SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE W700 according to IEEE 802.11ax Command Line Interface V2.2

Configuration Manual

Introduction 1

Security recommendations 2

Description 3

General CLI commands 4

Configuration 5

Functions specific to SCALANCE 6

System time 7

Network structures 8

Network protocols 9

Load control 10

Security and authentication 11

Diagnostics 12

08/2023
C79000-G8976-C619-06

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

Document order number: C79000-G8900-C619
Ⓟ 08/2023 Subject to change

Copyright © Siemens AG 2021 - 2023.
All rights reserved

Table of contents

1 Introduction 19

1.1 Purpose of the configuration manual 19
1.2 Scope of validity 19
1.3 Supplementary documentation 20
1.4 Further documentation 21
1.5 Terms used 21
1.6 SIMATIC NET glossary 21
1.7 Cybersecurity information 22
1.8 Firmware 22
1.9 Open source license conditions 23
1.10 Error/fault 23
1.11 Decommissioning 23
1.12 Recycling and disposal 23
1.13 Marken 23

2 Security recommendations 25

2.1 Security recommendations 25
2.2 Available services 29

3 Description 33

3.1 Planned operating environment 33
3.2 Availability of the system functions 33
3.3 Configuration limits 36
3.4 Working with the Command Line Interface (CLI) 37
3.5 CLI modes 40
3.6 The CLI command prompt 41
3.7 Permitted characters 42
3.8 Symbols of the CLI commands 44
3.9 Interface identifiers and addresses 45
3.9.1 Naming interfaces 45
3.9.2 Address types, address ranges and address masks 48
3.9.3 Structure of an IPv4 address 48
3.9.4 IPv4 / IPv6 50
3.9.5 IPv6 terms 52
3.9.6 Structure of an IPv6 address 54

4 General CLI commands 57

4.1 clear screen 57
4.2 do 57
4.3 end 58
4.4 exit 58
4.5 grep 59
4.6 Help functions and supported input 59
4.6.1 help 60
4.6.2 The command "?" 60
4.6.3 Completion of command entries 61
4.6.4 Abbreviated notation of commands 62
4.6.5 Reusing the last used commands 62
4.6.6 Working through a command sequence 63
4.6.7 The "show" commands 63
4.6.7.1 show history 63
4.6.8 clear history 64

5 Configuration 67

5.1 System 67
5.1.1 show commands 67
5.1.1.1 show coordinates 67
5.1.1.2 show device information 68
5.1.1.3 show im 69
5.1.1.4 show interfaces 69
5.1.1.5 show interfaces ... counters 70
5.1.1.6 show interface mtu 71
5.1.1.7 show ip interface 72
5.1.1.8 show lldp neighbors 72
5.1.1.9 show lldp status 73
5.1.1.10 show pnio 74
5.1.1.11 show traceroute 74
5.1.1.12 show versions 75
5.1.2 clear counters 76
5.1.3 configure terminal 77
5.1.4 clear line vty 77
5.1.5 disable 78
5.1.6 enable 79
5.1.7 logout 79
5.1.8 ping 80
5.1.9 ping ipv6 81
5.1.10 traceroute 82
5.1.11 Commands in the global configuration mode 83
5.1.11.1 coordinates height 83
5.1.11.2 coordinates latitude 84
5.1.11.3 coordinates longitude 85
5.1.11.4 Interface 86
5.1.11.5 no interface 87
5.1.11.6 pre-login message add 88
5.1.11.7 no pre-login message 89

5.1.11.8 pnio ... 90
5.1.11.9 pnio station-name ... 91
5.1.11.10 system contact ... 91
5.1.11.11 system location ... 92
5.1.11.12 system name ... 93
5.1.12 Commands in the Interface configuration mode ... 93
5.1.12.1 alias ... 94
5.1.12.2 no alias ... 95
5.1.12.3 lldp ... 95
5.1.12.4 no lldp ... 96
5.1.12.5 shutdown complete ... 97
5.1.12.6 no shutdown ... 98

5.2 Load and Save ... 99
5.2.1 File list ... 100
5.2.2 The "show" commands ... 105
5.2.2.1 show loadsave files ... 105
5.2.2.2 show loadsave tftp ... 106
5.2.2.3 show loadsave stftp ... 106
5.2.3 save filetype ... 107
5.2.4 load ... 108
5.2.5 Commands in the global configuration mode ... 109
5.2.5.1 loadsave ... 110
5.2.6 Commands in the LOADSAVE configuration mode ... 110
5.2.6.1 delete ... 111
5.2.6.2 tftp filename ... 111
5.2.6.3 tftp load ... 112
5.2.6.4 tftp save ... 113
5.2.6.5 tftp server ... 114
5.2.6.6 sftp filename ... 115
5.2.6.7 sftp load ... 116
5.2.6.8 sftp save ... 116
5.2.6.9 sftp server ... 117
5.2.6.10 password ... 118
5.2.6.11 no password ... 119
5.2.6.12 firmware-in-configpack ... 120
5.2.6.13 no firmeware-in-configpack ... 121

5.3 Reset and Defaults ... 121
5.3.1 restart ... 122
5.3.2 Commands in global configuration mode ... 123
5.3.2.1 schedule restart-configbackup ... 123
5.3.2.2 no schedule restart-configbackup ... 124
5.3.2.3 schedule restart-timer ... 125
5.3.2.4 cancel restart-timer ... 126
5.3.2.5 sleep ... 126

5.4 Configuration Save & Restore ... 127
5.4.1 The "show" commands ... 127
5.4.1.1 show running-config ... 127
5.4.2 write startup-config ... 129
5.4.3 Commands in the global configuration mode ... 129
5.4.3.1 auto-save ... 130
5.4.3.2 no auto-save ... 131

5.4.3.3 digital output retain ... 132
5.4.3.4 no digital output retain ... 132

5.5 Configuration backup ... 133
5.5.1 The "show" commands ... 133
5.5.1.1 show configbackup ... 133
5.5.2 Commands in the global configuration mode ... 134
5.5.2.1 configbackup create ... 135
5.5.2.2 configbackup restore ... 135
5.5.2.3 configbackup delete ... 136

5.6 Discovery and Set via PROFINET Discovery Protocol (DCP) ... 137
5.6.1 The "show" commands ... 137
5.6.1.1 show das info ... 137
5.6.2 Commands in the global configuration mode ... 138
5.6.2.1 das discover interface ... 138
5.6.2.2 das mac name ... 139
5.6.2.3 das mac ip ... 140
5.6.2.4 das mac blink ... 141
5.6.2.5 das delete ... 142

5.7 SINEMA ... 143
5.7.1 The "show" commands ... 143
5.7.1.1 show sinema ... 143
5.7.2 Commands in the global configuration mode ... 143
5.7.2.1 sinema ... 144
5.7.2.2 no sinema ... 144

6 Functions specific to SCALANCE ... 147

6.1 PLUG ... 147
6.1.1 The "show" commands ... 147
6.1.1.1 show plug ... 147
6.1.2 Commands in the global configuration mode ... 148
6.1.2.1 plug ... 148
6.1.3 Commands in the Plug Configuration mode ... 149
6.1.3.1 factoryclean ... 149
6.1.3.2 firmware-on-plug ... 149
6.1.3.3 no firmware on plug ... 150
6.1.3.4 write ... 151
6.1.3.5 presetplug ... 151

6.2 WBM ... 152
6.2.1 The "show" commands ... 152
6.2.1.1 show web-session-timeout ... 152
6.2.2 Commands in the global configuration mode ... 153
6.2.2.1 web-session-timeout ... 153
6.2.2.2 no web-session-timeout ... 154

6.3 CLI ... 154
6.3.1 The "show" commands ... 154
6.3.1.1 show cli-console-timeout ... 155
6.3.2 Commands in the global configuration mode ... 155
6.3.2.1 cli-console-timeout ... 156
6.3.2.2 no cli-console-timeout ... 157

6.4 iPRP ... 157
6.4.1 The "show" commands ... 158
6.4.1.1 show wlan iprp ... 158
6.4.1.2 show wlan iprp information ... 158
6.4.2 clear wlan iprp information ... 159
6.4.3 Commands in the WLAN configuration mode ... 159
6.4.3.1 wlan iprp ... 160
6.4.4 Commands in the WLAN iPRP configuration mode ... 161
6.4.4.1 wlan iprp interface ... 162
6.4.4.2 no wlan iprp interface ... 163
6.4.4.3 wlan iprp network ... 164
6.4.4.4 no wlan iprp network ... 164

6.5 iPCF-2 ... 165
6.5.1 The "show" commands ... 165
6.5.1.1 show wlan ipcf-2 ... 166
6.5.2 WLAN Interface configuration mode ... 166
6.5.2.1 wlan ipcf-2 ... 167
6.5.2.2 no wlan ipcf-2 ... 167

6.6 Packet Capture ... 168
6.6.1 show packet capture ... 168
6.6.2 Commands in the global configuration mode ... 168
6.6.2.1 packet capture ... 169
6.6.3 Commands in Packet Capture configuration mode ... 169
6.6.3.1 activate-after-restart ... 170
6.6.3.2 no-activate-after-restart ... 170
6.6.3.3 capture ... 171
6.6.3.4 no capture ... 173
6.6.3.5 port ... 174
6.6.3.6 no port ... 174

6.7 Signal recorder ... 175
6.7.1 The "show" commands ... 175
6.7.1.1 show wlan signal-recorder (Client) ... 175
6.7.2 wlan signal-recorder start (client) ... 176
6.7.3 wlan signal-recorder display (client) ... 178
6.7.4 wlan signal-recorder stop (client) ... 179

6.8 TCP Event ... 180
6.8.1 The "show" commands ... 180
6.8.1.1 show tcpevent ... 180
6.8.2 Commands in global configuration mode ... 180
6.8.2.1 tcpevent ... 181
6.8.3 Commands in the TCP EVENT configuration mode ... 181
6.8.3.1 enable ... 182
6.8.3.2 disable ... 182
6.8.3.3 port ... 183
6.8.3.4 event ... 184
6.8.3.5 event type wlan-roaming enable (client) ... 185
6.8.3.6 event type wlan-roaming disable (client) ... 185
6.8.3.7 password ... 186
6.8.3.8 user ... 186
6.8.3.9 event show-types ... 187

7 System time 189

7.1 System time setting 189
7.1.1 The "show" commands 189
7.1.1.1 show time 189
7.1.1.2 show dst info 190
7.1.2 Commands in the global configuration mode 190
7.1.2.1 time 190
7.1.2.2 time set 191
7.1.2.3 time dst date 192
7.1.2.4 time dst recurring 193
7.1.2.5 no time dst 194

7.2 NTP client 195
7.2.1 The "show" commands 195
7.2.1.1 show ntp info 195
7.2.2 Commands in the global configuration mode 196
7.2.2.1 ntp 196
7.2.3 Commands in the NTP configuration mode 197
7.2.3.1 ntp server 197
7.2.3.2 no ntp server 198
7.2.3.3 ntp time diff 199

7.3 SNTP client 200
7.3.1 The "show" commands 200
7.3.1.1 show sntp broadcast-mode status 200
7.3.1.2 show sntp status 200
7.3.1.3 show sntp unicast-mode status 201
7.3.2 Commands in the global configuration mode 201
7.3.2.1 sntp 202
7.3.3 Commands in the SNTP configuration mode 202
7.3.3.1 sntp time diff 203
7.3.3.2 sntp unicast-server 204
7.3.3.3 no sntp unicast-server 205
7.3.3.4 sntp client addressing-mode 206

8 Network structures 207

8.1 WLAN 207
8.1.1 Introduction to the section WLAN 207
8.1.2 The "show" commands 207
8.1.2.1 show wlan advanced 207
8.1.2.2 show wlan allowed channels 208
8.1.2.3 show wlan antennas 209
8.1.2.4 show wlan ap (access point) 209
8.1.2.5 show wlan available-ap-list (client) 210
8.1.2.6 show wlan basic 211
8.1.2.7 show wlan client (Client) 212
8.1.2.8 show wlan client-list (access point) 213
8.1.2.9 show wlan client-list-vap (access point) 214
8.1.2.10 show wlan device 214
8.1.2.11 show wlan ip-mapping 215
8.1.2.12 show wlan noise-floor 216
8.1.2.13 show wlan overlap-ap-list (access point) 216

8.1.2.14 show wlan overview 217
8.1.2.15 show wlan ssid-table (client) 218
8.1.2.16 show wlan vap (access point) 219
8.1.3 Commands in the global configuration mode 220
8.1.3.1 wlan 220
8.1.4 Commands in the WLAN configuration mode 221
8.1.4.1 commit mode 221
8.1.4.2 commit wlan-settings 222
8.1.4.3 country 223
8.1.4.4 device mode 224
8.1.5 Commands in the WLAN Interface configuration mode 224
8.1.5.1 wlan allowed channels only 225
8.1.5.2 wlan allowed channels 226
8.1.5.3 no wlan allowed channels only 227
8.1.5.4 wlan alternative channel (Access Point) 228
8.1.5.5 wlan ampdu 229
8.1.5.6 no wlan ampdu 229
8.1.5.7 wlan antenna additional-attenuation 230
8.1.5.8 wlan antenna cable-length 231
8.1.5.9 wlan antenna gain-2-4GHz 232
8.1.5.10 wlan antenna gain-5GHz 233
8.1.5.11 wlan antenna mode 233
8.1.5.12 wlan antenna type 235
8.1.5.13 wlan background scan interval (client) 236
8.1.5.14 wlan background scan mode (client) 236
8.1.5.15 wlan background scan threshold (Client) 237
8.1.5.16 wlan beacon interval (Access Point) 238
8.1.5.17 wlan channel (Access Point) 239
8.1.5.18 wlan channel width (Access Point) 240
8.1.5.19 wlan client mac mode (client) 240
8.1.5.20 wlan dfs 241
8.1.5.21 no wlan dfs 242
8.1.5.22 wlan frequency band 243
8.1.5.23 wlan hw-retries 243
8.1.5.24 wlan max tx-power 244
8.1.5.25 wlan mode 245
8.1.5.26 wlan outdoor 247
8.1.5.27 no wlan outdoor 247
8.1.5.28 wlan overlap-ap aging 248
8.1.5.29 wlan scan-time-per-channel (Client) 249
8.1.5.30 wlan ssid-table edit (client) 250
8.1.6 Commands in the VAP Interface Configuration mode 251
8.1.6.1 vap ssid (access point) 251
8.1.6.2 vap broadcast ssid (access point) 252
8.1.6.3 no vap broadcast ssid (access point) 253

8.2 VLAN 253
8.2.1 The "show" commands (VLAN Bridge) 254
8.2.1.1 show mac-address-table 254
8.2.1.2 show mac-address-table count 255
8.2.1.3 show mac-address-table dynamic unicast 255
8.2.1.4 show vlan 256
8.2.1.5 show vlan device info 257

8.2.1.6 show vlan learning params 257
8.2.1.7 show vlan port config 258
8.2.2 The "show" commands (Transparent Bridge) 259
8.2.2.1 show dot1d mac-address-table 259
8.2.2.2 show vlan device info 260
8.2.3 Commands in the global configuration mode 260
8.2.3.1 vlan 261
8.2.3.2 no vlan 262
8.2.3.3 base bridge-mode 263
8.2.4 Commands in the Interface configuration mode (VLAN Bridge) 263
8.2.4.1 mtu 264
8.2.4.2 shutdown complete 265
8.2.4.3 no shutdown 265
8.2.4.4 switchport acceptable-frame-type 266
8.2.4.5 no switchport acceptable-frame-type 267
8.2.4.6 switchport access vlan 268
8.2.4.7 no switchport access vlan 268
8.2.4.8 switchport ingress-filter 269
8.2.4.9 no switchport ingress-filter 270
8.2.4.10 switchport mode 270
8.2.4.11 no switchport mode 271
8.2.4.12 switchport priority default 272
8.2.4.13 no switchport priority default 273
8.2.4.14 switchport pvid 274
8.2.4.15 no switchport pvid 274
8.2.4.16 tia interface 275
8.2.5 Commands in the VLAN configuration mode (VLAN Bridge) 276
8.2.5.1 name 276
8.2.5.2 no name 277
8.2.5.3 ports 278
8.2.5.4 no ports 279

8.3 Spanning Tree 280
8.3.1 The "show" commands 280
8.3.1.1 show spanning-tree 281
8.3.1.2 show spanning-tree active 282
8.3.1.3 show spanning-tree bridge 282
8.3.1.4 show spanning-tree detail 283
8.3.1.5 show spanning-tree interface 284
8.3.1.6 show spanning-tree l2t-edge 285
8.3.1.7 show spanning-tree mst 285
8.3.1.8 show spanning-tree mst configuration 286
8.3.1.9 show spanning-tree mst interface 287
8.3.1.10 show spanning-tree root 288
8.3.2 clear spanning-tree counters 288
8.3.3 Commands in the global configuration mode 289
8.3.3.1 spanning-tree 289
8.3.3.2 no spanning-tree 290
8.3.3.3 spanning-tree compatibility 291
8.3.3.4 no spanning-tree compatibility 292
8.3.3.5 spanning-tree l2t-auto-edge 292
8.3.3.6 no spanning-tree l2t-auto-edge 293
8.3.3.7 spanning-tree l2t-edge 294

8.3.3.8 no spanning-tree l2t-edge ... 294
8.3.3.9 spanning-tree mst configuration ... 295
8.3.3.10 spanning-tree mst instance-id root ... 296
8.3.3.11 no spanning-tree mst instance-id root ... 297
8.3.3.12 spanning-tree mst max-hops ... 297
8.3.3.13 no spanning-tree mst max-hops ... 298
8.3.3.14 spanning-tree pathcost dynamic ... 299
8.3.3.15 no spanning-tree pathcost dynamic ... 300
8.3.3.16 spanning-tree priority ... 300
8.3.3.17 no spanning-tree priority ... 301
8.3.3.18 Time settings for the Spanning Tree protocol ... 302
8.3.4 Commands in the interface configuration mode ... 304
8.3.4.1 spanning-tree ... 305
8.3.4.2 no spanning-tree ... 307
8.3.4.3 spanning-tree auto-edge ... 308
8.3.4.4 no spanning-tree auto-edge ... 308
8.3.4.5 spanning-tree bdpufilter ... 309
8.3.4.6 spanning-tree bpdu-receive ... 310
8.3.4.7 spanning-tree bpdu-transmit ... 310
8.3.4.8 spanning-tree mst ... 311
8.3.4.9 no spanning-tree mst ... 312
8.3.4.10 spanning-tree mst hello-time ... 314
8.3.4.11 no spanning-tree mst hello-time ... 314
8.3.5 Commands in the MSTP configuration mode ... 315
8.3.5.1 instance ... 316
8.3.5.2 no instance ... 317
8.3.5.3 name ... 317
8.3.5.4 no name ... 318
8.3.5.5 revision ... 319
8.3.5.6 no revision ... 320

9 Network protocols ... 321

9.1 IPv4 protocol ... 321
9.1.1 The "show" commands ... 321
9.1.1.1 show dcp forwarding ... 321
9.1.1.2 show dcp server ... 322
9.1.1.3 show ip gateway ... 322
9.1.1.4 show ip route ... 323
9.1.1.5 show ip static route ... 324
9.1.1.6 show ip telnet ... 324
9.1.2 Commands in the global configuration mode ... 325
9.1.2.1 dcp server ... 325
9.1.2.2 no dcp server ... 326
9.1.2.3 ip route ... 326
9.1.2.4 no ip route ... 327
9.1.2.5 telnet-server ... 328
9.1.2.6 no telnet-server ... 329
9.1.2.7 telnet-server port ... 329
9.1.2.8 no telnet-server port ... 330
9.1.3 Commands in the Interface configuration mode ... 331
9.1.3.1 ip address ... 331
9.1.3.2 ip address dhcp ... 332

9.1.3.3 no ip address ... 333
9.1.3.4 dcp forwarding ... 334

9.2 IPv6 protocol ... 335
9.2.1 Configuration matrix ... 335
9.2.2 The "show" commands ... 335
9.2.2.1 show ipv6 interface ... 335
9.2.2.2 show ipv6 neighbors ... 336
9.2.2.3 show ipv6 pmtu ... 337
9.2.2.4 show ipv6 route ... 337
9.2.2.5 show ipv6 static route ... 338
9.2.2.6 show ipv6 traffic ... 338
9.2.3 Commands in the global configuration mode ... 339
9.2.3.1 ipv6 neighbor ... 340
9.2.3.2 no ipv6 neighbor ... 341
9.2.3.3 ipv6 path mtu ... 342
9.2.3.4 no ipv6 path mtu ... 342
9.2.3.5 ipv6 path mtu discover ... 343
9.2.3.6 no ipv6 path mtu discover ... 344
9.2.3.7 ipv6 route ... 344
9.2.3.8 no ipv6 route ... 345
9.2.4 Commands in the Interface configuration mode ... 346
9.2.4.1 ipv6 address ... 347
9.2.4.2 no ipv6 address ... 348
9.2.4.3 ipv6 address autoconfig ... 349
9.2.4.4 no ipv6 address autoconfig ... 349
9.2.4.5 ipv6 address dhcp ... 350
9.2.4.6 no ipv6 address dhcp ... 351
9.2.4.7 ipv6 address link-local ... 352
9.2.4.8 no ipv6 address link-local ... 353
9.2.4.9 ipv6 enable ... 353
9.2.4.10 no ipv6 enable ... 354

9.3 Domain Name System ... 355
9.3.1 The "show" commands ... 355
9.3.1.1 show dnsclient information ... 355
9.3.2 Commands in the global configuration mode ... 356
9.3.2.1 dnsclient ... 356
9.3.3 Commands in the DNS CLIENT configuration mode ... 357
9.3.3.1 manual srv ... 357
9.3.3.2 no manual srv ... 358
9.3.3.3 server type ... 358
9.3.3.4 shutdown ... 359
9.3.3.5 no shutdown ... 360

9.4 DHCPv4 client (IPv4) ... 360
9.4.1 The "show" commands ... 361
9.4.1.1 show ip dhcp client stats ... 361
9.4.1.2 show ip dhcp client ... 361
9.4.2 Commands in the global configuration mode ... 362
9.4.2.1 ip dhcp config-file-request ... 362
9.4.2.2 no ip dhcp config-file-request ... 363
9.4.2.3 ip dhcp client mode ... 363

9.5 DHCPv6 client (IPv6) ... 364
9.5.1 clear ipv6 dhcp client statistics ... 364
9.5.2 The "show" commands ... 365
9.5.2.1 show ipv6 dhcp ... 365
9.5.2.2 show ipv6 dhcp interface ... 366
9.5.2.3 show ipv6 dhcp client statistics ... 367

9.6 SNMP ... 368
9.6.1 The "show" commands ... 369
9.6.1.1 show snmp ... 369
9.6.1.2 show snmp community ... 369
9.6.1.3 show snmp engineID ... 370
9.6.1.4 show snmp filter ... 370
9.6.1.5 show snmp group ... 371
9.6.1.6 show snmp group access ... 371
9.6.1.7 show snmp inform statistics ... 372
9.6.1.8 show snmp notif ... 372
9.6.1.9 show snmp targetaddr ... 373
9.6.1.10 show snmp targetparam ... 373
9.6.1.11 show snmp user ... 374
9.6.1.12 show snmp viewtree ... 374
9.6.2 Commands in the global configuration mode ... 375
9.6.2.1 snmpagent ... 375
9.6.2.2 no snmpagent ... 376
9.6.2.3 snmp access ... 376
9.6.2.4 no snmp access ... 378
9.6.2.5 snmp agent version ... 379
9.6.2.6 snmp community index ... 379
9.6.2.7 no snmp community index ... 381
9.6.2.8 snmp engineid migrate ... 381
9.6.2.9 no snmp engineid migrate ... 382
9.6.2.10 snmp filterprofile ... 383
9.6.2.11 no snmp filterprofile ... 384
9.6.2.12 snmp group ... 385
9.6.2.13 no snmp group ... 386
9.6.2.14 snmp notify ... 386
9.6.2.15 no snmp notify ... 387
9.6.2.16 snmp targetaddr ... 388
9.6.2.17 no snmp targetaddr ... 390
9.6.2.18 snmp targetaddr remote-engine-id ... 390
9.6.2.19 snmp targetparams ... 391
9.6.2.20 no snmp targetparams ... 393
9.6.2.21 snmp v1-v2 readonly ... 393
9.6.2.22 no snmp v1-v2 readonly ... 394
9.6.2.23 snmpagent port ... 395
9.6.2.24 no snmpagent port ... 395
9.6.2.25 snmp user ... 396
9.6.2.26 no snmp user ... 397
9.6.2.27 snmp view ... 398
9.6.2.28 no snmp view ... 399

9.7 SMTP client ... 400
9.7.1 The "show" commands ... 400

9.7.1.1 show events smtp-server ... 400
9.7.1.2 show events smtp-port ... 401
9.7.2 Commands in the Events configuration mode ... 401
9.7.2.1 smtp-server ... 402
9.7.2.2 no smtp-server ... 403
9.7.2.3 send test mail ... 404
9.7.3 Commands in SMTP server configuration mode ... 404
9.7.3.1 auth username ... 405
9.7.3.2 no auth username ... 405
9.7.3.3 port ... 406
9.7.3.4 no port ... 407
9.7.3.5 receiver-address ... 407
9.7.3.6 no receiver-address ... 408
9.7.3.7 security ... 409
9.7.3.8 no security ... 410
9.7.3.9 sender address ... 410
9.7.3.10 no sender address ... 411
9.7.3.11 snmp-server-enable ... 412
9.7.3.12 no snmp server enable ... 412
9.7.3.13 test ... 413

9.8 HTTP server ... 413
9.8.1 The "show" commands ... 413
9.8.1.1 show ip http server status ... 414
9.8.2 Commands in the Global Configuration mode ... 414
9.8.2.1 ip http ... 414
9.8.2.2 no ip http ... 415
9.8.2.3 ip http port ... 416
9.8.2.4 no ip http port ... 417

9.9 HTTPS server ... 417
9.9.1 The "show" commands ... 417
9.9.1.1 show ip http secure server status ... 417
9.9.1.2 show ssl server-cert ... 418
9.9.2 Commands in the Global Configuration mode ... 418
9.9.2.1 ip http https redirection ... 419
9.9.2.2 ip http secure ... 419
9.9.2.3 no ip http secure ... 420
9.9.2.4 ip http secure minimum tls-version ... 421
9.9.2.5 ip http secure port ... 421
9.9.2.6 no ip http secure port ... 422

9.10 ARP ... 423
9.10.1 The "show" commands ... 423
9.10.1.1 show ip arp ... 423

9.11 SSH server ... 424
9.11.1 The "show" commands ... 424
9.11.1.1 show ip ssh ... 424
9.11.1.2 show ssh-fingerprint ... 425
9.11.2 Commands in the Global Configuration mode ... 425
9.11.2.1 ssh-server ... 426
9.11.2.2 no ssh-server ... 426
9.11.2.3 ssh-server port ... 427

9.11.2.4 no ssh-server port ... 428
9.11.2.5 ssh-server kex-algorithm-level ... 429

10 Load control ... 431

10.1 Dynamic MAC aging ... 431
10.1.1 The "show" commands ... 431
10.1.1.1 show mac-address-table aging-status ... 431
10.1.1.2 show mac-address-table aging-time ... 432
10.1.2 Commands in the global configuration mode ... 432
10.1.2.1 mac-address-table aging ... 433
10.1.2.2 no mac-address-table aging ... 433
10.1.2.3 mac-address-table aging-time ... 434
10.1.2.4 no mac-address-table aging-time ... 435

11 Security and authentication ... 437

11.1 User rights management ... 437
11.1.1 change password ... 437
11.1.2 whoami ... 438
11.1.3 The "show" commands ... 438
11.1.3.1 show function-rights ... 439
11.1.3.2 show password-policy ... 439
11.1.3.3 show roles ... 440
11.1.3.4 show user-accounts ... 440
11.1.3.5 show user-groups ... 441
11.1.3.6 show users ... 442
11.1.4 Commands in the global configuration mode ... 442
11.1.4.1 role ... 443
11.1.4.2 no role ... 444
11.1.4.3 user-account ... 445
11.1.4.4 no user-account ... 447
11.1.4.5 user-account-ext ... 448
11.1.4.6 no user-account-ext ... 449
11.1.4.7 user-group ... 450
11.1.4.8 no user-group ... 451
11.1.4.9 password-policy ... 452
11.1.4.10 password-policy min-length ... 453
11.1.4.11 password-policy (parameter) ... 454

11.2 RADIUS client ... 455
11.2.1 The "show" commands ... 455
11.2.1.1 show radius statistics ... 455
11.2.1.2 show radius server (IPv6) ... 456
11.2.2 Commands in the global configuration mode ... 456
11.2.2.1 login authentication ... 457
11.2.2.2 no login authentication ... 458
11.2.2.3 radius authorization-mode ... 458
11.2.2.4 radius-server ... 459
11.2.2.5 no radius-server ... 461

11.3 Brute Force Prevention ... 462
11.3.1 The "show" commands ... 462
11.3.1.1 show brute-force-prevention config ... 462
11.3.1.2 show brute-force-prevention status ... 463

11.3.2 Commands in global configuration mode ... 464
11.3.2.1 brute-force-prevention ip-specific-login-attempts ... 464
11.3.2.2 no brute-force-prevention ip-specific-login-attempts ... 465
11.3.2.3 brute-force-prevention user-specific-login-attempts ... 466
11.3.2.4 no brute-force-prevention user-specific-login-attempts ... 467
11.3.2.5 brute-force-prevention trigger-interval ... 468
11.3.2.6 brute-force-prevention auto-reset-timer ... 468
11.3.2.7 no brute-force-prevention auto-reset-timer ... 469
11.3.2.8 brute-force-prevention reset ... 470

11.4 NAT ... 471
11.4.1 The "show" commands ... 471
11.4.1.1 show firewallnat napt ... 472
11.4.1.2 show firewallnat masquerading ... 472
11.4.2 Commands in the global configuration mode ... 473
11.4.2.1 firewallnat ... 473
11.4.3 Commands in the FIREWALL NAT configuration mode ... 474
11.4.3.1 masquerading show-idx ... 474
11.4.3.2 napt show-idx ... 474
11.4.3.3 napt srcint ... 475
11.4.3.4 no napt srcint ... 477
11.4.3.5 no napt all ... 478

11.5 WLAN ... 478
11.5.1 Introduction to the section WLAN ... 478
11.5.2 The "show" commands ... 479
11.5.2.1 show wlan inter-ap-blocking allowed addresses (Access Point) ... 479
11.5.2.2 show wlan security ... 480
11.5.2.3 show wlan security ap-radius-authenticator (Access Point) ... 481
11.5.2.4 show wlan security fast-bss-transition (Access Point) ... 482
11.5.2.5 show wlan security server-cert (client) ... 482
11.5.2.6 show wlan security user-cert (client) ... 483
11.5.3 Commands in the WLAN configuration mode ... 483
11.5.3.1 wlan security ap-radius-authenticator (Access Point) ... 483
11.5.3.2 no wlan security ap-radius-authenticator (Access Point) ... 484
11.5.3.3 wlan security ap-radius-authenticator address (Access Point) ... 485
11.5.3.4 wlan security ap-radius-authenticator max-retransmit (Access Point) ... 486
11.5.3.5 wlan security ap-radius-authenticator port-number (Access Point) ... 487
11.5.3.6 wlan security ap-radius-authenticator primary (Access Point) ... 488
11.5.3.7 no wlan security ap-radius-authenticator primary (Access Point) ... 489
11.5.3.8 wlan security ap-radius-authenticator reauth-interval (Access Point) ... 489
11.5.3.9 wlan security ap-radius-authenticator reauth-mode (Access Point) ... 490
11.5.3.10 wlan security ap-radius-authenticator shared-secret (Access Point) ... 491
11.5.3.11 wlan security context (Client) ... 492
11.5.3.12 wlan security dot1x min-tls-version (Client) ... 493
11.5.3.13 vap inter-ap-blocking refresh time (Access Point) ... 494
11.5.4 Commands in the WLAN Interface configuration mode ... 495
11.5.4.1 wlan security ssid (Client) ... 495
11.5.5 Commands in the VAP Interface configuration mode ... 496
11.5.5.1 vap inter-ap-blocking (access point) ... 497
11.5.5.2 no vap inter-ap-blocking (access point) ... 497
11.5.5.3 vap inter-ap-blocking allowed address (access point) ... 498
11.5.5.4 no vap inter-ap-blocking allowed address (access point) ... 499

11.5.5.5 vap inter-ap-blocking block gratuitous arp (access point) ... 500
11.5.5.6 no vap inter-ap-blocking block gratuitous arp (access point) ... 500
11.5.5.7 vap inter-ap-blocking block non-ip-traffic (access point) ... 501
11.5.5.8 no vap inter-ap-blocking block non-ip-traffic (access point) ... 502
11.5.5.9 vap security authentication (access point) ... 502
11.5.5.10 vap security cipher (access point) ... 503
11.5.5.11 vap security fast-bss-transition (access point) ... 504
11.5.5.12 no vap security fast-bss-transition (Access Point) ... 505
11.5.5.13 vap security protected-management-frames (access point) ... 506
11.5.5.14 no vap security protected-management-frames (access point) ... 507
11.5.5.15 vap security wpa-group-key-update-interval (Access Point) ... 507
11.5.5.16 vap security wpa-psk-passphrase (access point) ... 508
11.5.6 Commands in the security context configuration mode ... 509
11.5.6.1 wlan security authentication (client) ... 509
11.5.6.2 wlan security cipher (client) ... 510
11.5.6.3 wlan security dot1x check-server-certificate (client) ... 511
11.5.6.4 no wlan security dot1x check-server-certificate (client) ... 512
11.5.6.5 wlan security dot1x eap-authentication-type (client) ... 513
11.5.6.6 wlan security dot1x password (client) ... 514
11.5.6.7 wlan security dot1x username (client) ... 515
11.5.6.8 wlan security protected-management-frames (client) ... 516
11.5.6.9 no wlan security protected-management-frames (client) ... 517
11.5.6.10 wlan security wpa-psk-passphrase (client) ... 517

12 Diagnostics ... 519

12.1 Event and fault handling ... 519
12.1.1 clear authlog ... 519
12.1.2 clear logbook ... 520
12.1.3 clear fault counter ... 520
12.1.4 fault report ack ... 521
12.1.5 logging console ... 522
12.1.6 no logging console ... 522
12.1.7 The "show" commands ... 523
12.1.7.1 show authlog ... 523
12.1.7.2 show events config ... 524
12.1.7.3 show events faults config ... 524
12.1.7.4 show events faults status ... 525
12.1.7.5 show events severity ... 526
12.1.7.6 show fault counter ... 526
12.1.7.7 show logbook ... 527
12.1.7.8 show power-line-state ... 527
12.1.7.9 show rmon ... 528
12.1.7.10 show startup-information ... 529
12.1.8 Commands in the global configuration mode ... 529
12.1.8.1 events ... 530
12.1.9 Commands in the EVENT configuration mode ... 530
12.1.9.1 add log ... 531
12.1.9.2 client config ... 531
12.1.9.3 no client config ... 532
12.1.9.4 event config ... 533
12.1.9.5 no event config ... 535
12.1.9.6 event config wlan-auth-log syslog ... 537

12.1.9.7 no event config wlan-auth-log syslog 537
12.1.9.8 link 538
12.1.9.9 no link 539
12.1.9.10 logbook alarm threshold 540
12.1.9.11 power 540
12.1.9.12 no power 541
12.1.9.13 power pnio redundancy 542
12.1.9.14 send test mail 543
12.1.9.15 severity 543
12.1.9.16 no severity 544

12.2 Syslog client 545
12.2.1 The "show" commands 546
12.2.1.1 show events syslogserver 546
12.2.2 Commands in the EVENT configuration mode 546
12.2.2.1 syslogserver 547
12.2.2.2 no syslogserver 548

Index 549

Introduction

1

1.1 Purpose of the configuration manual

This Configuration Manual is intended to provide you with the information you require to commission and operate the device. 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 devices.

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

1.2 Scope of validity

This Configuration Manual covers the following products:

Product	Article number	Certification ID
Access points		
SCALANCE WAM766-1	6GK5766-1GE00-7DA0 6GK5766-1GE00-7DB0 (US) 6GK5766-1GE00-7DC0 (ME)	MSAX65-W1-M12-E2
SCALANCE WAM766-1 EEC	6GK5766-1GE00-7TA0 6GK5766-1GE00-7TB0 (US) 6GK5766-1GE00-7TC0 (ME)	MSAX65-W1-M12-E2
SCALANCE WAM763-1	6GK5763-1AL00-7DA0 (DI/DO) 6GK5763-1AL00-7DB0 (US) (DI/DO) 6GK5763-1AL00-7DC0 (ME) (DI/DO)	MSAX-W1-RJ-E2
SCALANCE WAB762-1	6GK5762-1AJ00-6AA0	ELAX-W1-RJ-E2
Client		
SCALANCE WUM766-1	6GK5766-1GE00-3DA0 6GK5766-1GE00-3DB0 (US) 6GK5766-1GE00-3DC0 (ME)	MSAX65-W1-M12-E2
SCALANCE WUM763-1	6GK5763-1AL00-3AA0 6GK5763-1AL00-3AB0 (US)	MSAX-W1-RJ-E2-NO
	6GK5763-1AL00-3DA0 (DI/DO) 6GK5763-1AL00-3DB0 (US) (DI/DO)	MSAX-W1-RJ-E2
SCALANCE WUB762-1	6GK5762-1AJ00-1AA0	ELAX-W1-RJ-E2
SCALANCE WUB762-1 iFeatures	6GK5762-1AJ00-2AA0	ELAX-W1-RJ-E2

The configuration manual applies to the following firmware version:

- SCALANCE W700 IEEE 802.11ax firmware as of version V2.2

1.3 Supplementary documentation

Documentation on the Internet

You can find the current version of the document on the Internet at (https://support.industry.siemens.com/cs/de/en/ps/28575/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 following documentation is also available from SIMATIC NET on the topic of Industrial Wireless LANs:

- Configuration Manual: SCALANCE W700 according to IEEE 802.11ax Web Based Management
  This document is intended to provide you with the information you require to commission and configure SCALANCE W700ax devices using Web Based Management. It explains how to configure the SCALANCE W700ax devices and how to integrate SCALANCE W700ax devices into a WLAN network.
- Operating Instructions SCALANCE WxM766-1
  This document contains information on installing, connecting, maintaining and servicing the following products:
  - SCALANCE WAM766-1
  - SCALANCE WAM766-1 EEC
  - SCALANCE WUM766-1
- Operating Instructions SCALANCE WxM763-1
  This document contains information on installing, connecting, maintaining and servicing the following products:
  - SCALANCE WAM763-1
  - SCALANCE WUM763-1
- Operating Instructions SCALANCE WxM763-1
  This document contains information on installing, connecting, maintaining and servicing the following products:
  - SCALANCE WAB762-1
  - SCALANCE WUB762-1
  - SCALANCE WUB762-1 iFeatures
- SCALANCE W700 802.11ax approvals
  This document contains information on currently available country approvals.
- Performance data SCALANCE W700 802.11ax
  This document contains information about the frequency, modulation, transmit power and receiver sensitivity of the wireless card.

1.4 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

The RCoax system manual contains both an explanation of the basic technical aspects as well as a description of the individual RCoax components and their mode of operation. Installation/ commissioning and connection of RCoax components and their operating principle are explained. The possible applications of the various SIMATIC NET components are described.

You can find the RCoax system manual on the Internet pages of Siemens Industry Online Support under the following entry ID:

- 109480869 (https://support.industry.siemens.com/cs/de/en/view/109480869)
  SIMATIC NET: Industrial Wireless LAN RCoax

1.5 Terms used

The designation . . .	stands for . . .
IPv4 address	IPv4 address
IPv6 address	IPv6 address
IP address	IPv4/IPv6 address
IPv4 interface	Interface that supports IPv4.
IPv6 interface	Interface that supports IPv6. The interface can have more than one IPv6 address The IPv6 addresses have different ranges (scope), e.g. link local
IP interface	Interface that supports both IPv4 and IPv6. As default the IPv4 support is already activated. The IPv6 support needs to be activated extra.

1.6 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:

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

1.7 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).

1.8 Firmware

The firmware is available on the Internet pages of the Siemens Industry Online Support: (https://support.industry.siemens.com/cs/ww/en/ps/28575/dl)

Firmware

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

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.

1.9 Open source license conditions

Note

Open source software

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

The license terms and copyright information can be downloaded from the WBM or CLI as a zip file.

- WBM: System > Load&Save > HTTP / TFTP / SFTP > LicenseCondition
- CLI: `sftp save filetype LicenseConditions / tftp save filetype LicenseConditions`

1.10 Error/fault

If a fault develops, send the device to your SIEMENS representative for repair. Repairs on-site are not permitted.

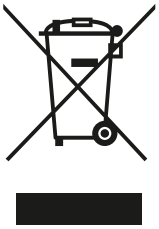
1.11 Decommissioning

Shut down the device properly to prevent unauthorized persons from accessing confidential data in the device memory.

To do this, restore the factory settings on the device.

Also restore the factory settings on the storage medium.

1.12 Recycling and disposal



The products are low in pollutants, can be recycled and meet the requirements of the WEEE directive 2012/19/EU for the disposal of electrical and electronic equipment.

Do not dispose of the products at public disposal sites.

For environmentally friendly recycling and the disposal of your old device contact a certified disposal company for electronic scrap or your Siemens contact (Product return (https://support.industry.siemens.com/cs/ww/en/view/109479891)).

Note the different national regulations.

1.13 Marken

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

SCALANCE, RCoax

Security recommendations

2

2.1 Security recommendations

To prevent unauthorized access to the device and/or network, observe the following security recommendations.

General

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products (https://www.siemens.com/industrialsecurity).
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- No product liability will be accepted for operation in a non-secure infrastructure.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- Separate connections correctly (WBM, SSH etc.).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.

WLAN

- We recommend that you ensure redundant coverage for WLAN clients.
- More information on data security and data encryption for SCALANCE W is available in SCALANCE W: Setup of a Wireless LAN in the Industrial Environment (https://support.industry.siemens.com/cs/ww/en/view/22681042)

Authentication

Note

Accessibility risk - Risk of data loss

Do not lose the passwords for the device. Access to the device can only be restored by resetting the device to factory settings which completely removes all configuration data.

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Define rules for the assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
  This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- Regularly change your passwords to increase security.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP or IPv4. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured or secure, higher layer protocols can be used, among other things.

Certificates and keys

- There is a preset SSL/TLS (RSA) certificate with 4096 bit key length in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate via the WBM ("System > Load and Save").
- Use certificates with a key length of 4096 bits.
- Use the certification authority including key revocation and management to sign the certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- Use password-protected certificates in the format "PKCS #12".
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Physical/remote access

- Operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Limit physical access to the device exclusively to trusted personnel.
  The memory card or the PLUG (C-PLUG, KEY-PLUG, CLP) contains sensitive data such as certificates and keys that can be read out and modified. An attacker with control of the device's removable media could extract critical information such as certificates, keys, etc. or reprogram the media.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.
- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device. For more information, see the configuration manuals, section "Brute Force Prevention (Page 462)".
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communication.
- When you establish a secure connection to a server (e.g. for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTP, HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it. For more information, refer to "Decommissioning (Page 23)".
- We recommend formatting a PLUG that is not being used.

Hardware / Software

- Use VLANs whenever possible as protection against denial-of-service (DoS) attacks and unauthorized access.
- Restrict access to the device by setting firewall rules or rules in an access control list (ACL).
- Selected services are enabled by default in the firmware. It is recommended to enable only the services that are absolutely necessary for your installation.
  For more information on available services, see "List of available services (Page 29)".
- To ensure you are using the most secure encryption methods available, use the latest web browser version compatible with the product. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).
- Ensure that the latest firmware version is installed, including all security-related patches. You can find the latest information on security patches for Siemens products at the Industrial Security (https://www.siemens.com/industrialsecurity) or ProductCERT Security Advisories (https://www.siemens.com/cert) website.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- Enable only those services that are used on the device, including physical ports. Free physical ports can potentially be used to gain access to the network behind the device.

- Use the authentication and encryption mechanisms of SNMPv3 if possible. Use strong passwords.
- Configuration files can be downloaded from the device. Ensure that configuration files are adequately protected.
  Configuration files can be password protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords".
- When using SNMP (Simple Network Management Protocol):
  - Configure SNMP to generate a notification when authentication errors occur.
    For more information, see WBM "System > SNMP > Notifications".
  - Ensure that the default community strings are changed to unique values.
  - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when absolutely necessary.
  - If possible, prevent write access.
- Use the security functions such as address translation with NAT (Network Address Translation) or NAPT (Network Address Port Translation) to protect receiving ports from access by third parties.
- Use WPA2/ WPA2-PSK / WPA3-SAE with AES to protect the WLAN. You can find additional information in the configuration manual Web Based Management "Security menu (Page 478)".
- Use PMF (Protected Management Frames) to cryptographically protect the management telegrams. You can find additional information in the configuration manual Web Based Management "Security menu".

Secure/ non-secure protocols

- Use secure protocols if access to the device is not prevented by physical protection measures.
- Disable or restrict the use of non-secure protocols. While some protocols are secure (e.g. HTTPS, SSH, 802.1X, etc.), others were not designed for the purpose of securing applications (e.g. SNMPv1/v2c, etc.).
  Therefore, take appropriate security measures against non-secure protocols to prevent unauthorized access to the device/network. Use non-secure protocols on the device using a secure connection (e.g. SINEMA RC).
- If non-secure protocols and services are required, ensure that the device is operated in a protected network area.

- Check whether use of the following protocols and services is necessary:
  - Non-authenticated and unencrypted ports
  - LLDP
  - Syslog
  - DHCP options 66/67
  - TFTP
  - Telnet
  - HTTP
  - SNMP v1/2c
  - SNTP
- The following protocols provide secure alternatives:
  - SNMPv1/v2c → SNMPv3
    Check whether use of SNMPv1/v2c is necessary. SNMPv1/v2c is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options.
    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
    Use SNMPv3 in conjunction with passwords.
  - HTTP → HTTPS
  - Telnet → SSH
  - TFTP → SFTP
  - Syslog Client → Syslog Client TLS
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- For the DCP function, enable the "Read Only" mode after commissioning.

2.2 Available services

List of available services

The following is a list of all available services and their ports through which the device can be accessed.

The table includes the following columns:

- **Service**
  The services that the device supports.
- **Protocol/port number**
  Port number assigned to the protocol.
- **Default status**
  The default status of the ports/service (e.g. open, closed, outgoing only).

- **Configurable port/service**
  Indicates whether the port number or the service can be configured via WBM / CLI.
- **Authentication**
  Specifies whether the communication partner is authenticated.
  If "optional", the authentication can be configured as required.
- **Encryption**
  Specifies whether the transfer is encrypted.
  If "optional", the encryption can be configured as required.

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [1]
			Port	Service		
DHCP Client IPv4	UDP/68	Outgoing only	--	✓	--	--
DHCP Client IPv6	UDP/546	Outgoing only	--	✓	--	--
DNS Client	TCP/53 UDP/53	Outgoing only	--	✓	--	--
HTTP	TCP/80	Open	✓	✓	✓	--
HTTPS	TCP/443	Open	✓	✓	✓	✓
NTP- Client	UDP/123	Outgoing only	✓	✓	--	--
Packet Capture	TCP/2002 TCP/2003 [2]	Closed	--	✓	--	--
PROFINET	UDP/34964 UDP/49154 UDP/49155	Open	--	✓	--	--
RADIUS	UDP/1812	Outgoing only	✓	✓	✓	--
SFTP Server	TCP/22	Closed	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	--	--
SMTP (secure)	TCP/465	Closed	✓	✓	Optional	✓
SNMPv1/v2c	UDP/161	Open	✓	✓	--	--
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outgoing only	--	✓	--	--
SNTP Client	UDP/123	Outgoing only	✓	✓	--	--
SSH	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Closed	✓	✓	--	--
Syslog Client TLS	TCP/6514	Closed	✓	✓	--	✓
Telnet	TCP/23	Closed	✓	✓	✓	--
TFTP Server	UDP/69	Closed	✓	✓	--	--
TCP Event	TCP/26864	Closed	✓	✓	✓	--

[1] You can find additional information on the encryption methods used in the WBM appendix "Ciphers used".

[2] The basic port of Packet Capture for the communication to Wireshark is TCP/2002. For each enabled interface, another port is enabled. Each additional port is an increment of TCP/2002, i.e. TCP/2003, TCP/2004, TCP/2005 etc.

The following is a list of all available Layer 2 services through which the device can be accessed.

The table includes the following columns:

- **Layer 2 service**
  The Layer 2 services that the device supports**.**
- **Default status**
  The default status of the service (open or closed).
- **Service configurable**
  Indicates whether the service can be configured via WBM / CLI.

Layer 2 service	**Default status**	**Service configurable**
DCP	Open	✓
LLDP	Open	✓
RSTP	Closed	✓
iPRP	Closed	✓
MSTP	Closed	✓
SIMATIC NET TIME	Closed	✓
802.1x	Closed	✓

Description 3

3.1 Planned operating environment

This section describes the recommended conditions for the most secure operation possible of the SCALANCE W700 components. These recommendations are not exhaustive and do not replace your own Threat and Risk Assessment with derivation of relevant measures.

- For secure operation, observe the security recommendations (Page 25).
- Make sure that only authorized persons have physical access to the component.
- Make sure that only authorized persons have permission to access the component via the network (user or access management).
- Introduce effective security incident handling processes.

Note

Interruption of the WLAN communication

The WLAN communication can be influenced by high frequency interference signals and can be totally interrupted.

Remember this and take suitable action.

3.2 Availability of the system functions

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

We reserve the right to make technical changes.

Menu item in the WBM	**System functions**		**SCALANCE WxM76x**		**SCALANCE WxB762**	
			Access point mode	**Clients Access points in client mode**	**Access point mode**	**Clients Access points in client mode**
Information	ARP table		✓		✓	
	Log table		✓		✓	
	Error		✓		✓	
	Redundancy protocol		✓		✓	
	Ethernet statistics		✓		✓	
	Unicast MAC table		✓		✓	
	LLDP neighbors		✓		✓	
	IPv4 Routing		✓		✓	
	IPv6 Routing		✓		✓	
	SNMPv3 Groups		✓		✓	
	Security		✓		✓	
	WLAN	Overview AP	✓	-	✓	-
		Client List	✓	-	✓	-
		Overlap AP	✓	-	✓	-
		Overview Client	-	✓	-	✓
		Available APs	-	✓	-	✓
		IP Mapping	-	✓	-	✓
	WLAN statistics		✓		✓	
	WLAN iFeatures		✓		-	✓[1)]

Menu item in the WBM	System functions		SCALANCE WxM76x		SCALANCE WxB762	
			Access point mode	Clients Access points in client mode	Access point mode	Clients Access points in client mode
System	DNS client		✓		✓	
	SMTP client		✓		✓	
	DHCP client		✓		✓	
	SNMP		✓		✓	
	Sleep Mode		✓		-	
	Manual time setting		✓		✓	
	DST		✓		✓	
	SNTP Client		✓		✓	
	NTP Client		✓		✓	
	NTP server		✓		✓	
	SIMATIC Time Client		✓		✓	
	Auto logout		✓		✓	
	Syslog client		✓		✓	
	Fault monitoring		✓		✓	
	PROFINET		✓		✓	
	PLUG		✓		-	
	Ping		✓		✓	
	DCP Discovery		✓		✓	
	Configuration backup		✓		✓	
	TCP Event		✓		✓ [1]	
Interfaces	Ethernet		✓		✓	
	WLAN	Basic	✓		✓	
		Extensions	✓		✓	
		Antennas&Power	✓		✓	
		Allowed Channels	✓		✓	
		Access point	✓	-	✓	-
		Client	-	✓	-	✓
	Packet Capture		✓	-	✓	-
Layer 2	Port Based VLAN		✓		✓	
	Dynamic MAC aging		✓		✓	
	Ring with RSTP		✓		✓	
	Spanning Tree		✓		✓	
	RSTP		✓		✓	
	MSTP		✓		✓	
	DCP forwarding		✓		✓	
	LLDP		✓		✓	
Layer 3	Agent IPv4/IPv6		✓		✓	
	NAT/NAPT		-	✓	-	✓
	Static routes		✓		✓	

Menu item in the WBM	System functions		SCALANCE WxM76x		SCALANCE WxB762	
			Access point mode	Clients Access points in client mode	Access point mode	Clients Access points in client mode
Security	Users		✓		✓	
	Passwords		✓		✓	
	RADIUS authentication		✓		✓	
	Brute Force Prevention		✓		✓	
	WLAN	Basic	✓	✓	✓	✓
		AP RADIUS Authenticator	✓	-	✓	-
		Client RADIUS Supplicant	-	✓	-	✓
		802.11r	✓	-	✓	-
iFeature	iPRP		✓[2)]	✓[2) 3)]	-	✓[1)]
	iPCF-2		✓[2)]	✓[2) 3)]	-	✓[1)]

1) Only for SCALANCE WUB762-1 iFeatures

2) CLP 2GB W700 AP iFeatures 6GK5907-8UA00-0AA0

3) CLP 2GB W700 Client iFeatures 6GK5907-4UA00-0AA0

3.3 Configuration limits

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

Depending on your device, some functions are not available.

Menu item in the WBM	Configurable function		Maximum number	
			SCALANCE WxM76x	SCALANCE WxB762
System	Syslog server		3	3
	DNS server	manual (IPv4)	3	3
		learned (IPv4)	2	2
		in total	7	7
	SMTP server		3	3
	SNMPv1/v2c and v3 Trap receiver		10	10
	SNMP queries		50	50
	SNTP server		2	2
	NTP server		1	1
Interfaces	Connected clients per WLAN interface		128	10
Layer 2	Virtual LANs (port-based, including VLAN 1)		24	5
	Multiple Spanning Tree instances		16	3
Layer 3	IP interface		2 1 subnet per IP interface	
	DHCP client		1	

Menu item in the WBM	Configurable function	Maximum number	
		SCALANCE WxM76x	SCALANCE WxB762
Security	IP addresses from RADIUS servers	• AAA:6 • WLAN: 2	• AAA:6 • WLAN: 2
	User roles	32 (incl. the predefined roles)	32 (incl. the predefined roles)
	User groups	32	32
	Users	30 (incl. the predefined users)	30 (incl. the predefined users)
	Firewall • NAPT rules (only with clients)	 32	 12

3.4 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.

SSH connection

Log in to a device with factory settings

1. Set up a SSH connection to the device and call the CLI.
   The login prompt is displayed. `login as:`
2. At "`Login:`", enter the preset factory user name "admin" 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 of the user "admin" preset at the factory: "admin" and confirm with "Enter".
   You can then rename the user preset in the factory "admin" once. Afterwards, renaming "admin" is no longer possible.
   The command prompt is: "`Default admin user to be changed (y/n)?`".

   Note

   The password for the "admin" user has been changed for devices with the US version. Specialist personnel for professional WLAN installations can obtain the password from Siemens support.

   Rename the user name "admin" preset in the factory:

   – Enter "`y`" and confirm with "Enter".

   – `Enter a new non-default admin username:`
   Enter a new user name and confirm with "Enter".
   The new user name has at least 8 and maximum 250 characters.

   – `Confirm new non-default admin username:`
   Enter the new user name again and confirm with "Enter".

   Do not rename the preset factory user name "admin":

   – Enter "`n`" and confirm with "Enter".

4. `Enter a new non-default admin password:`
   Enter a new password and confirm with "Enter".
   The new password must meet the password policy "High":
   - Password length: at least 8 characters, maximum 128 characters
   - At least 1 uppercase letter
   - At least 1 special character
   - At least 1 number
   - It must not contain the following characters: ; : ' ? ß § " ² ³ ° | € µ ä ö ü Ä Ö Ü
   - The characters for Space and Delete also cannot be contained.
5. `Confirm new non-default admin password:`
   Enter the new password again and confirm with "Enter".
   Once you have logged in successfully, the command prompt is: "`CLI#`".

Telnet connection

If you wish to access the CLI via a Telnet connection, select the option "Telnet Server" in "System > Configuration".

Use with Windows 10

If you want to access the Command Line Interface in Windows 10, make sure that the functions required for this are enabled in Windows 10.

Changing parameters

If you have enabled the "Automatic Save" mode and change a parameter, saving only starts after the timer has elapsed. How long saving takes depends on the device and the changes.

Switch off the device only when saving is complete. Because only when saving is complete is the parameter adopted in the current configuration.

Procedure

1. Enter the command `show device information`.
   - In Privileged EXEC mode: `show device information`
   - In every other mode: `do show device information`
2. Check the status with Config Change.
   - Saved: The change is saved in the current configuration.
   - Not Saved: Saving is still taking place.

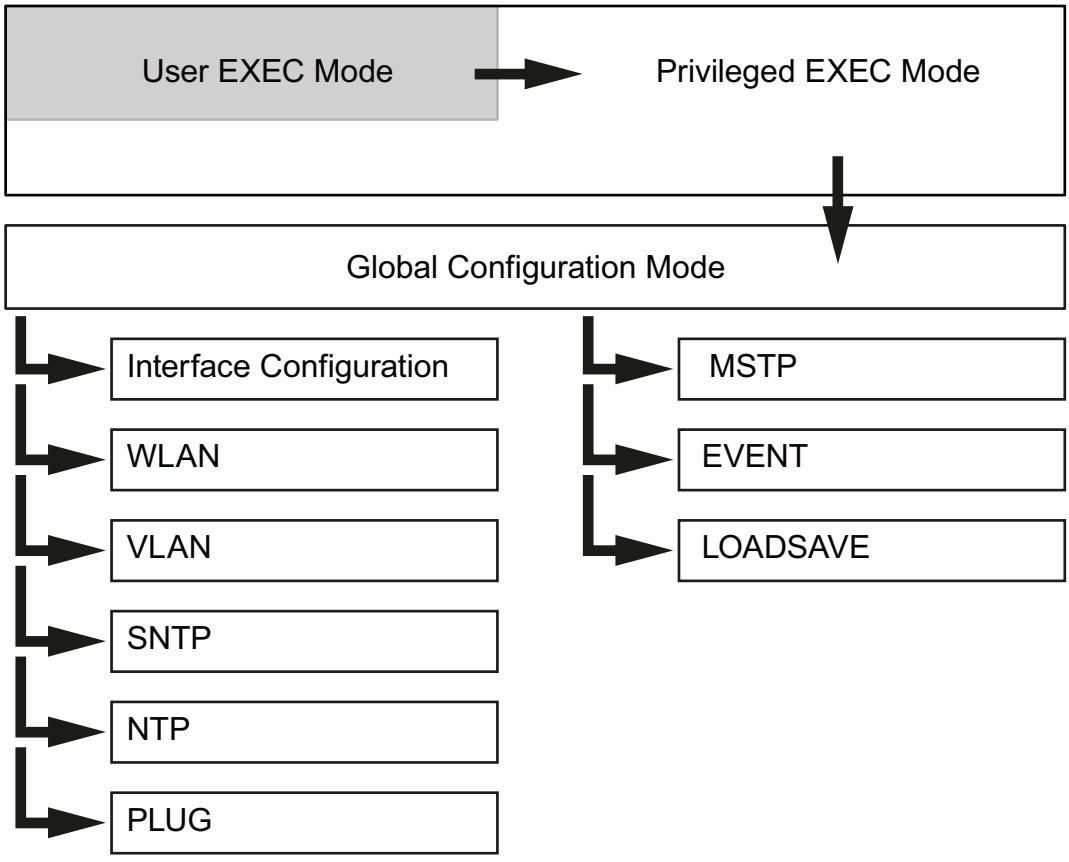
Service technician login

The device has a service technician login for servicing purposes. This is only available after activation by an administrator and may only be used by Siemens Support.

3.5 CLI modes

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 as "user" in a console window. In this mode, you can use show commands to display the current values of configuration parameters. You are logged out with the `exit` command.

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

In this mode, you can you display the configuration data and change it.

If you log in with the user "admin", you change directly to the Privileged EXEC mode.

To change from the User EXEC Mode to the Privileged EXEC mode, enter the `enable` command. When the command executes, you will be prompted to enter the password for the "admin" user. You are logged out with the `exit` command.

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. You exit this mode by entering `end` or `exit`.

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 LOADSAVE or interface configuration) or protocol-specific configuration modes (NTP, SNTP).

3.6 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.

3.7 Permitted characters

Passwords

Observe the following rules when creating or changing the passwords:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@, Space
Characters not allowed	:;"|€´?§³²°µ ä ö ü Ä Ö Ü
Length of the password	At least 8 characters and maximum 128 characters

Note

Passwords

To improve security, make sure that passwords are as long as possible.

Passwords must be at least 8 characters long and contain special characters, upper and lowercase characters as well as numbers.

User names

Observe the following rules when creating or changing the user names:

Allowed characters of a character set according to ANSI X 3.4-1986	0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@,
Characters not allowed	:;"|€´?§³²°µ ä ö ü Ä Ö Ü Space
Length of the user name	1 to 30 characters

Note

User names

To improve security, make sure that user names are as long as possible.

Role names

Observe the following rules when creating or changing the role names:

Allowed characters of a character set	0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@,: Space
Characters not allowed	;"|€´?§³²°µ ä ö ü Ä Ö Ü
Length of the role name	1 ... 64 characters

Group names

Observe the following rules when creating or changing the group names:

Allowed characters of a character set	0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@: Space
Characters not allowed	;",|€´?§³²°µ ä ö ü Ä Ö Ü
Length of the group name	1 ... 64 characters

User, role and group descriptions

Observe the following rules when creating or modifying descriptions:

Allowed characters of a character set		0123456789 A...Z a...z .-_#+'*~^!$%&/{([])}=\ `<>@, Space :;"| CLI only
Characters not allowed	WBM	:;"|€´?§³²°µ ä ö ü Ä Ö Ü
	CLI	€´?§³²°µ ä ö ü Ä Ö Ü
Length of description		1 ... 100 characters

Note

Question mark "?" in the user name/password

In the CLI the question mark "?" is a command. If the user name or the password contains a "?" for example for the login to the RADIUS server, it will be interpreted as a command. Configure this user name and password using the WBM.

3.8 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, enter a value.
[...]	optional parameter	Instead of the expression in parenthesis, you can enter a value.
(...)	Value or range of values	Instead of the expression in parenthesis, enter a value.
(... - ...)	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
< Parameter >	Instead of the expression in parentheses<>, enter a permitted value.
< < Unit (a - b) >	Instead of the expression in parentheses <>, enter a value from the range "a" to "b". The unit to be used is specified before the brackets () and is also replaced by the entry.

Character combinations	Meaning
[<Parameter 1 >< Parameter 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 < Unit (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 { 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 no or several of the values "A", "B" or "C".

3.9 Interface identifiers and addresses

3.9.1 Naming interfaces

Addressing interfaces

The device has several types of interface that are addressed in different ways:

Addressing physical interfaces

This notation also applies to other commands that address an 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. The interfaces permanently installed in the device are identified with module 0.

Examples:

Gigabit Ethernet: `interface gigabitethernet 0/1`

WLAN1: `interface wlan 0/1`

Addressing logical interfaces

This notation also applies to other commands that address a logical interface.

- VAP
  - 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. The interfaces permanently installed in the device are identified with module 0.

  Example:
  VAP 1.1: `interface vap1 0/1`
- VLAN
  - Enter the command "`interface`".
  - Enter the keyword for the VLAN interface.
  - After a space, enter the number of the VLAN interface you assigned when you created it.

  Example:
  VLAN 2: `interface vlan 2`

Available physical interfaces

Device	Interfaces	interface-type	interface-id	
WAM766-1	1 x gigabit Ethernet	`gi: gigabitethernet`	X = 1	`gi 0/X`
	2 x WLAN	`wlan`	X = 1 ... 2	`wlan 0/X`
WUM766-1	1 x gigabit Ethernet	`gi: gigabitethernet`	X = 1	`gi 0/X`
	1 x WLAN	`wlan`	X = 1	`wlan 0/X`
WAM763-1	4 x gigabit Ethernet	`gi: gigabitethernet`	X = 1 ... 4	`gi 0/X`
	2 x WLAN	`wlan`	X = 1 ... 2	`wlan 0/X`
WUM763-1	4 x gigabit Ethernet	`gi: gigabitethernet`	X = 1 ... 4	`gi 0/X`
	1 x WLAN	`wlan`	X = 1	`wlan 0/X`
WAB762-1	1 x gigabit Ethernet	`gi: gigabitethernet`	X = 1	`gi 0/X`
	1 x WLAN	`wlan`	X = 1	`wlan 0/X`
WUB762-1	1 x gigabit Ethernet	`gi: gigabitethernet`	X = 1	`gi 0/X`
	1 x WLAN	`wlan`	X = 1	`wlan 0/X`

Available logical interfaces

- VLAN
  The SCALANCE WxM76x devices support up to 24 virtual networks and SCALANCE WxB762 support up to 5 virtual networks.
  To be able to use a VLAN, create it with the `vlan` command.
- VAP
  The WLAN interface of a SCALANCE WAM76x supports up to 8 virtual access points (VAP), and that of a SCALANCE WxB762 only supports one VAP.

Device	interface-type	interface-id	
WAM766-1 WAM763-1	`vap`	X = 1 ... 2 Y = 1 ... 8	`vapX 0/Y`
WAB762-1	`vap`	X = 1 Y = 1	`vapX 0/Y`

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 identifier 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
`wlan 0/X`	`cli(config-if-wlan-0-X)#`
`vapX 0/Y`	`cli(config-if-vapX-0-Y)#`
`gi 0/X`	`cli(config-if-Gi0-X)#`
`vlan$`	`cli(config-if-vlan-$)#`

The placeholders `X, Y, $` stand for the numbering of the interface.

3.9.2 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
  An IPv4 address consists of 4 bytes. Each byte is represented in decimal, with a dot separating it from the previous one, refer to the section "Structure of an IPv4 address (Page 48)"

  Note

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

- IPv6 addresses
  IPv6 addresses consist of 8 fields each with four-character hexadecimal numbers (128 bits in total). The fields are separated by a colon, refer to the section "Structure of an IPv6 address (Page 54)".
- Network masks
  A network mask is a series of bits that describes the network part of an IPv4 address.
  The notation is normally decimal in keeping with the IPv4 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.

3.9.3 Structure of an IPv4 address

The IPv4 address consists of 4 decimal numbers separated by a dot. Each decimal number can have a value from 0 to 255.

Example: 192.168.16.2

The IPv4 address is composed of:

- Address of the (sub)network
- The address of the node (generally also called end node, host or network node)

Subnet mask

The subnet mask consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 255.255.0.0

The binary representation of the 4 subnet mask decimal numbers must contain a series of consecutive 1s from the left and a series of consecutive 0s from the right.

The "1" values determine the network address within the IPv4 address. The "0" values determine the device address within the IPv4 address.

Example:

Correct values

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

Incorrect value:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

In the example for the IP address mentioned above, the subnet mask shown here has the following meaning:

The first 2 bytes of the IP address determine the subnet - i.e. 192.168. The last two bytes address the device, i.e. 16.2.

The following applies in general:

- The network address results from the AND combination of IPv4 address and subnet mask.
- The device address results from the AND-NOT combination of IPv4 address and subnet mask.

Classless Inter-Domain Routing (CIDR)

CIDR is a method that groups several IPv4 addresses into an address range by representing an IPv4 address combined with its subnet mask. To do this, a suffix is appended to the IPv4 address that specifies the number of bits of the network mask set to 1. Using the CIDR notation, routing tables can be reduced in size and the available address ranges put to better use.

Example:

IPv4 address 192.168.0.0 with subnet mask 255.255.255.0

The network part of the address covers 3 x 8 bits in binary representation; in other words 24 bits.

This results in the CIDR notation 192.168.0.0/24.
The host part covers 1 x 8 bits in binary notation. This results in an address range of 2 to the power 8, in other words 256 possible addresses.

Masking additional subnets

Using the subnet mask, you can further structure a subnet assigned to one of the address classes A, B or C and form "private" subnets by setting further lower-level digits of the subnet mask to "1". For each bit set to "1", the number of "private" networks doubles and the number of nodes contained in them is halved. Externally, the network still looks like a single network.

Example:

You change the default subnet mask for a subnet of address class B (e.g. IP address 129.80.xxx.xxx) as follows:

Masks	Decimal	Binary
Default subnet mask	255.255.0.0	11111111.11111111.00000000 .00000000
Subnet mask	255.255.128.0	11111111.11111111.10000000 .00000000

Result:

All devices with addresses from 129.80.1.xxx to 129.80.127.xxx are on one IP subnet, all devices with addresses from 129.80.128.xxx to 129.80.255.xxx are on another IP subnet.

Network gateway (router)

The task of the network gateways (routers) is to connect the IP subnets. If an IP datagram is to be sent to another network, it must first be sent to a router. For make this possible, you need to enter the router address for each member of the IP subnet.

The IP address of a device in the subnet and the IP address of the network gateway (router) may only be different at the points where the subnet mask is set to "0".

3.9.4 IPv4 / IPv6

What are the essential differences?

	IPv4	IPv6
IP configuration	• DHCP server • Manual	• Stateless Address Autoconfiguration (SLAAC): Stateless autoconfiguration using NDP (Neighbor Discovery Protocol) – Creates a link local address for every interface that does not require a router on the link. – Checks the uniqueness of the address on the link that requires no router on the link. – Specifies whether the global addresses are obtained via a stateless mechanism, a stateful mechanism or via both mechanisms. (Requires a router on the link.) • Manual • DHCPv6 (stateful)
Available IP addresses	32-bit: 4, 29 * 10^9 addresses	128-bit: 3, 4 * 10^{38} addresses
Address format	Decimal: 192.168.1.1 with port: 192.168.1.1:20	Hexadecimal: 2a00:ad80::0123 with port: [2a00:ad80::0123]:20
Loopback	127.0.0.1	::1

	IPv4	IPv6
IP addresses of the interface	5 IP addresses	Multiple IP addresses • LLA: A link local address (formed automatically) fe80::/128 per interface • ULA: Several unique local unicast addresses per interface • GUA: Several global unicast addresses per interface
Header	• Checksum • Variable length • Fragmentation in the header • No security	• Checking at a higher layer • Fixed size • Fragmentation in the extension header
Fragmentation	Host and router	Only endpoint of the communication
Quality of service	Type of Service (ToS) for prioritization	The prioritization is specified in the header field "Traffic Class".
Types of frame	Broadcast, multicast, unicast	Multicast, unicast, anycast
Identification of DHCP clients/ server	Client ID: • MAC address • DHCP client ID • System name • PROFINET station name • IAID and DUID	DUID + IAID(s) = exactly one interface of the host DUID = DHCP unique identifier Unique identifier of server and clients IAID = Identity Association Identifier At least one per interface is generated by the client and remains unchanged when the DHCP client restarts Three methods of obtaining the DUID • DUID-LLT • DUID-EN • DUID-LL

	IPv4	IPv6
DHCP	via UDP with broadcast	via UDP with unicast RFC 3315, RFC 3363 **Stateful DHCPv6** Stateful configuration in which the IPv6 address and the configuration settings are transferred. Four DHVPv6 messages are exchanged between client and server: 1. SOLICIT: Sent by the DHCPv6 client to localize DHCPv6 servers. 2. ADVERTISE The available DHCPv6 servers reply to this. 3. REQUEST The DHCPv6 client requests an IPv6 address and the configuration settings from the DHCPv6 server. 4. REPLY The DHCPv6 server sends the IPv6 address and the configuration settings. If the client and server support the function "Rapid commit" the procedure is shortened to two DHCPv6 messages SOLICIT and REPLY . **Stateless DHCPv6** In stateless DHCPv6, only the configuration settings are transferred. **Prefix delegation** The DHCPv6 server delegates the distribution of IPv6 prefixes to the DHCPv6 client. The DHCPv6 client is also known as PD router.
Resolution of IP addresses in hardware addresses	ARP (Address Resolution Protocol)	NDP (Neighbor Discovery Protocol)

3.9.5 IPv6 terms

Network node

A network node is a device that is connected to one or more networks via one or more interfaces.

Router

A network node that forwards IPv6 packets.

Host

A network node that represents an end point for IPv6 communication relations.

Link

A link is, according to IPv6 terminology, a direct layer 3 connection within an IPv6 network.

Neighbor

Two network nodes are called neighbors when they are located on the same link.

IPv6 interface

Physical or logical interface on which IPv6 is activated.

Path MTU

Maximum permitted packet size on a path from a sender to a recipient.

Path MTU discovery

Mechanism for determining the maximum permitted packet size along the entire path from a sender to a recipient.

LLA

Link local address FE80::/10

As soon as IPv6 is activated on the interface, a link local address is formed automatically. Can only be reached by nodes located on the same link.

ULA

Unique Local Address

Defined in RFC 4193. The IPv6 interface can be reached via this address in the LAN.

GUA

Global unicast address

The IPv6 interface can be reached through this address, for example, via the Internet.

Interface ID

The interface ID is formed with the EUI-64 method or manually.

EUI-64

Extended Unique Identifier (RFC 4291); process for forming the interface ID. In Ethernet, the interface ID is formed from the MAC address of the interface. Divides the MAC address into the manufacturer-specific part (OUI) and the network-specific part (NIC) and inserts FFFE between the two parts.

Example:

MAC address = AA:BB:CC:DD:EE:FF

OUI = AA:BB:CC

NIC = DD:EE:FF

EUI-64 = OUI + **FFFE** + NIC = AA:BB:CC:**FF:FE**:DD:EE:FF

Scope

Defines the range of the IPv6 address.

3.9.6 Structure of an IPv6 address

IPv6 address format - notation

IPv6 addresses consist of 8 fields each with four-character hexadecimal numbers (128 bits in total). The fields are separated by a colon.

Example:

fd00:0000:0000:ffff:02d1:7d01:0000:8f21

Rules / simplifications:

- If one or more fields have the value 0, a shortened notation is possible.
  The address fd00:**0000:0000**:ffff:02d1:7d01:0000:8f21 can also be shortened and written as follows:
  fd00**::**ffff:02d1:7d01:0000:8f21
  To ensure uniqueness, this shortened form can only be used once within the entire address.
- Leading zeros within a field can be omitted.
  The address fd00:0000:0000:ffff:**02d1**:7d01:0000:8f21 can also be shortened and written as follows:
  fd00**::**ffff:**2d1**:7d01:0000:8f21
- Decimal notation with periods
  The last 2 fields or 4 bytes can be written in the normal decimal notation with periods.
  Example: The IPv6 address fd00::ffff.125.1.0.1 is equivalent to fd00::ffff:7d01:1

Structure of the IPv6 address

The IPv6 protocol distinguishes between three types of address: Unicast, Anycast and Multicast. The following section describes the structure of the global unicast addresses.

IPv6 prefix		**Suffix**
Global prefix: n bits	Subnet ID m bits	Interface ID 128 - n - m bits
Assigned address range	Description of the location, also subnet prefix or subnet	Unique assignment of the host in the network. The ID is generated from the MAC address.

The prefix for the link local address is always fe80:0000:0000:0000. The prefix is shortened and noted as follows: fe80::

IPv6 prefix

Specified in: RFC 4291

The IPv6 prefix represents the subnet identifier.

Prefixes and IPv6 addresses are specified in the same way as with the CIDR notation (Classless Inter-Domain Routing) for IPv4.

Design

IPv6 address / prefix length

Example

IPv6 address: 2001:0db8:1234::1111/48

Prefix: 2001:0db8:1234::/48

Interface ID: ::1111

Entry and appearance

The entry of IPv6 addresses is possible in the notations described above. IPv6 addresses are always shown in the hexadecimal notation.

General CLI commands

4

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

4.1 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.

4.2 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.

4.3 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#
```

4.4 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.

4.5 grep

Description

You use this command to search for regular expressions in the output of a CLI command. "grep" stands for "get regular expression print".

Syntax

Call up the command with the following parameters:

```
<CLI-Command> | grep [-v] <search string>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`CLI-Command`	Any CLI command	-
`-v`	Inverts the search. Lists the rows that do not match the search term.	-
`search string`	Looks for this search term in the output of the CLI command.	Enter the standard search term with quotation marks. Example: `show running-config interface vlan 1 | grep "ip address"`

Result

The rows that match the search term or that do not match the search term are listed.

4.6 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`)

4.6.1 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.

4.6.2 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.

4.6.3 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.

4.6.4 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`.

4.6.5 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.

See also

show history (Page 63)

4.6.6 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
```

4.6.7 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.

4.6.7.1 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.

4.6.8 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 5

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

5.1 System

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

5.1.1 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 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.

5.1.1.2 show device information

Description

This command shows the general device 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 device information
```

Result

The following device information is shown:

- MAC address of the device
- Serial Number
- System up time
- System name
- System contact
- System location
- Device Type
- Diagnostics Mode
- Restart counter
- Config Save mode
- Config Change: This indicates whether or not the current configuration has been saved.
- Login Authentication mode: This indicates whether the authentication is made locally or on the RADIUS server.
- Radius Authorization mode

5.1.1.3 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.

5.1.1.4 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
| status }] | {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	
`description`	Shows the description of the interface	-
`status`	Shows the status 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 "Interface identifiers and addresses (Page 45)".

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.

5.1.1.5 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 "Interface identifiers and addresses (Page 45)".

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.

5.1.1.6 show interface mtu

Description

With this command, you show the setting for the Maximum Transmission Unit (MTU) of the interfaces 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 up the command with the following parameters:

```
show interface mtu [{ 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 identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

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

Result

The settings are displayed.

5.1.1.7 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 "Interface identifiers and addresses (Page 45)".

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.

5.1.1.8 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.

5.1.1.9 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 "Interface identifiers and addresses (Page 45)".

Result

The information is displayed.

5.1.1.10 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.

5.1.1.11 show traceroute

Description

This command shows the route via which the packet comes to the requested IP 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 up the command with the following parameters:

```
show traceroute {ip | ipv6 }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ip`	The destination is an IPv4 address	-
`ipv6`	The destination is an IPv6 address	-

Result

The route is displayed.

Further notes

You enable the following of the route with the `traceroute` command.

5.1.1.12 show versions

Description

This command shows the versions of the hardware and software 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 versions
```

Result

The following settings are displayed:

- Basic device
- Name

- Revision
- Order ID
- Firmware
- Bootloader
- Description
- Version
- Date

5.1.2 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 "Interface identifiers and addresses (Page 45)".

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.

5.1.3 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.

5.1.4 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.

5.1.5 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>
```

5.1.6 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#
```

5.1.7 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.

5.1.8 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 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:

```
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 called node	Enter a valid IPv4 address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name) of the called node	Maximum of 100 characters
`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	-
`packet_count`	Number of packets	1 ... 10 Default: 3

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

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.

5.1.9 ping ipv6

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

- IPv6 is enabled.
- 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:

```
ping ipv6 { <prefix%interface> | fqdn-name <FQDN> } [count
<packet_count (1-10)>] [size <byte (0-2080)>] [anycast] [source
{vlan <vlan-id (1-4094)> | <source_prefix>}] [timeout <seconds
(1-100)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
prefix	IPv6 address of the destination	Enter a valid IPv6 address.
%interface	optional parameter Only necessary when the IPv6 address of the destination is a link-local address.	Specify the interface via which the packet will be sent.
fqdn-name	Keyword for a domain name	-

Parameter	Description	Range of values / note
`FQDN`	Domain name (Fully Qualified Domain Name) of the called node	Maximum of 100 characters
`count`	Keyword for the number of packets to be requested	-
`packet_count`	Number of packets	1 ... 10 Default: 3
`size`	Keyword for the size of the packets to be transferred	-
`byte`	Packet size in bytes	0 ... 2080 Default: 100
`anycast`	Addressing mode anycast	-
`source`	Keyword for the sender interface • VLAN • source_prefix	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`source_prefix`	Prefix of the sender	-
`timeout`	Keyword for the response wait time. If this time expires, the request is reported as "timed out".	-
`seconds`	Time until timeout	1 ... 100 s Default: 1

Result

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

5.1.10 traceroute

Description

With this command you enable the following of the route via which the packet comes to the requested IP address.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
traceroute {ip <ip-address> | ipv6 <ip6-address>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ip	Keyword for an IPv4 address	-
ip-address	IPv4 address of the destination	Enter a valid IPv4 address.
ipv6	Keyword for an IPv6 address	-
ip6-address	IPv6 address of the destination	Enter a valid IPv6 address.

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The tracing of the route is activated.

Further notes

You display the route with the `show traceroute` command.

5.1.11 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.

5.1.11.1 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.

5.1.11.2 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.

5.1.11.3 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.

5.1.11.4 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)> | <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	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 "Interface identifiers and addresses (Page 45)".

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	Range of values / note
`wlan`	`cli(config-if-wlan-0-$)#`	
`vap`	`cli(config-if-vap$-0-$)#`	The interface is only available in access point mode
`vlan`	`cli(config-if-vlan-$)#`	
`gigabit-ethernet`	`cli(config-if-Gi-0-$)#`	

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

For the value ranges for the VLAN logical interface, refer to the upper table. You can only call up interfaces that you created with the `vlan` 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.

5.1.11.5 no interface

Description

With this command, you delete a logical interface.

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 { vlan <vlan-id (1-4094)> | nve <integer (1-65535)> }
```

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

Parameter	Description	Range of values / note
`nve`	NVE interface (Network Virtual Endpoint Interface)	-
`integer`	Number of the NVE interface	1-65535

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.

5.1.11.6 pre-login message add

Description

With this command, you can enter an additional text that is displayed before login.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
pre-login message add <pre-login-message-content>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note

`pre-login-message-content`	Login text	Enter the required text in quotation marks.
		Multi-line texts are entered in one line.
		Example:
		`pre-login message add "Line 1"`
		`pre-login message add "Line 2"`
		`pre-login message add "Line 3"`
		The use of the following special characters is not supported:
		• Backslash (\)
		• Question mark (?)
		• Tabs: Use spaces instead of tabs.

Result

The text has been entered and is displayed before login.

If a login text already exists, the text is not overwritten; rather, the lines are added. Remove the existing login text with the `no pre-login message` command and enter the new text.

Note

Use in scripts

Always start the script with the `no pre-login-message` command to remove any login texts that may be present.

Additional notes

You remove the login text with the `no pre-login message` command.

5.1.11.7 no pre-login message

Description

With this command, you remove the login text.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no pre-login message
```

Result

The login text has been removed.

Additional notes

You configure the login text with the `pre-login message add` command.

5.1.11.8 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.	PROFINET is switched on. w

Result

PROFINET is enabled or disabled after the next restart.

Further notes

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

5.1.11.9 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.

5.1.11.10 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.

5.1.11.11 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.

5.1.11.12 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.

5.1.12 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.

5.1.12.1 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.

5.1.12.2 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.

5.1.12.3 lldp

Description

With this command, you enable the sending and 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:

```
lldp{transmit|receive}
```

The parameters have the following meaning:

Parameters	Description
`transmit`	the sending of LLDP packets is enabled
`receive`	the receipt of LLDP packets is enabled

At system start or when using the `restart` command with the option `memory`or `factory`, the following defaults apply:

- Sending and receipt of LLDP packets are 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

The setting is configured.

Further notes

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

You display the status of LLDP with the `show lldp status` command.

5.1.12.4 no lldp

Description

With this command, you disable the sending and 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:

Parameters	Description
`transmit`	the sending of LLDP packets is enabled
`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

The setting is configured.

Further notes

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

You display the status of LLDP with the `show lldp status` command.

5.1.12.5 shutdown complete

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 the command without parameters:

```
shutdown complete
```

Result

The Interface is shut down.

Note

If you use this command in the Interface Configuration mode for a VLAN (input prompt `CLI(config-if-vlan-$)#`, management access to the device is no longer possible. This relates to configuration using CLI, WBM and SNMP. Access is only possible again after resetting the device to the factory settings with the Reset button.

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.

5.1.12.6 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 shut down the interface with the `shutdown complete` command.

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

Note

Dual operation in access point mode 2.4 GHz + 5 GHz

If you want to activate two WLAN interfaces in parallel (dual AP mode), note the following procedure:

1. Insert the SCALANCE CLP 2GB W700 iFeatures into the device.
2. Specify the antenna type "2,4 GHz + 5 GHz" for all four antennas with the command `wlan antenna type`, see `wlan antenna type` (Page 98).
3. Switch on the WLAN interface with the command `no shutdown`, see `no shutdown` (Page 235).

5.2 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.

5.2.1 File list

Overview of the file types

For a clearer overview, the file list is divided into different areas.

Area	Type	Description	Down-load	Save	Delete[1)]
Update	Firmware	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be down-loaded to the device.	X	X	--

Area	Type	Description	Down-load	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 file "Users". The file can be supplied with a password before download. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords". If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.	X	X	--
	ConfigPack	Detailed configuration information. for example, start configuration, users, certificates, favorites, firmware of the device (if saved as well). The file can be supplied with a password before download. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords". For more detailed information on creating and using the ConfigPack incl. firmware, refer to the section "Maintenance". If the file is password-protected, you cannot load the file via DHCP with options 66 and 67.	X	X	--
	ConfigPack-Backup	This ZIP file stores all the configuration backups you have created.	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	--
	RunningSINEMAConfig	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	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.	X	--	--

Area	Type	Description	Down-load	Save	Delete[1)]
		See also "RunningSINEMAConfig"			
	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	Type	Description	Down-load	Save	Delete[1)]
Certificates & keys	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". After the upload, the existing HTTPS certificate is overwritten. It is recommended that you use password-protected certificates in the PKCS#12 format. The following certificates are supported: • ECDSA certificates that were generated with secp521r1 (NIST P-521) • RSA certificates with a maximum key length of 4096 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
	SSHPrivate-KeyRSA	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
	WLANCert (only in client mode)	User certificate. You can specify a password for the user certificate on the WBM page "Load&Save > Password". Maximum key length: 8192 bits	X	X	X

Area	Type	Description	Down-load	Save	Delete[1)]
	WLANServer-Cert (only in client mode)	Server certificate. You can specify a password for the server certificate on the WBM page "Load&Save > Password". Maximum key length: 8192 bits	X	X	X
Services & 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
	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	--
	WLANAuthlog	File with entries from the WLAN Authentication Log (information on successful or failed authentication attempts)	--	X	--
	WLANSigRec (only in client mode)	The ZIP file contains the following: • csv file with the measured values of the signal recorder • pdf file with the measured values and an additional graphic representation of the measured values. You will find information about the measured values and their graphic representation in the section "Signal recorder".	--	X	X
Information	CountryList	The ZIP file contains the country list as a csv file.	--	X	--
	GSDML	Information on the device properties (PROFINET)	--	X	--
	MIB	Private MSPS MIB file "Scalance_w_msps.mib"	--	X	--
License	LicenseConditions	The ZIP file contains the licensing conditions and copyright information	--	X	--

[1)] Deletion is only possible via HTTP/HTTPS.

Using configuration files

Note

Configuration files and Trial mode/Automatic Save

In "Automatic Save" mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.
In "Trial" mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI) and upload your own CLI scripts (Script).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

CLI commands for saving and loading files cannot be executed with the CLI script file (Script).

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
  You assign the password in the WBM under "System > Load&Save > Passwords".

You can use the file types as follows:

- For offline diagnostics
  You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
  No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

5.2.2 The "show" commands

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

5.2.2.1 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.

5.2.2.2 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.

5.2.2.3 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.

5.2.3 save filetype

Description

With this command, you save files on a TFTP server or an SFTP 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> | ipv6 <ip6_addr>} [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	Maximum of 100 characters
`tftp`	TFTP server	-
`sftp`	SFTP server	-
`ipv4`	Keyword for an IPv4 address	
`ucast_addr`	IPv4 unicast address of the TFTP server	Enter a valid unicast IPv4 address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name) of the TFTP server	Maximum of 100 characters
`ipv6`	Keyword for an IPv6 address	-
`ip6_addr`	IPv6 address of the TFTP server	Enter a valid unicast IPv6 address.
`port`	Keyword for the port of the server via which the TFTP connection runs	-
`tcp port`	Number of the port	1 ... 65535

Parameter	Description	Range of values / note
`file`	Keyword for a file name to be assigned	-
`filename`	Name of the file	Maximum of 100 characters
`user`	User name for access to the SFTP server	Enter a valid user name. The prerequisite is that a user with the corresponding rights has been created on the SFTP server.
`username`	Keyword for password	-
`password`	User password	Enter the password for the user.
`password`	Valid password	

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The file is saved on the TFTP server or the SFTP server.

5.2.4 load

Description

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

Requirement

You are in 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:

```
load {tftp | sftp} {ipv4 <ucast_addr> | fqdn-name <FQDN> | ipv6
<ip6_addr>} [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 an SFTP server	-
`ipv4`	Keyword for an IPv4 address	
`ucast_addr`	IPv4 unicast address of the TFTP server	Enter a valid unicast IPv4 address.
`fqdn-name`	Keyword for a domain name	-

Parameter	Description	Range of values/note
FQDN	Domain name (Fully Qualified Domain Name) of the TFTP server	Maximum of 100 characters
ipv6	Keyword for an IPv6 address	-
ip6_addr	IPv6 address of the TFTP server	Enter a valid unicast IPv6 address.
port	Keyword for the port of the server via which the TFTP connection runs	-
tcp port	Number of the port	1 ... 65535
file	Keyword for a file name to be assigned	-
filename	Name of the file	Maximum of 100 characters
filetype	Keyword for the file type to be loaded	-
filetype	Name of the file type	Maximum of 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 "Interface identifiers and addresses (Page 45)".

For information on the file types, refer to this list (Page 100).

Result

The file is loaded into the device from the TFTP or SFTP server.

Additional notes

The `show loadsave tftp` command shows the current configuration of the TFTP server for Load&Save.

The `show loadsave sftp` command shows the current configuration of the SFTP server for Load&Save.

5.2.5 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.

5.2.5.1 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.

5.2.6 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.

5.2.6.1 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.

5.2.6.2 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.

5.2.6.3 tftp load

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.

5.2.6.4 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.

5.2.6.5 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> | ipv6
<ip6_addr>} [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.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters
`ipv6`	Keyword for an IPv6 address	-
`ip6_addr`	Value for an IPv6 unicast address	Enter a valid IPv6 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 "Interface identifiers and addresses (Page 45)".

Result

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

Additional notes

The `show loadsave tftp` command shows the current configuration of the TFTP server for Load&Save.

5.2.6.6 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.

5.2.6.7 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.

5.2.6.8 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.

5.2.6.9 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 up the command with the following parameters:

```
sftp server {ipv4 <ucast-addr> | fqdn-name <FQDN> | ipv6
<ip6_addr>} [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	-
`ipv4-address`	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
`ipv6`	Keyword for an IPv6 address	-
`ip6_addr`	Value for an IPv6 unicast address	Enter a valid IPv6 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 assumes that a user with the corresponding rights has been created on the SFTP server. Refer to the information in the section "CLI command prompt (Page 41)".
`password`	Keyword for a password	-
`password`	Password of the user	Enter the password for the user. Refer to the information in the section "CLI command prompt (Page 41)".

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

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

Further notes

The `show loadsave sftp` command shows the current configuration of the SFTP server for Load&Save.

5.2.6.10 password

Description

With this command, you activate and configure the password for encrypted certificates.

User, server or HTTPS certificates can exist as PKCS#12 certificates (.p12 and .pfx) and PEM certificates (.pem).

Note

User and server certificate in one file

If the user and the server certificate are located in the same file, load this file on the device as the user certificate and as the server certificate.

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	Range of values / note
`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
`pw`	Keyword for the password	-
`password`	Password	Enter the password for the certificate with only the following readable ASCII characters: 0x20 - 0x7e.

Result

The password for the certificate is configured and activated.

Further notes

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

5.2.6.11 no password

Description

With this command, you disable the password for encrypted certificates.

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	Range of values / note
`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 is disabled.

Further notes

You enable the password for certificates with the `password` command.

5.2.6.12 firmware-in-configpack

Description

When you save the ConfigPack file, the file contains the start configuration, the users and the certificates. The firmware file is not included. With this command you include the firmware file in the ConfigPack file. When you save the ConfigPack file now, the firmware is included.

After a restart the setting is disabled.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

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

Syntax

Call the command without parameter assignment:

```
firmeware-in-configpack
```

Result

The setting is enabled.

Further notes

You disable the setting with the `no firmeware-in-configpack` command.

5.2.6.13 no firmeware-in-configpack

Description

With this command you take firmware file out of the ConfigPack file.

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

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

Syntax

Call the command without parameter assignment:

```
no firmeware-in-configpack
```

Result

The function is disabled.

Further notes

You enable the function with the `firmeware-in-configpack` command.

5.3 Reset and Defaults

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

5.3.1 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 with the exception of the protected presets. The protected presets include the following parameters:
  - IP addresses
  - Subnet mask
  - IP address of the default gateway.
  - DHCP client ID
  - DHCP
  - System name
  - System location
  - System contact
  - User names and passwords
  - Mode of the device
  - DHCPv6 Rapid Commit
  - PROFINET Name of Station
- Device restart with the factory configuration settings.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
restart [{memory|factory}]
```

The parameters have the following meaning:

- if no parameters are specified: restarts the system with the current configuration

Parameter	Description
`memory`	Restores the factory settings of the device and restarts the device. The protected presets are excluded from the reset.
`factory`	Restores the factory settings of the device and restarts the device. The protected defaults are also reset. The default factory settings depend on the device.

NOTICE
Loss of IP address / passwords with `factory`
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 SINEC PNI or via DHCP.
With the appropriate connection, a previously correctly configured device can cause circulating frames and therefore the failure of the data traffic.

Result

The device is restarted with the selected settings.

5.3.2 Commands in global configuration mode

5.3.2.1 schedule restart-configbackup

Description

With this command you specify which configuration backup is used. Before the scheduled restart, the device applies the configurations of the selected backup and continues working with them after the restart.

Requirement

- The configuration backup file has been created.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call up the command with the following parameters:

```
schedule restart-configbackup <configbackup-name>
```

Parameter	Description	Range of values / note
`configbackup-name`	Name of the backup file	Enter a valid name.

Result

The device applies the configurations of the selected backup and continues working with them after the restart.

All configurations made up to this point that have not been saved in a backup are lost.

Additional notes

You create a configuration backup file with the configbackup create command.

You remove the backup file with the `cancel restart-time` command.

5.3.2.2 no schedule restart-configbackup

Description

With this command, the setting is disabled. This means no backup file is selected, and the device uses the current configuration after the restart.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command with the following parameters:

```
no schedule restart-configbackup <configbackup-name>
```

Parameter	Description	Range of values/note
`configbackup-name`	Name of the backup file	Enter a valid name.

Result

The device uses the current configuration after the restart.

Additional notes

You enable the function with the `schedule restart-configbackup` command.

5.3.2.3 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.

5.3.2.4 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.

5.3.2.5 sleep

Description

With this command, you specify the idle state for the system and enable the sleep mode.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
sleep <minutes (1-44639)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`minutes`	Value for the time in minutes	1 ... 44639 (1 minute to 31 days) Default value 0: Power saving mode off

Result

The device applies the setting for the duration and immediately switches to sleep mode. Once the time has elapsed, the device returns to the active state. The digital output is deactivated after the restart.

Note

Retaining the state of the digital output

The device can note the current state of the digital output and restore it after a restart. You can find additional information in the section `digital output retain` (Page 132).

5.4 Configuration Save & Restore

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

5.4.1 The "show" commands

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

5.4.1.1 show running-config

Description

This command shows configuration settings 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 running-config [{syslog | dhcp | stp | vlan [ <vlan-id
(1-4094)>]
 | interface { <interface-type> <interface-list> | vlan <vlan-
id(1-4094)> }
 | ssh | ssl| acl | ip | snmp | sntp| http | auto-logout
 | time | ntp | auto-save | wlan | events | nat | radius | umac}]
[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	-
`stp`	shows the configuration settings of the Spanning Tree Protocol	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface`	Shows that an interface description follows	-
`interface-type`	Type or speed of the interface	Specify 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 list	-
`ip`	Shows the configuration settings of the Internet Protocol	-
`snmp`	Shows the configuration settings of the Simple Network Management Protocol	-
`sntp`	Shows the configuration settings of the Simple Network Time Protocol	-
`http`	Shows the configuration settings of the Hypertext Transfer Protocol	-
`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	-
`wlan`	Shows the configuration settings of the WLAN	-
`events`	Shows the configuration settings of the events	-
`nat`	Shows the configuration settings of the Network Address Translation	-
`radius`	Shows the configuration settings of the Remote Authentication Dial-In User service	-
`umac`	Shows the configuration settings of the user configuration	-
`all`	Shows all configuration settings	-

For information on identifiers of interfaces and addresses, refer to the section "Interface identifiers and addresses (Page 45)".

If you call up the command without parameters, only the active operational settings of all modules and all interfaces that do not match the preset values are displayed.

Result

The selected configuration settings of the device are displayed.

The password cannot be read as plain language, instead [PASSWORD] is displayed.

5.4.2 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.

5.4.3 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.

5.4.3.1 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.

5.4.3.2 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.

5.4.3.3 digital output retain

Description

With this command, you enable saving of the current state of the digital output in the configuration. The last configured state of the digital output is restored after a restart.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
digital output retain
```

The default value of the function is "disabled".

Result

The 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 digital output retain` command.

You display the status of this function and other information with the `show running-config` command.

5.4.3.4 no digital output retain

Description

With this command, you disable saving of the current state of the digital output in the configuration.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no digital output retain
```

Result

The last configured state of the digital output is lost after a restart.

Additional notes

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

You enable the function with the `digital output retain` command.

You display the status of this function and other information with the `show running-config` command.

5.5 Configuration backup

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

5.5.1 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.

5.5.1.1 show configbackup

Description

With this command, you display the stored backups. The first row "Available memory" shows how much memory is available for backups on the device. When you create a backup, the available memory space is reduced accordingly.

The other rows show each backup and its size.

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 configbackup
```

Result

The stored backups and the memory space are displayed.

Further notes

You create a backup of the current configuration with the `configbackup create` command.

You delete a backup with the `configbackup delete` command.

You load a backup with the `configbackup restore` command.

You save configuration backups on your client PC with the command `tftp save`.

You load configuration backups from your client PC with the command `tftp load`.

5.5.2 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.

5.5.2.1 configbackup create

Description

With this command, you create a backup of the current configuration.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
configbackup create <configbackup-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`configbackup-name`	Enter a name for the backup.	max. 64 characters

Result

A backup of the current configuration is saved.

Additional notes

You delete a backup with the `configbackup delete` command.

You load a backup with the `configbackup restore` command.

You save configuration backups on your client PC with the `tftp save` command.

You load configuration backups from your client PC with the `tftp load` command.

5.5.2.2 configbackup restore

Description

With this command, you load a stored backup on your device.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
configbackup restore <configbackup-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`configbackup-name`	Enter a name for the backup.	max. 64 characters

Result

The backup is loaded on the device

Additional notes

You create a backup of the current configuration with the `configbackup create` command.

You delete a backup with the `configbackup delete` command.

You save configuration backups on your client PC with the `tftp save` command.

You load configuration backups from your client PC with the `tftp load` command.

5.5.2.3 configbackup delete

Description

With this command, you delete a backup.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
configbackup delete <configbackup-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`configbackup-name`	Enter a name for the backup.	max. 64 characters

Result

The backup is deleted.

Additional notes

You create a backup of the current configuration with the `configbackup create` command.

You load a backup with the `configbackup restore` command.

5.6 Discovery and Set via PROFINET Discovery Protocol (DCP)

This section describes commands for displaying and setting network parameters.

5.6.1 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.

5.6.1.1 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.

5.6.2 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.

5.6.2.1 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)>}
```

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 45)".

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.

5.6.2.2 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 "Interface identifiers and addresses (Page 45)".

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.

5.6.2.3 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	

Parameter	Description	Range of values/note
`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
`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 "Interface identifiers and addresses (Page 45)".

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.

5.6.2.4 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 "Interface identifiers and addresses (Page 45)".

Result

The LEDs of the selected device flash. When the time (`timeout`) elapses, flashing stops.

5.6.2.5 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 "Interface identifiers and addresses (Page 45)".

Result

The selected device or the entire content of the table has been removed from the table.

5.7 SINEMA

5.7.1 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.

5.7.1.1 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.

5.7.2 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.

5.7.2.1 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`.

5.7.2.2 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 6

This part contains the sections that describe functions specific to SCALANCE.

6.1 PLUG

The CLP 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 CLP. The CLP is referred to as PLUG in the description.

6.1.1 The "show" commands

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

6.1.1.1 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.

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 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.

6.1.3 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.

6.1.3.1 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.

6.1.3.2 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.

6.1.3.3 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.

6.1.3.4 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.

6.1.3.5 presetplug

Description

With this command, you create a PRESET-PLUG. Apart from the configuration data, a PRESET-PLUG also contains the firmware version of the creating device. The PRESET PLUG is write-protected.

I a device starts with a PRESET-PLUG an upgrade/downgrade of the firmware is performed if there is a different firmware version on the device. This is indicated by the red LED flashing (flashing interval: 2 sec on/0.2 sec off). Afterwards the device is restarted and the device configuration incl. users and certificates on the PRESET-PLUG is transferred to the device.

To make the PLUG writable again, call the command `factoryclean`.

Requirement

- The PLUG is formatted.
- 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 parameter assignment:

```
presetplug
```

Result

The firmware of the executing device is written to the PLUG and write-protected.

6.2 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.

6.2.1 The "show" commands

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

6.2.1.1 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.

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 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.

6.2.2.2 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.

6.3 CLI

On the device, you can limit the time available for access with Command Line Interface. If no entry is made for a specific time, the CLI session is closed.

This section describes commands relevant for the configuration of this feature.

6.3.1 The "show" commands

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

6.3.1.1 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.

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 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.

6.3.2.2 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.

6.4 iPRP

This section describes the commands relevant for working with iPRP (industrial Parallel Redundancy Protocol).

Note

The commands are only available if the SCALANCE W device supports iPRP or the function can be enabled.

Note

iPRP with oversize frames (jumbo frames)

To be able to use oversize frames, oversize frames (jumbo frames) must be configured on all devices in the network.

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 wlan iprp

Description

This command shows the configuration of "industrial Parallel Redundancy Protocol (iPRP)".

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 wlan iprp
```

Result

The configuration is displayed.

6.4.1.2 show wlan iprp information

Description

This command displays information on existing iPRP 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 up the command with the following parameters:

`show wlan iprp information [<wlan 0/X>]`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The information on existing iPRP connections is displayed.

6.4.2 clear wlan iprp information

Description

With this command, you reset the saved information on the configuration of the iPRP.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

`cli#`

Syntax

Call the command without parameters:

`clear wlan iprp information`

Result

The information about iPRP is deleted.

Additional notes

You display the iPRP Information with the `show wlan iprp` command.

6.4.3 Commands in the WLAN configuration mode

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

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

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

- If you exit the WLAN configuration mode with the `exit` command, you return to the global configuration mode.
- If you exit the WLAN 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 WLAN configuration mode.

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

6.4.3.1 wlan iprp

Description

With this command, you change to the WLAN iPRP Configuration mode.

Note

Mutual interlock of iFeatures

iPRP and iPCF-2 are not compatible with each other and cannot be used at the same time on a device.

During dual operation of an access point, an iFeature cannot be enabled on a WLAN interface if an iFeature has already been enabled on the other interface.

Requirement

- The base bridge mode "802.1Q VLAN Bridge" is set.
- The VLANs have been created.
- Access Point mode: The VAP interfaces are enabled. The first two VAP interfaces per radio interface can be configured for iPRP.
- Client mode:
  - "Layer 2 Tunnel" is set for "MAC Mode".
  - Either "Always" or "Disabled" is set for "Background Scan Mode".
- The Spanning Tree Protocol is disabled.
- You are in WLAN configuration mode.
  The command prompt is as follows:
  `cli (config-wlan)#`

Syntax

Call the command without parameter assignment:

```
wlan iprp
```

Result

You are in the WLAN iPRP configuration mode. In this mode, you can configure the remaining settings.

The command prompt is as follows:

```
cli (config-wlan-iprp)#
```

Additional notes

You exit the WLAN iPRP configuration mode with the `end` or `exit` command.

You display this setting and other information with the `show wlan iprp` command.

Note

SCALANCE W700 IEEE802.11ax firmware does not support synchronization of the clients during scanning and roaming operations. Therefore, simultaneous scanning and roaming operations, which can result in brief transfer interruptions, can occur.

6.4.4 Commands in the WLAN iPRP configuration mode

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

In the WLAN configuration mode, enter the `wlan iprp` command to change to this mode.

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

- If you exit WLAN iPRP configuration mode with the `exit` command, you return to the WLAN configuration mode.
- If you exit WLAN iPRP 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 WLAN iPRP configuration mode.

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

Note

The availability of some commands in this section depends on the selected device mode. You will find the assignment of the commands to a specific device mode in the command header.

Example of a header:

- [Command] (Access Point) - The command is available only in access point mode
- [Command] (Client) - This command is only available in client mode

If a command is valid for both device modes, the header contains no additional note in parentheses.

6.4.4.1 wlan iprp interface

Description

With this command, you configure the "iPRP" function. You specify the PRP network in which the interface is a member. You can also enable the function for the required interface. Two VAPs are available for iPRP.

Requirement

- The interface is enabled.
- You are in the WLAN iPRP configuration mode.
  The command prompt is as follows:
  `cli (config-wlan-iprp)#`

Syntax

Call up the command with the following parameters:

`wlan iprp interface <wlan 0/X | vapX 0/Y> network {A | B} {enable | disable}`

The parameters have the following meaning:

Parameter	Description	Range of values / note

`interface`	The interface that will be assigned to the PRP network.	`wlan 0/X`
		`vapX 0/Y`
		Range of values:
		• X = 1 ... 2
		• Y = 1 ... 2

`network`	PRP Network	`A: PRP A`
		`B: PRP B`
		Both VAP interfaces of a radio interface cannot be used for the same iPRP network.
		Example of a valid configuration:
		VAP1.1 = PRP A
		VAP1.2 = PRP B

–		• `enable`: Enables iPRP • `disable`: Disables iPRP

Result

The iPRP function is configured.

Additional notes

You display the IPRP configuration with the `show wlan iprp command`.

You can obtain information on existing iPRP connections with the `show wlan iprp information [<wlan 0/X>]` command.

You remove the assignment with the `no wlan iprp interface <wlan 0/X | vapX 0/Y> network` command.

6.4.4.2 no wlan iprp interface

Description

With this command, you remove the assignment of the interface.

Requirement

You are in the WLAN iPRP configuration mode.

The command prompt is as follows:

```
cli (config-wlan-iprp)#
```

Syntax

Call up the command with the following parameters:

```
no wlan iprp interface <wlan 0/X | vapX 0/Y> network
```

The parameters have the following meaning:

Parameter	Description	Range of values / note

`interface`	The interface that will be assigned to the PRP network.	`wlan 0/X`
		`vapX 0/Y`
		Range of values:
		• X = 1 ... 2
		• Y = 1 ... 2

Result

The assignment is removed.

Additional notes

You configure the assignment with the `wlan iprp interface` command.

6.4.4.3 wlan iprp network

Description

With this command, you specify the VLAN assignment for PRP A and PRP B.

Requirement

You are in the WLAN iPRP configuration mode.

The command prompt is as follows:

```
cli (config-wlan-iprp)#
```

Syntax

Call up the command with the following parameters:

```
wlan iprp network {A | B} <vlan-id (1-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`network`	PRP Network	`A: PRP A` `B: PRP B`
`vlan-id`	Number of the addressed VLAN	`1 ... 4094`

Result

The VLAN assignment is configured.

Further notes

You display the IPRP configuration with the `show wlan iprp command`.

You can obtain information on existing iPRP connections with the `show wlan iprp information [<wlan 0/X>]` command.

You delete the assignment with the `no wlan iprp network` command.

6.4.4.4 no wlan iprp network

Description

With this command, you remove the VLAN assignment for PRP A and PRP B.

Requirement

You are in the WLAN iPRP configuration mode.

The command prompt is as follows:

```
cli (config-wlan-iprp)#
```

Syntax

Call up the command with the following parameters:

```
no wlan iprp network {A | B}
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`network`	PRP Network	`A: PRP A` `B: PRP B`

Result

The VLAN assignment is configured.

Further notes

You configure the VLAN assignment with the `wlan iprp network` command.

6.5 iPCF-2

This section describes the commands relevant for working with iPCF-2 (industrial Point Coordination Function 2).

Note

This commands are only available in connection with the inserted CLP iFeature:

- SCALANCE CLP 2GB W700 Access Point iFeatures (6GK5907-8UA00-0AA0)
- SCALANCE CLP 2GB W700 Client iFeatures (6GK5907-4UA00-0AA0)

6.5.1 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.

6.5.1.1 show wlan ipcf-2

Description

This command shows the settings of iPCF-2.

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 wlan ipcf-2 <wlan 0/X>`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The iPCF-2 settings are displayed.

6.5.2 WLAN Interface configuration mode

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

In global configuration mode, enter the `interface wlan 0/X` command to change to this mode.

- If you exit the WLAN Interface configuration mode with the `exit` command, you return to the global configuration mode.
- If you exit the WLAN Interface 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 WLAN Interface configuration mode.

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

6.5.2.1 wlan ipcf-2

Description

With this command, you enable iPCF-2 mode.

Requirement

You are in interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameters:

```
wlan ipcf-2
```

Result

iPCF-2 mode is enabled.

Additional notes

You disable iPCF mode with the `no wlan ipcf-2` command.

You display the setting with the `show wlan ipcf-2` command.

6.5.2.2 no wlan ipcf-2

Description

With this command, you disable iPCF-2 mode.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameters:

```
no wlan ipcf-2
```

Result

iPCF-2 mode is disabled.

Additional notes

You enable iPCF mode with the `wlan ipcf-2` command.

You display the setting with the `show wlan ipcf-2` command.

6.6 Packet Capture

This section describes the commands relevant for working with Packet Capture.

6.6.1 show packet capture

Description

This command shows the settings of Packet Capture of one or all interfaces.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show packet capture
```

Result

The settings are displayed.

6.6.2 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.

6.6.2.1 packet capture

Description

With this command, you change to PACKET CAPTURE configuration mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
packet capture
```

Result

You are now in PACKET CAPTURE configuration mode.

The command prompt is as follows:

```
cli(packet-capture)#
```

Additional notes

You exit PACKET CAPTURE configuration mode with the command `end` or `exit`.

6.6.3 Commands in Packet Capture configuration mode

This section describes commands that you can call up in PACKET CAPTURE configuration mode.

In global configuration mode, enter the packet capture command to change to this mode.

- If you exit PACKET CAPTURE configuration mode with the `exit` command, you return to global configuration mode.
- If you exit PACKET CAPTURE configuration mode with the `end` command, you return to Privileged EXEC mode.

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

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

6.6.3.1 activate-after-restart

Description

With this command, the configuration of "Packet Capture" is saved and retained after a restart.

Requirement

You are in PACKET CAPTURE configuration mode.

The command prompt is as follows:

```
cli(packet-capture)#
```

Syntax

Call the command without parameter assignment:

```
activate-after-restart
```

Result

The function is enabled.

Additional notes

You disable the setting with the `no activate-after-restart` command.

6.6.3.2 no-activate-after-restart

Description

With this command, you disable the function.

Requirement

You are in PACKET CAPTURE configuration mode.

The command prompt is as follows:

```
cli(packet-capture)#
```

Syntax

Call the command without parameter assignment:

```
no activate-after-restart
```

Result

Saving the configuration of "Packet Capture" is disabled. After a restart, the configuration is reset to the default setting.

6.6.3.3 capture

Description

With this command, you enable the function "Packet Capture" on the interface (WLAN, Ethernet). You can also enable the function on several interfaces at the same time. As default, this function is disabled.

When the function is enabled you can link the interface in Wireshark. In Wireshark, you can see the content of the packages or filter according to certain contents.

Note

The access point records all incoming frames. Encrypted data is not decrypted before the recording.

Performance

Enable the function only for diagnostics purposes. The increased data traffic could influence the performance of the device.

Ethernet interface with SCALANCE WAM763-1

- You can select one or more ports (P1 - P4) for the Ethernet interface.
- Data traffic that is only forwarded and not received or sent by the WLAN interface is not displayed.

Requirement

You are in PACKET CAPTURE configuration mode.

The command prompt is as follows:

```
cli(packet-capture)#
```

Syntax

Call up the command with the following parameters:

```
capture { <interface-type> <0/a-b,0/c,...> | vlan <vlan-id
(1-4094)> | usb <interface-id> | sinemarc | all }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`0/a-b,0/c,...`	Port no. of the interface	
`vlan-id` *)	Number of the addressed VLAN	1 ... 4094
`usb` *)	WAN interface	-
`sinemarc`	SINEMA Configuration Interface	-
`all`	All interfaces	-

*) Only with SCALANCE M-800/MUM85x

For information on names of addresses and interfaces, refer to the section "Naming interfaces (Page 45)".

Result

The "Packet Capture" function is enabled on the specified interface and the receive mode is specified. When the device restarts, the function is disabled. With the command "`activate-after-restart`" the function is enabled even after a restart.

Linking in the interface in Wireshark

Requirement:

- Wireshark V2.0.0 or higher is installed on the PC
- The PC and device must be reachable via IP (layer 3).

Procedure

To analyze the data traffic e.g. of the WLAN interface 1 in Wireshark, follow the steps below:

1. Enable the function on the interface, e.g. `cli(packet-capture)# capture wlan 0/1`
2. Start Wireshark.
3. Click "Options" in the "Capture" menu. The window "Wireshark - Capture Interfaces" opens.
4. Click the "Manage Interfaces..." button on the "Input" tab. In the following dialog, click on the "Remote Interfaces" tab.
5. To add the interface click on the Plus character in the "Remote Interfaces" tab.
6. In the following dialog, enter the IPv4 address for "Host" and 2002 for "Port".
7. Enable "No authentication" for "Authentication" and click the "OK" button.
8. On the "Remote Interfaces" tab, the host and the interfaces on which the function "Packet Capture" is enabled are displayed.
9. Select the interface and click the "OK" button.
10. To start the recording click "Start". You can obtain further information about handling the program in Wireshark.

If you analyze several interfaces, you can use a Wireshark instance for each interface.

Additional notes

You display this setting and other information with the `show packet capture` command.

You disable an interface with the `no capture { <interface-type> <0/a-b,0/c,...> | vlan <vlan-id (1-4094)> | usb <interface-id> | all }` command.

6.6.3.4 no capture

Description

With this command, you disable the "Packet Capture" function.

Requirement

You are in PACKET CAPTURE configuration mode.

The command prompt is as follows:

```
cli(packet-capture)#
```

Syntax

Call up the command with the following parameters:

```
no capture { <interface-type> <0/a-b,0/c,...> | vlan <vlan-id
(1-4094)> | usb <interface-id> | sinemarc | all }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`interface-type`	Type or speed of the interface	Specify a valid interface.
`0/a-b,0/c,...`	Port no. of the interface	
`vlan-id` *)	Number of the addressed VLAN	1 ... 4094
`usb` *)	WAN interface	-
`sinemarc`	SINEMA Configuration Interface	-
`all`	All interfaces	-

*) Only with SCALANCE M-800/MUM85x

For information on names of addresses and interfaces, refer to the section "Naming interfaces (Page 45)".

Result

The function is disabled.

6.6.3.5 port

Description

With this command, you change the default port for Packet Capture.

Requirement

You are in PACKET CAPTURE configuration mode.

The command prompt is as follows:

```
cli(packet-capture)#
```

Syntax

Call the command with the following parameters:

```
port <number(1-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`number`	Number of the port	If necessary, change the port. Default: 2002 Make sure that the specified port is not already used.

Result

The port has been changed.

Additional notes

You reset the port to the default value with the `no port` command.

6.6.3.6 no port

Description

With this command you reset the preconfigured port for Packet Capture to the default value.

Requirement

You are in PACKET CAPTURE configuration mode.

The command prompt is as follows:

```
cli(packet-capture)#
```

Syntax

Call the command without parameter assignment:

`no port`

Result

The port is reset to the default value 2002.

Additional notes

You can change the port with the `port` command.

6.7 Signal recorder

This section describes the commands relevant for working with the signal recorder.

Note

All commands in this section are only available in client mode.

6.7.1 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.

6.7.1.1 show wlan signal-recorder (Client)

Description

This command shows the status of the signal recorder and the recording. You can call the command before, after or during the recording.

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 wlan signal-recorder <wlan 0/X>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The status of the signal recorder and the recording are displayed.

- If the recording has started, the configured interval and the current number of recorded measured values are displayed.
- If the recording has stopped, the configured interval and the number of recorded measured values are displayed.

6.7.2 wlan signal-recorder start (client)

Description

With this command, you configure and start recording with the signal recorder. The recorded measured values are saved every 10 minutes and logged in files. On completion of the recording, the files can be downloaded as a zip file using http, tftp or sftp.

The automatic saving contains only the last fully elapsed 10 minutes. The remaining minutes are discarded.

If the signal recorder is ended manually or if the procedure was ended automatically, the file contains all the values since the start of the recording.

If a recording is interrupted before 10 minutes have elapsed (e.g. due to a restart or power down), no signal recorder file is saved.

Requirement

- The WLAN interface is enabled.

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:

```
wlan signal-recorder <wlan 0/X> <ms (1-60000)> <sample_number
(1-20000)> [bidirectional] start
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.
`ms`	The interval in milliseconds (ms) between acquisition of two measured values	1 - 60000 The first measured value is displayed only after the set time interval has elapsed.
`sample_number`	This parameter specifies how many measured values will be recorded.	1 - 20000
`bidirectional`	The values of the access point are recorded.	**Requirement** The setting is supported by access points with the following versions: • SCALANCE W700 11n > V6.1 • SCALANCE W1700 11ac > V1.0 • SCALANCE W700 11ax V1.1 or higher **Note** The access point sends its data to a maximum of 3 clients on which signal recorders are running. The access point data is not displayed on other clients.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The recording is configured and will be started. The measured values are logged in files. If these files already exist, they will be overwritten. If the set total number of measured values is reached, the recording stops automatically. Use the `wlan signal-recorder <wlan 0/X> stop` command to stop the recording early.

Further notes

You stop the recording early with the `wlan signal-recorder <wlan 0/X> stop` command.

You display the status of the signal recorder and the recording with the `show wlan signal-recorder <wlan 0/X>` command.

6.7.3 wlan signal-recorder display (client)

Description

With this command, you configure and start recording with the signal recorder without specifying a total for the measured values. The measured values are output in the CLI and logged in files. The files can be downloaded as a zip file using http, tftp or sftp. The values are stored every 10 minutes and overwrite the existing values. The file therefore contains the values the last time they were stored.

Requirement

- The WLAN interface is enabled.

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:

```
wlan signal-recorder <wlan 0/X> <ms (100-60000)> [bidirectional]
display
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.
`ms`	The interval in milliseconds (ms) between acquisition of two measured values	100 - 60000 The first measured value is displayed only after the set time interval has elapsed.
`bidirectional`	The values of the access point are recorded.	**Requirement** The setting is supported by access points with the following versions: • SCALANCE W700 11n > V6.1 • SCALANCE W1700 11ac > V1.0 • SCALANCE W700 11ax V1.1 or higher **Note** The access point sends its data to a maximum of 3 clients on which signal recorders are running. The access point data is not displayed on other clients.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The recording is configured and will be started. The measured values are output in the CLI and logged in files. If these files already exist, they will be overwritten.

Use the `wlan signal-recorder <wlan 0/X> stop` command to stop the recording.

During the recording, it is possible that working in the CLI becomes slower.

Further notes

You stop the recording early with the `wlan signal-recorder <wlan 0/X> stop` command.

You display the status of the signal recorder and the recording with the `show wlan signal-recorder <wlan 0/X>` command.

6.7.4 wlan signal-recorder stop (client)

Description

With this command, you stop the recording with the signal recorder.

Requirement

- A recording was started.

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:

`wlan signal-recorder <wlan 0/X> stop`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The recording was stopped.

Further notes

You start the recording with the `wlan signal-recorder start` command.

6.8 TCP Event

This section describes the commands relevant for working with the TCP Event.

6.8.1 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.

6.8.1.1 show tcpevent

Description

This command shows the configuration of the "TCP Event" function.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show tcpevent
```

Result

The configuration is displayed.

6.8.2 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.

6.8.2.1 tcpevent

Description

With this command, you change to the TCP EVENT configuration mode.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
tcpevent
```

Result

You are now in the TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Further notes

You exit the TCP EVENT configuration mode with the command `end` or `exit`.

6.8.3 Commands in the TCP EVENT configuration mode

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

In the Global configuration mode, enter the `tcpevent` command to change to this mode.

- When you exit the TCP EVENT configuration mode with the `exit` command, you return to the Global configuration mode.
- When you exit the TCP EVENT configuration mode with the `end` command, you return to the Privileged EXEC mode.

6.8.3.1 enable

Description

With this command, you enable the "TCP Event" function.

Requirement

You are now in the TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Syntax

Call the command without parameters:

```
enable
```

Result

The function is enabled.

Additional notes

You disable the function with the `disable` command.

You display the configuration of the function with the `show tcpevent` command.

6.8.3.2 disable

Description

With this command, you disable the "TCP Event" function.

Requirement

You are now in the TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Syntax

Call the command without parameters:

```
disable
```

Result

The function is disabled.

Additional notes

You enable the function with the `enable` command.

You display the configuration of the function with the `show tcpevent` command.

6.8.3.3 port

Description

With this command, you define the port at which the device waits for the TCP packets.

Requirement

You are now in the TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Syntax

Call up the command with the following parameters:

```
port <number(1-65535)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`number`	Port number	1 ... 65535 Default: 26864 (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 (Page 29)".

Result

The port is configured.

Further notes

You display the configuration of the function with the show `tcpevent` command.

6.8.3.4 event

Description

With this command, you specify whether an event, e.g. the "Sleep Mode" function, is triggered with TCP packets.

Requirement

You are now in the TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Syntax

Call the command with the following parameters:

```
event {show-types | type <name> {enable | disable} }
```

The parameters have the following meaning:

Parameter	Description
`show-list`	Lists the available events.
`name`	Name of the event. The following names are possible: • sleepmode • digital-out • wlan-roaming (only with client)
`enable`	The desired event can be controlled with TCP packets.
`disable`	Disables the function.

Result

The setting is specified.

6.8.3.5 event type wlan-roaming enable (client)

Description

With this command, you enable the TCP packet with which the WLAN roaming operation is controlled on the client.

Requirement

You are now in the TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Syntax

Call the command without parameters:

```
event type wlan-roaming enable
```

Result

The TCP package for WLAN roaming is disabled.

6.8.3.6 event type wlan-roaming disable (client)

Description

With this command, you disable the TCP packet with which the WLAN roaming operation is controlled on the client.

Requirement

You are now in the TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Syntax

Call the command without parameters:

```
event type wlan-roaming disable
```

Result

The function is disabled.

6.8.3.7 password

Description

With this command, you configure the password with which the incoming TCP packet is checked.

Requirement

You are now in the TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Syntax

Call up the command with the following parameters:

```
password <text(32)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`text`	Password	Enter the password. Maximum length: 32 characters

Result

The password is configured.

6.8.3.8 user

Description

With this command, you configure the user name with which the incoming TCP packet is checked.

Requirement

You are now in the TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Syntax

Call up the command with the following parameters:

```
user <text(32)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`text`	User name	Specify the user name. Maximum length: 32 characters The following characters are permitted: • 0123456789 • A...Z a...z • . -_

Result

The user name is configured.

6.8.3.9 event show-types

Description

This command shows available TCP events.

Requirement

You are in TCP EVENT configuration mode.

The command prompt is as follows:

```
cli(config-tcpevent)#
```

Syntax

Call the command without parameters:

```
event show-types
```

Result

The TCP events are displayed.

System time 7

This part contains the sections describing how the system time is obtained and the settings.

7.1 System time setting

This section describes commands relevant for the configuration of the system time.

7.1.1 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.

7.1.1.1 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.

7.1.1.2 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.

7.1.2 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.

7.1.2.1 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 }
```

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 .

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.

7.1.2.2 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.

7.1.2.3 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.

7.1.2.4 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.

7.1.2.5 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.

7.2 NTP client

This section describes commands for configuration of the NTP server and the NTP client.

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 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.

7.2.2 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.

7.2.2.1 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.

7.2.3 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.

7.2.3.1 ntp server

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 { ipv4 <ip_addr> | fqdn-name <FQDN> | ipv6 <ip6_addr> }
[port { <1025-36564> | default}] [poll <seconds(64-1024)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`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	-

Parameter	Description	Range of values/note
FQDN	Domain name	Maximum of 100 characters If you have stored a suitable domain name, you can specify a host name.
ipv6	Keyword for an IPv6 address	-
ip6_addr	Value for the IPv6 address of the time server	Enter a valid IPv6 address.
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 45)".

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` command.

You store a domain name with the `ip domain name` or `domain name` command.

7.2.3.2 no ntp server

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 the command without parameter assignment:

```
no ntp server
```

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` command.

7.2.3.3 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.

7.3 SNTP client

This section describes commands relevant for configuration of the SNTP client.

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 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.

7.3.1.2 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.

7.3.1.3 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.

7.3.2 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.

7.3.2.1 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.

7.3.3 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.

7.3.3.1 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.

7.3.3.2 sntp unicast-server

Description

With this command, you configure an SNTP unicast server.

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> | ipv6
<ip6_addr> }
 [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	Maximum of 100 characters
`ipv6`	Keyword for an IPv6 address	-
`ip6_addr`	Value for the IPv6 address of the time server	Enter a valid IPv6 address.
`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
`secondary`	Keyword to store the second SNTP server	If you do not specify this parameter, the first SNTP server is stored.

Result

The SNTP unicast server is configured.

Additional notes

You can reset the setting to the default with the `no sntp unicast-server` command.

You display this setting and other information with the `show sntp unicast-mode status` command.

7.3.3.3 no sntp unicast-server

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)> |
ipv6 <ip6_addr>}
```

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
`ipv6`	Keyword for an IPv6 address	-
`ip6_addr`	Value for the IPv6 address of the time server	Enter a valid IPv6 address.

Result

The SNTP unicast server is reset to the default value.

Additional notes

You configure the setting with the `sntp unicast-server` command.

You display this setting and other information with the `show sntp unicast-mode status` command.

7.3.3.4 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.

Network structures

8

8.1 WLAN

8.1.1 Introduction to the section WLAN

This section describes commands for configuring and managing wireless LANs (WLANs).

8.1.2 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.

Note

The availability of some commands in this section depends on the selected device mode. You will find the assignment of the commands to a specific device mode in the command header.

Example of a header:

- [Command] (Access Point) - The command is available only in access point mode
- [Command] (Client) - This command is only available in client mode

If a command is valid for both device modes, the header contains no additional note in parentheses.

8.1.2.1 show wlan advanced

Description

This command shows information about the send characteristics of the SCALANCE W device, for example the beacon rate.

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 wlan advanced <wlan 0/X>`

The parameter has the following meaning:

Parameter	Description	Range of values/note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The content depends on the operating mode that is set.

- Beacon Interval
- Overlap-AP aging interval
- HW Retries
- A-MPDU

8.1.2.2 show wlan allowed channels

Description

This command displays the available wireless channels. If you have selected channels explicitly for wireless communication, this information 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 wlan allowed channels <wlan 0/X>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Enter a valid interface.

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The list of wireless channels available for establishing a wireless link to the relevant WLAN interface is displayed.

See also

wlan allowed channels only (Page 225)

wlan allowed channels (Page 226)

8.1.2.3 show wlan antennas

Description

This command shows the antenna settings for the SCALANCE W device, for example cable length.

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 wlan antennas <wlan 0/X>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The antenna settings of the relevant WLAN interface are displayed.

8.1.2.4 show wlan ap (access point)

Description

The command displays the configuration parameters of the access point.

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 wlan ap <wlan 0/X>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The following settings of the access point are displayed:

- Channel
- Alternative channel
- Channel Width

See also

wlan alternative channel (Access Point) (Page 228)

wlan channel (Access Point) (Page 239)

8.1.2.5 show wlan available-ap-list (client)

Description

This command shows the access points to which the client device can establish a wireless link or with which the client device is connected.

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 wlan available-ap-list <wlan 0/X> [connected]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.
`connected`	shows the information of the access points with which the client is connected.	–

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The access points to which the client can set up a wireless link are displayed.

8.1.2.6 show wlan basic

Description

This command displays the WLAN-basic configuration, for example, transmission standard, frequency band.

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 wlan basic <wlan 0/X>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The following WLAN settings are displayed, for example:

- Admin status (whether the interface is switched on or off)
- Frequency band
- WLAN mode
- DFS (802.11h)
- Outdoor Mode

See also

wlan outdoor (Page 247)

wlan dfs (Page 241)

wlan frequency band (Page 243)

8.1.2.7 show wlan client (Client)

Description

This command shows the client configuration of the SCALANCE W device, for example how the MAC address is assigned to the 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 up the command with the following parameters:

```
show wlan client <wlan 0/X>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The following client settings are displayed:

- Client MAC Mode
- Roaming Threshold
- Background scan mode
- Background Scan Interval
- Scan Channels

8.1.2.8 show wlan client-list (access point)

Description

This command shows a table with the clients logged on with the access point as well as additional information, for example status, signal strength, MAC 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 up the command with the following parameters:

```
show wlan client-list [wlan 0/X [{mac <macaddr> | sys <sysname> |
AID}]]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.
`mac`	Keyword for the MAC address of the client	-
`macaddr`	MAC address	`aa:bb:cc:dd:ee:ff`
`sys`	Keyword for the system name of the client	-
`sysname`	System name	
`AID`	Connection ID of the client.	–

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The table with the logged-on clients is displayed.

8.1.2.9 show wlan client-list-vap (access point)

Description

This command shows the VAP interface via which the clients are logged on to the access point in the form of a 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 wlan client-list-vap vapX 0/Y [AID]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`vapX 0/Y`	VAP interface	Specify a valid interface.
`AID`	Connection ID of the client.	–

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The table with the logged-on clients is displayed.

8.1.2.10 show wlan device

Description

This command shows the WLAN basic configuration for the SCALANCE W device, for example the 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 wlan device
```

Result

The following settings of the SCALANCE W device are displayed:

- Device mode
- Commit Mode
- Country

See also

commit mode (Page 221)

device mode (Page 224)

8.1.2.11 show wlan ip-mapping

Description

This command shows the table for the IP mapping. The table contains the assignment of MAC address and IP address of the SCALANCE W700 devices for which the client makes WLAN access possible.

Note

This page is only available for clients or access points in client 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 with the following parameters:

```
show wlan ip-mapping <wlan 0/X>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The IP mapping table is displayed.

8.1.2.12 show wlan noise-floor

Description

This command shows the background noise of the channel at the respective antenna connector. When available, the background noise of the extended channel (HT-40) is 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 wlan noise-floor <wlan 0/X>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The background noise is displayed.

8.1.2.13 show wlan overlap-ap-list (access point)

Description

This command shows all access points that are visible on the set channel at 2.4 GHz or 5 GHz. If entries exist here, the maximum data throughput of the access point will be restricted.

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 wlan overlap-ap-list <wlan 0/X>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The access points are displayed.

8.1.2.14 show wlan overview

Description

The command shows configuration of the SCALANCE W 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 parameter assignment:

```
show wlan overview
```

Result

The configuration of the SCALANCE W device is displayed. The content depends on the operating mode that is set.

- Radio
- WLAN Mode
- Configured Channel
- Alternative DFS Channel
- Operative Channel
- Channel Width
- Status
- Port
- MAC Address
- SSID
- Status
- MAC Mode
- Connected BSSID
- Connected SSID

8.1.2.15 show wlan ssid-table (client)

Description

This command shows a table with the SSIDs of the access points to which the client device can establish a wireless link.

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 wlan ssid-table <wlan 0/X>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`wlan 0/X`	WLAN interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The table with the SSIDs configured on the client and their status is displayed.

8.1.2.16 show wlan vap (access point)

Description

This command shows the configuration of the VAP 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 wlan vap <vapX 0/Y>`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`vapX 0/Y`	VAP interface	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The following settings of the VAP are displayed:

- Admin status
- SSID
- Broadcast SSID

See also

vap ssid (access point) (Page 251)

8.1.3 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.

8.1.3.1 wlan

Description

With this command, you change to the WLAN Configuration mode.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
wlan
```

Result

You are in the WLAN Configuration mode.

The command prompt is as follows:

```
cli (config-wlan)#
```

Further notes

You exit the particular WLAN Configuration mode with the `end` or `exit` command.

8.1.4 Commands in the WLAN configuration mode

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

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

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

- If you exit the WLAN configuration mode with the `exit` command, you return to the global configuration mode.
- If you exit the WLAN 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 WLAN configuration mode.

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

Note

The availability of some commands in this section depends on the selected device mode. You will find the assignment of the commands to a specific device mode in the command header.

Example of a header:

- [Command] (Access Point) - The command is available only in access point mode
- [Command] (Client) - This command is only available in client mode

If a command is valid for both device modes, the header contains no additional note in parentheses.

8.1.4.1 commit mode

Description

With this command, you specify when the modified WLAN settings become effective on the device.

Requirement

You are in the WLAN Configuration mode.

The command prompt is as follows:

```
cli(config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
commit mode { auto | manual }
```

The parameters have the following meaning:

Parameters	Description
`auto`	Each change to the WLAN settings is automatically applied and is immediately effective.
`manual`	The changes are accepted, but are still not active. The changes only take effect when you confirm the changes with the "`commit wlan-settings`" command.

Result

The commit mode is specified.

Further notes

You show the settings for the commit mode with the `show wlan device` command.

See also

commit wlan-settings (Page 222)

show wlan device (Page 214)

8.1.4.2 commit wlan-settings

Description

With this command, you confirm modified WLAN settings. The modified WLAN settings are then effective on the device.

Requirement

- In `commit mode`, `manual` is set.
- You are in the WLAN configuration mode.
  The command prompt is as follows:
  `cli(config-wlan)#`

Syntax

Call the command without parameter assignment:

```
commit wlan-settings
```

Result

The changes are confirmed and effective.

See also

commit mode (Page 221)

8.1.4.3 country

Description

With this command, you specify the country in which the SCALANCE W device will be used. You do not need to know the data for the specific country, the channel division and output power are set by the device according to the country you select.

You can find more information on currently available country approvals in the "SCALANCE W700 802.11ax approvals (https://support.industry.siemens.com/cs/ww/en/view/109802595)" documentation.

Requirement

You are in the WLAN Configuration mode.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
country { show-countries | code <iso-code> }
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
`show-countries`	Shows a list of the countries that can be set along with their two-digit ISO code.	--
`iso-code`	Country code The country code complies with ISO 3166.	Enter the ISO code of the required country.

Result

The country is specified for the SCALANCE W700 device.

Further notes

You display the setting with the `show wlan device` command.

8.1.4.4 device mode

Description

With this command, you specify the mode of the SCALANCE W device.

Requirement

You are in WLAN configuration mode.

The command prompt is as follows:

```
cli(config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
device mode { ap | client }
```

The parameters have the following meaning:

Parameters	Description
`ap`	Mode: Access Point mode (default setting)
`client`	Mode: Client mode

Result

After the mode is changed, the following message is displayed with the command `(config-wlan)# device mode client`:

```
You are about to change the device mode!!!
Type 'y' to restart the device with memory defaults or 'n' to abort.
Continue with changing of the device mode (y/n): n
```

If you confirm the message with "`y`", the device is reset to the stored settings (protected parameters) and restarted in the selected mode.

Additional notes

You display the settings for the mode with the `show wlan device` command.

8.1.5 Commands in the WLAN Interface configuration mode

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

In global configuration mode, enter the `interface wlan 0/X` command to change to this mode.

- If you exit the WLAN Interface configuration mode with the `exit` command, you return to the global configuration mode.
- If you exit the WLAN Interface 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 WLAN Interface configuration mode.

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

Note

The availability of some commands in this section depends on the selected device mode. You will find the assignment of the commands to a specific device mode in the command header.

Example of a header:

- [Command] (Access Point) - The command is available only in access point mode
- [Command] (Client) - This command is only available in client mode

If a command is valid for both device modes, the header contains no additional note in parentheses.

8.1.5.1 wlan allowed channels only

Description

With this command, you enable the Use Allowed Channels only function. Only the channels you specified with the `wlan allowed channels` command are used.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameter assignment:

```
wlan allowed channels only
```

Result

The function is enabled.

Further notes

You display the setting with the `show wlan allowed channels <wlan 0/X>` command.

You disable the function with the `no wlan allowed channels only` command.

8.1.5.2 wlan allowed channels

Description

This command specifies which of the permitted channels the SCALANCE W device can use. A list of the permitted channels is created.

Requirement

- The function "Use Allowed Channels only" is active.
- You are in the Interface Configuration mode of the WLAN interface.
  The command prompt is as follows:
  `cli (config-if-wlan-0-X)#`

Syntax

Call up the command with the following parameters:

```
wlan allowed channels{ all | none | {[add]|[del]} [ 2.4 | 4 | 5 ]
<channels> }
```

The parameters have the following meaning:

Parameters	Description
`all`	All permitted channels are entered in the list.
`none`	• Access point: All channels except for the following channels are deleted: – Operative channel – Alternative DFS channel If "Auto" is set for the channel, the list is deleted and the first valid channel of the selected frequency band is applied. • Client: The list is deleted and the first valid channel of the selected frequency band is applied.
`add`	The channels located in the <channel> parameter are added to the list.
`del`	The channels located in the <channel> parameter are deleted from the list.
`2.4`	Optional parameter. Use this parameter to specify the frequency band from which you want to add one or more channels to the list.
`4`	Optional parameter. Use this parameter to specify the frequency band from which you want to add one or more channels to the list.

Parameters	Description
`5`	Optional parameter. Use this parameter to specify the frequency band from which you want to add one or more channels to the list.
`channels`	Number of permitted channels. To specify in more than one channel, write the channel numbers in quotes and use the <space> as the delimiter. Example: `wlan allowed channels 5 "40 36"` If you do not use the "`add`" parameter, the existing entries in the list are overwritten.

Result

The list of permitted channels has been created.

Further notes

You display the list of valid channels with the `show wlan allowed channels <wlan 0/X>` command.

You enable the "Use Allowed Channels only" function with the "`wlan allowed channels only`" command.

8.1.5.3 no wlan allowed channels only

Description

With this command, you disable the Use Allowed Channels only function. This is the default setting.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameter assignment:

```
no wlan allowed channels only
```

Result

The function is disabled.

Further notes

You display the setting with the `show wlan allowed channels <wlan 0/X>` command.

You enable the function with the `wlan allowed channels only` command.

See also

wlan allowed channels only (Page 225)

8.1.5.4 wlan alternative channel (Access Point)

Description

If you have activated the DFS function, you specify the alternative channel with this command. If the access point on the current channel discovers a disruption, it switches to the alternative channel.

Requirement

- The DFS function is enabled.

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan alternative channel { show-channels | <number (0=auto)> }
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
`show-channels`	Lists all available channels.	--
`number`	Number of the alternative channel If you want the access point to search for a free channel itself, use "0".	Default value: 0 (AUTO)

Result

The alternative channel is set.

Further notes

You display the setting with the `show wlan basic <wlan 0/X>` command.

You enable the DFS function with the `wlan dfs` command.

See also

show wlan basic (Page 211)

wlan dfs (Page 241)

8.1.5.5 wlan ampdu

Description

With this command, you enable the sending of AMPDU frames. Multiple MPDU frames with the same destination address are bundled and sent as one large A-MPDU.

Requirement

- The IEEE 802.11n/ac/ax transmission standard is enabled.

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameter assignment:

```
wlan ampdu
```

Result

The sending of AMPDU frames is enabled.

Further notes

You display the setting with the `show wlan advanced <wlan 0/X>` command.

You disable the function with the `no wlan ampdu` command.

8.1.5.6 no wlan ampdu

Description

With this command, you disable the sending of AMPDU frames. If the function is disabled, only AMPDU frames can be received.

Requirement

- The IEEE 802.11n/ac/ax transmission standard is enabled.

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameter assignment:

```
no wlan ampdu
```

Result

The sending of AMPDU frames is disabled.

Further notes

You display the setting with the `show wlan advanced <wlan 0/X>` command.

You enable the function with the `wlan ampdu` command (default setting).

8.1.5.7 wlan antenna additional-attenuation

Description

With this command, you specify the additional attenuation caused, for example by an additional splitter. Using the `show wlan basic` command, check whether or not the current WLAN settings violate the permitted transmit power restrictions (`TX Power Check`) of the selected country.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan antenna additional-attenuation <index (1-2)> <dB(0-70)>
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
`index`	Antenna connector	1...2
`dB`	Attenuation in decibels [dB]	0...70 Default: 0

Result

The additional attenuation is specified.

Further notes

You show the set value with the `show wlan antennas <wlan 0/X>` command.

8.1.5.8 wlan antenna cable-length

Description

With this command, you configure the cable length between the SCALANCE W device and the external antenna.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan antenna cable-length <index(1-2)> <m(0-30)>
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
index	Antenna connector	1...2
m	Cable length in meters [m]	0...30 Default: 0

Result

The cable length is specified.

Further notes

You show the set cable length with the `show wlan antennas <wlan 0/X>` command.

See also

show wlan antennas (Page 209)

8.1.5.9 wlan antenna gain-2-4GHz

Description

With this command, you specify the antenna gain of the antenna type "User defined" in the 2.4 GHz frequency band. With the `show wlan antennas` command, check whether the maximum transmit power is exceeded with the setting.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan antenna gain-2-4GHz <index(1-2)> <dBi(0-30)>
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
`index`	Slot no. of the interface	1...2
`dBi`	Antenna gain in decibels isotropic (dBi)	0 ... 30 0 = antenna is not connected

Result

The antenna gain is specified.

Further notes

You show the set antenna gain with the `show wlan antennas <wlan 0/X>` command.

See also

show wlan antennas (Page 209)

wlan antenna type (Page 235)

8.1.5.10 wlan antenna gain-5GHz

Description

With this command, you specify the antenna gain of the antenna type "User defined" in the 5 GHz frequency band. With the `show wlan antennas` command, check whether the maximum transmit power is exceeded with the setting.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan antenna gain-5GHz <index(1-2)> <dBi (0-30)>
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
`index`	Slot no. of the interface	1...2
`dbi`	Antenna gain in decibels isotropic (dBi)	0 ... 30 0 = antenna is not connected

Result

The antenna gain is specified.

Further notes

You show the set antenna gain with the `show wlan antennas <wlan 0/X>` command.

See also

show wlan antennas (Page 209)

wlan antenna type (Page 235)

8.1.5.11 wlan antenna mode

Description

With this command, you configure the settings for the antenna connected to the SCALANCE W device.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan antenna mode <index(1-2)> { RX | TX | RX-TX }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`index`	Antenna connector	1...2
`RX`	For receiving only	--
`TX`	For sending only	--
`RX-TX`	For sending and receiving (default setting)	--

Result

The use of the antenna is specified.

Note

50 Ω terminating resistor

Each WLAN interface has four antenna connectors. Connectors that are not used must have a 50 Ω terminating resistor fitted.
The antennas R1A1 and R2A1 must be always be connected as soon as the associated WLAN interface is turned on. If no antenna is connected, the relevant interface must also be disabled for RX and TX. Otherwise, there may be transmission disruptions.

The following table shows which combinations are possible:

Index1 **R1 A1**	**Index2** **R1 A2**
RX-TX	RX-TX
RX-TX	Rx
RX-TX	Tx
RX-TX	--[1)]

[1)] Antenna type "Not used (Connect 50 Ohm terminating resistor)"

Further notes

You display the setting with the `show wlan antennas <wlan 0/X>` command.

You configure the antenna type with the `wlan antenna type` command.

8.1.5.12 wlan antenna type

Description

With this command, you specify which antenna type is connected to the relevant antenna connector.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan antenna type {show-types | <index(1-2)> <antenna-index>}
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
`show-types`	Shows a list of supported antennas with the corresponding antenna index.	--
`index`	Antenna connector	1..2
`antenna-index`	Antenna index	Enter the required antenna index. You can obtain an overview of the antenna indexes available in the SCALANCE W device with the `wlan antenna type show-types` command.

Result

The antenna type is specified.

Note

Dual operation in access point mode 2.4 GHz + 5 GHz

If you want to activate two WLAN interfaces in parallel (dual AP mode), note the following procedure:

1. Insert the SCALANCE CLP 2GB W700 iFeatures into the device.
2. Specify the antenna type "2,4 GHz + 5 GHz" for all four antennas with the command `wlan antenna type`, see `wlan antenna type` (Page 235).
3. Switch on the WLAN interface with the command `no shutdown`, see `no shutdown` (Page 98).

8.1.5.13 wlan background scan interval (client)

Description

With this command, you specify the Interval at which the client scans for further access points.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan background scan interval <ms(300-60000)>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`ms`	Time in milliseconds (ms)	300 ... 60 000 Default: 5000

Result

The interval is specified.

Additional notes

You show the set interval with the `show wlan client <wlan 0/X>` command.

8.1.5.14 wlan background scan mode (client)

Description

With this command, you specify how the client scans for further access points.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan background scan mode { disable | always }
```

The parameters have the following meaning:

Parameters	Description
`disable`	As long as the client is connected, it does not scan for any other access points.
`always`	Continuous scanning for further access points. With the command, "`wlan background scan interval`" you specify the Interval at which the client scans for further access points.

Result

Scanning for further access points is specified.

Additional notes

You display the setting with the `show wlan client <wlan 0/X>` command.

8.1.5.15 wlan background scan threshold (Client)

Description

With this command, you specify the threshold value. If the threshold is undershot, the client searches for further access points.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan background scan threshold <dBm(-95-0)>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`ms`	Threshold value in decibel-milliwatts (dBm)	-95 ... 0

Result

The threshold value is specified.

Additional notes

You display the setting with the `show wlan client <wlan 0/X>` command.

Note

Set a higher background scan threshold

Enter a somewhat higher value for the threshold than the signal strength at which the client starts scanning.

Example: Roaming should take place at under -65 dBm. In this case, enter -63 dBm for the threshold.

8.1.5.16 wlan beacon interval (Access Point)

Description

With this command, you specify the interval at which the SCALANCE W device sends beacons. Beacons are packets that are sent cyclically by an access point to inform clients of its existence.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan beacon interval <ms (40-1000)>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`ms`	Length of the interval in milliseconds (ms).	40 ... 1000 Default: 100

Result

The interval is specified.

Additional notes

You show the set interval with the `show wlan advanced <wlan 0/X>` command.

8.1.5.17 wlan channel (Access Point)

Description

With this command, you specify the channel via which the access point communicates with the client.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan channel { show-channels | <number(0=auto)> }
```

The parameters have the following meaning:

Parameters	Description	Range of values / note
`show-channels`	Lists the available channels.	--
`number`	Channel number If you want the access point to search for a free channel itself, use "0".	Enter the channel number. Default setting for both frequency bands: 0 = Auto

Result

The channel is set.

Additional notes

You display the setting with the `show wlan ap <wlan 0/X>` command.

See also

show wlan ap (access point) (Page 209)

8.1.5.18 wlan channel width (Access Point)

Description

With this command, you specify the channel bandwidth for IEEE 802.11n/ac/ax.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan channel width { twenty | forty | eighty }
```

The parameters have the following meaning:

Parameters	Description
`twenty`	Channel bandwidth 20 MHz
`forty`	Channel bandwidth 40 MHz.
`eighty`	Only with IEEE 802.11 ac/ax Channel bandwidth 80 MHz

Result

The channel bandwidth is set.

Further notes

You display the setting with the `show wlan ap <wlan 0/X>` command.

See also

show wlan ap (access point) (Page 209)

8.1.5.19 wlan client mac mode (client)

Description

With this command, you specify how the MAC address is assigned to the client. This MAC address is used by the client for communication with the access point.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan client mac mode { own | l2t }
```

The parameters have the following meaning:

Parameters	Description
`own`	The client uses the MAC address of the Ethernet interface for the WLAN interface.
`l2t`	The L2T parameter activates layer 2 tunneling. The client uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected to the Ethernet interface of the client

Result

The MAC address was assigned to the client.

Additional notes

You display the setting with the `show wlan client <wlan 0/X>` command.

Note

Roaming

For problem-free roaming of the client between the access points, it is important not to block LLC (Link Layer Control) frames in the wired network. The LLC frames are used to update the FDB (Forwarding Database) table on the network devices.

8.1.5.20 wlan dfs

Description

With this command, you enable the "DFS(802.11h)" function. If the access point discovers a disruption on the current channel, for example due to a radar device, it automatically switches to an alternative channel.

Requirement

- Frequency band 5 GHz is used.

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameter assignment:

```
wlan dfs
```

Result

The DFS function is enabled.

Further notes

You display the setting with the `show wlan basic <wlan 0/X>` command.

You disable the function with the `no wlan dfs` command (default setting).

8.1.5.21 no wlan dfs

Description

With this command, you disable the "DFS" function. This setting is activated as default.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameter assignment:

```
no wlan dfs
```

Result

The DFS function is enabled.

Further notes

You display the setting with the `show wlan basic <wlan 0/X>` command.

You enable the function with the `wlan dfs` command.

8.1.5.22 wlan frequency band

Description

With this command, you specify the frequency band for the WLAN interface.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan frequency band { 2.4 | 5 }
```

The parameters have the following meaning:

Parameters	Description	Range of values/note
2.4	Frequency band 2.4 GHz	Default setting: WLAN1: 2.4 GHz
5	Frequency band 5.2 (4.9; 5.6; 5.8) GHz	Default setting: WLAN2: 5 GHz

Result

The frequency band for the WLAN interface is specified.

Further notes

You display the setting with the `show wlan basic <wlan 0/X>` command.

See also

show wlan basic (Page 211)

8.1.5.23 wlan hw-retries

Description

With this command, you specify the number of retries. The hardware repetition is performed by the WLAN chip itself when it tries to repeat an unacknowledged packet immediately.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan hw-retries <1-32>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
1-32	Number of retries	1 ... 32 Default: 16

Result

The number of retries is specified.

Further notes

You display the setting with the `show wlan advanced <wlan 0/X>` command.

8.1.5.24 wlan max tx-power

Description

You can use this command to set the value for the transmit power per antenna port.

Note

The maximum possible transmit power varies depending on the channel and data rate. For more detailed information on transmit power, refer to the documentation "Characteristics radio interface".

Using the `show wlan antennas` command, check whether or not the current WLAN settings violate the permitted transmit power restrictions (`TX Power Check`) of the selected country.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan max tx-power <dBm(1-20)>
```

The parameter has the following meaning:

Parameters	Description	Range of values/note
dBm	Transmit power in decibel-milliwatts (dBm)	1...2 Default: 20

Result

The transmit power is specified.

Further notes

You display the setting with the `show wlan antennas <wlan 0/X>` command.

See also

show wlan basic (Page 211)

8.1.5.25 wlan mode

Description

With this command, you specify the transmission standard.

Requirement

You are in interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan mode { show-modes | [2.4 | 5] <mode> }
```

The parameter has the following meaning:

Parameters	Description	Range of values/note
`show-modes`	Lists the transmission standards.	--
2.4	Optional. You can use the parameter in conjunction with "auto" and "n" or "ax". This only takes into account the transmission standard for 2.4 GHz. Use the parameter if the client operates in dual-frequency mode.	--
5	Optional. You can use the parameter in conjunction with "auto" and "n" or "ax". This only takes into account the transmission standard for 5 GHz. Use the parameter if the client operates in dual-frequency mode.	--
`mode`	Value corresponding to a specific transmission standard.	• `a` IEEE 802.11a (5 GHz) • `g` IEEE 802.11g (2.4 GHz) Is downwards compatible with IEEE 802.11b • `n` IEEE 802.11n (2.4 GHz + 5 GHz) Is downwards compatible with IEEE 802.11a and IEEE 802.11g • `ac` IEEE 802.11ac (5 GHz) • `ax` IEEE 802.11ax (2.4 GHz + 5 GHz) • `auto` (in client mode only) The transmission standard is determined automatically (2.4 GHz and 5 GHz).

Depending on the current configuration, some settings are not possible. In this case, a message to this effect is displayed.

If the transmission standard is changed from the `ax` value to another value, the enabled iPCF-2 mode is disabled. A message to this effect is displayed.

Result

The transmission standard is specified.

Additional notes

You display the setting with the `show wlan basic <wlan 0/X>` command.

8.1.5.26 wlan outdoor

Description

With this command, you enable the outdoor mode. In outdoor mode, the selection of country-dependent channels and the transmit power for operation are restricted for outdoor use.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameter assignment:

```
wlan outdoor
```

Result

The outdoor mode is enabled.

Further notes

You display the setting with the `show wlan basic <wlan 0/X>` command.

You disable the function with the `no wlan outdoor` command (default setting).

See also

show wlan basic (Page 211)

no wlan outdoor (Page 247)

8.1.5.27 no wlan outdoor

Description

With this command, you disable the outdoor mode or enable the indoor mode. This setting is activated as default.

In indoor mode, all the country-dependent permitted channels and transmit power settings are available for operation in a building.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call the command without parameter assignment:

```
no wlan outdoor
```

Result

The indoor mode is enabled or the outdoor mode is disabled.

Further notes

You display the setting with the `show wlan basic <wlan 0/X>` command.

You enable the outdoor mode with the `wlan outdoor` command.

See also

wlan outdoor (Page 247)

8.1.5.28 wlan overlap-ap aging

Description

With this command, you configure the aging time for the list of overlapping access points. If an access point is inactive for longer than the set time, it is removed from the list.

Requirement

You are in the Interface Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan overlap-ap aging <min(1-7200)>
```

The parameter has the following meaning:

Parameters	Description	Range of values/note
`min`	Time in minutes (min)	1...7200 Default: 120

Result

The aging time is specified.

Further notes

You display the setting with the `show wlan advanced <wlan 0/X>` command.

8.1.5.29 wlan scan-time-per-channel (Client)

Description

You define the scan time per channel with this command. There are three pre-defined settings for the scan time.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan scan-time-per-channel {short|medium|long}
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
--	Time in milliseconds (ms)	• `short` Active scan time: 50 ms, passive scan time: 90 ms • `medium` Active scan time: 200 ms, passive scan time: 300 ms • `long` Active scan time: 300 ms, passive scan time: 800 ms You need to adapt the beacon interval accordingly on the access point. The beacon interval should be no more than half of the passive scan time.

Result

The scan time is fixed.

Additional notes

You show the set interval with the `show wlan client <wlan 0/X>` command.

You configure the beacon interval with the `wlan beacon interval` command.

8.1.5.30 wlan ssid-table edit (client)

Description

With this command, you change or delete an entry in the SSID list.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan ssid-table edit <index> {enable | disable| delete} [ssid]
```

The parameters have the following meaning:

Parameters	Description	Range of values / note
`index`	Index entry in the SSID list	1
`enable`	Entry is used	--
`disable`	Entry is not used	Default
`delete`	Entry is deleted. The `ssid` parameter is ignored.	--
`ssid`	SSID	Enter the SSID of the access point. The length of the character string for SSID is 1 to 32 characters. ASCII code 0x20 to 0x7e is used for the SSID. To be able to use spaces in the SSID, enter the SSID in quotes: `wlan ssid-table edit "H a l l o"`

Result

The corresponding index entry in the SSID list is changed or deleted.

Additional notes

You display the list with the `show wlan ssid-table <wlan 0/X>` command.

You delete an SSID entry with the `wlan ssid-table edit <index (1-8)> delete` command.

8.1.6 Commands in the VAP Interface Configuration mode

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

In the Global Configuration mode, enter the `interface vapX 0/Y` command to change to this mode.

- If you exit the VAP Interface configuration mode with the `exit` command, you return to the global configuration mode.
- If you exit the VAP Interface 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 VAP Interface configuration mode.

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

Note

All commands in this section are only available in access point mode.

8.1.6.1 vap ssid (access point)

Description

With this command, you configure the SSID for the relevant VAP interface.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call up the command with the following parameters:

```
vap ssid <ssid>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`ssid`	SSID of the VAP interface	Enter the SSID. The length of the character string for SSID is 1 to 32 characters. ASCII code 0x20 to 0x7e is used for the SSID. To be able to use spaces in the SSID, enter the SSID in quotes: `vap ssid "H a l l o"`

Result

The SSID for the VAP interface is configured.

Additional notes

You display the setting with the `show wlan vap <vapX 0/Y>` command.

8.1.6.2 vap broadcast ssid (access point)

Description

With this command, you enable the "Broadcast SSID" function. The SSID is sent in the frame of the access point and is visible for other SCALANCE W devices.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call the command without parameter assignment:

```
vap broadcast ssid
```

Result

The function is enabled.

Additional notes

You display the setting with the `show wlan vap <vapX 0/Y>` command.

You disable the function with the `no vap broadcast ssid` command.

See also

no vap broadcast ssid (access point) (Page 253)

8.1.6.3 no vap broadcast ssid (access point)

Description

With this command, you disable the "Broadcast SSID" function. The SSID is no longer sent in the frame of the access point. This means that the SSID is not visible for other SCALANCE W devices. Only stations that know the SSID of the access point and that are configured with it can connect to the access point.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call the command without parameter assignment:

```
no vap broadcast ssid
```

Result

The function is disabled.

Additional notes

You display the setting with the `show wlan vap <vapX 0/Y>` command.

You enable the function with the `vap broadcast ssid` command (default setting).

See also

vap broadcast ssid (access point) (Page 252)

8.2 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.

8.2.1 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.

8.2.1.1 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 "Interface identifiers and addresses (Page 45)".

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.

8.2.1.2 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.

8.2.1.3 show mac-address-table dynamic unicast

Description

This command shows the MAC addresses of the dynamic unicast configuration.

Requirement

- In "base bridge-mode", the mode for the device is set to "transparent".

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 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 or VLAN range	-
`vlan-range`	Number of the addressed VLAN or VLAN range	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 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 "Interface identifiers and addresses (Page 45)".

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

Result

The entries are displayed.

8.2.1.4 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	-
`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.

8.2.1.5 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.

8.2.1.6 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.

8.2.1.7 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 "Interface identifiers and addresses (Page 45)".

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.

8.2.2 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.

8.2.2.1 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 "Interface identifiers and addresses (Page 45)".

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

Result

The entries are displayed.

8.2.2.2 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.

8.2.3 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.

8.2.3.1 vlan

Description

With this command, you create a VLAN on the device and change to the VLAN configuration mode.

Note

The device supports up to 24 virtual networks.

In the provider backbone bridge mode, this command is used to create user, service and backbone 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 <vlan-id(1-4094)>
```

The parameter has the following meaning:

Parameters	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

The VLAN is created.

You are now in the VLAN configuration mode.

The command prompt is as follows:

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

Further notes

You delete the VLAN with the `no vlan` command.

You configure the mode with the `base bridge-mode` command.

You can display information about the VLAN with the `show vlan` command.

8.2.3.2 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.

8.2.3.3 base bridge-mode

Description

With this command, you configure whether or not the device is configured as a bridge according to IEEE 802.1D for the Spanning Tree protocol or according to IEEE 802.1Q for a virtual bridged LAN.

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:

```
base bridge-mode {dot1d-bridge|dot1q-vlan}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`dot1d-bridge`	Sets the mode of the device to "transparent" for the Spanning Tree protocol.	Default setting
`dot1q-vlan`	sets the mode of the device to "VLAN-aware" for a virtual bridged LAN.	-

Result

The device mode is configured.

Further notes

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

8.2.4 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.

8.2.4.1 mtu

Description

With this command, you configure the size of the Maximum Transmission Unit (MTU) for a VLAN interface.

Requirement

- The Interface must be shut down.
- You are in interface configuration mode.
- The command prompt is as follows:
  `cli(config-if-$$$)#`

Syntax

Call up the command with the following parameters:

```
mtu <frame-size(64-1514)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`frame-size`	Size of the MTU in bytes	• 64 ... 1514 • With IPv4: 90 ... 1514 • With IPv6: 1280 ... 1514 Default: 1500

Result

The setting for the size of the MTU is configured.

Additional notes

You shut down the interface with the `shutdown complete` command.

You display this setting with the `show interface mtu` command.

You display this setting and other information with the `show interfaces` command.

8.2.4.2 shutdown complete

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 the command without parameters:

```
shutdown complete
```

Result

The Interface is shut down. A connection continues to be indicated if a switch port is turned off. The LED for the port status flashes 3 times cyclically. 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.

8.2.4.3 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.

8.2.4.4 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.	-
`untaggedAndPriori tytagged`	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.

8.2.4.5 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.

8.2.4.6 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.

8.2.4.7 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.

8.2.4.8 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.

8.2.4.9 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.

8.2.4.10 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 { trunk | hybrid }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`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.

8.2.4.11 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.

8.2.4.12 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.

8.2.4.13 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.

8.2.4.14 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.

8.2.4.15 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.

8.2.4.16 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.

8.2.5 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.

8.2.5.1 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.

8.2.5.2 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`.

8.2.5.3 ports

Description

With this command, you generate a static VLAN entry that specifies the use of the ports. Here, you configure the following types of ports:

- Member ports (tagged ports)
  These ports are permanently added to the list of outgoing connections
- Untagged ports
  These ports transfer data packets without a VLAN marking
- Forbidden ports
  These ports are not used for communication in a VLAN

The tagged and untagged ports specified 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,...>]
     )
    [
     untagged<interface-type> <0/a-b,0/c,...>
     (
      [<interface-type> <0/a-b,0/c,...>]     [all]
     )
    ]
    [
     forbidden<interface-type> <0/a-b,0/c,...>
     [<interface-type> <0/a-b,0/c,...>]
        ]
    [name<vlan-name>]
```

The parameters have the following meaning:

Parameters	Description	Range of values / note
`interface-type`	Type or speed of the interface	• `gigabitethernet`
`/a-b,0/c,...`	Port no. of the interface	Enter a valid interface name
`/a-b,0/c,...`	Port no. of the interface	Enter a valid interface name

Parameters	Description	Range of values / note
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 "Interface identifiers and addresses (Page 45)".

Result

The settings are enabled.

Additional notes

You display details of the function with the `show vlan` command.

You reset the settings with the `no ports` command.

8.2.5.4 no ports

Description

With this command, you reset the ports for a 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:

```
no ports
    [<interface-type> <0/a-b,0/c,...>]
    [<interface-type> <0/a-b,0/c,...>]    [all]
   [
    untagged ([<interface-type> <0/a-b,0/c,...>]
              [<interface-type> <0/a-b,0/c,...>]     [all])
   ]
   [
    forbidden ([<interface-type> <0/a-b,0/c,...>
               [<interface-type> <0/a-b,0/c,...>]     [all])
```

```
]
[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	
`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 identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The ports are reset.

Further notes

You display details of the function with the `show vlan` command.

You reset the setting with the `no ports` command.

8.3 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.

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.

Example

You are in the global configuration mode and you want to execute the `show spanning-tree active` command from the Privileged EXEC mode.

```
cli(config)# do show spanning-tree active
```

8.3.1.1 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`

8.3.1.2 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.

8.3.1.3 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.

8.3.1.4 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.

8.3.1.5 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 "Interface identifiers and addresses (Page 45)".

Result

The settings of the ports for the spanning tree function are displayed.

8.3.1.6 show spanning-tree l2t-edge

Description

This command displays the status of the layer 2 tunnel ports.

Note

This command is available only in access point 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 parameter assignment:

```
show spanning-tree l2t-edge
```

Result

The status of the layer 2 tunnel ports is displayed.

8.3.1.7 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.

8.3.1.8 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.

8.3.1.9 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 identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The settings are displayed.

Further notes

You display the general settings for the Spanning Tree Protocol with the `show spanning-tree` command.

8.3.1.10 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
`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.

8.3.2 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.

8.3.3 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.

8.3.3.1 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

You are in 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.

Further notes

As default the function is "enabled".

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.

8.3.3.2 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.

8.3.3.3 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 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

You can reset the setting to the default `mst` with the `no spanning-tree compatibility` 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.

8.3.3.4 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 MST.

Requirement

You are in 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.

8.3.3.5 spanning-tree l2t-auto-edge

Description

This command specifies that at all layer 2 tunnel ports it should be automatically detected whether or not an end device is connected.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
spanning-tree l2t-auto-edge
```

Result

The automatic detection is enabled.

Further notes

You disable the automatic detection with the `no spanning-tree l2t-auto-edge` command.

You can display the status of this function with the `show spanning-tree l2t-edge`command.

8.3.3.6 no spanning-tree l2t-auto-edge

Description

With this command, you disable automatic detection of an end device at layer 2 tunnel ports.

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 l2t-auto-edge
```

Result

The automatic discovery of a bridge on the interface is disabled.

Further notes

You enable the automatic detection with the `spanning-tree l2t-auto-edge` command.

You can display the status of this function with the `show spanning-tree l2t-edge`command.

8.3.3.7 spanning-tree l2t-edge

Description

With this command, you specify that an end device can be located at a layer 2 tunnel port. Otherwise a reconfiguration of the network will be triggered whenever a link to this port is modified. The L2T clients should be interconnected.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
spanning-tree l2t-edge
```

Result

The setting is enabled.

Further notes

You disable the setting with the `no spanning-tree l2t-edge` command.

You can display the status of this function with the `show spanning-tree l2t-edge`command.

8.3.3.8 no spanning-tree l2t-edge

Description

With this command, you disable the setting that an end device may be located at a layer 2 tunnel port.

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 l2t-edge
```

Result

The setting is disabled.

Further notes

The automatic discovery of a bridge on the interface is disabled with the `spanning-tree l2t-edge` command.

You can display the status of this function with the `show spanning-tree l2t-edge`command.

8.3.3.9 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.

8.3.3.10 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 ....`

8.3.3.11 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 ...`.

8.3.3.12 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.

8.3.3.13 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.

8.3.3.14 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 up 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.

8.3.3.15 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 up 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.

8.3.3.16 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 ...`.

8.3.3.17 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 ....`

8.3.3.18 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 ...`.

8.3.4 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.

8.3.4.1 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 ...`.

8.3.4.2 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 ...`.

8.3.4.3 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.

8.3.4.4 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.

8.3.4.5 spanning-tree bdpufilter

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.

8.3.4.6 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.

8.3.4.7 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.

8.3.4.8 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.	0 ... 200000000 Default: • 200000 for physical interfaces • 199999 for port channels
`port-priority`	Priority of the interface	0 ... 240 in increments of 16 Default: 128
`disable`	disables the interface for multiple spanning tree	- Default: The Multiple Spanning Tree function is enabled on 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 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 ...`.

8.3.4.9 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`	The Multiple Spanning Tree function is enabled on 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:

```
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 ...`.

8.3.4.10 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 ...`.

8.3.4.11 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 ...`.

8.3.5 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.

Requirements for changing to this mode:

- MSTP is enabled
- Base bridge mode: 802.1Q VLAN Bridge
- Compatibility mode: MSTP

8.3.5.1 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.

8.3.5.2 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.

8.3.5.3 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.

8.3.5.4 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.

8.3.5.5 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.

8.3.5.6 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.

Network protocols

9

This part contains the sections that describe the commands for working with the various network protocols.

9.1 IPv4 protocol

This section describes commands of the Internet Protocol (IP) version 4.

9.1.1 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.

9.1.1.1 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 "Interface identifiers and addresses (Page 45)".

Result

The overview of the DCP forwarding behavior is displayed.

9.1.1.2 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.

9.1.1.3 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.

9.1.1.4 show ip route

Description

This command shows the routes currently being used.

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 route [ { <ip-address> [<mask>] | connected | static |
dhcp } ]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ip-address`	Shows the information for a specific IP address	Enter a valid IP address
`mask`	Defines an address range using the sub-net mask	/8, /16 or /24
`connected`	Shows the direct connections	-
`static`	Shows the static connections	-
`dhcp`	Shows the DHCP routes.	

Result

The routing table is displayed.

9.1.1.5 show ip static route

Description

This command shows the routes that were generated statically.

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 static route
```

Result

The static routes are displayed.

9.1.1.6 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.

9.1.2 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.

9.1.2.1 dcp server

Description

With this command, you 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}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`read-only`	only reading is permitted on the DCP server	-
`read-write`	reading and writing is permitted on the DPC server	Default: `read-write`

Result

The read and write permissions for the DPC server are configured.

The DCP server is enabled.

Further notes

You disable the DCP server with the `no dcp server` command.

9.1.2.2 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.

9.1.2.3 ip route

Description

With this command, you configure a static entry in the IPv4 routing table.

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 route <prefix> <mask> <next-hop> [<distance(1-255)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`prefix`	IP address or address range	Enter a valid IPv4 address
`mask`	Subnet mask that is applied to `prefix`.	Enter a valid subnet mask. Use the decimal notation.
`next-hop`	IP address to which the selected addresses will be forwarded.	Enter a valid IPv4 address
`distance`	Value for the administrative distance	1 ... 255 Note: When you change the value to 255 with an active route, the route is deleted.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The entry in the IP routing table is configured.

Additional notes

You delete an entry from the IPv4 routing table with the `no ip route` command.

You display the IPv4 routing table with the `show ip route` command.

You display the static routes with the `show ip static route` command.

9.1.2.4 no ip route

Description

With this command, you delete a static entry from the IPv4 routing table.

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 ip route <prefix> <mask> <next-hop>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`prefix`	IP address or address range	Enter a valid IPv4 address
`mask`	Subnet mask that is applied to `prefix`.	Enter a valid subnet mask. Use the decimal notation.
`next-hop`	IP address to which the selected addresses were forwarded	Enter a valid IPv4 address

Result

The entry is deleted.

Additional notes

You delete an entry from the IPv4 routing table with the `no ip route` command.

You display the IPv4 routing table with the `show ip route` command.

You display the static routes with the `show ip static route` command.

9.1.2.5 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.

9.1.2.6 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.

9.1.2.7 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 (Page 29)".

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.

9.1.2.8 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

9.1.3 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.

9.1.3.1 ip address

Description

With this command, you assign an IPv4 address or an IPv4 subnet to the interface.

Requirement

- DHCP was disabled with the `no ip address` command.
- 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 parameters have the following meaning:

Parameter	Description	Range of values/note
`ip-address`	IPv4 address for the Interface	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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The IPv4 address is assigned to the VLAN interface.

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!

Additional notes

You delete the IPv4 address with the `no ip address` command.

You display this setting and other information with the `show ip interface` command.

9.1.3.2 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.

9.1.3.3 no ip address

Description

With this command, you delete the assignment of an IPv4 address to an interface 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 without parameters or with the following parameter assignment:

```
no ip address [<ip-address> | dhcp]
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`ip-address`	IPv4 address of the interface that will be deleted	Enter a valid IPv4 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 "Interface identifiers and addresses (Page 45)".

Result

If DHCP was enabled on this interface, DHCP is now disabled. Any existing dynamically learned IPv4 address will be automatically converted to a static IPv4 address.

If static IPv4 addresses were configured and if no explicit IPv4 address was transferred as a parameter, all static IPv4 addresses will be deleted from this interface.

If a static IPv4 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 configure the static IPv4 address with the `ip address` command.
You display this setting and other information with the `show ip interface` command.
You enable DHCP with the `ip address dhcp` command.

9.1.3.4 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.

9.2 IPv6 protocol

This section describes the commands relevant for working with IPv6.

9.2.1 Configuration matrix

Address configuration in WBM (Layer 3 (IPv6) > Subnets)	CLI commands		
	ipv6 address autoconfig	ipv6 address dhcp	ipv6 address
DHCPv6	-	x	-
SLAAC (Default)	x	-	-
Static	-	-	x

9.2.2 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.

9.2.2.1 show ipv6 interface

Description

This command shows the configuration of one, several or all IPv6 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 ipv6 interface [{vlan <vlan-id (1-4094)> | <interface-type>
<if-num>} [prefix]]
```

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
`if-num`	Module no. and port no. of the interface	
`prefix`	Shows the prefix information of the IPv6 interface	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

If you do not select any parameter from the parameter list, the configuration is displayed for all available IPv6 interfaces.

Result

The configuration is displayed.

Additional notes

You activate IPv6 to the VLAN or on the router with the command `ipv6 enable`.

You configure an IPv6 address with the `ipv6 address` command.

9.2.2.2 show ipv6 neighbors

Description

This command shows IPv6 neighbors table. The table contains the unique assignment of MAC address to IPv6 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 without parameter assignment:

```
show ipv6 neighbors
```

Result

The IPv6 neighbors table is displayed.

Further notes

You configure a static entry with the `ipv6 neighbor` command.

9.2.2.3 show ipv6 pmtu

Description

This command shows the settings for Path MTU.

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 ipv6 pmtu
```

Result

The settings are displayed.

9.2.2.4 show ipv6 route

Description

This command shows the routes currently being used.

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 ipv6 route
```

Result

The IPv6 routing table is displayed.

Further notes

You configure a static entry with the `ipv6 route` command.

9.2.2.5 show ipv6 static route

Description

This command shows the routes that were generated statically.

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 ipv6 static route
```

Result

The static routes are displayed.

9.2.2.6 show ipv6 traffic

Description

This command shows the statistics for UDP and ICMPv6 for the corresponding 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 ipv6 traffic [interface {vlan <vlan-id (1-4094)> | <interface-type> <interface-id>}] [hc]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface`	Keyword for the interface via which the statistics are created. • VLAN • Interface	-
`vlan`	Keyword for a VLAN	-
`vlan-id`	Keyword for a VLAN connection	1 ... 4094
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`hc`	Display of the High counters parameter	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

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

Result

The statistics are displayed.

Further notes

You reset the counters to zero with the `clear ipv6 traffic` command.

9.2.3 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.

9.2.3.1 ipv6 neighbor

Description

With this command, you configure a static entry in the IPv6 neighbors table.

Requirement

- The neighbor node is located on the same link.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call up the command with the following parameters:

```
ipv6 neighbor <prefix>
    {vlan <vlan-id (1-4094)> | [<interface-type> <interface-id>]}
    <MAC ADDRESS xx:xx:xx:xx:xx:xx>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`prefix`	IPv6 address of the neighbor node	Enter a valid IPv6 address.
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`MAC ADDRESS`	Link layer address (MAC address) of the neighbor node	`xx:xx:xx:xx:xx:xx`

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The entry is configured.

Additional notes

You delete an entry with the `no ipv6 neighbor` command.

You display the IPv6 neighbor table with the `show ipv6 neighbors` command.

9.2.3.2 no ipv6 neighbor

Description

With this command, you delete an entry from the IPv6 neighbor table.

Requirement

- The neighbor node is located on the same link.
- You are in global configuration mode.
  The command prompt is as follows:
  `cli(config)#`

Syntax

Call up the command with the following parameters:

```
no ipv6 neighbor <prefix>
   {vlan <vlan-id (1-4094)> | [<interface-type> <interface-id>]}
   <MAC ADDRESS xx:xx:xx:xx:xx:xx>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`prefix`	IPv6 address of the neighbor node	Enter a valid IPv6 address.
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`interface-type`	Type or speed of the interface	Specify a valid interface.
`interface-id`	Module no. and port no. of the interface	
`MAC ADDRESS`	Link layer address (MAC address) of the neighbor node	xx:xx:xx:xx:xx:xx

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The entry is deleted.

Additional notes

You configure an entry with the `no ipv6 neighbor` command.

You display the IPv6 neighbor table with the `show ipv6 neighbors` command.

9.2.3.3 ipv6 path mtu

Description

With this command, you configure maximum packet size (MTU). The setting is only effective if PMTU Discovery 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:

```
ipv6 path mtu <prefix addr> <mtu>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`prefix addr`	IPv6 address of the recipient	Enter a valid IPv6 address
`mtu`	Size in bytes	1280 ... 9194 Default: 1500

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The maximum packet size is configured.

Additional notes

You display the configuration with the `show ipv6 pmtu` command.

You disable the maximum packet size with the `no ipv6 path mtu` command.

You enable the PMTU Discovery function with the command `ipv6 path mtu discovery`.

9.2.3.4 no ipv6 path mtu

Description

With this command, you disable the use of the maximum package size. This means the setting is no longer used with the PMTU Discovery (PMTUD) technique.

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 ipv6 path mtu <prefix addr>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`prefix addr`	IPv6 address of the recipient	Enter a valid IPv6 address

Result

The setting for the maximum packet size is no longer used.

Further notes

You display the configuration with the `show ipv6 pmtu` command.

You configure the maximum packet size with the `ipv6 path mtu` command.

9.2.3.5 ipv6 path mtu discover

Description

With this command, you enable the PMTU Discovery function. The function automatically determines the optimum packet size along the path.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
ipv6 path mtu discover
```

Result

The PMTU Discovery function is enabled.

Further notes

You disable the PMTU Discovery function with the command `no ipv6 path mtu discover`.

You display the settings with the `show ipv6 pmtu` command.

9.2.3.6 no ipv6 path mtu discover

Description

With this command, you disable the PMTU Discovery function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ipv6 path mtu discover
```

Result

The PMTU Discovery function is disabled.

Further notes

You enable the PMTU Discovery function with the command `ipv6 path mtu discover`.

You display the settings with the `show ipv6 pmtu` command.

9.2.3.7 ipv6 route

Description

With this command, you configure a static entry in the IPv6 routing table.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ipv6 route <prefix> <prefix len> {<NextHop> [vlan <vlan-id
(1-4094)>] [<metric>]}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`prefix`	IPv6 address	Enter a valid IPv6 address.
`prefix len`	Number of bits belonging to the prefix (from left to right)	1 ... 128 bits 128: The node (host) itself
`NextHop`	IPv6 address to which the selected addresses will be forwarded	Enter a valid IPv6 address.
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`metric`	Value for the metric	0 ... 65535 Default: 1

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The entry is configured.

Additional notes

You delete a static entry from the IPv6 routing table with the `no ipv6 route` command.

You display the IPv6 routing table with the `show ipv6 route` command.

9.2.3.8 no ipv6 route

Description

With this command, you delete a static entry from the IPv6 routing table.

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 ipv6 route <prefix> <prefix len> [<NextHop>] {[vlan <vlan-id
(1-4094)> ] [<metric>]}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`prefix`	IPv6 address of the recipient	Enter a valid IPv6 address.
`prefix len`	Number of bits belonging to the prefix (from left to right)	1 ... 128 bits 128: The node (host) itself
`NextHop`	IPv6 address to which the selected addresses will be forwarded.	Enter a valid IPv6 address.
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`metric`	The value for the metric	0 ... 65535 Default: 1

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The entry is deleted.

Additional notes

You configure a static entry in the IPv6 routing table with the `ipv6 route` command.

You display the IPv6 routing table with the `show ipv6 route` command.

9.2.4 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.

9.2.4.1 ipv6 address

Description

With these commands, you assign an IPv6 address to the IPv6 interface.

Requirement

- IPv6 is activated
- The interface is an IP interface.
- 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:

```
ipv6 address <prefix> <prefix-length> [{unicast | eui64}
```

or

```
ipv6 address <prefix/prefix-length> [{unicast | eui-64| link-local}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`prefix`	IPv6 address	Enter a valid IPv6 address
`prefix-length`	Number of bits belonging to the prefix (from left to right)	1 ... 128 bits
`unicast`	Addressing mode unicast	-
`eui-64`	Interface ID according to the EUI-64 method	-
`link-local`	Link local address	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The IPv6 address is assigned to the interface. If you assign a link local address to the IP interface, the automatically created local address is overwritten.

Further notes

You delete the IPv6 address with the `no ipv6 address` command.

You enable IPv6 with the `ipv6 enable` command.

You display this setting and other information with the `show ipv6 interface` command.

You enable stateless autoconfiguration with the command `ipv6 address autoconfig`.

You enable stateful autoconfiguration with the command `ipv6 address dhcp`.

9.2.4.2 no ipv6 address

Description

With this command, you delete the IPv6 address.

Requirement

- IPv6 is activated
- The interface is an IP interface.
- 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 ipv6 address <prefix> <prefix-length> [{unicast | eui64}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`prefix`	IPv6 address	Enter a valid IPv6 address.
`prefix-length`	Number of bits belonging to the prefix (from left to right)	1 ... 128 bits
`unicast`	Addressing mode unicast	-
`eui-64`	Interface ID according to the EUI-64 method	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The IPv6 address has been deleted.

Further notes

You configure the IPv6 address with the `ipv6 address` command.

You display this setting and other information with the `show ipv6 interface` command.

9.2.4.3 ipv6 address autoconfig

Description

With this command you enable stateless autoconfiguration of the IPv6 address via NDP (Neighbor Discovery Protocol).

Requirement

- IPv6 is activated
- The interface is an IP interface.
- You are in the Interface configuration mode
  The command prompt is as follows:
  `cli(config-if-$$)#`

Syntax

Call the command without parameter assignment:

```
ipv6 address autoconfig
```

Result

Stateless autoconfiguration is enabled.

Further notes

You disable the setting with the `no ipv6 address autoconfig` command.

You show the setting with the `show ipv6 dhcp interface` command.

You can display the statistics of the DHCPv6 client with the `show ipv6 dhcp client statistics` command.

9.2.4.4 no ipv6 address autoconfig

Description

With this command you disable stateless autoconfiguration of the IPv6 address via NDP (Neighbor Discovery Protocol).

Requirement

- IPv6 is activated
- The interface is an IP 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 ipv6 address autoconfig
```

Result

Stateless autoconfiguration is disabled.

Further notes

You enable the setting with the `ipv6 address autoconfig` command.

You show the setting with the `show ipv6 dhcp interface` command.

You can display the statistics of the DHCPv6 client with the `show ipv6 dhcp client statistics` command.

9.2.4.5 ipv6 address dhcp

Description

With this command, you specify whether the DHCPv6 client obtains the IPv6 address from the DHCPv6 server.

Requirement

- IPv6 is activated
- The interface is an IP interface.
- 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:

```
ipv6 address dhcp [rapid-commit]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`rapid-commit`	Reduces the procedure of 4 DHCPv6 messages (SOLICIT, ADVERTISE, REQUEST, REPLY) to 2 DHCPv6 messages (SOLICIT, REPLY). This is only possible when the DHCPv6 server supports this.	-

Result

The setting is configured.

Further notes

You disable the setting with the `no ipv6 address dhcp` command.

You show the setting with the `show ipv6 dhcp interface` command.

You can display the statistics of the DHCPv6 client with the `show ipv6 dhcp client statistics` command.

9.2.4.6 no ipv6 address dhcp

Description

With this command, you delete the IPv6 address and disable DHCPv6.

Requirement

- IPv6 is activated
- The interface is an IP 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 ipv6 address dhcp
```

Result

DHCPv6 is disabled.

Further notes

You enable DHCPv6 with the `ipv6 address dhcp` command.

You configure the interface as a router port with the `no switchport` command.

You show the setting with the `show ipv6 dhcp interface` command.

You can display the statistics of the DHCPv6 client with the `show ipv6 dhcp client statistics` command.

9.2.4.7 ipv6 address link-local

Description

With this command, you assign a link local address to the interface.

Requirement

- IPv6 is activated
- The interface is an IP interface.
- 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:

`ipv6 address <prefix> link-local`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`prefix`	Link local address	Specify a valid link local address. fe80::XXXX:XXXX:XXXX:XXXX

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The link local address is assigned to the interface.

Further notes

You delete the link local address with the `no ipv6 address link-local` command.

You display this setting and other information with the `show ipv6 interface` command.

9.2.4.8 no ipv6 address link-local

Description

With this command, you delete the link local address.

Requirement

- IPv6 is activated
- The interface is an IP interface.
- 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 ipv6 address <prefix> link-local`

The parameter has the following meaning:

Parameter	Description	Range of values / note
`prefix`	Link local address	Specify a valid link local address. fe80::xxxx:xxxx:xxxx:xxxx

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The link local address is deleted.

Further notes

You assign a link local address to an IP interface with the command `ipv6 address link-local`.

You display this setting and other information with the `show ipv6 interface` command.

9.2.4.9 ipv6 enable

Description

With this command, you enable IPv6 on the interface. As default, IPv6 is disabled.

Requirement

- IPv6 routing is activated
- The interface is an IP interface.
- You are in the Interface configuration mode
  The command prompt is as follows:
  `cli(config-if-$$)#`

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 parameter assignment:

`ipv6 enable`

Result

IPv6 is enabled.

Further notes

You configure an IPv6 address with the `ipv6 address` command.

You display this setting and other information with the `show ipv6 interface` command.

You enable IPv6 routing with the `ipv6 route` command.

9.2.4.10 no ipv6 enable

Description

With this command, you disable IPv6 on the interface.

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 parameter assignment:

```
no ipv6 enable
```

Result

IPv6 is disabled.

Further notes

You enable IPv6 with the `ipv6 enable` command.

You display this setting and other information with the `show ipv6 interface` command.

9.3 Domain Name System

This section describes commands of the Domain Name System (DNS).

9.3.1 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.

9.3.1.1 show dnsclient information

Description

This command shows the configuration of the DNS client.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show dnsclient information
```

Result

The information is displayed.

9.3.2 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.

9.3.2.1 dnsclient

Description

With this command, you change to the DNS CLIENT configuration mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
dnsclient
```

Result

You are now in the DNS CLIENT configuration mode.

The command prompt is as follows:

```
cli(config-dnsclient)#
```

Further notes

You exit the DNS CLIENT configuration mode with the `end` or `exit` command.

9.3.3 Commands in the DNS CLIENT configuration mode

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

In the Global configuration mode, enter the `dnsclient` command to change to this mode.

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

9.3.3.1 manual srv

Description

With this command, you specify a manually configured DNS server. A maximum of three DNS servers can be configured.

Requirement

You are in the DNS CLIENT configuration mode.

The command prompt is as follows:

```
cli(config-dnsclient)#
```

Syntax

Call up the command with the following parameters:

```
manual srv <ip_addr>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`ip_addr`	IP address	Specify a valid IP address.

Result

The DNS server is configured.

Further notes

You display this setting and other information with the `show dnsclient informationen` command.

You configure the DNS server type with the `server type` command.

You delete the DNS server with the `no manual` command.

9.3.3.2 no manual srv

Description

With this command, you delete a specific DNS server or all DNS servers.

Requirement

You are in the DNS CLIENT configuration mode.

The command prompt is as follows:

```
cli(config-dnsclient)#
```

Syntax

Call up the command with the following parameters:

```
no manual {srv <ip_addr>|all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`srv`	Keyword for DNS server	-
`ip address`	IP address	Specify the IP address of the DNS server.
`all`	Deletes all DNS servers	-

Result

The specified DNS server is deleted.

Further notes

You create a DNS server entry with the `manual srv` command.

You display this setting and other information with the `show dnsclient information` command.

9.3.3.3 server type

Description

With this command, you specify which DNS server the device uses.

Requirement

You are in the DNS CLIENT configuration mode.

The command prompt is as follows:

```
cli(config-dnsclient)#
```

Syntax

Call up the command with the following parameters:

```
server type {all | manual | learned}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`all`	The device uses all available DNS servers.	Default
`manual`	The device uses only the manually configured DNS servers.	-
`learned`	The device uses the DNS servers that are transferred automatically.	-

Result

The device uses the specified DNS servers.

Further notes

You display this setting and other information with the `show dnsclient information` command.

You create a manually configured DNS server with the `manual srv` command.

9.3.3.4 shutdown

Description

With this command, you enable the DNS client.

Requirement

You are in the DNS CLIENT configuration mode.

The command prompt is as follows:

```
cli(config-dnsclient)#
```

Syntax

Call the command without parameter assignment:

```
shutdown
```

Result

The DNS client is disabled.

Further notes

You enable the DNS client with the `no shutdown` command.

You display this setting and other information with the `show dnsclient information` command.

9.3.3.5 no shutdown

Description

With this command, you enable the DNS client of the device. To be able to use the function, a DNS server must be reachable.

Requirement

You are in the DNS CLIENT configuration mode.

The command prompt is as follows:

```
cli(config-dnsclient)#
```

Syntax

Call the command without parameter assignment:

```
no shutdown
```

Result

The DNS client of the device is enabled and when necessary sends queries to the DNS server.

Further notes

You disable the DNS client with the `shutdown` command.

You display this setting and other information with the `show dnsclient information` command.

9.4 DHCPv4 client (IPv4)

This section describes commands of the Dynamic Host Configuration Protocol (DHCP).

9.4.1 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.

9.4.1.1 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.

9.4.1.2 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.

9.4.2 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.

9.4.2.1 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.

9.4.2.2 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.

9.4.2.3 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 up 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`	The client registers with its MAC address	-
`client-id`	The client registers with the assigned ID	-
`client-id`	Name of the assigned ID	max. 32 characters
`sysname`	The client registers with the assigned system name	-
`pnio-name-of-station`	Name of the connected PROFINET device	-

Result

The registration mode of the DHCP client is configured.

9.5 DHCPv6 client (IPv6)

This section describes commands for DHCPv6.

9.5.1 clear ipv6 dhcp client statistics

Description

With this command, you reset the counter to zero on the required interface.

Requirement

- DHCPv6 is enabled.

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
clear ipv6 dhcp client statistics [interface {vlan <VlanId(1-4094)> |<interface-type> <interface-id>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface`	Shows that an interface description follows	-
`vlan`	Keyword for a VLAN connection	-
`VlanId`	Number of the addressed VLAN	1 ... 4094
`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 "Interface identifiers and addresses (Page 45)".

If no parameters are specified, all counters are reset.

Result

The counter is reset.

Additional notes

You enable DHCPv6 with the `ipv6 address dhcp` command.

You display the setting with the `show ipv6 dhcp interface` command.

You display the statistics with the `show ipv6 dhcp client statistics` command.

9.5.2 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.

9.5.2.1 show ipv6 dhcp

Description

This command shows the DHCPv6 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 ipv6 dhcp
```

Result

The configuration is displayed.

9.5.2.2 show ipv6 dhcp interface

Description

This command shows the DHCPv6 configuration and the DHCPv6 information that was received from the DHCPv6 server.

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 ipv6 dhcp 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	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 "Interface identifiers and addresses (Page 45)".

Result

The information is displayed.

9.5.2.3 show ipv6 dhcp client statistics

Description

With this command, you display the statistics of the DHCPv6 client. It provides information about how many PDUs were received or sent per interface.

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 ipv6 dhcp client statistics [interface {vlan <vlan-id(1-4094)>
| <interface-type> <interface-id>} ]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`interface`	Shows that an interface description follows	-
`vlan`	Keyword for a VLAN connection	-
`vlan-id`	Number of the addressed VLAN	1 ... 4094
`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 "Interface identifiers and addresses (Page 45)".

If no parameters are specified, the statistics for all interfaces are displayed.

Result

The statistics are displayed.

Further notes

You can reset the counter to zero with the command `clear ipv6 dhcp client statistics`.

9.6 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".

9.6.1 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.

9.6.1.1 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.

9.6.1.2 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.

9.6.1.3 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.

9.6.1.4 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.

9.6.1.5 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.

9.6.1.6 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.

9.6.1.7 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.

9.6.1.8 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.

9.6.1.9 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.

9.6.1.10 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.

9.6.1.11 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.

9.6.1.12 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.

9.6.2 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.

9.6.2.1 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.

9.6.2.2 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.

9.6.2.3 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.

9.6.2.4 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.

9.6.2.5 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.

9.6.2.6 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.

9.6.2.7 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.

9.6.2.8 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.

9.6.2.9 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.

9.6.2.10 snmp filterprofile

Description

With this command, you configure a filter that describes the access rights to the MIB tree.

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 filterprofile <profile-name> <OIDTree> [mask<OIDMask>]
     {included|excluded}[{volatile|nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`profile-name`	Name of the filter profile	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
-	Specifies whether the filtered elements are used or excluded	• `included` • `excluded`
-	specifies whether the settings remain following a restart:	• `volatile` (volatile): The default settings are used after a restart • `nonvolatile` (non-volatile): The saved settings are used after a restart

Note that the meaning of the filter mask changes depending on the "`included`/`excluded`" parameter:

- ...`0`... and "`included`" means: Access denied
- ...`0`... and "`excluded`" means: Access permitted

- ...1... and "included" means: Access permitted
- ...1... and "excluded" means: Access denied

Result

The filter is created.

Further notes

You delete a filter with the `no snmp filterprofile` command.

You display the created filter with the `show snmp filter` command.

9.6.2.11 no snmp filterprofile

Description

With this command, you delete a filter.

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 filterprofile <profilename> <OIDTree>`

The parameters have the following meaning:

Parameters	Description	Range of values/note
`profilename`	Name of the filter profile	max. 32 characters
`OIDTree`	Object ID	Path information of the MIB tree

Result

The filter is deleted.

Further notes

You create a filter with the `snmp filterprofile` command.

You display the created filter with the `show snmp filter` command.

9.6.2.12 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.

9.6.2.13 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.

9.6.2.14 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.

9.6.2.15 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.

9.6.2.16 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> | ipv6 <IP6-Address> }
```

```
[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 of the trap recipient:	Enter a valid IPv4 unicast address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name) of the trap recipient	Maximum of 100 characters If you have stored a suitable domain name, you can specify a host name.
`ipv6`	Keyword for an IPv6 address	-
`IP6-Address`	IPv6 address of the trap recipient	Enter a valid IPv6 address.
`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".

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.

You store trhe domain name with the `ip domain name` or `domain name` command.

9.6.2.17 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.

9.6.2.18 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.

9.6.2.19 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.

9.6.2.20 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.

9.6.2.21 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.

9.6.2.22 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.

9.6.2.23 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 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)

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 (Page 29)".

Result

The port for the SNMP agent has been changed.

Additional notes

You reset the port to the standard port with the `no snmpagent port` command.

9.6.2.24 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.

9.6.2.25 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.	-

Parameter	Description	Range of values/note
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.

9.6.2.26 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.

9.6.2.27 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

Parameter	Description	Range of values / note
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.

9.6.2.28 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.

9.7 SMTP client

This section describes commands of the Simple Mail Transfer Protocol (SMTP).

9.7.1 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.

9.7.1.1 show events smtp-server

Description

This command shows the configured SMTP 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 SMTP servers are displayed.

9.7.1.2 show events smtp-port

Description

This command shows the configured SNMP 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 parameters:

```
show events smtp-port
```

Result

The configured SMTP port is displayed.

9.7.2 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.

9.7.2.1 smtp-server

Description

With this command, you change to the SMTP server configuration mode. There are two options here:

- New creation
  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 server configuration mode takes place. In this mode, you can change the settings of the SMTP 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:

```
smtp-server { ipv4 <ucast_addr> | fqdn-name <FQDN> | ipv6
<ip6_addr> }
```

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 If you have stored a suitable domain name, you can specify a host name.
`ipv6`	Keyword for an IPv6 address	-
`ip6_addr`	IPv6 address of the SMTP server	Enter a valid IPv6 address.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 45)".

Result

An entry for the SMTP server has been created.

You are now in SMTP server configuration mode.

The command prompt is as follows:

```
cli(events-smtp-server)#
```

Additional notes

You delete an SMTP server entry with the `no smtp-server` command.

You display the configuration of the SMTP server with the `show events smtp-server` command.

You store a domain name with the `ip domain name` or `domain name` command.

9.7.2.2 no smtp-server

Description

With this command, you delete an SMTP server entry.

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 smtp-server { ipv4 <ucast_addr> | fqdn-name <FQDN)> | ipv6
<ip6_addr>}
```

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
`ipv6`	Keyword for an IPv6 address	-
`ip6_addr`	IPv6 address of the SMTP server	Enter a valid IPv6 address.

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 45)".

Result

The SMTP server entry is deleted.

Additional notes

You configure an SMTP server entry with the `smtp-server` command.

9.7.2.3 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 was sent.

Further notes

You can display the current SMTP settings with the `show events emailserver` command.

9.7.3 Commands in 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.

9.7.3.1 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.

9.7.3.2 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.

9.7.3.3 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.

9.7.3.4 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.

9.7.3.5 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.

9.7.3.6 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.

9.7.3.7 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.

9.7.3.8 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.

9.7.3.9 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.

9.7.3.10 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.

9.7.3.11 snmp-server-enable

Description

With this command, you enable the SNMP mail 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 SNMP mail server is enabled.

Additional notes

You disable the SNMP mail server with the `no smtp-server-enable` command.

9.7.3.12 no snmp server enable

Description

With this command, you disable the SNMP mail 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:

```
no smtp-server-enable
```

Result

The SNMP mail server is disabled.

Additional notes

You enable the SNMP mail server with the `smtp-server-enable` command.

9.7.3.13 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.

9.8 HTTP server

This section describes commands of the Hypertext Transfer Protocol (HTTP).

9.8.1 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.

9.8.1.1 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.

9.8.2 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.

9.8.2.1 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.

9.8.2.2 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.

9.8.2.3 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 (Page 29)".

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.

9.8.2.4 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

9.9 HTTPS server

This section describes commands of the Hypertext Transfer Protocol Secure (HTTPS).

9.9.1 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.

9.9.1.1 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.

9.9.1.2 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.

9.9.2 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.

9.9.2.1 ip http https redirection

Description

With this command, you enable the redirection of HTTP to HTTPS.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip http https redirection
```

As default the function is "enabled".

Result

The redirection is enabled on the device.

Further notes

You can display the setting of this function and other information with the `show ip http server status`command.

9.9.2.2 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.

9.9.2.3 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.

9.9.2.4 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.

9.9.2.5 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 (Page 29)".

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.

9.9.2.6 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

9.10 ARP

This section describes commands of the Address Resolution Protocol (ARP).

9.10.1 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.

9.10.1.1 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 "Interface identifiers and addresses (Page 45)".

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.

9.11 SSH server

This section describes commands of the Secure Shell (SSH) Server.

9.11.1 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.

9.11.1.1 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.

9.11.1.2 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.

9.11.2 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 mode with the `do [command]` in global configuration mode.

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

9.11.2.1 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.

9.11.2.2 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.

9.11.2.3 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 (Page 29)".

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.

9.11.2.4 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

9.11.2.5 ssh-server kex-algorithm-level

Description

With this command you specify the level of the SSH key exchange algorithm 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 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@libssh.org Ecdh-sha2-nistp256 Ecdh-sha2-nistp384 Ecdh-sha2-nistp521	Default

Result

The level of the SSH key exchange algorithm has been specified.

Additional notes

The supported SSH key exchange algorithms are listed with the command `show ip ssh`.

Load control 10

This part contains the sections describing the functions for controlling and balancing network load.

10.1 Dynamic MAC aging

The section describes commands with which the aging of dynamically learned entries is configured in a MAC address list.

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 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.

10.1.1.2 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.

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 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.

10.1.2.2 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.

10.1.2.3 mac-address-table aging-time

Description

With this command, you configure the aging of a dynamically learned entry in the MAC address list.

Note

Addresses with light data traffic

For addresses with low data traffic, it is recommended to enter a higher value for the aging.

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 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

At system start or when using the `restart` command with the option `memory` or `factory`, the following defaults apply:

- The default value is 300 seconds.

Result

The value of the aging of a dynamically learned entry is configured.

Further 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.

10.1.2.4 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.

Security and authentication 11

This part contains the sections that describe the access rights and authentication methods.

11.1 User rights management

This section describes commands for access as administrator and the configuration of the authentication methods.

11.1.1 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.

11.1.2 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.

11.1.3 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.

11.1.3.1 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.

11.1.3.2 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.

Further notes

You configure the password policy with the `password-policy` command.

11.1.3.3 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.

11.1.3.4 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.

11.1.3.5 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.

11.1.3.6 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.

11.1.4 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.

11.1.4.1 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.

11.1.4.2 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.

11.1.4.3 user-account

Description

With this command, you specify a new user. You can also change the password/role/description of a created user.

When you create a local user an entry is generated automatically in the table "External User Accounts".

Requirement

- 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 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. • The following characters must not be included: | § ? " ; : • It must not include Extended ASCII Codes (characters > 0x7F).
`password`	Keyword for a password	-

Parameter	Description	Range of values / note
`user-password`	Value for the password	Enter the password. The password must meet the following conditions: • It must be unique. • It must not contain the following characters: ; : ' ? ß § " ² ³ ° | € µ ä ö ü Ä Ö Ü • 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
`role`	Keyword for a role	-
`user-role`	Role	Enter a role. You can choose between system-defined and self-defined roles.
`description`	Keyword for the description	-
`user-description`	Content of the description	Enter a description for the user account. The description text can be up to 100 characters long.

Result

The user has been created.

Note

Changes in "Trial" mode

Even if the device is in "Trial" mode, changes that you carry out on this page are saved immediately.

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 user with the `no user-account` command.

You configure the password policy with the `password policy` command.

You show the created users with the `show user-accounts` command.

You display the currently valid password policy with the `show password-policy` command.

11.1.4.4 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.

11.1.4.5 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.

11.1.4.6 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.

11.1.4.7 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.

11.1.4.8 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.

11.1.4.9 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

11.1.4.10 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.

11.1.4.11 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.

11.2 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.

11.2.1 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.

11.2.1.1 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.

11.2.1.2 show radius server (IPv6)

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> | <ip6_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.
`ip6_addr`	Value for an IPv6 address	Enter a valid IPv6 address.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

If no parameters are specified, all configured RADIUS servers are displayed.

Result

The RADIUS server configuration is displayed.

11.2.2 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.

11.2.2.1 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.

11.2.2.2 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.

11.2.2.3 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.

11.2.2.4 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> | ipv6 <ipv6-address> } [auth-port <portno(1-65535)>] [retransmit <1-5>] [key <secret-key-string>] [primary] [test] [timeout <1-120>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ipv4`	Keyword for an IPv4 address	-
`ipv4-address`	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)	Maximum of 100 characters If you have stored a suitable domain name, you can specify a host name.
`ipv6`	Keyword for an IPv6 address	-
`ipv6-address`	IPv6 address of the RADIUS server	Enter a valid IPv6 address.
`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	-
–	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	128 characters Default: "default"
`primary`	Identifies the RADIUS server as primary server	-
`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`	Time in seconds for which the RADIUS client waits for a response from the RADIUS server before attempting login again.	1 ... 120

For information on names of addresses and interfaces, refer to the section "Addresses and interface names (Page 45)".

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.

Further notes

You store a domain name with the `ip domain name` or `domain name` command.

11.2.2.5 no radius-server

Description

With this command, you delete a RADIUS server entry on the RADIUS client.

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 radius-server { ipv4 <ipv4-address> | fqdn-name <FQDN> | ipv6
<ipv6-address>} [primary]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ipv4`	Keyword for an IPv4 address	-
`ipv4-address`	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)	Maximum of 100 characters
`ipv6`	Keyword for an IPv6 address	-
`ipv6-address`	IPv6 address of the RADIUS server	Enter a valid IPv6 address.
`primary`	Identifies the RADIUS server as primary server	-

For information on addresses and interfaces, refer to the section "Addresses and interface names (Page 45)".

Result

The entry for a connection between the RADIUS client and a server or the identification as primary server is deleted.

Further 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.

11.3 Brute Force Prevention

This section describes commands relevant for Brute Force Prevention.

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 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.

11.3.1.2 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.

11.3.2 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.

11.3.2.1 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.

11.3.2.2 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.

11.3.2.3 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.

11.3.2.4 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.

11.3.2.5 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.

11.3.2.6 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.

11.3.2.7 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.

11.3.2.8 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.

11.4 NAT

This section describes commands relevant for NAT / NAPT.

Note

All commands in this section are only available in client mode.

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 firewallnat napt

Description

This command shows the configured NAPT rules.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewallnat napt
```

Result

The configured NAPT rules are displayed.

11.4.1.2 show firewallnat masquerading

Description

This command shows the interfaces on which IP masquerading is enabled.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewallnat masquerading
```

Result

The interfaces are displayed.

11.4.2 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.

11.4.2.1 firewallnat

Description

With this command, you change to the FIREWALL NAT configuration mode.

Requirement

You are now in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
firewallnat
```

Result

You are now in the FIREWALL NAT configuration mode.

The command prompt is as follows:

```
cli(config-fwnat)#
```

Further notes

You exit the FIREWALL NAT configuration mode with the `end` or `exit` command.

11.4.3 Commands in the FIREWALL NAT configuration mode

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

In the Global configuration mode, enter the `firewallnat` command to change to this mode.

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

11.4.3.1 masquerading show-idx

Description

With this command, you show the numbers of the configured rules for masquerading.

Requirement

You are in the FIREWALL NAT configuration mode.

The command prompt is as follows:

```
cli(config-fwnat)#
```

Syntax

Call the command without parameter assignment:

```
masquerading show-idx
```

Result

The numbers are listed.

Further notes

You delete a rule for masquerading with the `no masquerading` command.

You create a rule for masquerading with the `masquerading` command.

11.4.3.2 napt show-idx

Description

With this command, you show the numbers of the configured NAPT rules.

Requirement

You are in the FIREWALL NAT configuration mode.

The command prompt is as follows:

```
cli(config-fwnat)#
```

Syntax

Call the command without parameter assignment:

```
napt show-idx
```

Result

The numbers are listed.

Further notes

You delete a NAPT rule with the `no napt` command.

You create a NAPT rule with the `napt` command.

11.4.3.3 napt srcint

Description

With this command, you can configure a port translation in addition to the address translation.

The following port translations are possible:

- From a single port to the same port
  If the ports are the same, the frames will be forwarded without port translation.
- From a single port to a single port
  The frames are translated to the port.
- From a port range to a single port
  The frames from the port range are translated to the same port (n:1).
- From a port range to the same port range
  If the port ranges are the same, the frames will be forwarded without port translation.

Requirement

- VLAN interface with subnet assignment.
- A second VLAN is set up and the IPv4 interface is configured.
- The `base bridge-mode` is `dot1q-vlan`.

- Masquerading is enabled.
- You are in the FIREWALL NAT configuration mode.
  The command prompt is as follows:
  `cli(config-fwnat)#`

Syntax

Call up the command with the following parameters:

```
napt srcint <gigabitethernet|vlan> <num(0-4094)> proto {udp|tcp}
dstport <num(1-65535)|range> transport <num(1-65535)|range> type
ipv4 transip <ip> [dstip <ip>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`srcint`	Keyword for the source interface	-
`gigabitethernet`	Ethernet interface	-
`vlan`	VLAN interface	-
`num`	Number of the addressed VLAN	0 ... 4094
`proto`	Keyword for a protocol	-
`udp`	Address assignment for UDP valid.	-
`tcp`	Address assignment for TCP valid.	-
`dstport`	Keyword for destination port	-
`num`	Destination port	1 ... 65535
`range`	Port range	Specify the start port and end port, e.g. 10 - 20.
`transport`	Keyword for new destination port	-
`num`	New destination port	1 ... 65535
`range`	New port range	Specify the start port and end port, e.g. 10 - 20.
`type ipv4 transip`	Keyword for the IPv4 address of the node to which this frame will be forwarded	-
`ip`	IPv4 address	Enter a valid IPv4 address.
`destip`	Keyword for the destination IP address	-
`ip`	IPv4 address	Enter a valid IPv4 address.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Note

If the port is already occupied by a local service, for example Telnet, a warning is displayed. In this case, avoid using the following ports: TCP port 23 (Telnet), port 22 (SSH), the ports 80/443 (http/https: Reachability of the client with the WBM, UDP port 161 (SNMP).

Result

The NAPT rule is created. During creation, an entry with a unique number (index) is created.

Further notes

You delete a NAPT rule with the `no napt` command.

You delete all NAPT rules with the `no napt all` command.

You display the numbers of the NAPT rules with the `napt show-idx` command.

You display the NAPT rule with the `show firewallnat napt` command.

11.4.3.4 no napt srcint

Description

With this command, you delete a specific NAPT rule.

Requirement

- VLAN interface with subnet assignment
- You are in the FIREWALL NAT configuration mode.
  The command prompt is as follows:
  `cli(config-fwnat)#`

Syntax

Call up the command with the following parameters:

```
no napt srcint <gigabitethernet|vlan> <num(1-4094)> idx <num(1-32)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`srcint`	Keyword for the source interface	-
`gigabitethernet`	Ethernet interface	-
VLAN	VLAN interface	-
`num`	Number of the addressed VLAN	0... 4094
`idx`	Number corresponding to a specific NAPT rule. Specify a valid number.	1 ... 32

Result

The specified NAPT rule is deleted.

Further notes

You display the numbers of the NAPT rules with the `napt show-idx` command.

You delete all NAPT rules with the `no napt all` command.

You create a NAPT rule with the `napt type ipv4` command.

11.4.3.5 no napt all

Description

With this command, you delete all NAPT rules.

Requirement

You are in the FIREWALL NAT configuration mode.

The command prompt is as follows:

```
cli(config-fwnat)#
```

Syntax

Call the command without parameter assignment:

```
no napt all
```

Result

All NAPT rules are deleted.

Further notes

You create a NAPT rule with the `napt type ipv4` command.

11.5 WLAN

11.5.1 Introduction to the section WLAN

This section describes commands for configuring and managing wireless LANs (WLANs).

Note

The availability of some commands in this section depends on the selected device mode. You will find the assignment of the commands to a specific device mode in the command header.

Example of a header:

- [Command] (Access Point) - The command is available only in access point mode
- [Command] (Client) - This command is only available in client mode

If a command is valid for both device modes, the header contains no additional note in parentheses.

11.5.2 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.

11.5.2.1 show wlan inter-ap-blocking allowed addresses (Access Point)

Description

This command shows a list of the SCALANCE W devices with which the clients are allowed to communicate.

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 wlan inter-ap-blocking allowed addresses vapX 0/Y
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`vapX 0/Y`	VAP interface Only available in client mode	Specify a valid interface.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The value of the update interval for ARP is shown along with a list with the following information:

- Index, the consecutive number of the list entry.
- Type, e.g. IPv4
- The IP address of the SCALANCE W device.
- The MAC address of the SCALANCE W device.

Note

This function can only be enabled when the CLP 2GB W700 AP iFeatures (6GK5 907-8UA00-0AA0) is inserted in the device and the configuration has been applied.

11.5.2.2 show wlan security

Description

This command shows the security settings of the SCALANCE W device, for example the encryption method.

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 wlan security <wlan 0/X | vapX 0/Y> [context <Id>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`wlan 0/X`	WLAN interface Only available in client mode	Specify a valid interface.
`vapX 0/Y`	VAP interface Only available in Access Point mode	Specify a valid interface.
`context`	Keyword for a security context	-
`Id`	Enter a valid security context ID.	Available only in client mode 1

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The settings are displayed.

See also

vap security wpa-psk-passphrase (access point) (Page 508)

11.5.2.3 show wlan security ap-radius-authenticator (Access Point)

Description

This command shows the settings of the RADIUS 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 parameter assignment:

```
show wlan security ap-radius-authenticator
```

Result

The settings are displayed.

See also

wlan security ap-radius-authenticator (Access Point) (Page 483)

wlan security ap-radius-authenticator max-retransmit (Access Point) (Page 486)

wlan security ap-radius-authenticator port-number (Access Point) (Page 487)

wlan security ap-radius-authenticator primary (Access Point) (Page 488)

wlan security ap-radius-authenticator reauth-interval (Access Point) (Page 489)

wlan security ap-radius-authenticator reauth-mode (Access Point) (Page 490)

wlan security ap-radius-authenticator shared-secret (Access Point) (Page 491)

11.5.2.4 show wlan security fast-bss-transition (Access Point)

Description

This command shows the setting of Fast BSS Transition.

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 wlan security fast-bss-transition
```

Result

The settings are displayed.

11.5.2.5 show wlan security server-cert (client)

Description

This command shows the 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 parameter assignment:

```
show wlan security server-cert
```

Result

The server certificate is displayed.

11.5.2.6 show wlan security user-cert (client)

Description

This command shows the user 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 parameter assignment:

```
show wlan security user-cert
```

Result

The user certificate is displayed.

11.5.3 Commands in the WLAN configuration mode

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

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

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

- If you exit the WLAN configuration mode with the `exit` command, you return to the global configuration mode.
- If you exit the WLAN 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 WLAN configuration mode.

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

11.5.3.1 wlan security ap-radius-authenticator (Access Point)

Description

With this command, you enable the RADIUS server.

Requirement

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security ap-radius-authenticator <index (1-2)>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`index`	Index of the RADIUS server	1...2

Result

The RADIUS server is enabled.

Additional notes

You disable the RADIUS server with the `no wlan security ap-radius-authenticator` command.

You display the setting with the `show wlan security ap-radius-authenticator` command.

See also

no wlan security ap-radius-authenticator (Access Point) (Page 484)

show wlan security ap-radius-authenticator (Access Point) (Page 481)

11.5.3.2 no wlan security ap-radius-authenticator (Access Point)

Description

With this command, you disable the RADIUS server.

Requirement

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
no wlan security ap-radius-authenticator <index (1-2)>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
index	Index of the RADIUS server	1...2

Result

The RADIUS server is disabled.

Additional notes

You disable the RADIUS server with the `wlan security ap-radius-authenticator` command.

You display the setting with the `show wlan security ap-radius-authenticator` command.

See also

wlan security ap-radius-authenticator (Access Point) (Page 483)

11.5.3.3 wlan security ap-radius-authenticator address (Access Point)

Description

With this command, you configure the IP address of the RADIUS server.

Requirement

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security ap-radius-authenticator address <index (1-2)> {ipv4
<ucast_addr> | fqdn-name <FQDN(100) | ipv6 <ipv6-addr>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`index`	Index of the RADIUS server	1...2
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	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)	Maximum of 100 characters
`ipv6`	Keyword for an IPv6 address	-
`ipv6-address`	IPv6 address of the RADIUS server	Enter a valid IPv6 address.

Result

The RADIUS server is enabled.

Additional notes

You display the setting with the `show wlan security ap-radius-authenticator` command.

11.5.3.4 wlan security ap-radius-authenticator max-retransmit (Access Point)

Description

With this command, you configure maximum number of attempts to establish a connection.

Requirement

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security ap-radius-authenticator max-retransmit <index (1-2)>
<1-5>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`index`	Index of the RADIUS server	1...2
`1-5`	Number of connection attempts	1...5

Result

The maximum number of attempts to establish a connection is configured.

Additional notes

You display the setting with the `show wlan security ap-radius-authenticator` command.

See also

show wlan security ap-radius-authenticator (Access Point) (Page 481)

11.5.3.5 wlan security ap-radius-authenticator port-number (Access Point)

Description

With this command, you configure the input port of the RADIUS server.

Requirement

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security ap-radius-authenticator port-number <index (1-2)>
<1-65535>
```

The parameters have the following meaning:

Parameters	Description	Range of values / note
`index`	Index of the RADIUS server	1...2
`1-65535`	Number of the port	1...6553

Result

The input port is configured.

Additional notes

You display the setting with the `show wlan security ap-radius-authenticator` command.

See also

show wlan security ap-radius-authenticator (Access Point) (Page 481)

11.5.3.6 wlan security ap-radius-authenticator primary (Access Point)

Description

With this command, you configure the RADIUS server as primary server.

Requirement

You are in the WLAN Configuration mode and the "wlan security ap-radius-authenticator address" is configured.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security ap-radius-authenticator primary <index (1-2)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`index`	Index of the RADIUS server	1...2

Result

The RADIUS server is configured as primary server.

Additional notes

You disable the setting with the `no wlan security ap-radius-authenticator primary` command.

You display the setting with the `show wlan security ap-radius-authenticator` command.

See also

no wlan security ap-radius-authenticator primary (Access Point) (Page 489)

show wlan security ap-radius-authenticator (Access Point) (Page 481)

11.5.3.7 no wlan security ap-radius-authenticator primary (Access Point)

Description

With this command, you disable the primary server.

Requirement

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
no wlan security ap-radius-authenticator primary <index (1-2)>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`index`	Index of the RADIUS server	1...2

Result

The primary server is disabled.

Additional notes

You enable the setting with the `wlan security ap-radius-authenticator primary` command.

You display the setting with the `show wlan security ap-radius-authenticator` command.

See also

wlan security ap-radius-authenticator primary (Access Point) (Page 488)

11.5.3.8 wlan security ap-radius-authenticator reauth-interval (Access Point)

Description

With this command, you configure the lifetime of the authentication (in seconds).

Requirement

- Local time management is active.

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security ap-radius-authenticator reauth-interval
<sec(60-43200)>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`sec`	Lifetime in seconds	60 ... 43200 Default: 3600

Result

The lifetime is configured.

Additional notes

You display the setting with the `show wlan security ap-radius-authenticator` command.

You configure the local time management with the `wlan security ap-radius-authenticator reauht-mode` command.

See also

show wlan security ap-radius-authenticator (Access Point) (Page 481)

11.5.3.9 wlan security ap-radius-authenticator reauth-mode (Access Point)

Description

With this command, you specify who decides the time before the clients are forced to reauthenticate.

Requirement

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security ap-radius-authenticator reauth-mode {show-modes |
<mode>}
```

The parameters have the following meaning:

Parameters	Description	Range of values / note
`show-modes`	Lists the available values.	• `disabled` Function is disabled • `server` Time management on the server • `local` Local time management. You specify the period of validity with the `wlan security ap-radius-authenticator reauth-interval` command.
`mode`	Method of time management	

Result

The function is configured.

Additional notes

You display the setting with the `show wlan security ap-radius-authenticator` command.

See also

show wlan security ap-radius-authenticator (Access Point) (Page 481)

11.5.3.10 wlan security ap-radius-authenticator shared-secret (Access Point)

Description

With this command, you configure the password for the RADIUS server.

Requirement

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security ap-radius-authenticator shared-secret <index(1-2)>
<password>
```

The parameters have the following meaning:

Parameters	Description	Range of values / note
`index`	Index of the RADIUS server	1...2
`string`	Password	Enter the password of the RADIUS server.

Result

The password is configured.

Additional notes

You display the setting with the `show wlan security ap-radius-authenticator` command.

See also

show wlan security ap-radius-authenticator (Access Point) (Page 481)

11.5.3.11 wlan security context (Client)

Description

With this command, you create a new security context and change to the security context configuration mode.

Requirement

You are in WLAN configuration mode.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security context <ID>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`ID`	ID of the security context	1

Result

The security context is created,

You are in the security context configuration mode.

The command prompt is as follows:

```
cli (config-wlan-context-$)#
```

Additional notes

You exit the security context configuration mode with the command `end` or `exit`.

You display the setting with the `show wlan security` command.

11.5.3.12 wlan security dot1x min-tls-version (Client)

Description

This command is used to specify the minimum TLS version to be used for WLAN RADIUS authentication.

Note

This command is only available in the client mode.

Requirement

You are in the WLAN configuration mode.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
wlan security dot1x min-tls-version { v10 | v11 | v12 }
```

The parameter has the following meaning:

Parameters	Description	Range of values/note
-	TLS version	• v10 • v11 • V12 (default setting)

Result

The TLS version is specified.

Note
RADIUS Server
This is only possible when the RADIUS Server supports the TLS version.

Further notes

You display the setting with the `show wlan security` command.

11.5.3.13 vap inter-ap-blocking refresh time (Access Point)

Description

This command defines the update interval for the ARP resolution of the allowed IP addresses.

Requirement

You are in the WLAN Configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan)#
```

Syntax

Call up the command with the following parameters:

```
vap inter-ap-blocking refresh time <seconds(30-300)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`seconds`	Update interval for the ARP resolution of the allowed IP addresses	30 ... 300 Default: 60

Result

The ARP resolution of the allowed IP addresses is updated when the set time elapses.

Note

This function can only be enabled when the CLP 2GB W700 AP iFeatures (6GK5 907-8UA00-0AA0) is inserted in the device and the configuration has been applied.

11.5.4 Commands in the WLAN Interface configuration mode

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

In global configuration mode, enter the `interface wlan 0/X` command to change to this mode.

- If you exit the WLAN Interface configuration mode with the `exit` command, you return to the global configuration mode.
- If you exit the WLAN Interface 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 WLAN Interface configuration mode.

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

11.5.4.1 wlan security ssid (Client)

Description

With this command, you assign the SSID of a WLAN interface a security context.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-if-wlan-0-X)#
```

Syntax

Call up the command with the following parameters:

```
wlan security ssid <index> context <ID>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`index`	Index of the SSID list	1
`context`	Keyword for a security context	-
`ID`	Enter a valid security context ID.	Available only in client mode 1

Result

The security context was assigned.

Additional notes

You create a security context and change to the security context configuration mode with the command `wlan security context`.

You display the setting with the `show wlan ssid-table` command.

11.5.5 Commands in the VAP Interface configuration mode

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

In the Global Configuration mode, enter the `interface vapX 0/Y` command to change to this mode.

- If you exit the VAP Interface configuration mode with the `exit` command, you return to the global configuration mode.
- If you exit the VAP Interface 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 VAP Interface configuration mode.

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

Note

This function can only be enabled when the CLP 2GB W700 AP iFeatures (6GK5 907-8UA00-0AA0) is inserted in the device and the configuration has been applied.

11.5.5.1 vap inter-ap-blocking (access point)

Description

This command restricts the communication of the clients. Clients can only access SCALANCE W devices whose IP address was configured on the access point with the command `vap inter-ap-blocking allowed address`.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call the command without parameters:

```
vap inter-ap-blocking
```

Result

The client can only communicate via the Ethernet interface with SCALANCE W devices that were configured as permitted communications partners.

Additional notes

The `show wlan inter-ap-blocking allowed addresses vapX 0/Y` command shows information about the SCALANCE W devices with which communication is possible.

With the `vap inter-ap-blocking allowed address` command, you configure a SCALANCE W device as a permitted communications partner.

See also

no vap inter-ap-blocking (access point) (Page 497)

11.5.5.2 no vap inter-ap-blocking (access point)

Description

This command allows unrestricted communication from a client to all SCALANCE W devices that can be reached via the access point.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call the command without parameters:

```
no vap inter-ap-blocking
```

Result

The client can communicate with all available SCALANCE W devices via the Ethernet interface. If permitted communications partners were configured previously, this information is retained after calling this command.

Additional notes

The `show wlan inter-ap-blocking allowed addresses vapX 0/Y` command shows information about the SCALANCE W devices with which communication is possible.

With the `vap inter-ap-blocking allowed address` command, you configure a SCALANCE W device as a permitted communications partner.

See also

vap inter-ap-blocking (access point) (Page 497)

11.5.5.3 vap inter-ap-blocking allowed address (access point)

Description

With this command, you specify which SCALANCE W devices are accessible to the clients.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call up the command with the following parameters:

```
vap inter-ap-blocking allowed address {ipv4 <ucast_addr>} [resolver-
address {ipv4 <ucast_addr>}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	IPv4 address	Enter a valid IPv4 address.
`resolver-address`	Address resolution	-
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	The IPv4 address that the access point uses to resolve the allowed IP address. The entry is necessary if the management IP address of the access point is located in a different subnet.	Enter a valid IPv4 address.

If you do not configure address resolution, the management IPv4 address is used for resolution.

Result

The client can communicate with the SCALANCE W device whose IPv4 address was specified as the parameter via the Ethernet interface.

Additional notes

You display the IPv4 addresses with the `show wlan inter-ap-blocking allowed addresses` command.

11.5.5.4 no vap inter-ap-blocking allowed address (access point)

Description

This command deletes the SCALANCE W device with the specified IP address from the list of SCALANCE W devices with which clients are allowed to communicate.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call up the command with the following parameters:

```
no vap inter-ap-blocking allowed address {ipv4 <ipv4-address>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ipv4`	Keyword for an IPv4 address	-
`ipv4-address`	IP address	Enter a valid IPv4 address.

Result

The entry was deleted from the list.

11.5.5.5 vap inter-ap-blocking block gratuitous arp (access point)

Description

This command blocks the forwarding of gratuitous ARP packets of the VAP interface to Ethernet.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call the command without parameters:

```
vap inter-ap-blocking block gratuitous arp
```

Result

Gratuitous ARP packets are not forwarded.

See also

no vap inter-ap-blocking block gratuitous arp (access point) (Page 500)

11.5.5.6 no vap inter-ap-blocking block gratuitous arp (access point)

Description

This command allows the forwarding of gratuitous ARP packets.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call the command without parameters:

```
no vap inter-ap-blocking block gratuitous arp
```

Result

Gratuitous ARP packets are also forwarded.

See also

vap inter-ap-blocking block gratuitous arp (access point) (Page 500)

11.5.5.7 vap inter-ap-blocking block non-ip-traffic (access point)

Description

This command restricts the communication between the client and the SCALANCE W devices configured as permitted communications partners in the access points to IP packets.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call the command without parameters:

```
vap inter-ap-blocking block non-ip-traffic
```

Result

There is no exchange of non-IP packets, for example layer 2 packets, between the client and the SCALANCE W devices configured in the access points as permitted communications partners.

See also

no vap inter-ap-blocking block non-ip-traffic (access point) (Page 502)

11.5.5.8 no vap inter-ap-blocking block non-ip-traffic (access point)

Description

This command allows the exchange of non-IP packets between the client and the SCALANCE W devices that are configured in the access points as permitted communications partners.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call the command without parameters:

```
no vap inter-ap-blocking block non-ip-traffic
```

Result

Non-IP packets can also be exchanged between the client and the SCALANCE W devices configured in the access points as permitted communications partners.

See also

vap inter-ap-blocking block non-ip-traffic (access point) (Page 501)

11.5.5.9 vap security authentication (access point)

Description

With this command, you specify the type of authentication.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call up the command with the following parameters:

```
vap security authentication { show-methods | <method> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`show-methods`	Lists the available types of authentication	• `open-system` No authentication • `wpa (RADIUS)` WPA authentication • `wpa-psk` WPA authentication without RADIUS server • `wpa2 (RADIUS)` WPA2 authentication • `wpa2-psk` WPA2 authentication without a RADIUS server with the stored key • `wpa-wpa2-auto (RADIUS)` WPA and WPA2 authentication • `wpa-wpa2-auto-psk` WPA and WPA2 authentication without a RADIUS server with the stored key • `wpa3-sae` WPA3 authentication with the stored key and PMF. Only in WLAN mode"802.11ax"
`method`	Value corresponding to an authentication method.	

Note

Encrypted management frames with the WPA3 authentication type

When WPA3-SAE is enabled, PMF (Protected Management Frames) is enabled automatically.

Result

The type of authentication is specified.

Additional notes

You display the settings with the `show wlan security <vapX 0/Y>` command.

See also

vap security protected-management-frames (access point) (Page 506)

11.5.5.10 vap security cipher (access point)

Description

With this command, you configure the encryption method for the WPA authentication.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call up the command with the following parameters:

```
vap security cipher { auto | aes | tkip }
```

The parameters have the following meaning:

Parameter	Description
`auto`	TKIP, WEP or AES is used depending on the capability of the other station.
`aes`	AES (Advanced Encryption Standard): Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.
`tkip`	TKIP (Temporal Key Integrity Protocol): A symmetrical stream encryption method with the RC4 (Ron's Code 4) algorithm. In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key.

Note

The encryption method "TKIP" is not available with the transmission standards "802.11n", "802.11ac" and "802.11ax".

Result

The encryption method is configured.

Additional notes

You display the settings with the `show wlan security <vapX 0/Y>` command.

11.5.5.11 vap security fast-bss-transition (access point)

Description

With this command, you enable the "Fast BSS Transition" function and specify the ID for the mobility domain.

Requirement

- Only possible with WPA2 (WPA2-PSK and WPA2 RADIUS) and WPA3 encryption.
- You are in the Interface Configuration mode of the VAP interface.
  The command prompt is as follows:
  `cli (config-if-vapX-0-Y)#`

Syntax

Call up the command with the following parameters:

`vap security fast-bss-transition mobility-domain-id <1-65535>`

The parameters have the following meaning:

Parameter	Description	Range of values/note
-	ID of the mobility domain	1..65535

Result

The function is enabled and the ID is configured.

Additional notes

You display the setting with the `show wlan security fast-bss-transition` command.

You disable the setting with the `no vap security fast-bss-transition` command.

11.5.5.12 no vap security fast-bss-transition (Access Point)

Description

With this command, you disable the "Fast BSS Transition" function and delete the ID for the mobility domain.

Requirement

- Only possible with WPA2 (WPA2-PSK and WPA2 RADIUS) and WPA3 encryption.
- You are in the Interface Configuration mode of the VAP interface.
  The command prompt is as follows:
  `cli (config-if-vapX-0-Y)#`

Syntax

Call the command without parameter assignment:

`no vap security fast-bss-transition`

Result

The ID is deleted and the function is disabled.

Additional notes

You display the setting with the `show wlan security fast-bss-transition` command.

You enable the setting with the `vap security fast-bss-transition` command.

11.5.5.13 vap security protected-management-frames (access point)

Description

With this command, you specify whether management frames are cryptographically protected. This prevents, for example, the WLAN client being separated from the access point due to corrupted disassociation / deauthenticate frames. With the WPA3-SAE authentication type, this setting is always selected and cannot be configured. You can find more information on this in the IEEE 802.11w standard.

Requirement

- The IEEE 802.11n/ac/ax transmission standard is enabled.

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call up the command with the following parameters:

```
vap security protected-management-frames { optional | required }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
-	Setting for management frames	• `disabled(0)` The management frames are unencrypted • `optional(1)` The management frames are encrypted or unencrypted depending on support of the WLAN client. • `required(2)` The management frames are always encrypted. A connection of the WLAN clients to the access point is only possible when these also support PMF.

Result

The management frames are encrypted.

Additional notes

You display the setting with the `show wlan security` command.

You set the transmission standard IEEE 802.11 ax/ac/n with the `wlan mode` command.

You disable the setting with the `no vap security protected-management-frames` command.

11.5.5.14 no vap security protected-management-frames (access point)

Description

With this command, you disable protection of management frames.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call the command without parameter assignment:

```
no vap security protected-management-frames
```

Result

The management frames are no longer encrypted.

Additional notes

You enable the setting with the `vap security protected-management-frames` command.

11.5.5.15 vap security wpa-group-key-update-interval (Access Point)

Description

With this command you specify the time after which the key is renewed.

Requirement

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call up the command with the following parameters:

```
vap security wpa-group-key-update-interval {0|seconds (30-36000)}
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
`0`	The key will not be renewed.	-
`seconds`	When the time expires (second), the key is renewed.	30 ... 36000

Result

The time for renewal of the key is specified.

11.5.5.16 vap security wpa-psk-passphrase (access point)

Description

With this command, you store the key that is used in WPA3-SAE or WPA2-PSK authentication.

Note

The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. It should be selected so that is complex for example consisting of random numbers, letters (upper-/lowercase), have few repetitions and special characters. Do not use known names, words or terms that could be guessed. If a SCALANCE W device is lost or if the key becomes known, the key should be changed on all SCALANCE W devices to maintain security.

Requirement

- WPA3-SAE or WPA2-PSK is set for the authentication type.

You are in the Interface Configuration mode of the VAP interface.

The command prompt is as follows:

```
cli (config-if-vapX-0-Y)#
```

Syntax

Call up the command with the following parameters:

```
vap security wpa-psk-passphrase <string>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`string`	Key	`8....63ASCII` or `exactly 64 hex`

Result

A key for authentication with WPA3-SAE or WPA2-PSK is defined. When the authentication type is changed, the key is deleted.

Additional notes

You display the settings with the `show wlan security <vapX 0/Y>` command.

11.5.6 Commands in the security context configuration mode

11.5.6.1 wlan security authentication (client)

Description

With this command, you specify the type of authentication.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call up the command with the following parameters:

```
wlan security authentication { show-methods | <method> }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`show-methods`	Lists the available types of authentication	• `open-system` Without authentication. Encryption with a fixed (unchanging) key can be selected as an option. To enable encryption, use the "`wlan security encryption`" command. • `wpa2 (Radius)` WPA2 authentication • `wpa2-psk` WPA2 authentication without RADIUS server with the stored pass phrase • `wpa3-sae` WPA3 authentication with the stored protected pass phrase and PMF. Only in WLAN mode"802.11ax"
`methods`	Value corresponding to an authentication method.	

Note

Encrypted management frames with the WPA3 authentication type

When WPA3-SAE is enabled, PMF (Protected Management Frames) is enabled automatically.

Result

The type of authentication is specified.

Additional notes

You display the settings with the `show wlan security` command.

See also

wlan security protected-management-frames (client) (Page 516)

11.5.6.2 wlan security cipher (client)

Description

With this command, you configure the encryption method for the WPA(2) authentication.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call up the command with the following parameters:

```
wlan security cipher { auto | aes | tkip }
```

The parameters have the following meaning:

Parameter	Description
`auto`	TKIP or AES is used depending on the capability of the other station.
`aes`	AES (Advanced Encryption Standard): Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.
`tkip`	TKIP (Temporal Key Integrity Protocol): A symmetrical encryption method with the RC4 algorithm (Ron's Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key.

Note

The encryption method "TKIP" is not available with the transmission standards "802.11n" and "802.11n only".

Result

The encryption method is configured.

Additional notes

You display the settings with the `show wlan security` command.

You define the WEP key with the `wlan security edit key` command.

11.5.6.3 wlan security dot1x check-server-certificate (client)

Description

With this command, you enable the validation of the server certificate on the client.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call the command without parameter assignment:

```
wlan security dot1x check-server-certificate
```

Result

Validation is enabled.

Additional notes

You display the settings with the `show wlan security` command.

You disable the validity check with the `no wlan security dot1x check-server-certificate` command (default setting).

11.5.6.4 no wlan security dot1x check-server-certificate (client)

Description

With this command, you disable the validation of the server certificate on the client. This setting is activated as default.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call the command without parameter assignment:

```
no wlan security dot1x check-server-certificate
```

Result

Validation is disabled.

Additional notes

You display the settings with the `show wlan security` command.

You enable the validation with the `wlan security dot1x check-server-certificate` command.

11.5.6.5 wlan security dot1x eap-authentication-type (client)

Description

With this command, you specify which RADIUS authentication methods the client offers to the RADIUS server. With "`auto`", the client offers a RADIUS server all supported methods. Any other selection restricts the support by the client to this one method.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call up the command with the following parameters:

```
wlan security dot1x eap-authentication-type { show-types | <type> }
```

The parameters have the following meaning:

Parameters	Description	Range of values / note
`show-types`	Lists the available authentication methods	• `auto` Client offers RADIUS server all methods • `eap-tls` Extensible Authentication Protocol - Transport Layer Security: Uses certificates for authentication • `eap-ttls` Extensible Authentication Protocol - Tunnel Transport Layer Security: After setting up the TLS tunnel, MS-CHAPv2 is used for internal authentication. • `peap` Protected Extensible Authentication Protocol: Alternative draft protocol of IETF for EAP-TTLS
`type`	Value that contains the authentication method	

Result

The authentication method is specified.

Additional notes

You display the settings with the `show wlan security` command.

11.5.6.6 wlan security dot1x password (client)

Description

With this command, you specify the password for the RADIUS server.
When assigning the password, ASCII code 0x20 to 0x7e is used.

Note

Dot1X user name and Dot1X user password

With WPA (RADIUS), WPA2 (RADIUS), EAP-TLS, EAP-TTLS and PEAP the Dot1X user name and the Dot1X user password must be configured.

With the setting "Auto" either the certificate must be loaded or the Dot1X user name and the Dot1X user passport must be configured.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call up the command with the following parameters:

```
wlan security dot1x password <string>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`string`	New password	Enter the password for the user name. You specify the user name with the `wlan security dot1x username` command

Result

The password is specified.

Additional notes

You display the settings with the `show wlan security` command.

11.5.6.7 wlan security dot1x username (client)

Description

With this command, you specify the user name for the RADIUS server.

Note

Dot1X user name and Dot1X user password

With WPA2 (RADIUS), EAP-TLS, EAP-TTLS and PEAP, the Dot1X user name and the Dot1X user password must be configured.

With the setting "Auto" either the certificate must be loaded or the Dot1X user name and the Dot1X user passport must be configured.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call up the command with the following parameters:

```
wlan security dot1x username <string>
```

The parameter has the following meaning:

Parameters	Description	Range of values / note
`string`	User name	Enter the user name for the RADIUS server. You specify the corresponding password with the `wlan security dot1x password` command.

Result

The user name is specified.

Additional notes

You display the settings with the `show wlan security` command.

11.5.6.8 wlan security protected-management-frames (client)

Description

With this command, you specify whether management frames are cryptographically protected. This prevents, for example, the WLAN client being separated from the access point due to corrupted disassociation / deauthenticate frames. With the WPA3-SAE authentication type, this setting is always selected and cannot be configured. You can find more information on this in the IEEE 802.11w standard.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call up the command with the following parameters:

```
wlan security protected-management-frames { optional | required }
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
-	Setting for management frames	• `disabled(0)` The management frames are unencrypted. • `optional(1)` The management frames are encrypted or unencrypted depending on support of the access point/WLAN client. • `required(2)` The management frames are always encrypted. A connection of the WLAN clients to the access point is only possible when they both also support PMF.

Result

The management frames are encrypted.

Additional notes

You display the setting with the `show wlan security` command.

You disable the setting with the `no wlan security protected-management-frames` command.

11.5.6.9 no wlan security protected-management-frames (client)

Description

With this command, you disable protection of management frames.

Requirement

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call up the command with the following parameters:

```
no wlan security protected-management-frames
```

Result

The management frames are no longer encrypted.

Additional notes

You enable the setting with the `wlan security protected-management-frames` command.

11.5.6.10 wlan security wpa-psk-passphrase (client)

Description

With this command, you store the key that is used in WPA3-SAE and WPA2-PSK authentication.

Note

The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. It should be selected so that is complex for example consisting of random numbers, letters (upper-/lowercase), have few repetitions and special characters. Do not use known names, words or terms that could be guessed. If a SCALANCE device is lost or if the key becomes known, the key should be changed on all SCALANCE devices to maintain security.

Requirement

- WPA3-SAE or WPA2-PSK is set for the authentication type.

You are in Interface configuration mode of the WLAN interface.

The command prompt is as follows:

```
cli (config-wlan-context-x)#
```

Syntax

Call up the command with the following parameters:

```
wlan security wpa-psk-passphrase <string>
```

The parameter has the following meaning:

Parameter	Description	Range of values/note
`string`	Key	`8....63ASCII` or `exactly 64 hex`

Result

A key for authentication with WPA3-SAE or WPA2-PSK is defined. When the authentication type is changed, the key is deleted.

Additional notes

You display the settings with the `show wlan security` command.

Diagnostics 12

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

12.1 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.

12.1.1 clear authlog

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 authlog
```

Result

The content of the logbook is deleted.

12.1.2 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.

12.1.3 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.

12.1.4 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.

12.1.5 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".

12.1.6 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".

12.1.7 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.

12.1.7.1 show authlog

Description

With this command, you show the information about successful or failed authentication attempts.

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 authlog
```

or

Call up the command with the following parameters:

```
show authlog [{ 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.

12.1.7.2 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.

12.1.7.3 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:

Parameters	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.

12.1.7.4 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.

12.1.7.5 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.

12.1.7.6 show fault counter

Description

This command shows the number of fault transitions 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 fault counter
```

Result

The number of indicated faults is displayed.

12.1.7.7 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.

12.1.7.8 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.

12.1.7.9 show rmon

Description

This command shows the Ethernet statistics. The displayed values are transferred by RMON (Remote Network Monitoring).

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 rmon [statistics [<stats-index (1-52)>]]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`statistics`	Shows the Ethernet statistics.	-
`stats-index`	Index number for the statistical values	1 ... 52

- If you specify the command without parameters, the display shows whether RMON is enabled or disabled.
- If no index number is specified, the statistics for all Ethernet interfaces are displayed.

Result

The Ethernet statistics are displayed.

12.1.7.10 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.

12.1.8 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.

12.1.8.1 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`.

12.1.9 Commands in the EVENT 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.

12.1.9.1 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.

12.1.9.2 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.

12.1.9.3 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.

12.1.9.4 event config

Description

With this command, you configure which of the various events 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 status change in the power supply
- Message when there is a status change in the error monitoring
- Message when there is a change in the spanning tree
- Message if radio channels overlap (only in access point mode)
- Message if a radar signal is received or if there is a status change in the DFS scan (only in access point mode)
- Message if the configuration changes

- Message on non-configurable entry in the log table
- Message on successful or failed authentication attempts (only in client mode)

These messages can be processed by the device in different ways:

- Entry in the logbook of the device
- Sending the message to the Syslog server of the system
- Sending an e-mail
- Sending an SNMP trap
- Lighting up of the error LED.

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
| power-change | faultstate-change | stp-change | overlap-ap | wds
| dfs | config-change | service-information | wlan-general | client-
wlan-auth | 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
`power-change`	Message when there is a status change in the power supply
`faultstate-change`	Message when there is a status change in the error monitoring
`stp-change`	Message when there are changes in the Spanning Tree
`overlap-ap`	Message if there is an entry in the "Overlap AP" list Only available in access point mode
`wds`	Message when there is a change in the connection status of a WDS link Only available in access point mode
`dfs`	Message when a radar signal was received or the DFS scan was started or stopped. Only available in access point mode
`config-change`	Message when the configuration of the device has changed.
`service-information`	Message on non-configurable entry in the log table
`wlan-general`	This setting has no function.
`client-wlan-auth`	Message on successful or failed authentication attempts. Only available in client mode

Parameter	Description
`all`	All messages
`logtable`	Client that processes the logbook entries.
`syslog`	Client that sends the messages to the log server.
`email`	Client that sends the e-mails.
`trap`	Client that sends the SNMP traps.
`faults`	The device triggers an error. The error LED lights up.
`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.

You display the content of the log with the command `show logbook`.

You display the currently pending errors with the `show events faults status` 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, first select the `all` option and then disable individual elements.

12.1.9.5 no event config

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:

```
no event config {cold-warmstart | linkchange | authentication-
failure | power-change | faultstate-change | stp-change | overlap-
ap | wds | dfs | config-change | service-information | wlan-general
| client-wlan-auth | 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
`power-change`	Message when there is a status change in the power supply
`faultstate-change`	Message when there is a status change in the error monitoring
`stp-change`	Message when there are changes in the Spanning Tree
`overlap-ap`	Message if there is an entry in the "Overlap AP" list Only available in access point mode
`wds`	Message when there is a change in the connection status of a WDS link Only available in access point mode
`dfs`	Message when a radar signal was received or the DFS scan was started or stopped. Only available in access point mode
`config-change`	Message when the configuration of the device has changed.
`service-information`	Message on non-configurable entry in the log table
`wlan-general`	This setting has no function.
`client-wlan-auth`	Message on successful or failed authentication attempts. Only available in client mode
`all`	All messages
`logtable`	Client that processes the logbook entries.
`syslog`	Client that sends the messages to the log server.
`email`	Client that sends the e-mails.
`trap`	Client that sends the SNMP traps.
`faults`	The device triggers an error. The error LED lights up.
`all`	All clients at once

Result

The setting deciding which messages of the device should not be stored or sent 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.

12.1.9.6 event config wlan-auth-log syslog

Description

With this command, you enable the forwarding of WLAN Authentication Log entries to the Syslog-Server.

Requirement

You are in the EVENTS Configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call the command without parameters:

```
event config wlan-auth-log syslog
```

Result

Messages from the WLAN Authentication Log are forwarded to the Syslog-Server .

Further notes

You display the status of the events and the clients with the `show events config` command.

You disable the forwarding of WLAN Authentication Log entries to the Syslog-Server with the `no event config wlan-auth-log syslog` command.

12.1.9.7 no event config wlan-auth-log syslog

Description

With this command, you disable the forwarding of WLAN Authentication Log entries to the Syslog-Server.

Requirement

You are in the EVENTS Configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call the command without parameters:

```
no event config wlan-auth-log syslog
```

Result

The forwarding of entries from the WLAN Authentication Log ist an den Syslog-Server is disabled.

Further notes

You display the status of the events and the clients with the `show events config` command.

You enable the forwarding of entries from the WLAN Authentication Log to the Syslog-Server with the `event config wlan-auth-log syslog` command.

12.1.9.8 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}[{<interface-type><interface-id>}]
```

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	-
`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 "Interface identifiers and addresses (Page 45)".

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.

12.1.9.9 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}[{<interface-type><interface-id>}]
```

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	-
`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 "Interface identifiers and addresses (Page 45)".

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.

12.1.9.10 logbook alarm threshold

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>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
-	Threshold value for the logbook entries	50 ... 1950

Result

The threshold value is specified.

12.1.9.11 power

Description

With this command, you disable the monitoring of the power supplies. Depending on the hardware variant there are one or two power connectors (L 1 / L 2) and a PoE power supply.

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:

```
power [{l1 | l2 | poe}]
```

The parameters have the following meaning:

Parameter	Description
l1	Monitoring of power supply 1
l2	Monitoring of power supply 2
poe	Monitoring of the PoE power supply

If you do not select any parameter from the parameter list, all power supplies are monitored.

Result

The setting for monitoring the power supplies is configured.

Further 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 disable the function with the `power` command.

12.1.9.12 no power

Description

With this command, you disable the monitoring of the power supplies. Depending on the hardware variant there are one or two power connectors (L 1 / L 2) and a PoE power supply.

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 power [{l1 | l2 | poe}]
```

The parameters have the following meaning:

Parameter	Description
`l1`	No monitoring of power supply 1
`l2`	No monitoring of power supply 2
`poe`	No monitoring of the PoE power supply.

If you do not select any parameter from the parameter list, the monitoring of all power supplies is disabled.

Result

The setting for monitoring the power supplies is configured.

Further 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 `power` command.

12.1.9.13 power pnio redundancy

Description

With this command, you specify which power supply is to be monitored by PROFINET:

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:

```
power pnio redundancy {all | l1-l2 | l1-poe | l2-poe}
```

The parameters have the following meaning:

Parameter	Description
`all`	Monitoring of all power supply connectors by PROFINET.
`l1-l2`	Monitoring of the power supply connectors L1 and L2 by PROFINET.
`l1-poe`	Monitoring of the power supply connectors L1 and PoE by PROFINET.
`l2-poe`	Monitoring of the power supply connectors L2 and PoE by PROFINET.

Result

Monitoring of the power supply by PROFINET is configured.

Further 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.

12.1.9.14 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.

12.1.9.15 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 | authlog } { info | warning |
critical }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`mail`	System event messages are sent by e-mail.	-
`log`	System event messages are entered in the log table.	-
`syslog`	System event messages are entered in the syslog file.	-
`authlog`	System event messages are entered in the log table for authentications.	-
`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`

12.1.9.16 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 | authlog }
```

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.	-
`authlog`	The setting of the threshold value for entering system event messages in the log table for authentications 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`.

12.2 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)

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 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.

12.2.2 Commands in the EVENT 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.

12.2.2.1 syslogserver

Description

With this command, you configure the Syslog server.

Requirement

You are in EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call the command with the following parameters:

```
syslogserver { ipv4 <ucast_addr> | fqdn-name <FQDN> | ipv6
<ip6_addr>} [<port(1-65535)>] [tls]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	IPv4 unicast address of the Syslog server	Specify 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.
`ipv6`	Keyword for an IPv6 address	-
`ip6_addr`	IPv6 address of the Syslog server	Specify a valid IPv6 address.
`port`	Port of the Syslog server on which the messages are received	0 ... 65535 Default: 514
`tls`	Communication with the syslog server is encrypted.	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

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. The Syslog server was entered in the table.

Additional notes

You delete the entry with the `no syslogserver` command.

You display the status of this function and other information with the `show events syslogserver` command.

You store a domain name with the `ip domain name` or `domain name` command.

12.2.2.2 no syslogserver

Description

With this command, you delete a Syslog 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:

```
no syslogserver { ipv4 <ucast_addr> | fqdn-name <FQDN> | ipv6
<ip6_addr>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
`ipv4`	Keyword for an IPv4 address	-
`ucast_addr`	IPv4 unicast address of the Syslog server	Enter a valid IPv4 address.
`fqdn-name`	Keyword for a domain name	-
`FQDN`	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters
`ipv6`	Keyword for an IPv6 address	-
`ip6_addr`	IPv6 address of the Syslog server	Enter a valid IPv6 address.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 45)".

Result

The Syslog server is deleted.

Further notes

You add a Syslog server with the `syslogserver` command.

Index

A

Access point
no event config, 535
no vap broadcast ssid, 253
no vap inter-ap-blocking, 497
no vap inter-ap-blocking allowed address, 499
no vap inter-ap-blocking block non-ip-traffic, 502
no vap security fast-bss-transition, 505
no wlan security ap-radius-authenticator, 484
no wlan security ap-radius-authenticator primary, 489
show spanning-tree l2t-edge, 285
show wlan ap, 209
show wlan client-list, 213
show wlan client-list-vap, 214
show wlan inter-ap-blocking allowed addresses, 479
show wlan overlap-ap-list, 216
show wlan security ap-radius-authenticator, 481
show wlan security fast-bss-transition, 482
show wlan vap, 219
vap broadcast ssid, 252
vap inter-ap-blocking, 497
vap inter-ap-blocking allowed address, 498
vap inter-ap-blocking block gratuitous arp, 500
vap inter-ap-blocking block non-ip-traffic, 501
vap inter-ap-blocking refresh time, 494
vap security authentication, 502
vap security cipher, 503
vap security fast-bss-transition, 504
vap security protected-management-frames, 506
vap security wpa-group-key-update-interval, 507
vap security wpa-psk-passphrase, 508
vap ssid, 251
wlan beacon interval, 238
wlan channel, 239
wlan channel width, 240
wlan mode, 245
wlan security ap-radius-authenticator, 483
wlan security ap-radius-authenticator address, 485
wlan security ap-radius-authenticator max-retransmit, 486
wlan security ap-radius-authenticator port-number, 487
wlan security ap-radius-authenticator primary, 488
wlan security ap-radius-authenticator reauth-interval, 489
wlan security ap-radius-authenticator reauth-mode, 490
wlan security ap-radius-authenticator shared-secret, 491
Access Point
no vap security protected-management-frames, 507
activate-after-restart, 170
no activate-after-restart, 170
add log, 531
alias, 94
no alias, 95
auth username
no auth username, 405
auth usernamet, 405
auto-save, 130
no auto-save, 131
Available system functions, 34

B

base bridge mode, 263
brute-force-prevention auto-reset-timer, 468
no brute-force-prevention auto-reset-timer, 469
brute-force-prevention ip-specific-login-attempts, 464
brute-force-prevention ip-specific-login-attempts, 465
brute-force-prevention reset, 470
brute-force-prevention trigger-interval, 468
brute-force-prevention user-specific-login-attempts, 466
no brute-force-prevention user-specific-login-attempts, 467

C

cancel restart-time, 126
capture, 171
no capture, 173
change password, 437
clear authlog, 519
clear counters, 76
clear fault counter, 520
clear history, 64
clear ipv6 dhcp client statistics, 364
clear line vty, 77

clear logbook, 520
clear screen, 57
clear spanning-tree counters, 288
clear wlan iprp information, 159
CLI commands
    Symbolic representation, 44
cli-console-timeout, 156
    no cli-console-timeout, 157
Client
    no password, 119
    no wlan security dot1x check-server-certificate"}, 512
    no wlan security protected-management-frames, 517
    password, 118
    show wlan available-ap-list, 210
    show wlan client, 212
    show wlan security server-cert, 482
    show wlan security user-cert, 483
    show wlan signal-recorder, 175
    show wlan ssid-table, 218
    wlan background scan interval, 236
    wlan background scan mode, 236
    wlan background scan threshold, 237
    wlan client mac mode, 240
    wlan iprp interface, 162
    wlan scan-time-per-channel, 249
    wlan security authentication, 509
    wlan security cipher, 510
    wlan security context, 492
    wlan security dot1x check-server-certificate, 511
    wlan security dot1x eap-authentication-type, 513
    wlan security dot1x min-tls-version, 493
    wlan security dot1x password, 514
    wlan security dot1x username, 515
    wlan security protected-management-frames, 516
    wlan security ssid, 495
    wlan security wpa-psk-passphrase, 517
    wlan signal-recorder, 178
    wlan signal-recorder start, 176
    wlan signal-recorder stop, 179
    wlan ssid-table edit, 250
commit mode, 221
commit wlan-settings, 222
configbackup create, 135
configbackup delete, 136
configbackup restore, 135
configure terminal, 77
Configuring the network via Ethernet
    Connecting to network, 50
coordinates height, 83
coordinates latitude, 84
coordinates longitude, 85
country, 223

D

das delete, 142
das discover interface, 138
das mac blink, 141
das mac ip, 140
das mac name, 139
dcp forwarding, 334
dcp server, 325
    no dcp server, 326
delete, 111
device mode, 224
digital output retain, 132
    no digital output retain, 132
disable, 78
    TCP Event, 182
dnsclient, 356
do, 57
Documentation on the Internet, 20

E

enable, 79
    TCP Event, 182
event, 184, 185
event config, 533
    no event config, 535
event config wlan-auth-log syslog, 537
event show-types, 187
events, 530
exit, 58

F

factoryclean, 149
fault report ack, 521
firewallnat, 473
firmeware-in-configpack
    no firmeware-in-configpack, 121
firmware in configpack, 120
firmware-on-plug, 149
    no firmware-on-plug, 150

G

grep, 59

Group name
Permitted characters, 43

H

help, 60

I

instance, 316
no instance, 317
interface, 86
no interface, 87
ip address, 331, 332
no ip address, 333
ip dhcp client mode, 363
ip dhcp config-file-request, 362
no ip dhcp config-file-request, 363
ip http, 414, 421
no ip http, 415
ip http https redirection, 419
ip http port, 416
no ip http port, 417
ip http secure, 419
no ip http secure, 420
ip http secure port, 421
no ip http secure port, 422
ip ipv6 neighbor
no ipv6 neighbor, 341
ip route, 326
no ip route, 327
IPv6
Notation, 54
ipv6 address, 347
no ipv6 address, 348
ipv6 address autoconfig, 349
no ipv6 address autoconfig, 349
ipv6 address dhcp
no ipv6 address dhcp, 351
ipv6 address link-local, 352
no ipv6 address link-local, 353
ipv6 enable, 353
no ipv6 enable, 354
ipv6 neighbor, 340
ipv6 path mtu, 342
no ipv6 path mtu, 342
ipv6 path mtu discover, 343
no ipv6 path mtu discover, 344
ipv6 route, 344
no ipv6 route, 345

L

link, 538
no link, 539
lldp, 95
no lldp, 96
load tftp, 108
loadsave, 110
logbook alarm threshold, 540
login authentication, 457
logout, 79

M

mac-address-table aging, 433
no mac-address-table aging, 433
mac-address-table aging-time, 434
no mac-address-table aging-time, 435
manual srv, 357
no manual srv, 358
masquerading show-idx, 474
mtu, 264

N

name, 276, 317
no name, 277, 318
napt show-idx, 474
napt type ipv4, 475
no napt, 477
no napt all, 478
no event config wlan-auth-log syslog, 537
no login authentication, 458
no port, 174
no role, 444
no sinema, 144
no snmp engineid migrate, 382
no snmp filterprofile, 384
no user-account-ext, 449
no user-group, 451
no wlan security protected-management-frames, 517
ntp, 196
ntp server
no ntp server, 198
ntp server id, 197
ntp time diff, 199

P

packet capture, 169
password, 118, 186
    no password, 119
Password
    Permitted characters and length, 42
password policy, 452
password policy (parameter), 454
password policy min-length, 453
Permitted characters and length, 42
ping, 80
ping ipv6, 81
plug, 148
pnio, 90
pnio station-name, 91
port, 174, 183, 406
    no port, 407
ports, 278
    no ports, 279
power
    no power, 540, 541
power pnio redundancy, 542
pre-login message add, 88
    no pre-login message, 89
presetplug, 151

R

radius authorization-mode, 458
radius server, 459
    no radius-server, 461
receiver-address, 407
    no receiver-address, 408
restart, 122
revision, 319
    no revision, 320
role, 443
Role name
    Permitted characters, 43

S

save filetype, 107
schedule restart-configbackup
    no schedule restart-configbackup, 124
schedule restart-timer, 125
security, 409
    no security, 410
send test mail, 404, 543
sender-address, 410
    no sender address, 411
server type, 358
severity, 543
    no severity, 544
sftp filename, 115
sftp load, 116
sftp save, 116
sftp server, 117
    Saving, 107
SFTP server
    Downloading, 108
show authlog, 523
show brute-force-prevention config, 462
show brute-force-prevention status, 463
show cli-console-timeout, 155
show configbackup, 134
show coordinates, 67
show das info, 137
show dcp forwarding, 321
show dcp server, 322
show device information, 68
show dnsclient information, 355
show dot1d mac-address-table, 259
show dst info, 190
show events config, 524
show events faults config, 524
show events faults status, 525
show events severity, 526
show events smtp-port, 401
show events smtp-server, 400
show events syslogserver, 546
show fault counter, 526
show firewallnat masquerading, 472
show firewallnat napt, 472
show function-rights, 439
show history, 63
show in, 69
show interface mtu, 71
show interfaces, 69
show interfaces ... counters, 70
show ip arp, 423
show ip dhcp client, 361
show ip dhcp client stats, 361
show ip gateway, 322
show ip http secure server status, 417
show ip http server status, 414
show ip interface, 72
show ip route, 323
show ip ssh, 424
show ip static route, 324
show ip telnet, 324

show ipv6 dhcp, 365
show ipv6 dhcp client statistics, 367
show ipv6 dhcp interface, 366
show ipv6 interface, 335
show ipv6 neighbors, 336
show ipv6 pmtu, 337
show ipv6 route, 337
show ipv6 static route, 338
show ipv6 traffic, 338
show lldp neighbors, 72
show lldp status, 73
show loadsave files, 105
show loadsave stftp, 106
show loadsave tftp, 106
show logbook, 527
show mac-address-table, 254
show mac-address-table aging-status, 431
show mac-address-table aging-time, 432
show mac-address-table count, 255
show mac-address-table dynamic unicast, 255
show ntp info, 195
show packet capture, 168
show password-policy, 439
show plug, 147
show pnio, 74
show power-line-state, 527
show radius server, 456
show radius statistics, 455
show rmon, 528
show roles, 440
show running-config, 127
show sinema, 143
show snmp, 369
show snmp community, 369
show snmp engineID, 370
show snmp filter, 370
show snmp group, 371
show snmp group access, 371
show snmp inform statistics, 372
show snmp notif, 372
show snmp targetaddr, 373
show snmp targetparam, 373
show snmp user, 374
show snmp viewtree, 374
show sntp broadcast-mode status, 200
show sntp status, 200
show sntp unicast-mode status, 201
show spanning-tree, 281
show spanning-tree active, 282
show spanning-tree bridge, 282
show spanning-tree detail, 283
show spanning-tree interface, 284
show spanning-tree l2t-edge, 285
show spanning-tree mst, 285
show spanning-tree mst configuration, 286
show spanning-tree mst interface, 287
show spanning-tree root, 288
show ssh-fingerprint, 425
show ssl server-cert, 418
show startup-information, 529
show tcpevent, 180
show time, 189
show traceroute, 74
show user-accounts, 440
show user-groups, 441
show users, 442
show versions, 75
show vlan, 256
show vlan device info, 257, 260
show vlan learning params, 257
show vlan port config, 258
show web-session-timeout, 152
show wlan advanced, 207
show wlan allowed channels, 208
show wlan antennas, 209
show wlan ap, 209
show wlan available-ap-list, 210
show wlan basic, 211
show wlan client, 212
show wlan client-list, 213
show wlan client-list-vap, 214
show wlan device, 214
show wlan inter-ap-blocking allowed addresses, 479
show wlan ipcf-2, 166
show wlan ip-mapping, 215
show wlan iprp, 158
show wlan iprp information, 158
show wlan noise-floor, 216
show wlan overlap-ap-list, 216
show wlan overview, 217
show wlan security, 480
show wlan security ap-radius-authenticator, 481
show wlan security fast-bss-transition, 482
show wlan security server-cert, 482
show wlan security user-cert, 483
show wlan signal-recorder, 175
show wlan ssid table, 218
show wlan vap, 219
shutdown
  no shutdown (DNS-Client), 360
  shutdown (DNS-Client), 359
shutdown complete, 97, 265
  no shutdown, 98, 265
sinema, 144

sleep, 126
smtp-server, 402
    no smtp-server, 403
smtp-server-enable, 412
    no smtp-server-enable, 412
snmp
    client config, 531
    no client config, 532
snmp access, 376
    no snmp access, 378
snmp agent version, 379
snmp community index, 379
    no snmp community index, 381
snmp engineid migrate, 381
snmp filterprofile, 383
snmp group, 385
    no snmp group, 386
snmp notify, 386
    no snmp notify, 387
snmp targetaddr, 388
    no snmp targetaddr, 390
snmp targetaddr remote-engine-id, 390
snmp targetparams, 391
    no snmp targetparams, 393
snmp user, 396
    no snmp user, 397
snmp v1-v2 readonly, 393
    no snmp v1-v2 readonly, 394
snmp view, 398
    no snmp view, 399
snmpagent, 375
    no snmpagent, 376
snmpagent port, 395
    no snmpagent port, 395
sntp, 202
sntp client addressing-mode, 206
sntp time diff, 203
sntp unicast-server, 204
    no sntp unicast-server, 205
spanning-tree, 289
    no spanning-tree, 290
spanning-tree (properties), 305
    no spanning-tree, 307
spanning-tree (time settings), 302
    no spanning-tree, 303
spanning-tree auto-edge, 308
    no spanning-tree auto-edge, 308
spanning-tree bpdufilter, 309
spanning-tree bpdu-receive, 310
spanning-tree bpdu-transmit, 310
spanning-tree compatibility, 291
    no spanning-tree compatibility, 292
spanning-tree l2t-auto-edge, 292
    no spanning-tree l2t-auto-edge, 293
spanning-tree l2t-edge, 294
    no spanning-tree l2t-edge, 294
spanning-tree mst, 311
spanning-tree mst (properties)
    no spanning-tree mst, 312
spanning-tree mst configuration, 295
spanning-tree mst hello-time, 314
    no spanning-tree mst hello-time, 314
spanning-tree mst instance-id root, 296
    no spanning-tree mst instance-id root, 297
spanning-tree mst max-hops, 297
    no spanning-tree mst max-hops, 298
spanning-tree pathcost dynamic, 299
    no spanning-tree pathcost dynamic, 300
spanning-tree priority, 300
    no spanning-tree priority, 301
ssh-server, 426
    no ssh-server, 426
ssh-server port, 427
    no ssh-server port, 428
ssh-server portssh-server kex-algorithm-level, 429
switchport acceptable-frame-type, 266
    no switchport acceptable-frame-type, 267
switchport access vlan, 268
    no switchport access vlan, 268
switchport ingress-filter, 269
    no switchport ingress-filter, 270
switchport mode, 270
    no switchport mode, 271
switchport priority default, 272
    no switchport priority default, 273
switchport pvid, 274
    no switchport pvid, 274
syslogserver, 547
    no syslogserver, 548
system contact, 91
system location, 92
System manual, 21
system name, 93

T

tcpevent, 181
telnet-server, 328
    no telnet-server, 329
telnet-server port, 329
    no telnet-server port, 330
test, 413
tftp filename, 111
tftp load, 112

tftp save, 113
tftp server, 114
    Saving, 107
TFTP server
    load, 108
time, 190
time dst date, 192
    no time dst, 194
time dst recurring, 193
time set, 191
traceroute, 82

U

user, 186
User name
    Permitted characters and length, 43
user-account, 445
    no user-account, 447
user-account-ext, 448
user-group, 450

V

vap broadcast ssid, 252
    no vap broadcast ssid, 253
vap inter-ap-blocking, 497
    no vap inter-ap-blocking, 497
vap inter-ap-blocking allowed address, 498
    no vap inter-ap-blocking allowed address, 499
vap inter-ap-blocking block gratuitous arp, 500
    no vap inter-ap-blocking block gratuitous arp, 500
vap inter-ap-blocking block non-ip-traffic, 501
    no vap inter-ap-blocking block non-ip-traffic, 502
vap inter-ap-blocking refresh time, 494
vap security authentication, 502
vap security cipher, 503
vap security fast-bss-transition, 504
    no vap security fast-bss-transition, 505
vap security protected-management-frames, 506
    no vap security protected-management-frames, 507
vap security wpa-group-key-update-interval), 507
vap security wpa-psk-passphrase, 508
vap ssid, 251
vlan, 261
    no vlan, 262

W

web-session-timeout, 153
    no web-session-timeout, 154
whoami, 438
wlan, 220
wlan allowed channels, 226
wlan allowed channels only, 225
    no wlan allowed channels only, 227
wlan alternative channel, 228
wlan ampdu, 229
    no wlan ampdu, 229
wlan antenna additional-attenuation, 230
wlan antenna cable-length, 231
wlan antenna gain-2-4GHz, 232
wlan antenna gain-5GHz, 233
wlan antenna mode, 233
wlan antenna type, 235
wlan background scan interval, 236
wlan background scan mode, 236
wlan background scan threshold, 237
wlan beacon interval, 238
wlan channel, 239
WLAN channel width, 240
wlan client mac mode, 240
WLAN Configuration mode, 220
wlan dfs, 241
    no wlan dfs, 242
wlan frequency band, 243
wlan hw entries, 243
wlan ipcf-2, 167
    no wlan ipcf-2, 167
wlan iprp, 160
wlan iprp interface, 162
    no wlan iprp interface, 163
wlan iprp network, 164
    no wlan iprp network, 164
wlan max tx-power, 244
wlan mode, 245
wlan outdoor, 247
    no wlan outdoor, 247
wlan overlap-ap aging, 248
wlan scan-time-per-channell, 249
wlan security ap-radius-authenticator, 483
    no wlan security ap-radius-authenticator, 484
wlan security ap-radius-authenticator address, 485
wlan security ap-radius-authenticator max-retransmit, 486
wlan security ap-radius-authenticator port-number, 487

wlan security ap-radius-authenticator primary, 488
    no wlan security ap-radius-authenticator primary, 489
wlan security ap-radius-authenticator reauth-interval, 489
wlan security ap-radius-authenticator reauth-mode, 490
wlan security ap-radius-authenticator shared-secret, 491
wlan security authentication, 509
wlan security cipher, 510
wlan security context, 492
wlan security dot1x check-server-certificate, 511
    no wlan security dot1x check-server-certificate, 512
wlan security dot1x eap-authentication-type, 513
wlan security dot1x min-tls-version, 493
wlan security dot1x password, 514
wlan security dot1x username, 515
wlan security protected-management-frames, 516
wlan security ssid, 495
wlan security wpa-psk-passphrase, 517
wlan signal-recorder display, 178
wlan signal-recorder start, 176
wlan signal-recorder stop, 179
wlan ssid-table edit, 250
write, 151
write startup-config, 129