- LLDP is turned off
- Unicast, multicast and broadcast blocking is turned on

The previous statuses of these functions are no longer restored after disabling monitor barrier again. They are reset to the default values and may need to be reconfigured.

You can reconfigure these functions manually even if monitor barrier is turned on. The data traffic on the monitor port is, however, also allowed again. If you do not require this, make sure that only the data traffic you want to monitor is forwarded to the interface.

If mirroring is disabled, the listed port-specific functions are reset to the default values. This reset takes place regardless of whether the functions were configured manually or automatically by enabling "Monitor Barrier".

Requirement

You are in global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`monitor barrier enabled`

Result

Communication via the monitor port is disabled.

Additional notes

You enable the communication with the `no monitor barrier enabled` command.

You display the configuration settings with the `show monitor barrier` command.

13.5.2.4 no monitor barrier enabled

Description

With this command, you enable the communication via the monitor port.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`no monitor barrier enabled`

Result

Communication via the monitor port is enabled.

Further notes

You disable the communication with the `monitor barrier enabled` command.

You display the configuration settings with the `show monitor barrier` command.

13.5.2.5 monitor session destination

Description

With this command, you configure the destination for mirroring a port.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
monitor session <session-id(1-1)> destination
  {interface <interface-type><interface-id>}
```

The parameters have the following meaning:

Parameter	Description	Values
`session-id`	Number of the session	1
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Note

Selecting the destination port

A port that is part of a port channel cannot be configured as the destination port for a monitor session.

Result

As soon as you have configured the settings for the port to be monitored and the destination port, the session is complete and active.

Note

If you change the settings for an existing session, all previous configurations of this session are lost.

Further notes

You delete the destination for mirroring a port with the `no monitor session ... destination` command.

You end and delete a session with the `no monitor session` command.

You display the configuration settings with the `show monitor session` command.

13.5.2.6 no monitor session destination

Description

With this command, you delete the destination for mirroring a port.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no monitor session <session-id(1-1)> destination
  {interface <interface-type><interface-id>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`session-id`	Number of the session	1
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

Result

The destination for the mirroring of a port is deleted.

Further notes

You configure the destination for mirroring a port with the `monitor session ... destination` command.

You end and delete a session with the `no monitor session` command.

You display the configuration settings with the `show monitor session` command.

13.5.2.7 monitor session source

Description

With this command, you configure the source for mirroring a port.

Requirement

- Monitoring is enabled.
- You are in the Global configuration mode.
  The command prompt is:
  `cli(config)#`

Syntax

Call up the command for the port to be monitored with the following parameter assignment:

```
monitor session <session-id(1-1)> source
  {interface {<interface-type> <interface-id> | port-channel <port-
channel-id (1-8)>} [{rx|tx|both}]}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
session-id	Number of the session	1
interface	Keyword for a an interface description	-
interface-type	Type or speed of the interface	Enter a valid interface.
interface-id	Module no. and port no. of the interface	
port-channel	Keyword for a port channel connection	-
port-channel-id	Number of the addressed port channel	1 ... 8
rx	Received data traffic will be mirrored (received)	If you enable the mirroring function for a ring port, the ring port sends test frames even in the "link down" status.
tx	Transmitted data traffic will be mirrored (transmitted)	
both	Received and transmitted data traffic will be mirrored	

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value (both) is used.

Result

As soon as you have configured the settings for the port to be monitored and the destination port, the session is complete and active.

Further notes

You delete the source for mirroring a port with the `no monitor session ... source` command.

You end and delete a session with the `no monitor session` command.

You display the configuration settings with the `show monitor session` command.

See also

Features not supported (Page 40)

13.5.2.8 no monitor session source

Description

With this command, you delete the source for mirroring a port or a VLAN.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command for the port to be monitored with the following parameter assignment:

```
no monitor session <session-id(1-1)> source
   {interface { <interface-type> <interface-id> | port-channel
<port-channel-id (1-8)> }
   {rx|tx|both}]}
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`session-id`	Number of the session	1
`interface`	Keyword for a an interface description	-

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`port-channel`	Keyword for a port-channel connection	-
`port-channel-id`	Number of the addressed port channel	1 ... 8
`rx`	Received data traffic will be mirrored (**r**eceived)	-
`tx`	Transmitted data traffic will be mirrored (**t**ransmitted)	-
`both`	Received and transmitted data traffic will be mirrored	-

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value (both) is used.

Result

The source for the mirroring of a port is deleted.

Additional notes

You configure the source for mirroring a port with the `monitor session ... source` command.

You end and delete a session with the `no monitor session` command.

You display the configuration settings with the `show monitor session` command.

13.5.2.9 no monitor session

Description

With this command, you delete the monitor session.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no monitor session<session-id(1-1)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`session-id`	Number of the session	1

Result

The monitor session is deleted.

Further notes

You display the configuration settings with the `show monitor session` command.

You configure and start mirroring of a port with the `monitor session` command.

13.6 Loop detection

With the "Loop detection" function, you specify the ports for which loop detection will be activated. The ports involved send special test frames - the loop detection frames. If these frames are sent back to the device, there is a loop.

A "Local loop" involving this device means that the frames are received again at a different port of the same device. If the sent frames are received again at the same port, there is a "remote loop" involving other network components.

With the commands in this section, you start loop detection and decide which actions will be used on the ports affected if loops are detected.

Note

A loop is an error in the network structure that needs to be eliminated. The loop detection can help to find the errors more quickly but does not eliminate them.

Note

Note that loop detection is only possible at ports that were not configured as ring ports or standby ports.

Note

Changing the configured port status with loop detection

The configuration of the port status can be changed with the "Loop Detection" function. If, for example, the administrator has disabled a port, the port can be enabled again after a device restart by "Loop Detection". The port status "link down" is not changed by "Loop Detection".

13.6.1 The "show" commands

This section describes commands with which you display various settings.

With the `do [command]`, you can execute the commands from the Privileged EXEC mode in any configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.6.1.1 show loopd

Description

With this command, you display the information on loop detection.

Detected loops are shown.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call the command without parameters:

```
show loopd
```

Result

Information on loop detection is displayed.

13.6.1.2 show loopd interface

Description

Displays information on the loop interface.

Requirement

You are in User EXEC mode or in Privileged EXEC mode.

The command prompt is as follows:

`cli>` or `cli#`

Syntax

Call up the command without parameters or with the following parameter assignment:

```
show loopd interface [{<interface-type> <interface-id> | port-
channel <port-channel-id (1-8)>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface`	Keyword for a an interface description	-
`interface-type`	Type or speed of the interface	Enter a valid interface.
`interface-id`	Module no. and port no. of the interface	
`port-channel`	Keyword for a port channel connection	-
`port-channel-id`	Number of the addressed port channel	1 ... 8

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 50)".

If you do not select any parameters from the parameter list, the default value is used.

Result

The loop interface is displayed.

Additional notes

You can display the status of this function and other information with the `show loopd` command.

13.6.2 Commands in the global configuration mode

This section describes commands that you can call up in the Global configuration mode.

In Privileged EXEC mode, enter the `configure terminal` command to change to this mode.

Commands relating to other topics that can be called in the Global configuration mode can be found in the relevant sections.

You exit the Global configuration mode with the `end` or `exit` command and are then in the Privileged EXEC mode again.

You can run commands from Privileged EXEC Modus with the `do [command]` in global configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.6.2.1 loopd

Description

With this command, you enable the loop detection function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

`loopd`

Result

The loop detection function is enabled

Further notes

You disable the function with the `no loopd` command.

You can display the status of this function and other information with the `show loopd` command.

13.6.2.2 no loopd

Description

With this command, you disable the loop detection function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

`cli(config)#`

Syntax

Call the command without parameters:

```
no loopd
```

Result

The loop detection function is disabled

Further notes

You enable the function with the `loopd` command.

You can display the status of this function and other information with the `show loopd` command.

13.6.2.3 loopd vlan mode

Description

With this command, you enable the loop detection function for VLAN.

Requirement

- Loopd is activated
- You are in the Global configuration mode.
  The command prompt is:
  `cli(config)#`

Syntax

Call the command without parameters:

```
loopd vlan mode
```

Result

The loop detection function is enabled for VLAN.

Further notes

You disable the function with the `no loopd vlan mode` command.

You can display the status of this function and other information with the `show loopd` command

13.6.2.4 no loopd vlan mode

Description

With this command, you disable the loop detection function for VLAN.

Requirement

- Loopd is activated
- You are in the Global configuration mode.
  The command prompt is:
  `cli(config)#`

Syntax

Call the command without parameters:

`no loopd vlan mode`

Result

The loop detection function is disabled for VLAN.

Further notes

You enable the function with the `loopd vlan mode` command.

You can display the status of this function and other information with the `show loopd` command

13.6.3 Commands in the Interface Configuration mode

This section describes commands that you can call up in the interface configuration mode. Depending on the Interface selected, various command sets are available.

In global configuration mode, enter the `interface` command to change to this mode.

Commands relating to other topics that can be called in the interface configuration mode can be found in the relevant sections.

- If you exit the Interface configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the Interface configuration mode with the `end` command, you return to the Privileged EXEC mode.

You can run commands from Privileged EXEC Modus with the `do [command]` in interface configuration mode.

To do this, you replace `[command]` with the command that you want to execute.

13.6.3.1 loopd {blocked | forwarder | sender}

Description

With this command you specify how the port handles loop detection frames.

Requirement

- Loop detection is enabled
- A Spanning Tree port, ring port or standby port cannot be the sender port.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

`loopd {blocked | forwarder | sender}`

The parameters have the following meaning:

Parameter	Description	Range of values / note
`blocked`	The forwarding of loop detection frames is blocked.	-
`forwarder`	Loop detection frames from other devices are forwarded.	Default after enabling loop detection.
`sender`	Loop detection frames are sent out and forwarded.	-

If you do not select any parameters from the parameter list, the default value is used.

Result

It has been configured how the port handles loop detection frames.

Further notes

You can display the status of this function and other information with the `show loopd` command.

13.6.3.2 loopd {tx-interval | detect-threshold | reaction-timeout}

Description

With this command you configure the send interval, threshold value and reaction time for loop detection.

Requirement

- Loop detection is enabled
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

```
loopd {tx-interval <mSec(500-5000)> | detect-threshold
<integer(1-500)> | reaction-timeout <seconds(0-86400)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`tx-interval`	Keyword for the send interval	-
`mSec`	Specifies the send interval for loop detection frames in milliseconds.	500 ... 5000 Default: 1000
`detect-threshold`	Keyword for the threshold value	-
`integer`	Specifies the threshold value after how many received loop detection frames, a loop is assumed and the device reacts according to the setting.	1 ... 500 Default: 2
`reaction-timeout`	Keyword for the time to the end of the reaction time	-
`seconds`	Specifies the number of seconds after which the device automatically changes to the status in which it was before the loop.	0 ... 86400 Default: 0 If you set the value "0", you need to enable the port manually again following a loop using the command `loopd port reset`.

If you do not select any parameters from the parameter list, the default value is used. The default values apply only to a port enabled earlier with `loopd sender`.

Result

The settings are suitably configured.

Further notes

You can display the status of this function and other information with the `show loopd` command.

13.6.3.3 loopd port reset

Description

With this command, you enable a port that was blocked by loop detection.

Requirement

- Loop detection is enabled
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameters:

```
loopd port reset
```

Result

The blocked port is enabled again.

Further notes

You disable the setting with the `no loopd port reset` command.

You can display the status of this function and other information with the `show loopd` command.

13.6.3.4 no loopd port reset

Description

With this command, you disable the port reset for loop detection.

Requirement

- Loop detection is enabled
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameters:

```
no loopd port reset
```

Result

The port reset function is disabled.

Further notes

You enable the setting with the `loopd port reset` command.

You can display the status of this function and other information with the `show loopd` command.

13.6.3.5 loopd reaction local

Description

With this command, you activate the "disable" reaction for a local loop. If a local loop is detected, the port is blocked.

Requirement

- Loop detection is enabled.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameters:

```
loopd reaction local
```

Result

"disable" is activated for the `loopd reaction local` function.

"disable" is the default after enabling loop detection.

Further notes

You enable the "no action" reaction with the `no loopd reaction local` command.

You can display the status of this function and other information with the `show loopd` command.

13.6.3.6 no loopd reaction local

Description

With this command, you enable the "no action" reaction for a local loop. If a local loop is detected, this has no effect on the port.

Requirement

- Loop detection is enabled.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameters:

```
no loopd reaction local
```

Result

"no action" is activated for the `loopd reaction local` function.

"disable" is the default after enabling loop detection.

Further notes

You enable the "disable" reaction with the `loopd reaction local` command.

You can display the status of this function and other information with the show loopd command.

13.6.3.7 loopd reaction remote

Description

With this command, you enable the "disable" reaction for a remote loop. If a remote loop is detected, the port is blocked.

Requirement

- Loop detection is enabled.
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameters:
`loopd reaction remote`

Result

"disable" is activated for the `loopd reaction remote` function.

"disable" is the default after enabling loop detection.

Further notes

You enable the "no action" reaction with the `no loopd reaction remote` command.

You can display the status of this function and other information with the `show loopd` command.

13.6.3.8 no loopd reaction remote

Description

With this command, you enable the "no action" reaction for a remote loop. If a remote loop is detected, this has no effect on the port.

Requirement

- loopd is enabled
- You are in the Interface configuration mode.
  The command prompt is:
  `cli(config-if-$$$)#`

Syntax

Call the command without parameters:
`no loopd reaction remote`

Result

"no action" is activated for the `loop reaction remote` function.

"disable" is the default after enabling loop detection.

Further notes

You enable the "disable" setting with the `loopd reaction remote` command.

You can display the status of this function and other information with the `show loopd` command.

Troubleshooting/FAQ 14

14.1 Downloading new firmware using TFTP without WBM and CLI

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Operating the button

To load new firmware, you require the button. When pressing the button, remember the information in the appropriate operating instructions.

Press the "RESET" button on the SCALANCE XB-200 with only slight force.

Press the "SELECT/SET" button on the SCALANCE XC-200.

Press the "SET" button on the SCALANCE XF-200BA.

Press the "RESET" button on the SCALANCE XF-200G with only slight force.

Press the "RESET" button on the SCALANCE XP-200 as far as the pressure point.

Press the "RESET" button on the SCALANCE XP-200G as far as the pressure point.

Press the "RESET" button on the SCALANCE XR-300WG.

Procedure with Microsoft Windows

You can download new firmware to the device using TFTP. To do this, the device does not need to be reachable either using Web Based Management (WBM) or using the Command Line Interface (CLI). This can be the case if there was a power failure during a firmware update.

When pressing the button, observe the information in the section "Downloading new firmware using TFTP without WBM and CLI (Page 783)".

Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the device.
2. Press the SELECT/SET button and reconnect the device to the power supply with the button pressed.
3. Hold down the button until the red fault LED "F" starts to flash.
4. Release the button as long as the red error LED is still flashing..
   This time only lasts a few seconds.
   The bootloader of the device waits in this status for a new firmware file that you can download by TFTP.
5. Connect a PC to an Ethernet port of the device with an Ethernet cable.

6. Assign an IP address to the device using DHCP or SINEC PNI.
7. In a Windows command prompt, go to the directory where the file with the new firmware is located and use the following command:
   `tftp -i <IP address> put <firmware file>.`

   Note

   You can enable TFTP in Microsoft Windows as follows:

   "Control Panel" > "Programs and Features" > "Turn Windows features on or off" > "TFTP Client".

   Once the firmware has been transferred completely to the device and validated, the device restarts. This may take a few minutes.

14.2 Message: SINEMA configuration not yet accepted

When the following message is displayed in the display area an error has occurred transferring the configuration from STEP 7 Basic / Professional as of V13 to the device:

"SINEMA Configuration not accepted yet. With restart of device, all configuration changes will be lost."

One possible cause is, for example, that during transfer the device was not reachable.

If you now change a parameter directly on the device (WBM/CLI/SNMP) these changes are lost when the device restarts.

Solution

1. Open the relevant STEP 7 project in STEP 7 Basic / Professional
2. Open the project view.
3. Select the device in the project tree.
4. Select the "Go to network view" command in the shortcut menu.
5. Select the device in the network view.
6. In the shortcut menu of the selected device select the command "SCALANCE configuration > Save as start configuration".

Result

The configuration is saved on the device. The message is no longer visible in the display area. A configuration change directly on the device is no longer lost due to a restart of the device.

14.3 Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" ("System > Load&Save > HTTP/TFTP/SFTP") to exchange configuration data between a device (WBM) and STEP7 Basic/Professional using a file. The export/import of a file via STEP 7 Basic/Professional is described below.

Exporting configuration data via STEP 7 Basic/Professional

To export configuration data via STEP 7 Basic/Professional, follow these steps:

1. Open the relevant STEP 7 project in STEP 7 Basic/Professional.
2. Open the project view.
3. Open the network view or the topology view.
4. Open the Hardware catalog.
5. In the hardware catalog, navigate to the device with the relevant article number.
6. Select the desired device with a mouse click.
7. Set the matching firmware version via the drop-down list of the hardware catalog.
8. Drag-and-drop the device to the network view or to the topology view.
9. Select the device in the network view on in the topology view.
10. Configure the device in the Inspector window under "Properties > General".
11. In the Inspector window, navigate to the "Management" parameter under "Properties > General".
12. In the parameter group "Load / save file", click the "Save to file" button.
13. Select a storage location for the file.
14. Assign a name for the file.
15. Click the "Save" button.
    The "Save configuration file" dialog opens.
16. Assign a password for the encryption of the file.

    Note

    You need this password when you load the file to a device via the WBM.

17. Click the "OK" button.

Importing configuration data via STEP 7 Basic/Professional

To import configuration data via STEP 7 Basic/Professional, follow these steps:

1. Open the relevant STEP 7 project in STEP 7 Basic/Professional.
2. Open the project view.
3. Open the network view or the topology view.

4. Open the Hardware catalog.
5. In the hardware catalog, navigate to the device with the relevant article number.
6. Select the desired device with a mouse click.
7. Set the matching firmware version via the drop-down list of the hardware catalog.
8. Drag-and-drop the device to the network view or to the topology view.
9. Select the device in the network view on in the topology view.
10. In the Inspector window, navigate to the "Management" parameter under "Properties > General".
11. In the parameter group "Load / save file", click the "Load from file" button.
12. Select the desired file.
13. Click the "Open" button.
    The "Load configuration file" dialog opens.
14. Enter the password for the decryption of the file.

    Note

    You assign this password in the WBM under "System > Load&Save > Passwords".

15. Click the "OK" button.

Index

A

add log, 722
agent-priority, 621
alias, 104, 251
    no alias, 105, 252
arp timeout, 471
    no arp timeout, 471
auth username
    no auth username, 452
auth usernamet, 452
authorized-manager, 664
    no authorized-manager, 664
authorized-manager ip-source, 665
    no authorized-manager ip-source, 667
auto-learn, 670
auto-save, 151
    no auto-save, 152
Available system functions, 33

B

base bridge mode, 243
boot-integrity-check, 144
bridge-mode, 249
broadcast-block, 106
broadcast-priority, 622
brute-force-prevention auto-reset-timer, 700
    no brute-force-prevention auto-reset-timer, 701
brute-force-prevention ip-specific-login-attempts, 701
    brute-force-prevention ip-specific-login-attempts, 702
brute-force-prevention reset, 706
brute-force-prevention trigger-interval, 705
brute-force-prevention user-specific-login-attempts, 703
    no brute-force-prevention user-specific-login-attempts, 704

C

cancel restart-time, 145
change password, 637
channel-group, 283
    no channel-group, 284
clear counters, 82
clear fault counter, 716
clear history, 61
clear hrp counters, 503
clear line vty, 83
clear logbook, 716
clear ring-redundancy manager counters, 504
clear screen, 55
clear spanning-tree counters, 296
clear spanning-tree detected protocols, 295
clear standby counter, 505
clear-all-static-unicast, 669
CLI commands
    Symbolic representation, 49
cli-console-timeout, 90
    no cli-console-timeout, 91
client-position, 537
Command Line Interface (CLI), 783
Configuration limits, 36
configure terminal, 83
coordinates height, 91
coordinates latitude, 92
coordinates longitude, 93
cos-map, 623
cos-remap, 625
cos-remap enable, 626

D

das delete, 154
das discover interface, 155
das mac blink, 158
das mac ip, 156
das mac name, 157
dcp forwarding, 357
dcp server, 348
    no dcp server, 349
delay mechanism, 224
delete, 132
dhcp snooping, 358
    no dhcp snooping, 358
disable, 84
do, 55
Documentation on the Internet, 29
domain name, 365
domain-id, 534
domain-name, 532, 534
dot1x fallback retry count, 678
dot1x fallback timeout, 677
dot1x guest-vlan, 676, 681
    no dot1x guest-vlan, 677, 682

dot1x guest-vlan reset, 684
dot1x guest-vlan vlan-id, 682
    no dot1x guest-vlan vlan-id, 683
dot1x mac-auth, 679, 685
    no dot1x mac-auth, 687
dot1x mac-auth default-value, 688
    no dot1x mac-auth default-value, 689
dot1x mac-auth mac-addr count, 693
dot1x mac-auth port reset, 689
dot1x mac-auth vlan-assign, 690
    no dot1x mac-auth vlan-assign, 691
dot1x nas-id, 680
dot1x port-control, 692
    no dot1x port-control, 693
dot1x reauthentication, 694
    no dot1x reauthentication, 695
dot1x timeout reauth-period, 695
    no dot1x timeout reauth-period, 696
dot1x timeout tx-period, 697
dscp-map, 628
duplex, 107
    no duplex, 108

E

enable, 85
environmental diagnostics threshold monitoring, 95
    no environmental diagnostics threshold monitoring, 96
environmental temperature entry, 94
ethernetip, 97
ethernetip dlr, 97
ethernetip dlr p1 p2, 98
ethernetip dlr vlan, 99
event config, 725
    no event config, 728
events, 718
exit, 56

F

factoryclean, 179
fault report ack, 717
firmware-on-plug, 179
    no firmware-on-plug, 180
flowcontrol, 613
fmp, 741
fmp power-loss, 743
fmp rx-power, 744
fsu-support, 108
    no fsu-support, 109

H

help, 57
host, 386
hrp-redundancy-loss, 730
    no hrp-redundancy-loss, 730

I

instance, 334
    no instance, 335
Interconnection, 539
interface, 87
    no interface, 89
Interface, 535
interface range, 246
    no interface range, 247
ip address, 359, 361
ip address dhcp, 377
ip dhcp client keepalive, 374
ip dhcp client mode, 373
ip dhcp config-file-request, 375
    no ip dhcp config-file-request, 376
ip dhcp config-file-request setup, 376
ip dhcp relay circuit-id, 412
    no ip dhcp relay circuit-id, 413
ip dhcp relay circuit-id option, 405
ip dhcp relay common-agent-address, 406
ip dhcp relay common-agent-address-interface, 408
ip dhcp relay information option, 409, 414
    no ip dhcp relay information option, 410, 414
ip dhcp relay remote-id, 415
ip dhcp server, 404
    no ip dhcp server, 404
ip dhcp-server, 381
    no ip dhcp-server, 382
ip dhcp-server icmp-probe, 383
    no ip dhcp-server icmp-probe, 383
ip dhcp-server pool, 384
    no ip dhcp-server pool, 385
ip domain lookup, 369
    no ip domain lookup, 369
ip domain name, 366
ip domain used server, 368
ip echo-reply, 351
    no ip echo-reply, 352
ip gateway, 350
    no ip gateway, 351
ip http, 461, 468
    no ip http, 462

ip http port, 463
no ip http port, 464
ip http secure, 466
no ip http secure, 466
ip http secure port, 467
no ip http secure port, 468
ip igmp snooping, 497
no ip igmp snooping, 498
ip igmp snooping clear counters, 488
ip igmp snooping port-purge-interval, 489
no ip igmp snooping port-purge-interval, 490
ip igmp snooping querier, 499, 500
no ip igmp snooping querier, 499, 501
ip igmp snooping report-forward, 490
no ip igmp snooping report-forward, 491
ip igmp snooping send-query, 492
ip igmp snooping switch-ip, 493
ip igmp snooping version, 494
ip igmp vlan-snooping, 494
no ip igmp vlan-snooping, 495
ip name server, 370
no ip name server, 371
ip nat, 575, 578
ip nat napt, 580
ip nat pool, 581
ip nat service, 582
ip nat service portrange, 585
ip nat static, 587
ip nat timeout, 576, 577
ip single-hop inter-vlan-routing, 589
ipv4 nexthop arp_keep_alive, 353

L

lacp timeout, 285
no lacp timeout, 285
lease time, 389
link, 731
no link, 732
linkcheck, 517
lldp, 110
no lldp, 110
load tftp, 128
loadsave, 131
logbook alarm threshold, 733
login authentication, 655
logout, 85
loopd, 777

M

mac-address-table aging, 611
no mac-address-table aging, 611
mac-address-table aging-time, 609
no mac-address-table aging-time, 610
mac-address-table static multicast, 560, 598
no mac-address-table static multicast, 599
mac-address-table static unicast, 546, 600
no mac-address-table static unicast, 547, 601
mac-address-table static unicast (VLAN-unaware), 552, 604
no mac-address-table static unicast (VLAN-unaware), 553, 605
media type, 111
minimum config version, 142
mode, 531
monitor, 763
no monitor, 763
monitor barrier enabled, 764
no monitor barrier enabled, 765
monitor session
destination, 766
no ... destination, 767
no ... source, 769
no monitor session, 770
source, 768
MRP multiple rings, 528
mrpinterconnection, 529
multicast-block, 113

N

name, 269, 336
no name, 270, 337
negotiation, 116
no negotiation, 117
network, 390
no agent-priority, 621
no broadcast-block, 106
no broadcast-priority, 623
no cos-remap, 626
no cos-remap enable, 627
no domain name, 365
no dot1x mac-auth, 679
no fmp, 742
no host, 388
no ip address, 360, 378
no ip dhcp client keepalive, 374
no ip dhcp relay common-agent-address, 407

no ip dhcp relay common-agent-address-interface, 409
no ip dhcp relay remote-id, 416
no ip domain name, 367
no ip igmp snooping send-query, 492
no ip nat, 575, 579
no ip nat napt, 580
no ip nat pool, 582
no ip nat service, 584
no ip nat service portrange, 586
no ip nat static, 587
no ip single-hop inter-vlan-routing, 590
no ipv4 nexthop arp_keep_alive, 353
no linkcheck, 519
no login authentication, 656
no mac-address-table static multicast (VLAN-unaware), 566, 603
no mrpinterconnection, 530
no multicast-block, 113
no panel-button control-factory-defaults, 185
no panel-button control-faultmask, 186
no passive listening, 342
no passive-listening bpdu-vlan-flood, 341
no ports, 396
no priority, 275
no priority enable, 276
no private-vlan, 278
no private-vlan association, 279
no private-vlan mapping, 254
no radius-server, 661
no relay-information, 398
no ring-redundancy hrpobserver, 511
no ring-redundancy mrpinterconnection, 516
no rmon, 751
no rmon collection history preset, 754
no role, 643
no sinema, 175
no smtp-server-enable, 459
no snmp engineid migrate, 433
no spanning-tree passive-listening-compatibility, 306
no spanning-tree rstp-plus, 309
no switchport mode dot1q-tunnel, 261
no switchport private-vlan host-association, 264
no switchport private-vlan mapping, 266
no unicast mac learning, 522, 555
no unicast-block, 121
no user-account-ext, 647
no user-group, 651
no wait-for-completion, 539
noa port config, 115
nodes monitoring action, 114
nodes monitoring threshold, 115
ntp, 199
ntp secure, 201
    no ntp secure, 202
ntp server, 199
    no ntp server, 200
ntp server configuration, 200
ntp server id, 202
    no ntp server id, 204
ntp server interface, 206
    no ntp server interface, 208
ntp server listen interface, 209
    no ntp server listen interface, 210
ntp server secure, 204
ntp server secure interface, 211
    no ntp server secure interface, 211
ntp time diff, 205

O

option, 392
    no option, 393
option value-string, 391
    no option, 393

P

panel-button control-factory-defaults, 184
panel-button control-faultmask, 186
passive listening, 341
passive-listening bpdu-vlan-flood, 340
password, 133
    no password, 134
password policy, 639
password policy (parameter), 640
password policy min-length, 640
ping, 86
plug, 178
pnio, 100
pnio station-name, 101
poe custom maxpwr, 164
poe schedule, 169
    no poe schedule, 170
poe schedule day, 172
    no poe schedule day, 172
poe schedule time, 170
    no poe schedule time, 171
pool-enable, 394
    no pool-enable, 395
port, 453
    no port, 454
Port groups, 520

ports, 271, 395
    no ports, 272
power, 734
    no power, 734
Predefined defaults, 28
primary domain, 225
priority, 274
priority enable, 276
private-vlan, 277
private-vlan association, 278
private-vlan mapping, 253
ptp, 221, 226
    no ptp, 221, 227
ptp time diff, 222
ptp transparent-clock configuration, 223
ptp transparent-clock transport-mechanism, 228

Q

qos, 619
qos-trust-mode, 629

R

radius authorization-mode, 657
radius disconnect-packet, 658
    no radius disconnect-packet, 659
radius server, 659
rate-limit-output, 592
    no rate-limit-output, 593
receiver-address, 456
    no receiver-address, 457
redundancy, 508
relay information, 397
RESET button, 783
restart, 143
revision, 338
    no revision, 338
ring ports, 520, 532
ring redundancy, 511
    no ring redundancy, 512
ringid, 528
ring-redundancy dna-redundancy, 513
    no ring-redundancy dna-redundancy, 513
ring-redundancy hrpobserver, 510
ring-redundancy mrpinterconnection, 515
ring-redundancy restore-default, 509
rmon, 750
rmon alarm, 751
    no rmon alarm, 753
rmon collection history, 758
    no rmon collection history, 759
rmon collection history preset, 754
rmon collection stats, 757
    no rmon collection stats, 758
rmon event, 755
    no rmon event, 756
role, 536, 641

S

save filetype, 130
schedule restart-timer, 146
scheduling mode, 630
Scope of the manual, 27
security, 457
    no security, 458
SELECT/SET button, 783
send test mail, 451
sender-address, 454
    no sender address, 455
service dhcp-relay, 411
    no service dhcp-relay, 411
SET button, 783
set dot1x guest-vlan mac-addr count, 684
set gmrp, 480, 481
set gvrp, 481, 482
set-interface, 399
severity, 735
    no severity, 736
sftp filename, 138
sftp load, 139
sftp save, 140
sftp server, 141
show authorized-managers, 663
show broadcast-block config, 63
show brute-force-prevention config, 698
show brute-force-prevention status, 699
show cabletest interface, 714
show cli-console-timeout, 64
show coordinates, 64
show counter discards, 65
show counter in-errors, 65
show counter log-events, 709
show das info, 153
show dcp forwarding, 345
show dcp server, 346
show device information, 66
show dhcp server, 402
show dhcp snooping, 346
show dot1d mac-address-table, 240, 548, 562

show dot1d mac-address-table static multicast, 241, 563
show dot1d mac-address-table static unicast mode, 241, 549
show dot1x, 674
show dot1x guest-vlan mac-info, 675
show dot1x mac-auth mac-info, 675
show dst info, 191
show environmental temperature, 66
show etherchannel, 280
show ethernetip, 67
show events config, 710
show events faults config, 711
show events faults status, 711
show events severity, 710
show events smtp-server, 448
show events syslogserver, 745
show fault counter, 713
show flow-control, 612
show fmp limit, 740
show fmp status, 740
show function-rights, 633
show hardware, 67
show history, 61
show hrp counters, 506
show in, 68
show interface transceiver details, 715
show interfaces, 69
show interfaces ... counters, 70
show interfaces etherchannel, 281
show ip arp, 469
show ip dhcp client, 372
show ip dhcp client stats, 372
show ip dhcp relay information, 403
show ip dhcp-server bindings, 380
show ip dhcp-server pools, 380
show ip dns, 362
show ip dns cache, 362
show ip dns domain name, 363
show ip dns name server, 363
show ip dns statistics, 364
show ip gateway, 347
show ip http secure server status, 464
show ip http server status, 461
show ip igmp snooping, 483
show ip igmp snooping forwarding-database, 484
show ip igmp snooping globals, 485
show ip igmp snooping groups, 485
show ip igmp snooping mrouter, 486
show ip igmp snooping statistics, 487
show ip igmp snooping switch-ip, 487
show ip interface, 71
show ip nat, 570
show ip nat config, 571
show ip nat service, 572
show ip nat service portrange, 573
show ip nat statistics, 573
show ip nat summary, 574
show ip ssh, 472
show ip telnet, 347
show lacp, 282
show linkcheck, 506
show lldp neighbors, 71
show lldp status, 72
show loadsave files, 127
show loadsave minimum config-file version, 126
show loadsave stftp, 127
show loadsave tftp, 128
show lock port, 668
show logbook, 712
show loopd, 772
show loopd interface, 772
show mac-address-table, 231, 541, 556
show mac-address-table aging-status, 608
show mac-address-table aging-time, 608
show mac-address-table count, 232
show mac-address-table dynamic multicast, 232, 557
show mac-address-table dynamic unicast, 233, 542
show mac-address-table static multicast, 234, 558
show mac-address-table static unicast, 235, 543
show monitor, 761, 762
show monitor barrier, 761
show multicast-block config, 73, 559, 564
show noa config, 74
show nodes monitoring, 74
show ntp info, 197
show ntp server info, 198
show passive-listening, 339
show password-policy, 634
show plug, 177
show pnio, 76
show poe schedule info, 160
show poe status, 159
show pof limit, 76
show pof status, 75
show power-line-state, 715
show pse status, 160
show ptp info, 220
show qos agent-priority, 615
show qos broadcast-priority, 615
show qos cos-map, 616
show qos cos-remap, 616
show qos dscp-map, 617
show qos scheduling mode, 618

show qos-trust-mode, 618
show radius server, 654
show radius statistics, 654
show rate-limit output, 591
show ring-redundancy, 507
show ring-redundancy manager counters, 507
show rmon, 749
show roles, 634
show running-config, 147
show signaling contact, 187
show sinema, 173
show snmp, 418
show snmp community, 418
show snmp engineID, 419
show snmp filter, 419
show snmp group, 420
show snmp group access, 420
show snmp inform statistics, 421
show snmp notif, 421
show snmp targetaddr, 422
show snmp targetparam, 422
show snmp tcp, 423
show snmp user, 423
show snmp viewtree, 424
show sntp broadcast-mode status, 213
show sntp status, 213
show sntp unicast-mode status, 214
show spanning-tree, 286
show spanning-tree active, 287
show spanning-tree bridge, 288
show spanning-tree detail, 289
show spanning-tree interface, 289
show spanning-tree interface layer2-gateway-port, 290
show spanning-tree mst, 291
show spanning-tree mst configuration, 292
show spanning-tree mst interface, 292
show spanning-tree passive-listening-compatibility, 293
show spanning-tree root, 294
show ssh-fingerprint, 473
show ssl server-cert, 465
show startup-information, 712
show tcp connections, 77
show tcp listeners, 77
show tcp retransmission details, 78
show tcp statistics, 78
show time, 191
show udp connections, 79
show udp statistics, 79
show unicast-block config, 80, 543, 550
show unicast-mac flush config, 544, 550
show unicast-mac learning config, 545, 551
show usage, 80
show user-accounts, 635
show user-groups, 636
show users, 636
show versions, 81
show vlan, 236
show vlan device info, 237, 242
show vlan learning params, 237
show vlan port config, 238
show vlan private-vlan, 239
show web-session-timeout, 181
shutdown, 117
    no shutdown, 118
shutdown complete, 117
signaling contact mode, 188
signaling-contact status, 189
sinema, 174
smtp-server
    no smtp-server, 450
smtp-server-enable, 459
snmp
    client config, 723
    no client config, 724
snmp access, 427
    no snmp access, 429
snmp agent version, 430
snmp community index, 430
    no snmp community index, 432
snmp engineid migrate, 432
snmp group, 434
    no snmp group, 435
snmp notify, 436
    no snmp notify, 437
snmp targetaddr, 437
    no snmp targetaddr, 439
snmp targetaddr remote-engine-id, 440
snmp targetparams, 440
    no snmp targetparams, 442
snmp user, 443
    no snmp user, 444
snmp v1-v2 readonly, 444
    no snmp v1-v2 readonly, 445
snmp view, 446
    no snmp view, 447
snmpagent, 425
    no snmpagent, 425
snmpagent port, 426
    no snmpagent port, 426
snooping report-process config-level, 496
sntp, 215
sntp client addressing-mode, 216

sntp time diff, 216
sntp unicast-server, 217
sntp unicast-server ipv4
    no sntp unicast-server ipv4, 218
spanning-tree, 296
    no spanning-tree, 297
spanning-tree (properties), 331
    no spanning-tree, 333
spanning-tree (time settings), 311
    no spanning-tree, 313
spanning-tree auto-edge, 314
    no spanning-tree auto-edge, 315
spanning-tree bpdufilter, 317
spanning-tree bpdu-guard, 317
    no spanning-tree bpdu-guard, 318
spanning-tree bpdu-receive, 315
spanning-tree bpdu-transmit, 316
spanning-tree compatibility, 298
    no spanning-tree compatibility, 299
spanning-tree layer2-gateway-port, 319
    no spanning-tree layer2-gateway-port, 319
spanning-tree limited-tcn, 320
    no spanning-tree limited-tcn, 321
spanning-tree loop-guard, 321
    no spanning-tree loop-guard, 322
spanning-tree mst (properties), 323
    no spanning-tree mst, 324
spanning-tree mst configuration, 299
spanning-tree mst hello-time, 325
    no spanning-tree mst hello-time, 326
spanning-tree mst instance-id root, 302
    no spanning-tree mst instance-id root, 303
spanning-tree mst max-hops, 300
    no spanning-tree mst max-hops, 301
spanning-tree mst pseudoRootId, 327
    no spanning-tree mst pseudoRootId, 328
spanning-tree passive-listening-compatibility, 305
spanning-tree pathcost dynamic, 306
    no spanning-tree pathcost dynamic, 307
spanning-tree priority, 303
    no spanning-tree priority, 304
spanning-tree restricted-role, 329
    no spanning-tree restricted-role, 329
spanning-tree restricted-tcn, 330
    no spanning-tree restricted-tcn, 330
spanning-tree rstp-plus, 308
spanning-tree rstp-plus mrp-intercon-domain-id, 309
spanning-tree tc-protection-backoff, 310
speed, 120
ssh-server, 474
    no ssh-server, 474
ssh-server port, 476
    no ssh-server port, 477
ssh-server portssh-server kex-algorithm-level, 475
standby connection name, 523, 524
standby ports, 525, 526
standby wait-for-partner, 527
    no standby wait-for-partner, 528
start, 672
static-lease, 400
    no static-lease, 401
stop, 673
storm-control, 594
    no storm-control, 595
storm-control level, 596
    no storm-control level, 596
switchport acceptable-frame-type, 254
    no switchport acceptable-frame-type, 255
switchport access vlan, 256
    no switchport access vlan, 257
switchport ingress-filter, 606
    no switchport ingress-filter, 607
switchport lock, 671
    no switchport lock, 671
switchport mode, 257
    no switchport mode, 259
switchport mode dot1q-tunnel, 260
switchport mode private vlan, 259
switchport priority default, 262
    no switchport priority default, 263
switchport private-vlan host-association, 263
switchport private-vlan mapping, 265
switchport pvid, 267
    no switchport pvid, 268
syslogserver, 737, 746
    no syslogserver, 738, 747
system contact, 102
system location, 103
System manual, 30
system name, 103

T

telnet-server, 354
    no telnet-server, 354
telnet-server port, 355
    no telnet-server port, 356
test, 460
tftp filename, 135
tftp load, 136
tftp save, 137

tftp server, 137
    Downloading, 128
    Saving, 130
time, 192
time dst date, 194
    no time dst, 196
time dst recurring, 195
time set, 193

U

unicast mac learning, 554
unicast-block, 120
unicast-mac flush, 122
user-account, 643
    no user-account, 645
user-account-ext, 646
user-group, 649
username, 652
user-name case-insensitive, 648
    no user-name case-insensitive, 649

V

vlan, 245
    no vlan, 246
vlan range, 248
vlan tag-priority override, 250

W

wait-for-completion, 538
Web Based Management (WBM), 783
web-session-timeout, 182
    no web-session-timeout, 183
whoami, 638
write, 181
write startup-config, 150