

SIMATIC NET

Industrial Ethernet Security SCALANCE S615 Command Line Interface

Configuration Manual

Preface

Security recommendation

1

General

2

General CLI commands

3

Configuration

4

Functions specific to SCALANCE

5

System time

6

Network structures

7

Network protocols

8

Load control

9

Layer 3 functions

10

Security and authentication

11

Diagnostics

12

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.

Preface

Validity of the configuration manual

This Configuration Manual covers the following product:

- SCALANCE S615

This Configuration Manual applies to the following software version:

- SCALANCE S-615 firmware as of version V6.1

Purpose of the Configuration Manual

This Configuration Manual contains the CLI commands that are supported by the SCALANCE S615. You will find the document on the supplied data medium.

Orientation in the documentation

Apart from the Configuration Manual you are currently reading, the following documentation is also available on the topic of remote network:

- Configuration manual SCALANCE S615 Web Based Management

This document is intended to provide you with the information you require to commission and configure SCALANCE S615 devices using the Web Based Management.

- Getting Started

Based on examples, this document explains the configuration of the SCALANCE M800/S 615 device.

- Operating Instructions SINEMA RC Server

You will find this document on the Internet pages of Siemens Industry Online Support. It contains information on the installation, configuration and operation of the application SINEMA Remote Connect Server.

- IP-based remote networks

In this document, the possible configurations of an IP-based remote network are explained in an overview with the requirements and a link to detailed configuration instructions.

You will find this document on the Internet under the following entry ID: 26662448

SIMATIC NET manuals

You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:

- Using the search function:

Link to Siemens Industry Online Support

(<https://support.industry.siemens.com/cs/ww/en/>)

Enter the entry ID of the relevant manual as the search term.

- In the navigation panel on the left-hand side in the "Industrial Communication" area:

Link to the "Industrial Communication" area

(<https://support.industry.siemens.com/cs/ww/en/ps/15247/pm>)

Go to the required product group and make the following settings:

"Entry list" tab, Entry type "Manual"

You will find the documentation for the SIMATIC NET products relevant here on the data storage medium that ships with some products:

- Product CD / product DVD
- SIMATIC NET Manual Collection

Training, Service & Support

You will find information on Training, Service & Support in the multi--language document "DC_support_99.pdf" on the data medium supplied with the documentation.

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary on the Internet at the following address:

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

Security information

Siemens provides products and solutions with industrial security 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 security 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 security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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 customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/industrialsecurity>.

Firmware

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

License conditions

Note

Open source software

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

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

- M87x, M81x, M826, M804PB, S615: OSS_Scalance-M-800-S615_86.pdf

Trademarks

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

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

Table of contents

	Preface	3
1	Security recommendation.....	25
2	General.....	31
2.1	Features not supported.....	31
2.2	Configuration limits for WBM and CLI.....	32
2.3	Use in a PROFINET environment.....	34
2.4	CLI modes.....	35
2.5	Working with the Command Line Interface (CLI).....	37
2.6	The CLI command prompt.....	39
2.7	Symbols of the CLI commands.....	40
2.8	Interface identifiers and addresses.....	41
2.8.1	Naming interfaces.....	41
2.8.2	Address types, address ranges and address masks.....	42
2.8.3	IPv4 address.....	43
3	General CLI commands	45
3.1	clear screen	45
3.2	do	46
3.3	end	47
3.4	exit.....	48
3.5	Help functions and supported input	49
3.5.1	help	49
3.5.2	The command "?"	50
3.5.3	"grep" command	51
3.5.4	Completion of command entries	52
3.5.5	Abbreviated notation of commands	53
3.5.6	Reusing the last used commands.....	53
3.5.7	Working through a command sequence	54
3.5.8	clear history.....	55
3.5.9	The "show" commands	55
3.5.9.1	show history	56
4	Configuration	57
4.1	System	57
4.1.1	The "show" commands	57
4.1.1.1	show cli-console-timeout.....	58
4.1.1.2	show coordinates.....	58
4.1.1.3	show device information	59
4.1.1.4	show interfaces	60

4.1.1.5	show im	61
4.1.1.6	show interface mtu	61
4.1.1.7	show interfaces ... counters	62
4.1.1.8	show lldp neighbors	63
4.1.1.9	show lldp status	63
4.1.1.10	show ip interface	64
4.1.1.11	show versions	65
4.1.2	clear counters	66
4.1.3	configure terminal	67
4.1.4	clear line vty	67
4.1.5	disable	68
4.1.6	enable	69
4.1.7	logout	70
4.1.8	ping	70
4.1.9	Commands in the global configuration mode	71
4.1.9.1	coordinates height	72
4.1.9.2	coordinates latitude	72
4.1.9.3	coordinates longitude	73
4.1.9.4	interface	74
4.1.9.5	no interface	75
4.1.9.6	cli-console-timeout	76
4.1.9.7	no cli-console-timeout	77
4.1.9.8	system contact	78
4.1.9.9	system location	78
4.1.9.10	system name	79
4.1.10	Commands in the Interface configuration mode	80
4.1.10.1	alias	80
4.1.10.2	no alias	81
4.1.10.3	duplex	82
4.1.10.4	no duplex	83
4.1.10.5	lldp	83
4.1.10.6	no lldp	84
4.1.10.7	negotiation	85
4.1.10.8	no negotiation	86
4.1.10.9	shutdown complete	86
4.1.10.10	no shutdown	87
4.1.10.11	speed	88
4.2	Load and Save	89
4.2.1	The "show" commands	89
4.2.1.1	show loadsave files	89
4.2.1.2	show loadsave tftp	90
4.2.1.3	show loadsave stftp	90
4.2.2	load tftp	91
4.2.3	save filetype	92
4.2.4	Commands in the global configuration mode	93
4.2.4.1	loadsave	93
4.2.5	Commands in the LOADSAVE configuration mode	94
4.2.5.1	delete	94
4.2.5.2	tftp filename	95
4.2.5.3	tftp load	96
4.2.5.4	tftp save	97
4.2.5.5	tftp server	97

4.2.5.6	sftp filename.....	98
4.2.5.7	sftp load	99
4.2.5.8	sftp save.....	100
4.2.5.9	sftp server	101
4.2.5.10	password.....	102
4.2.5.11	no password.....	103
4.3	Reset and Defaults	104
4.3.1	restart.....	104
4.4	Configuration Save & Restore	106
4.4.1	The "show" commands	106
4.4.1.1	show running-config.....	106
4.4.2	write startup-config.....	108
4.4.3	Commands in the global configuration mode	108
4.4.3.1	auto-save	109
4.4.3.2	no auto-save	110
4.5	DCP Discovery.....	111
4.5.1	The "show" commands	111
4.5.1.1	show das info	111
4.5.2	Commands in the global configuration mode	112
4.5.2.1	das discover interface	112
4.5.2.2	das mac name	113
4.5.2.3	das mac ip.....	114
4.5.2.4	das mac blink	115
4.5.2.5	das delete	116
4.6	SINEMA	117
4.6.1	The "show" commands	117
4.6.1.1	show sinema	117
4.6.2	Commands in the global configuration mode	117
4.6.2.1	sinema	118
4.6.2.2	no sinema	119
5	Functions specific to SCALANCE.....	121
5.1	PLUG	121
5.1.1	The "show" commands	121
5.1.1.1	show plug.....	121
5.1.2	Commands in the global configuration mode	122
5.1.2.1	plug	122
5.1.3	Commands in the Plug Configuration mode	123
5.1.3.1	presetplug	123
5.1.3.2	firmware-on-plug	124
5.1.3.3	no firmware on plug	124
5.1.3.4	factoryclean.....	125
5.1.3.5	write.....	125
5.2	WBM	127
5.2.1	The "show" commands	127
5.2.1.1	show web-session-timeout	127
5.2.2	Commands in the global configuration mode	128
5.2.2.1	web-session-timeout	128
5.2.2.2	no web-session-timeout	129

5.3	Digital input/output	130
5.3.1	The "show" commands	130
5.3.1.1	show digital input.....	130
5.3.1.2	show digital output	131
5.3.2	Commands in the global configuration mode	131
5.3.2.1	digital output closed	131
5.3.2.2	digital output open.....	132
5.4	cRSP / SRS.....	133
5.4.1	The "show" commands	133
5.4.1.1	show srs	133
5.4.1.2	show srs logon	134
5.4.2	Commands in the global configuration mode	134
5.4.2.1	srs	135
5.4.3	Commands in the SRS configuration mode.....	135
5.4.3.1	logon	136
5.4.3.2	no logon	136
5.4.3.3	logon idx authority	137
5.4.3.4	logon idx fragment	138
5.4.3.5	logon idx path.....	139
5.4.3.6	logon idx query	140
5.4.3.7	logon show-idx	141
5.4.3.8	shutdown.....	141
5.4.3.9	no shutdown.....	142
5.4.3.10	interval.....	143
5.4.3.11	validate cert.....	144
5.5	SINEMA RC	145
5.5.1	Introduction to the SRC section	145
5.5.2	The "show" commands	145
5.5.2.1	show sinemarc	145
5.5.3	Commands in the global configuration mode	146
5.5.3.1	sinemarc.....	146
5.5.4	Commands in the SINEMARC configuration mode	147
5.5.4.1	addr	147
5.5.4.2	autoenrollment interval.....	148
5.5.4.3	autofwnat.....	149
5.5.4.4	connection type	150
5.5.4.5	no autofwnat.....	151
5.5.4.6	device id	152
5.5.4.7	device pw	153
5.5.4.8	port	154
5.5.4.9	proxy	155
5.5.4.10	no proxy	156
5.5.4.11	shutdown.....	156
5.5.4.12	no shutdown.....	157
5.5.4.13	verification cacert	158
5.5.4.14	verification fingerprint.....	159
5.6	SELECT/SET button	160
5.6.1	Commands in the global configuration mode	160
5.6.1.1	panel-button control-restart.....	160
5.6.1.2	no panel-button control-restart.....	161

6	System time.....	163
6.1	System time setting.....	163
6.1.1	The "show" commands	163
6.1.1.1	show dst info	163
6.1.1.2	show time	164
6.1.2	Commands in the global configuration mode	164
6.1.2.1	time	165
6.1.2.2	time dst date	166
6.1.2.3	time dst recurring	167
6.1.2.4	no time dst	168
6.1.2.5	time set	169
6.2	NTP client	170
6.2.1	The "show" commands	170
6.2.1.1	show ntp info	170
6.2.2	Commands in the global configuration mode	171
6.2.2.1	ntp	171
6.2.3	Commands in the NTP configuration mode.....	172
6.2.3.1	ntp server id	172
6.2.3.2	no ntp server id	173
6.2.3.3	ntp server secure	174
6.2.3.4	ntp secure	175
6.2.3.5	no ntp secure	176
6.2.3.6	ntp time diff	176
6.3	NTP server.....	178
6.3.1	show ntp server info.....	178
6.3.2	Commands in the global configuration mode	178
6.3.2.1	ntp server	179
6.3.2.2	no ntp server	179
6.3.3	Commands in the NTP server configuration mode.....	180
6.3.3.1	ntp server interface	180
6.3.3.2	no ntp server interface	182
6.3.3.3	ntp server secure interface	183
6.3.3.4	no ntp server secure interface	184
6.4	SNTP client	185
6.4.1	The "show" commands	185
6.4.1.1	show sntp broadcast-mode status	185
6.4.1.2	show sntp status	186
6.4.1.3	show sntp unicast-mode status	186
6.4.2	Commands in the global configuration mode	187
6.4.2.1	sntp	187
6.4.3	Commands in the SNTP configuration mode	188
6.4.3.1	sntp time diff.....	188
6.4.3.2	sntp unicast-server.....	189
6.4.3.3	no sntp unicast-server.....	191
6.4.3.4	sntp client addressing-mode.....	192
7	Network structures	193
7.1	VLAN.....	193
7.1.1	The "show" commands	193
7.1.1.1	show vlan	193

7.1.1.2	show vlan device info	194
7.1.1.3	show vlan learning params	195
7.1.1.4	show vlan port config	196
7.1.1.5	show vlan protocols-group	197
7.1.2	Commands in the global configuration mode	197
7.1.2.1	base bridge-mode	198
7.1.2.2	interface range	199
7.1.2.3	no interface range	200
7.1.2.4	map protocol	201
7.1.2.5	no map protocol	202
7.1.2.6	no protocol-vlan.....	203
7.1.2.7	protocol-vlan.....	203
7.1.2.8	subnet-vlan.....	204
7.1.2.9	no subnet-vlan.....	205
7.1.2.10	vlan.....	205
7.1.2.11	no vlan.....	206
7.1.3	Commands in the interface configuration mode	207
7.1.3.1	mtu	207
7.1.3.2	shutdown complete	208
7.1.3.3	no shutdown.....	209
7.1.3.4	switchport acceptable-frame-type	209
7.1.3.5	no switchport acceptable-frame-type	210
7.1.3.6	switchport ingress-filter	211
7.1.3.7	no switchport ingress-filter	212
7.1.3.8	switchport mode	212
7.1.3.9	no switchport mode.....	213
7.1.3.10	switchport priority default	214
7.1.3.11	no switchport priority default	215
7.1.3.12	switchport pvid	216
7.1.3.13	no switchport pvid	216
7.1.4	Commands in the VLAN configuration mode.....	217
7.1.4.1	ip address.....	217
7.1.4.2	no ip address.....	218
7.1.4.3	name	219
7.1.4.4	no name	220
7.1.4.5	ports	221
7.1.4.6	no ports	222
7.1.4.7	tia interface.....	223
7.2	PPP	225
7.2.1	The "show" commands	225
7.2.1.1	show ppp information	225
7.2.2	Commands in the global configuration mode	226
7.2.2.1	interface ppp	226
7.2.3	Commands in the Interface configuration mode	227
7.2.3.1	forced disconnect	227
7.2.3.2	forced disconnect time	228
7.2.3.3	interface vlan.....	229
7.2.3.4	ip address.....	229
7.2.3.5	ip address dhcp.....	230
7.2.3.6	no ip address.....	231
7.2.3.7	password.....	232
7.2.3.8	shutdown.....	232

7.2.3.9	no shutdown.....	233
7.2.3.10	type ppo-ex	234
7.2.3.11	username	235
7.3	Passive Listening	236
7.3.1	The "show" commands	236
7.3.1.1	show passive-listening	236
7.3.2	Commands in the global configuration mode	236
7.3.2.1	passive-listening bpdu-vlan-flood	237
7.3.2.2	no passive-listening bpdu-vlan-flood	237
7.3.2.3	passive-listening	238
7.3.2.4	no passive-listening	239
7.4	Spanning Tree	240
7.4.1	The "show" commands	240
7.4.1.1	show spanning-tree.....	240
7.4.1.2	show spanning-tree active	241
7.4.1.3	show spanning-tree bridge	242
7.4.1.4	show spanning-tree detail.....	243
7.4.1.5	show spanning-tree interface.....	243
7.4.1.6	show spanning-tree interface layer2-gateway-port.....	244
7.4.1.7	show spanning-tree root	245
7.4.2	clear spanning-tree detected protocols.....	246
7.4.3	clear spanning-tree counters	247
7.4.4	Commands in the global configuration mode	247
7.4.4.1	spanning-tree	247
7.4.4.2	no spanning-tree	248
7.4.4.3	spanning-tree (time settings)	249
7.4.4.4	no spanning-tree (time settings)	250
7.4.5	Commands in the Interface configuration mode	251
7.4.5.1	spanning-tree	252
7.4.5.2	no spanning-tree	254
7.4.5.3	spanning-tree auto-edge.....	255
7.4.5.4	no spanning-tree auto-edge.....	256
8	Network protocols	257
8.1	IPv4 protocol	257
8.1.1	The "show" commands	257
8.1.1.1	show ip dns	257
8.1.1.2	show dcp forwarding	258
8.1.1.3	show dcp server.....	259
8.1.1.4	show ip route.....	259
8.1.1.5	show ip routing.....	260
8.1.1.6	show ip static route	261
8.1.1.7	show ip telnet	261
8.1.2	Commands in the global configuration mode	262
8.1.2.1	dcp server	262
8.1.2.2	no dcp server	263
8.1.2.3	ip echo-reply	263
8.1.2.4	no ip echo-reply	264
8.1.2.5	ip route	265
8.1.2.6	no ip route	266
8.1.2.7	ip routing	267

8.1.2.8	no ip routing	268
8.1.2.9	telnet-server	268
8.1.2.10	no telnet-server	269
8.1.3	Commands in the Interface configuration mode	270
8.1.3.1	dcp forwarding.....	270
8.1.3.2	ip address.....	271
8.1.3.3	ip address dhcp.....	272
8.1.3.4	no ip address.....	273
8.2	ARP	274
8.2.1	The "show" commands	274
8.2.1.1	show ip arp.....	274
8.3	DHCP client.....	276
8.3.1	The "show" commands	276
8.3.1.1	show ip dhcp client.....	276
8.3.2	Commands in the global configuration mode	277
8.3.2.1	ip dhcp config-file-request.....	277
8.3.2.2	no ip dhcp config-file-request.....	278
8.3.2.3	ip dhcp client mode	279
8.3.2.4	dhcp duid type.....	280
8.4	DHCP server.....	281
8.4.1	The "show" commands	281
8.4.1.1	show ip dhcp-server bindings	282
8.4.1.2	show ip dhcp-server pools	282
8.4.2	Commands in the global configuration mode	283
8.4.2.1	ip dhcp-server	283
8.4.2.2	no ip dhcp-server	284
8.4.2.3	no ip dhcp-server icmp-probe	285
8.4.2.4	ip dhcp-server icmp-probe	286
8.4.2.5	ip dhcp-server pool	287
8.4.2.6	no ip dhcp-server pool	288
8.4.3	Commands in the DHCPPOOL configuration mode.....	289
8.4.3.1	lease-time.....	289
8.4.3.2	network.....	290
8.4.3.3	option (IP address).....	291
8.4.3.4	option value-hex.....	293
8.4.3.5	option value-string.....	294
8.4.3.6	no option	295
8.4.3.7	pool-enable	296
8.4.3.8	no pool-enable	297
8.4.3.9	set-interface	298
8.4.3.10	static-lease	299
8.4.3.11	no static-lease	300
8.5	DNS.....	301
8.5.1	The "show" commands	301
8.5.1.1	show dnsclient information.....	301
8.5.1.2	show ddnsclient information.....	302
8.5.2	Commands in the global configuration mode	302
8.5.2.1	dnsclient	303
8.5.2.2	dnsproxy.....	303
8.5.2.3	ddnsclient	304

8.5.3	Commands in the DNS CLIENT configuration mode	305
8.5.3.1	manual srv	305
8.5.3.2	no manual srv	306
8.5.3.3	server type	306
8.5.3.4	shutdown.....	307
8.5.3.5	no shutdown.....	308
8.5.4	Commands in the DNS PROXY configuration mode.....	309
8.5.4.1	cachenxdomain.....	309
8.5.4.2	no cachenxdomain.....	309
8.5.4.3	shutdown.....	310
8.5.4.4	no shutdown.....	311
8.5.5	Commands in the DDNS Client configuration mode	311
8.5.5.1	service.....	312
8.5.5.2	no service.....	312
8.5.5.3	userhost	313
8.5.5.4	username	314
8.5.5.5	password.....	315
8.6	SNMP.....	316
8.6.1	The "show" commands	317
8.6.1.1	show snmp.....	317
8.6.1.2	show snmp community	317
8.6.1.3	show snmp engineID	318
8.6.1.4	show snmp filter	318
8.6.1.5	show snmp group.....	319
8.6.1.6	show snmp group access	319
8.6.1.7	show snmp inform statistics.....	320
8.6.1.8	show snmp notif	320
8.6.1.9	show snmp targetaddr	321
8.6.1.10	show snmp targetparam	321
8.6.1.11	show snmp tcp	322
8.6.1.12	show snmp user.....	322
8.6.1.13	show snmp viewtree	323
8.6.2	Commands in the global configuration mode	323
8.6.2.1	snmpagent	324
8.6.2.2	no snmpagent	324
8.6.2.3	snmp agent version.....	325
8.6.2.4	snmp access	325
8.6.2.5	no snmp access	327
8.6.2.6	snmp community index	328
8.6.2.7	no snmp community index	329
8.6.2.8	snmp filterprofile.....	330
8.6.2.9	no snmp filterprofile.....	331
8.6.2.10	snmp group	332
8.6.2.11	no snmp group	333
8.6.2.12	snmp notify.....	334
8.6.2.13	no snmp notify.....	335
8.6.2.14	snmp targetaddr.....	335
8.6.2.15	no snmp targetaddr.....	337
8.6.2.16	snmp targetparams	338
8.6.2.17	no snmp targetparams	340
8.6.2.18	snmp v1-v2 readonly.....	340
8.6.2.19	no snmp v1-v2 readonly.....	341

8.6.2.20	snmp user	342
8.6.2.21	no snmp user	343
8.6.2.22	snmp view	343
8.6.2.23	no snmp view	345
8.7	HTTP server	346
8.7.1	The "show" commands	346
8.7.1.1	show ip http server status	346
8.7.2	Commands in the Global Configuration mode	347
8.7.2.1	ip http	347
8.7.2.2	no ip http	348
8.8	HTTPS server	349
8.8.1	The "show" commands	349
8.8.1.1	show ip http secure server status	349
8.8.1.2	show ssl server-cert	349
8.8.2	Commands in the Global Configuration mode	350
8.8.2.1	ip http secure minimum tls-version	350
8.8.2.2	ip http https redirection	351
8.9	Proxy server	352
8.9.1	The "show" commands	352
8.9.1.1	show proxyserver table	352
8.9.2	Commands in the global configuration mode	352
8.9.2.1	proxyserver	353
8.9.3	Commands in the PROXYSERVER configuration mode	353
8.9.3.1	srv name	354
8.9.3.2	no srv	355
8.9.3.3	srv name addr	356
8.9.3.4	srv name auth	357
8.9.3.5	srv name port	358
8.9.3.6	srv name pw	359
8.9.3.7	srv name type	360
8.9.3.8	srv name user	361
8.9.3.9	srv show-names	362
8.10	SMTP client	363
8.10.1	The "show" commands	363
8.10.1.1	show events smtp-server	363
8.10.1.2	show events sender email	363
8.10.1.3	show events smtp-port	364
8.10.2	Commands in the Events configuration mode	364
8.10.2.1	send test mail	365
8.10.2.2	smtp-server	365
8.10.2.3	no smtp-server	366
8.10.3	Commands in SMTP server configuration mode	367
8.10.3.1	auth username	367
8.10.3.2	no auth username	368
8.10.3.3	port	369
8.10.3.4	no port	370
8.10.3.5	receiver-address	370
8.10.3.6	no receiver-address	371
8.10.3.7	security	372
8.10.3.8	no security	372

8.10.3.9	sender address	373
8.10.3.10	no sender address	374
8.10.3.11	test	375
8.11	SSH server.....	376
8.11.1	The "show" commands	376
8.11.1.1	show ip ssh	376
8.11.2	Commands in the Global Configuration mode.....	377
8.11.2.1	ssh-server	377
8.11.2.2	no ssh-server	378
9	Load control.....	379
9.1	Flow control.....	379
9.1.1	The "show" commands	379
9.1.1.1	show flow-control	379
9.1.2	Commands in the interface configuration mode	380
9.1.2.1	flowcontrol.....	381
9.2	Dynamic MAC aging	382
9.2.1	The "show" commands	382
9.2.1.1	show mac-address-table aging-time.....	382
9.2.1.2	show mac-address-table aging-status	383
9.2.2	Commands in the global configuration mode	383
9.2.2.1	mac-address-table aging	384
9.2.2.2	no mac-address-table aging	385
9.2.2.3	mac-address-table aging-time	386
10	Layer 3 functions.....	387
10.1	VRRPv3 (IPv4).....	387
10.1.1	clear vrrp3 statistics	387
10.1.2	The "show" commands	388
10.1.2.1	show vrrp3	388
10.1.2.2	show vrrp3 interface.....	389
10.1.2.3	show vrrp3 track.....	390
10.1.3	Commands in the global configuration mode	390
10.1.3.1	router vrrp3	391
10.1.3.2	no router vrrp3	391
10.1.4	Commands in the VRRP3 Router configuration mode	392
10.1.4.1	interface	392
10.1.4.2	no interface	393
10.1.4.3	track interface	394
10.1.4.4	no track interface	395
10.1.4.5	track links	396
10.1.4.6	no track links	397
10.1.4.7	vrrp vrid-track	398
10.1.4.8	no vrrp vrid-track	399
10.1.5	Commands in the Interface Configuration mode	399
10.1.5.1	vrrp associated-ip.....	400
10.1.5.2	no vrrp associated-ip.....	400
10.1.5.3	vrrp primary-ip	401
10.1.5.4	no vrrp primary-ip	402
10.1.5.5	vrrp priority	403
10.1.5.6	no vrrp priority	404

10.1.5.7	vrrp timer	405
10.1.5.8	no vrrp timer	406
10.1.5.9	vrrp track decrement	407
10.1.5.10	no vrrp track	408
10.2	NAT	409
10.2.1	The "show" commands	409
10.2.1.1	show firewallnat masquerading.....	409
10.2.1.2	show firewallnat napt	409
10.2.1.3	show firewallnat netmap	410
10.2.1.4	show firewallnat src-nat	410
10.2.2	Commands in the global configuration mode	411
10.2.2.1	firewallnat	411
10.2.3	Commands in the FIREWALL NAT configuration mode.....	412
10.2.3.1	Introductory sentence for the FirewallNAT configuration mode.....	412
10.2.3.2	ipsec connection show-idx	412
10.2.3.3	masquerading show-idx	413
10.2.3.4	masquerading	414
10.2.3.5	no masquerading	415
10.2.3.6	napt show-idx	416
10.2.3.7	napt type ipv4.....	416
10.2.3.8	no napt	418
10.2.3.9	no napt all.....	419
10.2.3.10	netmap destination srcint	420
10.2.3.11	netmap show-idx	422
10.2.3.12	netmap source type ipv4	423
10.2.3.13	no netmap srcint.....	425
10.2.3.14	no netmap all.....	426
10.2.3.15	src-nat show-idx	427
10.2.3.16	src-nat type ipv4	428
10.2.3.17	no src-nat all.....	430
10.2.3.18	no src-nat	430
11	Security and authentication	433
11.1	RADIUS client	433
11.1.1	The "show" commands	433
11.1.1.1	show radius statistics	433
11.1.1.2	show radius server.....	434
11.1.2	Commands in the global configuration mode	434
11.1.2.1	login authentication	435
11.1.2.2	no login authentication	436
11.1.2.3	radius authorization-mode	436
11.1.2.4	radius-server	437
11.1.2.5	no radius-server	439
11.2	User management	440
11.2.1	The "show" commands	440
11.2.1.1	show password-policy.....	440
11.2.1.2	show roles	441
11.2.1.3	show user-accounts	441
11.2.1.4	show user-groups.....	442
11.2.1.5	show users	443
11.2.2	change password	443

11.2.3	whoami.....	444
11.2.4	Commands in the global configuration mode	445
11.2.4.1	loginpage	445
11.2.4.2	password-policy	446
11.2.4.3	role	447
11.2.4.4	no role	448
11.2.4.5	user-account	449
11.2.4.6	no user-account	451
11.2.4.7	user-account-ext	452
11.2.4.8	no user-account-ext	454
11.2.4.9	user-group.....	454
11.2.4.10	no user-group.....	455
11.2.4.11	username	456
11.3	Firewall.....	458
11.3.1	Introduction to the Firewall section	458
11.3.2	The "show" commands	458
11.3.2.1	show firewall icmp-services ipv4.....	458
11.3.2.2	show firewall information.....	458
11.3.2.3	show firewall ip-protocols.....	459
11.3.2.4	show firewall ip-rules ipv4	459
11.3.2.5	show firewall ip-services	460
11.3.2.6	show firewall pre-rules ipv4	460
11.3.2.7	show firewall ruleset.....	461
11.3.2.8	show firewall ruleset assignment	461
11.3.3	Commands in the global configuration mode	462
11.3.3.1	firewall	462
11.3.4	Commands in the FIREWALL configuration mode.....	463
11.3.4.1	Introductory sentence for the Firewall configuration mode.....	463
11.3.4.2	di-input set address.....	465
11.3.4.3	di-input set ruleset.....	466
11.3.4.4	di-input show-idx	467
11.3.4.5	icmp name	467
11.3.4.6	no icmp	469
11.3.4.7	icmp name set type.....	469
11.3.4.8	icmp show-names	471
11.3.4.9	icmp show-types-codes	471
11.3.4.10	idle timeout icmp	472
11.3.4.11	idle timeout tcp.....	472
11.3.4.12	idle timeout udp.....	473
11.3.4.13	ipv4rule	474
11.3.4.14	ipv4rule del ruleset.....	477
11.3.4.15	no ipv4 rule	477
11.3.4.16	ipv4rule set action	478
11.3.4.17	ipv4rule set dstip	479
11.3.4.18	ipv4rule set from	480
11.3.4.19	ipv4rule set log.....	481
11.3.4.20	ipv4rule set prior	482
11.3.4.21	ipv4rule set ruleset.....	483
11.3.4.22	ipv4rule set service	484
11.3.4.23	ipv4rule set srcip	485
11.3.4.24	ipv4rule set to.....	486
11.3.4.25	ipv4rule ipsec connection	487

11.3.4.26	ipv4rule show interfaces	488
11.3.4.27	ipv4rule show-rules	489
11.3.4.28	prerule all ipv4.....	489
11.3.4.29	prerule cloudconnector ipv4	490
11.3.4.30	prerule dhcp ipv4.....	491
11.3.4.31	prerule dns ipv4.....	492
11.3.4.32	prerule http ipv4	493
11.3.4.33	prerule https ipv4.....	494
11.3.4.34	prerule ipsec ipv4	495
11.3.4.35	prerule ipv4 show-int.....	496
11.3.4.36	prerule ping ipv4.....	497
11.3.4.37	prerule snmp ipv4.....	498
11.3.4.38	prerule ssh ipv4.....	499
11.3.4.39	prerule systime ipv4	500
11.3.4.40	prerule telnet ipv4.....	501
11.3.4.41	proto name	502
11.3.4.42	no proto	503
11.3.4.43	proto show-names	503
11.3.4.44	ruleset idx.....	504
11.3.4.45	ruleset name	505
11.3.4.46	ruleset show-idx	506
11.3.4.47	no ruleset	507
11.3.4.48	service name.....	508
11.3.4.49	no service.....	509
11.3.4.50	service name set dst.....	510
11.3.4.51	service name set prot.....	511
11.3.4.52	service name set src	512
11.3.4.53	service show-names	513
11.3.4.54	shutdown.....	513
11.3.4.55	no shutdown.....	514
11.3.4.56	useraccount show-idx	515
11.3.4.57	useraccount ruleset.....	516
11.3.4.58	no useraccount ruleset.....	517
11.4	IPsec VPN.....	518
11.4.1	The "show" commands	518
11.4.1.1	show ipsec conn-authentication.....	518
11.4.1.2	show ipsec connections	519
11.4.1.3	show ipsec conn-phase1	519
11.4.1.4	show ipsec conn-phase2	520
11.4.1.5	show ipsec information	520
11.4.1.6	show ipsec remoteend	521
11.4.2	Commands in the global configuration mode	521
11.4.2.1	ipsec.....	522
11.4.3	Commands in the IPSEC configuration mode	522
11.4.3.1	crl-policy	522
11.4.3.2	connection name.....	523
11.4.3.3	no connection name.....	524
11.4.3.4	no connection all	525
11.4.3.5	nat-keep-alive.....	525
11.4.3.6	remote-end name.....	526
11.4.3.7	no remote-end name.....	527
11.4.3.8	no remote-end all	528

11.4.3.9	shutdown.....	529
11.4.3.10	no shutdown.....	529
11.4.4	Commands in the IPSEC REMOTE END configuration mode	530
11.4.4.1	addr	530
11.4.4.2	addr-mode.....	531
11.4.4.3	conn-mode	532
11.4.4.4	subnet	533
11.4.4.5	vir-ip	534
11.4.4.6	no vir-ip	535
11.4.5	Commands in the IPSEC CONNECTION configuration mode.....	535
11.4.5.1	authentication.....	536
11.4.5.2	k-proto	536
11.4.5.3	loc-subnet	537
11.4.5.4	operation	538
11.4.5.5	phase	539
11.4.5.6	rmend name.....	539
11.4.5.7	timeout	540
11.4.5.8	vir-ip	541
11.4.5.9	no vir-ip	542
11.4.6	Commands in the IPSEC AUTHENTICATION configuration mode	542
11.4.6.1	auth cacert	543
11.4.6.2	auth psk	544
11.4.6.3	auth remcert.....	545
11.4.6.4	no auth	546
11.4.6.5	local-id.....	546
11.4.6.6	no local-id.....	547
11.4.6.7	rem-id	548
11.4.6.8	no rem-id	549
11.4.7	Commands in the IPSEC PHASE1 configuration mode.....	549
11.4.7.1	aggressive.....	550
11.4.7.2	no aggressive.....	551
11.4.7.3	default-ciphers	552
11.4.7.4	no default-ciphers	553
11.4.7.5	dpd	554
11.4.7.6	no dpd	554
11.4.7.7	dpd-period	555
11.4.7.8	dpd-timeout	556
11.4.7.9	ike-auth	557
11.4.7.10	ike-encryption.....	557
11.4.7.11	ike-keyderivation	559
11.4.7.12	ike-keytries	560
11.4.7.13	ike-lifetime	560
11.4.8	Commands in the IPSEC PHASE2 configuration mode.....	561
11.4.8.1	auto-fwrules	562
11.4.8.2	no auto-fwrules	562
11.4.8.3	default-ciphers	563
11.4.8.4	no default-ciphers	564
11.4.8.5	esp-auth	565
11.4.8.6	esp-encryption	566
11.4.8.7	esp-keyderivation.....	567
11.4.8.8	lifebyte.....	568
11.4.8.9	lifetime.....	569

11.4.8.10	port	570
11.4.8.11	proto	571
11.5	Certificates	572
11.5.1	Commands in the global configuration mode	572
11.5.1.1	certificate	572
11.5.2	Commands in the CERT configuration mode	573
11.5.2.1	The "show" commands	573
11.5.2.2	cacert	574
11.5.2.3	del	575
11.5.2.4	passphrase	576
11.5.2.5	passphrase show-idx	577
11.6	OpenVPN	578
11.6.1	The "show" commands	578
11.6.1.1	show openvpn authentication	578
11.6.1.2	show openvpn connections	579
11.6.1.3	show openvpn remoteend	579
11.6.2	Commands in the global configuration mode	580
11.6.2.1	openvpn	580
11.6.3	OPENVPN configuration mode	581
11.6.3.1	connection name	581
11.6.3.2	no conn	582
11.6.3.3	remote name	583
11.6.3.4	no remote	584
11.6.3.5	shutdown	584
11.6.3.6	no shutdown	585
11.6.4	Commands in the OPENVPN REMOTE END configuration mode	586
11.6.4.1	connection	586
11.6.4.2	port	587
11.6.4.3	proto	587
11.6.4.4	proxy	588
11.6.4.5	remote-addr	589
11.6.4.6	show-context	590
11.6.5	Commands in the OPENVPN CONNECTION configuration mode	590
11.6.5.1	auth-algo	591
11.6.5.2	authentication	591
11.6.5.3	autoFW	592
11.6.5.4	encryp-algo	593
11.6.5.5	NAT	594
11.6.5.6	operation	595
11.6.5.7	LZO	596
11.6.5.8	no LZO	596
11.6.5.9	show auth-names	597
11.6.5.10	show context	598
11.6.6	Commands in the OPENVPN AUTHENTICATION configuration mode	598
11.6.6.1	auth	598
11.6.6.2	no auth	600
11.6.6.3	auth user	601
12	Diagnostics	603
12.1	Event and fault handling	603
12.1.1	The "show" commands	603

12.1.1.1	show events config	604
12.1.1.2	show events severity.....	604
12.1.1.3	show events faults config.....	605
12.1.1.4	show events faults status.....	605
12.1.1.5	show fault counter.....	606
12.1.1.6	show fwlog	607
12.1.1.7	show logbook	607
12.1.1.8	show power-line-state	608
12.1.1.9	show seclog	609
12.1.2	clear fault counter	609
12.1.3	clear fwlog	610
12.1.4	clear logbook.....	611
12.1.5	clear seclog	611
12.1.6	fault report ack	612
12.1.7	no logging console	612
12.1.8	logging console	613
12.1.9	Commands in the global configuration mode	614
12.1.9.1	events	614
12.1.10	Commands in the Events configuration mode	615
12.1.10.1	add log	615
12.1.10.2	client config	616
12.1.10.3	no client config	617
12.1.10.4	event config.....	618
12.1.10.5	no event config.....	621
12.1.10.6	link.....	622
12.1.10.7	no link.....	623
12.1.10.8	severity.....	624
12.1.10.9	no severity.....	625
12.2	Syslog client.....	626
12.2.1	The "show" commands	626
12.2.1.1	show events syslogserver.....	626
12.2.2	Commands in the Events configuration mode	626
12.2.2.1	syslogserver	627
12.2.2.2	no syslogserver.....	628
Index.....		629

Security recommendation

To prevent unauthorized access, note the following security recommendations.

A checklist supports you in setting up your device. You can find the checklist at the following address: (<https://support.industry.siemens.com/cs/ww/en/view/109745536>)

General

- You should make regular checks to make sure that the device meets these recommendations and/or other security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products:
Link: (<https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx>)
- 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.
- 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, Open VPN).
- Separate connections correctly (WBM, Telnet, SSH etc.).

Physical access

- Limit physical access to the device to qualified personnel.
The memory card or the PLUG (C-PLUG, KEY-PLUG) contains sensitive data such as certificates, keys etc. that can be read out and modified.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.

Software (security functions)

- Keep the software up to date. Check regularly for security updates of the product. You will find information on this on the Internet pages "Industrial Security (<https://www.siemens.com/industrialsecurity>)".
- Inform yourself regularly about security advisories and bulletins published by Siemens ProductCERT (<https://www.siemens.com/cert/en/cert-security-advisories.htm>).
- Only activate protocols that you really require to use the device.
- Restrict access to the management of the device with firewall rules.
- The option of VLAN structuring provides good protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.

- Use a central logging server to log changes and accesses. Operate your logging server within the protected network area and check the logging information regularly.
- We recommend formatting a PLUG that is not being used.

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update passwords and keys to increase security.
- Change all default passwords for users before you operate the device.
- Only use passwords with a high password strength. Avoid weak passwords for example password1, 123456789, abcdefgh.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems or after it has expired.

Keys and certificates

This section deals with the security keys and certificates you require to set up TLS, VPN (IPsec, OpenVPN) and SINEMA RC.

- The device contains a pre-installed X.509 certificate with key. Replace this certificate with a self-made certificate with key. We recommend that you use a certificate signed by a reliable external or internal certification authority.
- 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.
- Verify certificates and fingerprints on the server and client to prevent "man in the middle" attacks.
- It is recommended that you use password-protected certificates in the PKCS#12 format.
- It is recommended that you use certificates with a key length of at least 2048 bits.
- Change keys and certificates immediately, if there is a suspicion of compromise.

Secure/non-secure protocols

- Avoid or disable non-secure protocols, for example Telnet and TFTP. For historical reasons, these protocols are still available, however not intended for secure applications. Use non-secure protocols on the device using a secure connection (e.g. SINEMA RC).
- Avoid or disable non-secure protocols. Check whether use of the following protocols is necessary:
 - Telnet
 - HTTP
 - Broadcast pings
 - Non authenticated and unencrypted interfaces
 - ICMP (redirect)
 - LLDP
 - Syslog
 - DHCP Options 66/67
 - SNTP
 - NTP
 - TFTP
 - TIA Portal Cloud Connector
- The following protocols provide secure alternatives:
 - SNMPv1/v2 → SNMPv3
Check whether use of SNMPv1 is necessary. SNMPv1 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.
 - HTTP → HTTPS
 - Telnet → SSH
 - NTP → Secure NTP
 - SNTP → Secure NTP
 - TFTP → SFTP
 - TIA Portal Cloud Connector using a secure connection.
Use the "TIA Portal Cloud Connector" integrated in the product over a VPN solution (e.g. SINEMA RC).
Configure the firewall settings of the SCALANCE M800/S615 (e.g. predefined IPv4 rules "Cloud Connector" to prevent unauthorized access of network devices to the "TIA Portal Cloud Connector Server").
- Use secure protocols when access to the device is not prevented by physical protection measures.

- To prevent unauthorized access to the device or network, take suitable protective measures against non-secure protocols.
- If you require non-secure protocols and services, activate these at interfaces that are located within a protected network area.
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- For the DCP function, enable the "DCP read-only" mode after commissioning.

List of available protocols

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

Service	Protocol/ Port number	Default port status		Configurable		Authentica- tion	Encryption
		Local access	External access ¹⁾	Service	Port		
DHCP client	UDP/68	Closed	Closed	✓	--	--	--
DHCP server	UDP/67	Closed ²⁾	Closed ³⁾	✓	--	--	--
DNS client	TCP/53 UDP/53	Outgoing only	Outgoing only	✓	--	--	--
DNS server	TCP/53 UDP/53	Open ⁴⁾	Closed	✓	--	--	--
DynDNS	TCP/80	Outgoing only	Outgoing only	✓	--	✓	--
HTTP	TCP/80	Open	Closed	--	--	✓	--
HTTP Proxy	TCP/80 TCP/443	Outgoing only	Outgoing only	✓	✓	Optional	--
HTTPS	TCP/443	Open	Closed	✓	--	✓	✓
IPsec/IKE	UDP/500 UDP/4500	Closed	Closed	✓	--	✓	✓
NTP client	UDP/123	Outgoing only	Outgoing only	✓	✓	--	--
NTP client (se- cure)	UDP/123	Outgoing only	Outgoing only	✓	✓	✓	--
NTP server	UDP/123	Closed	Closed	✓	✓	--	--
NTP server (secure)	UDP/123	Closed	Closed	✓	✓	✓	--
OpenVPN	UDP/1194 TCP/1194	Outgoing only	Outgoing only	✓	✓	✓	✓
Ping	ICMP	Open	Closed	✓	--	✓	--
PROFINET	UDP/34964	Closed	Closed	--	--	--	--
RADIUS client	TCP/1812 UDP/1812	Outgoing only	Outgoing only	✓	✓	✓	--
SFTP	TCP/22	Outgoing only	Outgoing only	✓	✓	✓	✓
Siemens Re- mote Service (cRSP/SRS)	TCP/443	Outgoing only	Outgoing only	✓	--	Optional	✓

Service	Protocol/ Port number	Default port status		Configurable		Authentica- tion	Encryption
		Local access	External access ¹⁾	Service	Port		
SINEMA RC	HTTPS/443 and TCP/UDP depending on the server configuration	Outgoing only	Outgoing only	✓	✓	✓	✓
SMTP	TCP/25	Outgoing only	Outgoing only	✓	✓	--	--
SMTP (Secure)	TCP/465 TCP/587	Outgoing only	Outgoing only	✓	✓	Optional	✓
SNMPv1	UDP/161	Open	Closed	✓	--	--	--
SNMPv3	UDP/161	Open	Closed	✓	--	Optional	Optional
SNTP	UDP/123	Closed	Closed	✓	--	--	--
SSH	TCP/22	Open	Closed	✓	--	✓	✓
Syslog	UDP/514	Outgoing only	Outgoing only	✓	✓	--	--
Telnet	TCP/23	Closed	Closed	✓	--	✓	--
TFTP	UDP/69	Outgoing only	Outgoing only	✓	✓	--	--
TIA Portal Cloud Connector ⁵⁾	TCP/9023	Closed	Closed	✓	✓	--	--

¹⁾ SCALANCE M826 and M804PB can only be accessed via vlan1 when delivered (factory setting).

²⁾ Only open with SCALANCE M826

³⁾ Only open with SCALANCE S615

⁴⁾ Only closed with SCALANCE S615

⁵⁾ Only with SCALANCE M804PB

Explanation for table:

- Default port status

The port status on delivery (factory setting) distinguishes between local and external access.

- Local access: The port is accessed via a local connection (vlan1).
- External access: The port is accessed via an external connection (vlan2).

- Service / Port configurable

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.

General

2.1 Features not supported

The following feature is not supported by the SCALANCE M-800 devices:

- IPv6

Even if this feature is listed as a parameter in the documentation and is displayed with the help functions `help` and `?`, you cannot execute it with a SCALANCE XB-800.

2.2 Configuration limits for WBM and CLI

Configuration limits of the device

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

Depending on your device, some functions are not available.

	Configurable function	Maximum number
System	Syslog server	3
	SMTP server	3
	E-mail recipient	60 20 per SMTP server
	SNMPv1 trap recipient	10
	SNTP server	2
	NTP server	3 One per layer 3 interface
	DHCP pools	8
	IPv4 addresses managed by the DHCP server (dynamic + static)	100
	Static assignments per DHCP pool	20
	DHCP options (1, 2, 3, 4, 5, 6, 42, 66, 67)	9
	SINEMA RC	1
	Proxy server	5
Layer 2	Virtual LANs (port-based; including VLAN 1)	16
	Maximum frame size	2048 bytes
Layer 3	IP interfaces	12
	Static routes	100
	NETMAP	256
	SourceNAT	32
	NAPT	32
	VRRPv3	VRRPv3 instances (VRID): 2 Assigned IP addresses: 1 per VRID

	Configurable function	Maximum number
Security	Users	30 (incl. user preset in the factory "admin")
	Groups	32
	Roles	32 (incl. the predefined roles)
	RADIUS server	4
	Firewall	IP protocols:16 IP services:32 ICMP services:16 IP rules: 128 User-specific firewall: <ul style="list-style-type: none"> • Maximum number: 8 rule sets • Parallel user access: 4 • Maximum of 128 IP rules per firewall rule set
	IPsec VPN	20 You can create a maximum of 20 phase 2 connections per phase 1.
	OpenVPN	Connections: 5 Remote end points: 25

2.3 Use in a PROFINET environment

Note

Validity of CCA declaration

The CCA declaration applies to PROFINET RT without the use in media redundancy structures.

Configuration information

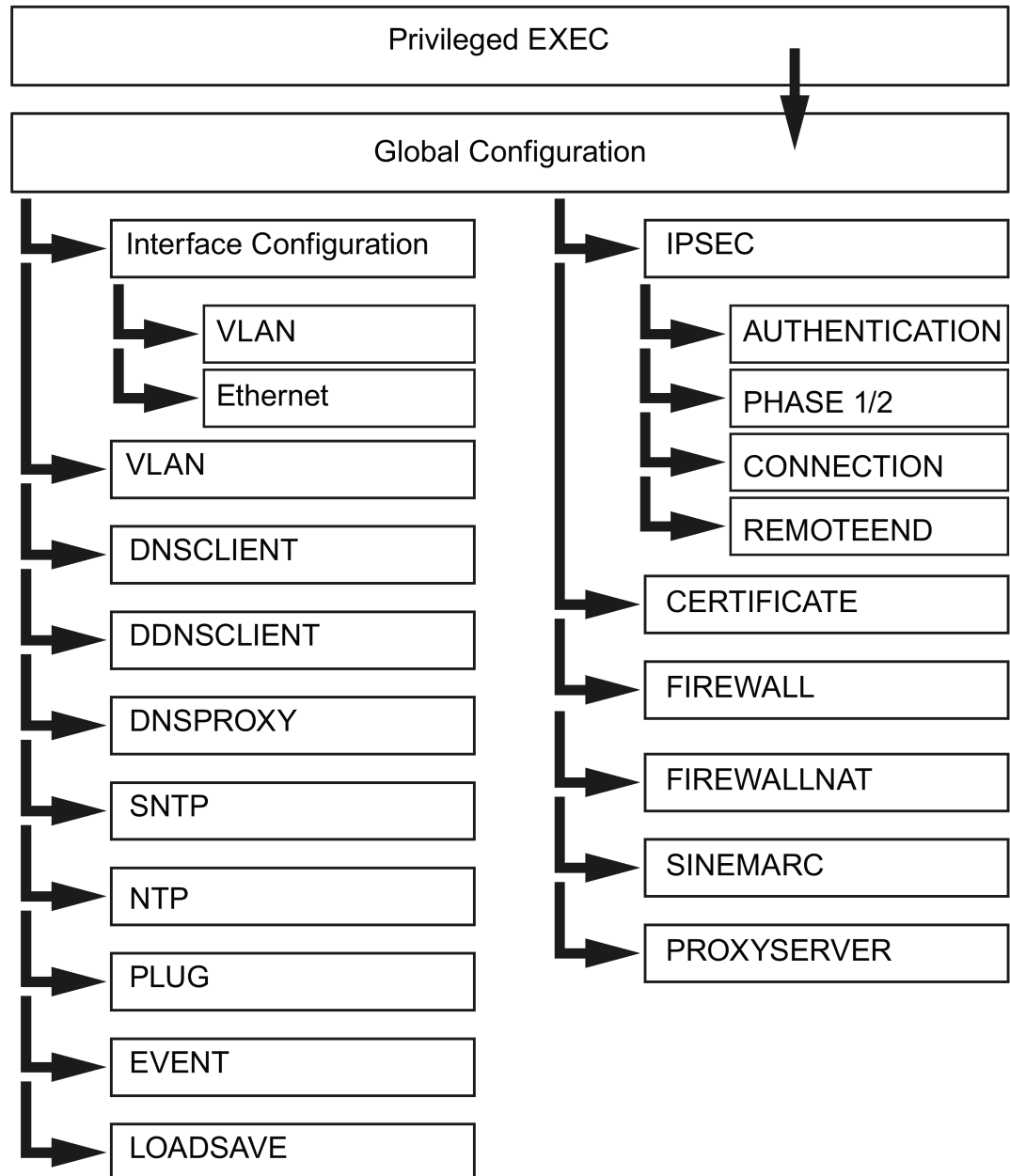
When using the device in a PROFINET environment, follow the following configuration instructions:

- Set the "Aging Time" to 45 seconds.
- Disable Spanning Tree and enable Passive Listening.

2.4 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.



Privileged EXEC mode

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

If you log with the "admin" user, 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 or a PLUG. 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 line configuration, interface configuration) or protocol-specific configuration modes (FTP, NTP).

2.5 Working with the Command Line Interface (CLI)

Introduction

All the configuration settings for the device can be made using the Command Line Interface (CLI). The CLI therefore provides the same options as Web Based Management (WBM). You should read the detailed explanations of the parameters in the configuration manual "SCALANCE M-800 Web Based Management". The CLI allows remote configuration over Telnet and SSH.

Access via SSH is enabled as default. If you wish to access the CLI via a Telnet connection, activate the option "Telnet Server" in "System > Configuration".

SSH connection

For access using SSH you require an SSH client for Windows.

Telnet connection: Starting the CLI in a Windows console

Note

Telnet - use with Windows 7

If you want to access the Command Line Interface in Windows 7, make sure that the functions required for this are enabled in Windows 7.

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 "telnet" followed by the IP address of the device you are configuring:

```
C:\>telnet <IP address>
```

2. Enter your login and password.

As an alternative, you can also enter the command "telnet" followed by the IP address of the device you are configuring in the Start > Run menu.

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.

Changing parameters

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

Turn the device off 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 in Config Change.
 - Saved: The change is saved in the current configuration.
 - Not Saved: Saving is still taking place.

2.6 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"

2.7 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.
[<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".

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.

2.8 Interface identifiers and addresses

2.8.1 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.

Example:

Fast Ethernet: `interface fa 0/1`

Addressing logical interfaces

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

- 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	
S615	5 x Fast Ethernet	fa: fast-ethernet	X = 1 .. 5	fa 0/X

Available logical interfaces

- VLAN
The device supports up to 16 virtual networks.
To be able to use a VLAN, create it with the `vlan` command.

Configuring an interface in the Interface configuration mode

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

Syntax

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

- Enter the interface you want to configure. With this command, you change to the Interface 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:

Interface	Command prompt
fastethernet: fa 0/x	cli (config-if-F0-X) #
vlan \$	cli (config-if-vlan-\$) #

The placeholders \$, x stand for the numbering of the interface.

2.8.2 Address types, address ranges and address masks

Overview

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

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

Note

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

- Network masks
A network mask is a series of bits that describes the network part of an IP address. The notation is normally decimal in keeping with the IP address.
- Alternative notation for network masks
In contrast to the notation described above, network masks can also be represented as a number of 1 bits. The mask of the decimal representation 255.255.0.0 is then written as /16.
The syntax is then for example: <ipaddress> / 16
Note that there must be a space before and after the "/".
- MAC addresses
In the syntax of the Command Line Interface, a MAC address is represented as a

sequence of 6 bytes in hexadecimal format, in each case separated by a colon.

The syntax is then, for example aa:aa:aa:aa:aa:aa

- Multicast addresses
Layer 2 multicast addresses as used on this device use the notation of MAC addresses.
For permitted address ranges, check the rules or ask your network administrator.

2.8.3 IPv4 address

Range of values for IPv4 address

The IPv4 address consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 141.80.0.16

IPv4 address format - notation

An IPv4 address consists of 4 bytes. Each byte is represented in decimal, with a dot separating it from the previous one.

XXX.XXX.XXX.XXX

XXX stands for a number between 0 and 255

The IPv4 address consists of two parts:

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

Range of values for 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 1s specify the network number within the IPv4 address. The 0s specify the host 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

Relationship between the IPv4 address and subnet mask

The first decimal number of the IPv4 address (from the left) determines the structure of the subnet mask with regard to the number of "1" values (binary) as follows (where "x" is the host address):

First decimal number of the IPv4 address	Subnet mask
0 to 127	255.x.x.x
128 to 191	255.255.x.x
192 to 223	255.255.255.x

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.

Value range for gateway address

The address consists of four decimal numbers taken from the range 0 to 255, each number being separated by a period; example: 141.80.0.1

Relationship between IPv4 address and gateway address

The only positions of the IPv4 address and gateway address that may differ are those in which "0" appears in the subnet mask.

Example:

You have entered the following: 255.255.255.0 for the subnet mask; 141.30.0.5 for the IPv4 address and 141.30.128.0 for the gateway address. The IPv4 address and gateway address may only be different in the 4th decimal number. In the example, however, the 3rd position is different.

You must, therefore, change one of the following in the example:

The subnet mask to: 255.255.0.0 or

the IPv4 address to: 141.30.128.1 or

the gateway address to: 141.30.0.1

General CLI commands

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

3.1 clear screen

Description

With this command, you clear the screen.
The command prompt is displayed.

Syntax

Call the command without parameters:

```
clear screen
```

Result

The screen is cleared.
The command prompt is displayed.

3.2 do

Description

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

Syntax

Call up the command with the following parameters:

```
do [command ]
```

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

Example

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

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

Result

The command from the Privileged EXEC mode will be executed.

3.3 end

Description

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

Requirement

You are in a configuration mode.

Syntax

Call the command without parameters:

```
end
```

Result

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

3.4 exit

Description

With this command, you close the current mode.

Syntax

Call the command without parameters:

```
exit
```

Result

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

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

3.5 Help functions and supported input

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

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

3.5.1 help

Description

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

Syntax

Call up help with the following parameters:

```
help [command]
```

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

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

Result

The syntax of the command is displayed.

Syntax

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

```
help
```

Result

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

Note

Incomplete command names

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

3.5.2 The command "?"

Description

With this command, you call up the command list.

Syntax

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

?

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

Result

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

Note

Incomplete command name

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

Note

Output in pages

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

3.5.3 "grep" command

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: <pre>show running-config interface vlan 1 grep "ip address"</pre>

Result

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

3.5.4 Completion of command entries

Description

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

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

This can be repeated after entering further characters.

Procedure

Enter the first characters of the command.

Press the tab key.

Result

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

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

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

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

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

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

3.5.5 Abbreviated notation of commands

Description

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

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

Example

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

3.5.6 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 56)

3.5.7 Working through a command sequence

Separators for multiple commands in one line

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

Separate the commands with a semicolon (;).

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

Example

The command sequence

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

has the same effect as:

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

3.5.8 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.

3.5.9 The "show" commands

This section describes commands with which you display various settings.

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

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

3.5.9.1 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.

Configuration

The following is described in this section:

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

4.1 System

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

4.1.1 The "show" commands

This section describes commands with which you display various settings.

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

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

4.1.1.1 show cli-console-timeout

Description

This command shows the timeout setting of the CLI session.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

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

Result

The timeout setting of the CLI session is displayed.

4.1.1.2 show coordinates

Description

This command shows the geographical coordinates.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show coordinates
```

Result

The geographical coordinates are displayed.

4.1.1.3 show device information

Description

This command shows information about the device.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show device information
```

Result

The following information about the device is displayed:

- MAC address of the device
- Serial Number
- System up time
- System name
- System contact
- System location
- Device Type
- 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.

4.1.1.4 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 41)".

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

Result

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

4.1.1.5 **show im**

Description

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

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show im
```

Result

The information is displayed.

4.1.1.6 **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 41)".

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

Result

The settings are displayed.

4.1.1.7 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 41)".

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

Result

The counters of the selected interfaces are displayed.

Further notes

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

4.1.1.8 **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 the command without parameter assignment:

```
show lldp neighbors
```

Result

The neighborhood table is displayed.

4.1.1.9 **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 up 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	Enter a valid interface.
interface-id	Module no. and port no. of the interface	

For information on identifiers of interfaces and addresses, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The information is displayed.

4.1.1.10 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 41)".

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

Result

The configuration of the selected IP interface is displayed.

4.1.1.11 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

4.1.2 clear counters

Description

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

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

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

Result

The counters of the interface are reset.

Further notes

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

4.1.3 **configure terminal**

Description

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

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
configure terminal
```

Result

You are now in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Further notes

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

4.1.4 **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.

4.1.5 disable

Description

With this command, you close the Privileged EXEC mode.

You are then in the User EXEC mode.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
disable
```

Result

You are in the User EXEC mode.

The command prompt is as follows:

```
cli>
```

4.1.6 enable**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. Enter the password of the factory-set user "admin". The password is changed on the first login and the name can also be changed.

After logging in successfully, you are in the Privileged EXEC mode. The command prompt is as follows:

```
cli#
```

4.1.7 logout

Description

With this command, you exit the Command Line Interface.

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

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
logout
```

Result

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

4.1.8 ping

Description

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

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

Requirement

You are in 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
<code>destination-address</code>	Address of the called node	Enter a valid IPv4 address.
<code>fqdn-name</code>	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name) of the called node	Maximum of 100 characters
<code>size</code>	Keyword for the size of the packets to be transferred	-
<code>byte</code>	Keyword for the size of the packets in bytes	0 ... 2080 Default: 32
<code>count</code>	Keyword for the number of packets to be requested	-
<code>packet_count</code>	Number of packets	1 ... 10 Default: 3
<code>timeout</code>	Response wait time If this time expires, the request is reported as "timed out".	-
<code>seconds</code>	Time to the timeout in seconds	1 ... 100 Default: 1

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

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

Result

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

4.1.9 Commands in the global configuration mode

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

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

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

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

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

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

4.1.9.1 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
<code>meter</code>	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: <code>coordinates height "123 456"</code>

Result

The geographical height has been created.

Further notes

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

4.1.9.2 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: <code>coordinates latitude "123 456"</code>

Result

The latitude has been created.

Further notes

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

4.1.9.3 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: <code>coordinates longitude "123 456"</code>

Result

The longitude has been created.

Further notes

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

4.1.9.4 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 the 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	Values
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 identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

You are in the 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
vlan	cli (config-if-vlan-\$) #
fastethernet	cli (config-if-F-X) #

The placeholders \$ and x stand for the numbering of the interface.

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

Further notes

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

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

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

4.1.9.5 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)> }
```

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

Result

The logical interface is deleted.

Further notes

You configure an interface with the `interface` command.

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

4.1.9.6 cli-console-timeout

Description

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

Note

No automatic logout from the CLI

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

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

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

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

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

Result

The time is configured and automatic logout is enabled.

Further notes

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

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

4.1.9.7 no cli-console-timeout

Description

With this command, you disable the automatic logout.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no cli-console-timeout
```

Result

Automatic logout is disabled.

Further notes

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

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

4.1.9.8 system contact

Description

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

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

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

The parameter has the following meaning:

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

Result

The contact information is created in the system.

Further notes

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

4.1.9.9 system location

Description

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

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

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

The parameter has the following meaning:

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

Result

The location information is created in the system.

Further notes

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

4.1.9.10 system name

Description

This command, you enter a name for the system.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

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

The parameter has the following meaning:

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

Result

The name is created in the system.

The corresponding system name is displayed instead of "cli" in the command prompt:

```
system name(config)#
```

Further notes

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

4.1.10 Commands in the Interface configuration mode

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

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

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

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

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

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

4.1.10.1 alias

Description

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

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
alias <interface-name>
```

The parameter has the following meaning:

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

Result

The interface was assigned a name.

Further notes

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

4.1.10.2 no alias**Description**

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

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

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

Syntax

Call the command without parameter assignment:

```
no alias
```

Result

The name of the interface is removed.

Further notes

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

4.1.10.3 duplex

Description

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

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

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

Requirement

- Autonegotiation is disabled.
- You are in the Interface configuration mode of an electrical interface.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

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

Result

The duplex mode of the interface is configured.

Further notes

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

You disable autonegotiation with the `no negotiation` command.

4.1.10.4 no duplex

Description

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

The default value is `full`.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

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

Syntax

Call the command without parameters:

```
no duplex
```

Result

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

Further notes

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

4.1.10.5 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.

4.1.10.6 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.

4.1.10.7 negotiation**Description**

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

Autonegotiation must be set for every interface of connected interfaces.

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

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

Syntax

Call the command without parameters:

```
negotiation
```

Result

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

Further notes

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

4.1.10.8 `no negotiation`

Description

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

Requirement

You are in the Interface Configuration mode.

The command prompt is as follows:

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

Syntax

Call the command without parameters:

```
no negotiation
```

Result

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

Further notes

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

4.1.10.9 `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.

4.1.10.10 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.

4.1.10.11 speed

Description

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

Note

Availability of this function

The transmission speed can only be configured for electrical data transfer.

On optical connections, the transmission speed is fixed.

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:

```
speed {10|100}
```

The parameters have the following meaning:

Parameter	Description
10	Transmission speed 10 Mbps
100	Transmission speed 100 Mbps

Result

The transmission speed of the interface is configured.

4.2 Load and Save

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

Note

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

4.2.1 The "show" commands

This section describes commands with which you display various settings.

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

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

4.2.1.1 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.

4.2.1.2 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.

4.2.1.3 show loadsave sftp

Description

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

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show loadsave sftp
```

Result

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

4.2.2 load tftp

Description

With this command, you load files from 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:

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

The parameters have the following meaning:

Parameter	Description	Range of values / note
tftp	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
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
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.
password	Keyword for a password	-
password	Password of the user	Enter the password for the user.

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

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

4.2.3 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>} [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
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

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

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

4.2.4 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.

4.2.4.1 loadsave

Description

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

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
loadsave
```

Result

You are now in the LOADSAVE configuration mode.

The command prompt is as follows:

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

Further notes

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

4.2.5 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.

4.2.5.1 delete

Description

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

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

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

Result

The files are displayed or the file is deleted.

Further notes

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

4.2.5.2 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.

4.2.5.3 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 up the command with the following parameters:

```
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.

Further notes

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

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

4.2.5.4 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 up the command with the following parameters:

```
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.

Further notes

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

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

4.2.5.5 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 up the command with the following parameters:

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

The parameters have the following meaning:

Parameter	Description	Range of values / note
ipv4	Keyword for an IPv4 address	-
ipv4-address	Value for an IPv4 unicast address	Enter a valid IPv4 unicast address.
fqdn-name	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name)	Maximum 100 characters
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 identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

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

4.2.5.6 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.

4.2.5.7 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 up the command with the following parameters:

```
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.

Further notes

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

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

4.2.5.8 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 up the command with the following parameters:

```
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.

Further notes

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

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

4.2.5.9 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>} [port <tcp port (1-65535)>] [user  
<username>] [password <password>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ipv4	Keyword for an IPv4 address	-
ucast_addr	Value for an IPv4 unicast address	Enter a valid IPv4 unicast address.
fqdn-name	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters
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.
password	Keyword for a password	-
password	Password of the user	Enter the password for the user.

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

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

4.2.5.10 password

Description

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

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

Parameter	Description	Values
showfiles	Shows the available files. The status is displayed in addition for the HTTPSCert file type. The available options are as follows: <ul style="list-style-type: none">Invalid The password does not match the certificate. The default certificate is used after a restart.Valid The password matches the certificate. The downloaded certificate is used after a restart.- No password was assigned. The default certificate is used after a restart.	-
filetype	Keyword for the file type.	-
filetype	Name of the file type	max. 100 characters
pw	Keyword for the password	-
password	Password	Enter the password for the file.

Result

The password for the file is configured and activated.

Additional notes

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

4.2.5.11 no password

Description

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

Requirement

You are in the LOADSAVE configuration mode.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

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

Result

The password for the file is disabled.

Further notes

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

4.3 Reset and Defaults

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

4.3.1 restart

Description

With this command, you restart the device.

Select one of the following configuration settings:

- Device restart with the current configuration
- Device restart with the factory configuration settings with the exception of 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
- 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	Resets the system to the factory configuration settings and restarts the system. The parameters listed above are unaffected by a reset.
factory	Resets the system to the factory configuration settings and restarts the system.

Note

By resetting to the factory configuration settings, the device loses its configured IP address and is reachable again with the IP address 192.168.1.1 set in the factory.

Result

The device is restarted with the selected settings.

4.4 Configuration Save & Restore

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

4.4.1 The "show" commands

This section describes commands with which you display various settings.

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

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

4.4.1.1 show running-config

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 | vlan [ <vlan-id (1-4094)>] | interface {
<interface-type> <interface-id> | vlan <vlan-id(1-4094)> | ppp <id(0-6)>} | ssh | ssl
| ip | snmp | snmp | http | auto-logout | time | ntp | auto-save | events | firewall
| firewallnat | openvpn | sinemarc | proxyserver | srs | ipsec | ddnsclient |
dnsclient | dnsproxy | modem}] [all]
```

The parameters have the following meaning:

Parameter	Description	Range of values
syslog	Shows the configuration settings of the Syslog function.	-
dhcp	Shows the configuration settings of the Dynamic Host Configuration 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-id	Module no. and port no. of the interface	
ppp	Keyword for the PPP interface	

Parameter	Description	Range of values
id	Number of the interface	0 ... 6
ssh	Shows the configuration settings of the Secure Shell protocol.	-
ssl	Shows the configuration settings of the Secure Sockets Layer protocol.	-
ip	Shows the configuration settings of the Internet protocol.	-
snmp	Shows the configuration settings of the Simple Network Management protocol.	-
http	Shows the configuration settings of the Hypertext Transfer 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.	-
events	Shows the configuration settings of the system events.	-
firewall	Shows the configuration settings of the firewall.	-
firewallnat	Shows the configuration settings of the NAT.	-
openvpn	Shows the configuration settings of OpenVPN.	-
sinemarc	Shows the configuration settings of the SINEMA RC connection.	-
proxyserver	Shows the configuration settings of the proxy servers.	-
srs	Shows the configuration settings of SRS.	-
ipsec	Shows the configuration settings of the IPsec.	-
ddnsclient	Shows the configuration settings of the dynamic DNS client.	-
dnsclient	Shows the configuration settings of the DNS client.	-
dnsproxy	Shows the configuration settings of the DNS proxy.	-
modem	Shows configuration of the device.	-
all	Shows all configuration settings.	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

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.

4.4.2 write startup-config

Description

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

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

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

*cli# or cli#

Syntax

Call the command without parameter assignment:

```
write startup-config
```

Result

The changes are saved in the configuration file.

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

Further notes

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

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

4.4.3 Commands in the global configuration mode

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

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

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

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

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

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

4.4.3.1 auto-save

Description

The CLI can save changes to the configuration automatically.

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

You are then in the Trial mode.

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 the 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.

Further notes

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

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

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

4.4.3.2 no auto-save

Description

With this command, you disable the auto save function.

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.

Further notes

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

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

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

4.5 DCP Discovery

This section describes commands for displaying and setting network parameters.

4.5.1 The "show" commands

This section describes commands with which you display various settings.

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

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

4.5.1.1 show das info

Description

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

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

Requirement

- The command `das discover interface` is executed.
- You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show das info
```

Result

The reachable devices and their network parameters are listed in the table.

Further notes

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

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

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

You configure the PROFINET device name of the reachable device with the `das mac name` command.

4.5.2 Commands in the global configuration mode

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

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

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

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

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

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

4.5.2.1 das discover interface

Description

With this command, you start the search for devices reachable via the selected interface. The function is only available with the VLAN associated with the TIA interface.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

Parameter	Description	Range of values/note
interface-type	Type or speed of the interface	Enter a valid interface.
interface-id	Module no. and port no. of the interface	
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094
port-channel	Keyword for a link aggregation	-
port-channel-id	Number of the addressed link aggregation	1 ... 8

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The reachable devices are searched for. On completion of the search the reachable devices are saved in a table. You display the table with the `show das info` command.

4.5.2.2 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 up the command with the following parameters:

```
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 41)".

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.

Further notes

You display the configured PROFINET device name with the `show das info` command.

4.5.2.3 das mac ip

Description

With this command, you configure the network parameters of the selected device.

Requirement

- The command `das discover interface` is executed.
- You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
das mac <aa:aa:aa:aa:aa:aa> ip <ip address> {<subnet-mask> | / <prefix-length(1-32)>}  
[gateway <ip address>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
-	MAC address of the reachable device	aa:aa:aa:aa:aa:aa
ip	Keyword for IPv4 address	
ip address	IPv4 address of the device	Enter a valid IPv4 address.
subnet-mask	Subnet mask	
prefix-length	Decimal representation of the mask as a number of "1" bits	1 ... 32
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 41)".

Result

The network parameters of the selected device are configured.

To ensure that the property was applied correctly, run the `das discover interface` command again.

Further notes

You display the network parameters with the `show das info` command.

4.5.2.4 das mac blink

Description

With this command, you make the port LEDs of the selected 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 up the command with the following parameters:

```
das mac <aa:aa:aa:aa:aa:aa> blink [timeout <seconds(5-60)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values/note
-	MAC address of the reachable device	aa:aa:aa:aa:aa:aa
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 41)".

Result

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

4.5.2.5 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 41)".

Result

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

4.6 SINEMA

4.6.1 The "show" commands

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

4.6.1.1 show sinema

Description

This command shows whether the SINEMA configuration interface is enabled or disabled.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show sinema
```

Result

The setting of the SINEMA configuration interface is displayed.

4.6.2 Commands in the global configuration mode

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

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

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

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

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

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

4.6.2.1 sinema

Description

With this command, you enable the SINEMA configuration interface.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
sinema
```

Result

The SINEMA configuration interface is enabled.

Further notes

You disable the SINEMA configuration interface with the `no sinema` command.

You display the setting whether the SINEMA configuration interface is enabled or disabled with the command `show sinema`.

4.6.2.2 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

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

5.1 PLUG

The C-PLUG or KEY-PLUG stores the configuration of a device and can therefore transfer the configuration of the old device to the new device when a device is replaced.

In addition to the configuration, the KEY-PLUG also contains a license that enables the use of certain functions.

This section describes commands relevant for working with the C-PLUG or KEY-PLUG.

5.1.1 The "show" commands

This section describes commands with which you display various settings.

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

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

5.1.1.1 show plug

Description

This command shows the current information of the PLUG.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show plug
```

Result

The current information of the PLUG is displayed.

5.1 PLUG

5.1.2 Commands in the global configuration mode

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

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

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

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

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

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

5.1.2.1 plug

Description

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

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
plug
```

Result

You are now in the Plug Configuration mode.

The command prompt is as follows:

```
cli(config-plug)#
```

Further notes

You exit the Plug Configuration mode with the `end` or `exit` command.

5.1.3 Commands in the Plug Configuration mode

This section describes commands that you can call up in the Plug Configuration mode.

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

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

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

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

5.1.3.1 `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.

If 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.

5.1 PLUG

5.1.3.2 firmware-on-plug

Description

With this command, you specify that the firmware is stored on the PLUG.

Requirement

- There is a device configuration on the PLUG.
- You are in the Plug Configuration mode.

The command prompt is:

```
cli (config-plug) #
```

Syntax

Call the command without parameters:

```
firmware-on-plug
```

Result

The firmware is stored on the PLUG.

When the device starts up there is a check whether the version on the PLUG is valid and whether this version matches the version on the device. If this is not the case, the firmware is installed on the device and it is restarted. This means that automatic firmware updates/downgrades can be made with the PLUG.

Further notes

You disable this setting with the `no firmware-on-plug` command.

5.1.3.3 no firmware on plug

Description

With this command, you disable the function. The firmware is removed from the PLUG.

Requirement

- There is a device configuration on the PLUG.
- You are in the Plug Configuration mode.

The command prompt is:

```
cli (config-plug) #
```

Syntax

Call the command without parameters:

```
no firmware-on-plug
```

Result

The firmware is removed from the PLUG.

5.1.3.4 factoryclean**Description**

With this command, you delete the device configuration stored on the PLUG.

Requirement

- There is a device configuration on the PLUG.
- You are in the Plug Configuration mode.
The command prompt is:

```
cli(config-plug) #
```

Syntax

Call the command without parameters:

```
factoryclean
```

Result

The device configuration on the PLUG is deleted.

5.1.3.5 write**Description**

With this command, you format the PLUG and copy the current device configuration to it.

Requirement

- The PLUG is formatted.
- You are in the Plug Configuration mode.
The command prompt is:

```
cli(config-plug) #
```

5.1 PLUG

Syntax

Call the command without parameter assignment:

```
write
```

Result

The current device configuration has been copied to the formatted PLUG.

5.2 WBM

On the device, you can limit the time available for access with Web Based Management. If no entry is made for a specific time, the WBM session is closed.

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

5.2.1 The "show" commands

This section describes commands with which you display various settings.

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

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

5.2.1.1 show web-session-timeout

Description

This command shows the timeout setting for the WBM.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show web-session-timeout
```

Result

The timeout setting for the WBM is displayed.

5.2.2 Commands in the global configuration mode

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

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

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

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

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

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

5.2.2.1 web-session-timeout

Description

With this command, you enable the automatic logoff and you configure the timeout setting for the WBM.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
web-session-timeout [<seconds(60-3600)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
seconds	Time in seconds until automatic logout after the last entry	60 ... 3600 Default: 900

Result

The time is configured and automatic logout is enabled.

Further notes

You disable automatic logoff with the `no web-session-timeout` command.

You display the current timeout setting with the `show web-session-timeout` command.

5.2.2.2 no web-session-timeout

Description

With this command, you disable the automatic logoff.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
no web-session-timeout
```

Result

Automatic logoff is disabled.

Further notes

You enable automatic logoff with the `web-session-timeout` command.

You display the current timeout setting with the `show web-session-timeout` command.

5.3 Digital input/output

Introduction

The SCALANCE S device has a digital input/output. The connection is made using two 2-pin terminal blocks. You will find information about the pin assignment in the operating instructions of the device.

With CLI commands, you can open or close the digital output.

Application examples

- Digital input to signal one item of information, for example "door open", "door closed"
- Digital output, for example for "go to sleep" for devices on an automated guided transport system.

5.3.1 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.

5.3.1.1 show digital input

Description

This command shows the current setting of the digital input.

Requirement

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 digital output
```

Result

The current setting of the digital input is displayed.

5.3.1.2 show digital output

Description

This command shows the current setting of the digital output.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show digital output
```

Result

The current setting of the digital output is displayed.

5.3.2 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.

5.3.2.1 digital output closed

Description

This command closes the digital output.

Requirement

You are in the Global configuration mode.

5.3 Digital input/output

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
digital output close
```

Result

The digital output is closed.

Further notes

You open the digital output with the `digital output open` command.

You can display the setting of the digital output with the `show digital output` command

5.3.2.2 digital output open

Description

This command opens the digital output.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
digital output open
```

Result

The digital output is opened.

Further notes

You close the digital output with the `digital output close` command.

You can display the setting of the digital output with the `show digital output` command

5.4 cRSP / SRS

This section describes commands for the cRSP / SRS.

Note

Common Remote Service Platform (cRSP) / Siemens Remote Service (SRS) is a remote maintenance platform via which remote maintenance access is possible.

To use the platform, additional service contracts are necessary and certain constraints must be kept to. If you are interested in cRSP / SRS, call your local Siemens contact or visit the following Web page (<https://support.industry.siemens.com/cs/de/en/sc/2281>).

5.4.1 The "show" commands

This section describes commands with which you display various settings.

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

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

5.4.1.1 show srs

Description

This command shows whether use of cRSP / SRS is enabled and whether the device checks the received server certificate for validity.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show srs
```

Result

The configuration is displayed.

5.4.1.2 show srs logon

Description

This command shows the configured destination server of the Common Remote Service Platform (cRSP) / Siemens Remote Service (SRS).

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show srs overview
```

Result

The configuration is displayed.

5.4.2 Commands in the global configuration mode

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

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

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

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

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

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

5.4.2.1 srs

Description

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

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
srs
```

Result

You are now in the SRS configuration mode.

The command prompt is as follows:

```
cli (config-srs) #
```

Further notes

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

5.4.3 Commands in the SRS configuration mode

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

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

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

5.4.3.1 logon

Description

With this command you specify which destination server will be used.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli(config-srs)#
```

Syntax

Call up the command with the following parameters:

```
logon {idx <num(1-20)> | all} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for the number of the destination server	-
index	Number corresponding to a specific destination server.	Enter the required number. 1 ... 20
all	Uses all destination servers	-
enabled	Enables the entry	-
disabled	Disables the entry.	

Result

The specified destination server is enabled.

Further notes

You display this setting and other information with the `show srs logon` command.

You disable the destination server with the `no logon` command.

You display the numbers of the destination servers with the `logon show-idx` command.

5.4.3.2 no logon

Description

With this command, you delete a specific destination server or all destination servers.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli(config-srs)#
```

Syntax

Call up the command with the following parameters:

```
no logon {idx <num(1-20)> | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for the number of the destination server	-
num	Number corresponding to a specific destination server.	Enter the required number.
all	Deletes all destination servers	-

Result

The specified destination server entry is deleted.

Further notes

You display the numbers of the destination servers with the `logon show-idx` command.

5.4.3.3 logon idx authority

Description

With this command, you configure the address of a specific destination server.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli(config-srs)#
```

Syntax

Call up the command with the following parameters:

```
logon idx <num(1-20)> authority <string(255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
num	Number corresponding to a specific destination server.	Enter the required number.
string	Address of the destination server	Enter the address of the destination server.

Result

The address of the destination server has been configured.

Further notes

You display this setting and other information with the `show srs logon` command.

You display the numbers of the entry with the `logon show-idx` command.

5.4.3.4 logon idx fragment

Description

With this command you can address local parts of the resource e.g. the anchor attribute of a Web page.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli(config-srs)#
```

Syntax

Call up the command with the following parameters:

```
logon idx <num(1-20)> fragment <string(255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
num	Number corresponding to a specific destination server.	Enter the required number.
string	Part of the resource	Maximum of 255 characters

Result

The setting is configured.

Further notes

You display this setting and other information with the `show srs logon` command.

You display the numbers of the destination servers with the `logon show-idx` command.

5.4.3.5 logon idx path

Description

With this command, you specify destination path to the resource.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli(config-srs)#
```

Syntax

Call up the command with the following parameters:

```
logon idx <num(1-20)> path <string(255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
num	Number corresponding to a specific destination server.	Enter the required number.
string	Destination path to the resource.	Maximum of 255 characters

Result

The setting is configured.

Further notes

You display this setting and other information with the `show srs logon` command.

You display the numbers of the destination servers with the `logon show-idx` command.

5.4.3.6 logon idx query

Description

With this command, you configure queries that can contain the parameter values for an application.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli(config-srs)#
```

Syntax

Call up the command with the following parameters:

```
logon idx <num(1-20)> query <string(255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
num	Number corresponding to a specific destination server.	Enter the required number.
string	Query	Maximum of 255 characters

Result

The setting is configured.

Further notes

You display this setting and other information with the `show srs logon` command.

You display the numbers of the destination servers with the `logon show-idx` command.

5.4.3.7 logon show-idx

Description

With this command, you display the available destination servers.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli (config-srs) #
```

Syntax

Call the command without parameter assignment:

```
logon show-idx
```

Result

The destination servers are listed.

Further notes

You create a destination server entry with the `logon addr` command.

5.4.3.8 shutdown

Description

With this command, you disable the use of SRS.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli (config-srs) #
```

Syntax

Call the command without parameter assignment:

```
shutdown
```

Result

The use of SRS is disabled.

Further notes

You enable the use with the `no shutdown` command.

5.4.3.9 no shutdown

Description

With this command, you enable the use of SRS.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli(config-srs)#
```

Syntax

Call the command without parameter assignment:

```
no shutdown
```

Result

The use of SRS is enabled.

Further notes

You disable use with the `shutdown` command.

5.4.3.10 interval

Description

With this command, you configure the time after which the IPv4 address will be transferred to the required destination server.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli(config-srs)#
```

Syntax

Call up the command with the following parameters:

```
interval <time (60-86400)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
time	Interval in seconds	60 ... 86400

Result

The interval is configured.

Further notes

You display this setting and other information with the `show srs logon` command.

5.4.3.11 validate cert

Description

With this command, you specify whether the device checks the received server certificate for validity.

Requirement

You are in the SRS configuration mode.

The command prompt is as follows:

```
cli(config-srs)#
```

Syntax

Call up the command with the following parameters:

```
validate cert {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description
enabled	Enables the check
disabled	Disables the check

Result

The setting is configured.

Further notes

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

5.5 SINEMA RC

5.5.1 Introduction to the SRC section

This section describes commands for access to the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

5.5.2 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.

5.5.2.1 show sinemarc

Note

This command is only available with a KEY-PLUG.

Description

This command shows information on SINEMA RC.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show sinemarc
```

Result

The information is displayed.

5.5.3 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.

5.5.3.1 sinemarc

Note

This command is only available with a KEY-PLUG.

Description

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

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
sinemarc
```

Result

You are now in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

Further notes

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

5.5.4 Commands in the SINEMARC configuration mode

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

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

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

5.5.4.1 `addr`

Note

This command is only available with a KEY-PLUG.

Description

With this command you configure the IPv4 address or the DNS host name of the SINEMA RC Server.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

Syntax

Call up the command with the following parameters:

```
addr <ip_addr|dns(50)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ip_addr	IPv4 address	Enter the IPv4 address of the SINEMA RC Server.
dns	DNS host name	Enter the DNS host name of the SINEMA RC Server. Maximum of 50 characters

Result

The IPv4 address of the SINEMA RC Server is configured.

Further notes

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

5.5.4.2 autoenrollment interval

Note

This command is only available with a KEY-PLUG.

Description

With this command, you specify the interval after which queries are sent to the SINEMA RC Server. With this query, the device checks whether there is a newer firmware file on the SINEMA RC server or whether the connection settings have changed.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

Syntax

Call up the command with the following parameters:

```
autoenrollment interval {0 | <minute(10-10080)>}
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
0	Interval	The query is never sent.
minute		Enter the interval in minutes. 10 ... 10080

Result

The interval is configured.

Further notes

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

5.5.4.3 autofwnat

Note

This command is only available with a KEY-PLUG.

Description

With this command, you enable the automatic creation of the firewall and NAT rules for the connection to the SINEMA RC Server.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli (config-sinemarc) #
```

Syntax

Call the command without parameter assignment:

```
autofwnat
```

Result

The automatic firewall and NAT rules are created. The connections between the configured exported subnets and the subnets that can be reached via the SINEMA RC Server are allowed. The NAT settings are implemented as configured in the SINEMA RC Server.

Further notes

You enable the setting with the `autofwnat` command.

You disable the setting with the `no autofwnat` command.

5.5.4.4 connection type

Note

This command is only available with a KEY-PLUG.

Description

With this command you specify how the connection is established.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

Syntax

Call up the command with the following parameters:

```
connection type {auto|permanent|di|sms|di-sms}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
auto	The device adopts the settings of the SINEMA RC server. You configure the settings on the SINEMA RC Server in "Remote Connections > Devices". You will find further information on this topic in the operating instructions "SINEMA RC Server".	-
permanent	The settings of the SINEMA RC server are ignored. The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is established permanently	-
di	The settings of the SINEMA RC server are ignored. If the "Digital In" event occurs, the device attempts to establish a VPN connection to the SINEMA RC Server. This is on condition that the event "Digital In" is passed on to the VPN connection. To do this activate "VPN Tunnel" for the "Digital In" event in "System > Events > Configuration".	-

Parameter	Description	Range of values / note
sms	M87x only The settings of the SINEMA RC server are ignored. When the device receives a command SMS message (wake-up SMS message), it attempts to establish a connection to the SINEMA RC Server. On condition that in "System > SMS > SMS Command" it is specified who a command SMS of the class "System" will be accepted from.	-
di-sms	M87x only The settings of the SINEMA RC server are ignored. If the "Digital In" event occurs or when the device receives a command SMS message, it attempts to establish a VPN connection to the SINEMA RC Server.	-

Result

The setting is configured.

Further notes

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

5.5.4.5 no autofwnat**Note**

This command is only available with a KEY-PLUG.

Description

With this command, you disable the firewall and NAT rules.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

Syntax

Call the command without parameter assignment:

```
autofwnat
```

Result

The firewall and NAT rules are disabled.

Further notes

You enable the setting with the `autofwnat` command.

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

5.5.4.6 device id

Note

This command is only available with a KEY-PLUG.

Description

With this command, you configure the device ID. The device ID is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

Syntax

Call up the command with the following parameters:

```
device id <number>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
number	Device ID	Enter the device ID.

Result

The device ID is configured.

Further notes

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

5.5.4.7 device pw

Note

This command is only available with a KEY-PLUG.

Description

With this command, you configure the password with which the device logs on to the SINEMA RC Server. The password is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli (config-sinemarc) #
```

Syntax

Call up the command with the following parameters:

```
device pw <password(256)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
password	Device password	Enter the password. Maximum of 256 characters

Result

The device password is configured.

Further notes

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

5.5.4.8 port

Note

This command is only available with a KEY-PLUG.

Description

With this command, you set the port via which the WBM of the SINEMA RC Server can be reached.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

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	Specify the port. 1 ... 65535

Result

The port is configured.

Further notes

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

5.5.4.9 proxy

Note

This command is only available with a KEY-PLUG.

Description

With this command, you specify that the connection to the defined SINEMA RC Server is established via a proxy server.

Requirement

- The proxy server is configured.
- You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

Syntax

Call up the command with the following parameters:

```
proxy <string(128)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
string	Proxy server name	Specify the proxy server name. Maximum of 128 characters

Result

The proxy server via which the connection is established is configured.

Further notes

You remove the proxy server with the `no proxy` command.

You display the available proxy server names with the `srv show-names` command.

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

5.5.4.10 no proxy

Note

This command is only available with a KEY-PLUG.

Description

With this command, you remove the proxy server.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

Syntax

Call the command without parameter assignment:

```
no proxy
```

Result

The proxy server is removed.

Further notes

You configure the proxy server with the `proxy` command.

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

5.5.4.11 shutdown

Note

This command is only available with a KEY-PLUG.

Description

With this command, you disable the connection to the configured SINEMA RC Server.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli (config-sinemarc) #
```

Syntax

Call the command without parameter assignment:

```
shutdown
```

Result

The connection to the SRC server is terminated.

Further notes

You enable the connection with the `no shutdown` command.

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

5.5.4.12 no shutdown

Note

This command is only available with a KEY-PLUG.

Description

With this command, you establish a connection to the configured SINEMA RC Server.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli (config-sinemarc) #
```

Syntax

Call the command without parameter assignment:

```
no shutdown
```

Result

The connection is enabled.

Further notes

You disable the connection with the `shutdown` command.

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

5.5.4.13 verification cacert

Note

This command is only available with a KEY-PLUG.

Description

With this command, you specify the CA certificate of the server used to sign the server certificate.

Requirement

- The certificate is loaded.
- You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli(config-sinemarc)#
```

Syntax

Call up the command with the following parameters:

```
verification cacert [<name(256)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
name	Name of the server certificate	Enter the name of the server certificate. Maximum of 256 characters.

Result

The CA certificate of the server is configured.

Further notes

You load certificates with the `tftp load` command.

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

5.5.4.14 verification fingerprint

Note

This command is only available with a KEY-PLUG.

Description

With this command, you configure the fingerprint of the device. The fingerprint is assigned during commissioning of the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

Requirement

You are in the SINEMARC configuration mode.

The command prompt is as follows:

```
cli (config-sinemarc) #
```

Syntax

Call up the command with the following parameters:

```
verification fingerprint [<string(95)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
string	Fingerprint of the device	Specify the fingerprint of the device. Maximum of 95 characters

Result

The fingerprint is configured. Based on the fingerprint, the device checks whether the correct SINEMA RC Server is involved.

Further notes

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

5.6 SELECT/SET button

This section describes the commands relevant for working with the button.

You will find a detailed description of the function available using the button in the device operating instructions.

5.6.1 Commands in the global configuration mode

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

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

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

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

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

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

5.6.1.1 panel-button control-restart

Description

With this command, you enable the following functions of the SET button:

- Restart: This function corresponds to calling the `restart` command.
- Resetting to factory settings. This function corresponds to calling the `restart` command with the parameter `factory`.

You will find a detailed description of the functions in the device operating instructions.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```


Syntax

Call the command without parameter assignment:

```
panel-button control-restart
```

Result

The functions of the SET button are enabled.

Further notes

You disable these functions with the `no panel-button control-restart` command.

5.6.1.2 no panel-button control-restart**Description**

With this command, you disable the functions of the SET button. The SET button cannot be used for a restart or to restore factory defaults.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no panel-button control-restart
```

Result

The functions of the SET button are disabled.

Further notes

You enable these functions with the `panel-button control-restart` command.

System time

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

6.1 System time setting

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

6.1.1 The "show" commands

This section describes commands with which you display various settings.

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

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

6.1.1.1 show dst info

Description

This command shows all the entries for daylight saving time stored on the device.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show dst info
```

Result

The entries for daylight saving time are displayed.

6.1.1.2 show time

Description

This command shows the settings of the system clock.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show time
```

Result

The settings for the system clock are displayed.

6.1.2 Commands in the global configuration mode

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

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

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

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

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

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

6.1.2.1 time

Description

With this command, you configure the way in which the system time is obtained.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
time { manual | ntp | sntp | sinec }
```

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.

6.1.2.2 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.	-
MMDDhh	Time for the start of daylight saving time.	Time in the format MM Month DD Day hh Hour
end	Keyword for the end of daylight saving time.	-
MMDDhh	Time for the end of daylight saving time.	Time in the format MM Month DD Day hh Hour

Result

The entry for the start and end of daylight saving time was created.

Further notes

You display the settings for the daylight saving time changeover with the `show dst info` command.

6.1.2.3 time dst recurring

Description

With this command, you configure the start and end of daylight saving time with a generic description.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
time dst recurring <name(16)> begin {<week(1-5)> | last} <weekday> <month> <hour> end  
{<week(1-5)> | last} <weekday> <month> <hour>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Name of the entry	maximum 16 characters
begin	Keyword for the start of daylight saving time.	-
week	Calendar week in a month	1 ... 5
last	Keyword for the last calendar week in a month	-
weekday	Weekday	monday, tuesday, wednesday, thursday, friday, saturday, sunday
month	Month	january, february, march, april, may, june, july, august, september, october, november, december
hour	Hour	0 ... 23
end	Keyword for the end of daylight saving time.	-

Result

The entry for the start and end of daylight saving time was created.

Further notes

You display the settings for the daylight saving time changeover with the `show dst info` command.

6.1.2.4 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 the 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

An entry or the entries for the start and end of daylight saving time was/were deleted.

Further notes

You display the settings for the daylight saving time changeover with the `show dst info` command.

6.1.2.5 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)>
{j|january|february|march|april|may|june|july|august|september|october|november|decembe
r}
<year (2000 - 2035)>
```

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 ... 2035

Result

The system time is set.

Further notes

You display the settings for the system clock with the `show time` command.

6.2 NTP client

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

6.2.1 The "show" commands

This section describes commands with which you display various settings.

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

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

6.2.1.1 show ntp info

Description

This command shows the current settings for the Network Time Protocol (NTP).

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show ntp info
```

Result

The current NTP settings are displayed.

6.2.2 Commands in the global configuration mode

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

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

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

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

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

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

6.2.2.1 ntp

Description

With this command, you change to the Network Time Protocol (NTP).

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ntp
```

Result

You are now in the NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Further notes

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

6.2.3 Commands in the NTP configuration mode

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

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

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

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

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

6.2.3.1 ntp server id

Description

With this command, you configure the connection to a server on the NTP client.

Requirement

You are in the NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Syntax

Call up the command with the following parameters:

```
ntp server id <1-3> { ipv4 <ip_addr> | fqdn-name <Fully Qualified Domain Name> }  
[port { <1025-36564> | default}] [poll <seconds(64-1024)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
id	Number of the NTP server.	1 ... 3
ipv4	Keyword for an IPv4 address	-
ip_addr	Value for the IPv4 address of the time server	Enter a valid IPv4 address.
fqdn-name	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters If you have stored a suitable domain name, you can specify a host name.
port	UDP port of the time server	1025 ... 36564
default	Default value for the UDP port	123

Parameter	Description	Range of values / note
poll	Keyword for the time after which the time of day is requested again	-
seconds	Value for the time in seconds	64 ... 2592000

For information on identifiers of addresses and interfaces, refer to the section "Addresses and interface identifiers (Page 41)".

Result

The connection to a server is configured on the NTP client.

Further notes

You delete the connection to a server with the `no ntp server id` command.

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

6.2.3.2 no ntp server id

Description

With this command, you delete the connection to a server on the NTP client.

Requirement

You are in the NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Syntax

Call up the command with the following parameters:

```
no ntp server id <1-3>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
id	Number of the NTP server.	1 ... 3

Result

The connection to a server is deleted on the NTP client.

Further notes

You configure the connection to a server with the `ntp server id` command.

6.2.3.3 ntp server secure

Description

With this command, you configure the parameters for authentication.

Requirement

You are in the NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Syntax

Call up the command with the following parameters:

```
ntp server id <1-3> secure [ntpkeyid <1-65534>] [hashalg {des-cbc|md5|sha1}] [ntp-key  
<secret-key-string(1-128)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
id	NTP server index to which the parameters relate	1 ... 3
secure	Key for the authentication	-
keyid	Authentication key ID	The entry must exist on the NTP server. 1 ... 65534
hashalg	Authentication key format	des-cbc md5 sha1
ntp-key	Keyword for the authentication key	-
secret-key-string	Authentication key	The entry must match the key stored on the NTP server.

Result

The parameters are configured.

Further notes

You display the settings and other information with the `show ntp server` command.

6.2.3.4 **ntp secure**

Description

With this command, you enable the "Secure NTP Client only" function. The device receives the system time from a secure NTP server.

Requirement

- You are in NTP configuration mode.
The command prompt is as follows:

```
cli(config-ntp)#
```
- The parameters for authentication (key ID, hash algorithm, key) are configured.

Syntax

Call up the command with the following parameters:

```
ntp secure
```

Result

The function is enabled.

Additional notes

You disable the function with the `no ntp secure` command.

You configure the parameters for authentication with the `ntp server id` command.

6.2.3.5 no ntp secure

Description

With this command, you disable the "Secure NTP Client only" function.

Requirement

You are in NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Syntax

Call up the command with the following parameters:

```
no ntp secure
```

Result

The function is disabled.

Additional notes

You enable the function with the `ntp secure` command.

6.2.3.6 ntp time diff

Description

With this command, you configure the time difference between the device and the NTP server.

Requirement

You are in the NTP configuration mode.

The command prompt is as follows:

```
cli(config-ntp)#
```

Syntax

Call up the command with the following parameters:

```
ntp time diff <(+/-hh:mm)>
```


The parameter has the following meaning:

Parameter	Description
+	Time zones to the west of the NTP server time zone
-	Time zones to the east of the NTP server time zone
hh	Number of hours difference
mm	Number of minutes difference

Enter the number of hours and number of minutes with two digits each.

Default: No time difference.

Result

The time difference between the device and the NTP server is configured.

6.3 NTP server

This section describes commands relevant for configuration of the NTP server.

6.3.1 show ntp server info

Description

This command shows the current settings for the NTP server.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show ntp server info
```

Result

The current NTP server settings are displayed.

6.3.2 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 ntp server

Description

With this command, you enable the NTP server service.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
ntp server
```

Result

The NTP server service is configured.

Further notes

You disable the service with the `no ntp server` command.

6.3.2.2 no ntp server

Description

With this command, you disable the NTP server service.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
no ntp server
```

Result

The NTP server service is disabled.

Further notes

You enable the service with the `ntp server` command.

6.3.3 Commands in the NTP server configuration mode

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

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

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

6.3.3.1 ntp server interface

Description

With this command, you enable the NTP server at the desired interface. The other devices can call up the time via these interfaces.

Requirement

You are in the NTP Server configuration mode.

The command prompt is as follows:

```
cli(config-ntp-server)#
```

Syntax

Call up the command with the following parameters:

```
ntp server interface { <interface-type> <interface-id> | vlan <vlan-id(1-4094)> | all  
}  
[port {<1025-36564> | default}][secure ntpkeyid <1-65534> hashalg {des-cbc|md5|sha1}  
ntp-key <secret-key-string(1-128)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
<code>interface-type</code>	Type or speed of the interface	Specify a valid interface.
<code>interface-id</code>	Module no. and port no. of the interface	
<code>vlan</code>	Keyword for a VLAN connection	-
<code>vlan-id</code>	Number of the addressed VLAN	1 ... 4094
<code>all</code>	Enables the function on all available interfaces.	-
<code>port</code>	NTP Server Port	<ul style="list-style-type: none"> 1025 ... 36564 default (123)
<code>secure</code>	The following parameters are only relevant for "NTP (secure)".	-
<code>ntpkeyid</code>	Authentication key ID	1 ... 65534
<code>hashalg</code>	Hash algorithm for the authentication key	<ul style="list-style-type: none"> des-cbc md5 sha1
<code>ntp-key</code>	Keyword for the authentication key	-
<code>secret-key-string</code>	Authentication key	<p>The length of the authentication key depends on the hash algorithm.</p> <ul style="list-style-type: none"> DES: ASCII 8 characters MD5: ASCII 16 – 128 characters SHA1: ASCII 20 – 128 characters

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The interfaces via which the other devices can call up the current time are specified.

Further notes

You display the settings and other information with the `show ntp server info` command.

You disable the function with the `no ntp server interface` command.

You enable "NTP (secure)" with the `ntp server secure interface` command.

6.3.3.2 no ntp server interface

Description

With this command, you disable the function on the interface.

Requirement

You are in the NTP Server configuration mode.

The command prompt is as follows:

```
cli(config-ntp-server)#
```

Syntax

Call up the command with the following parameters:

```
no ntp server interface {<interface-type> <interface-id> | vlan <vlan-id(1-4094)>}
```

The parameter has the following meaning:

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The function is disabled on the interfaces.

Further notes

You display the settings and other information with the `show ntp server info` command.

You enable the function with the `ntp server interface` command.

6.3.3.3 ntp server secure interface

Description

With this command, the NTP server becomes an NTP server of the type "NTP (secure)".

Requirement

You are in the NTP Server configuration mode.

The command prompt is as follows:

```
cli(config-ntp-server)#
```

Syntax

Call up the command with the following parameters:

```
ntp server secure interface { vlan <vlan-id(1-4094)> | all }
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
interface-type	Type or speed of the interface	Specify a valid interface.
interface-id	Module no. and port no. of the interface	
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094
all	Enables the function on all available interfaces.	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The NTP server of the type "NTP (secure)" is enabled.

Further notes

You display the settings and other information with the `show ntp server info` command.

You disable the function with the `no ntp server secure interface` command.

6.3.3.4 no ntp server secure interface

Description

With this command, you disable NTP (secure).

Requirement

You are in the NTP Server configuration mode.

The command prompt is as follows:

```
cli(config-ntp-server)#
```

Syntax

Call up the command with the following parameters:

```
ntp server secure interface {<interface-type> <interface-id> | vlan <vlan-id>(1-4094)>}
```

The parameter has the following meaning:

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The function is disabled on the interfaces.

Further notes

You display the settings and other information with the `show ntp server info` command.

You enable the function with the `ntp server secure interface` command.

6.4 SNTP client

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

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 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.

6.4.1.2 show sntp status

Description

This command shows the settings of the Simple Network Time Protocol.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show sntp status
```

Result

The settings of SNTP are displayed.

6.4.1.3 show sntp unicast-mode status

Description

This command shows the current configuration of the unicast mode of SNTP.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show sntp unicast-mode status
```

Result

The current SNTP unicast configuration is displayed.

6.4.2 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.

6.4.2.1 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 mode with the `end` or `exit` command.

6.4.3 Commands in the SNTP configuration mode

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

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

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

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

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

6.4.3.1 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.

6.4.3.2 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 <Fully Qualified Domain  
Name(100)> | 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	-
Fully Qualified Domain Name	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	-

Parameter	Description	Range of values / note
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.

Further 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.

6.4.3.3 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 <Fully Qualified Domain  
Name(100)> | 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	-
Fully Qualified Domain Name(100)	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.

Further 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.

6.4.3.4 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

7.1 VLAN

This section describes commands for configuring and managing virtual networks (VLANs).

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 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.

7.1 VLAN

Result

The information for the selected VLAN is displayed.

7.1.1.2 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.

7.1.1.3 show vlan learning params

Description

This command shows the parameters for the automatic learning of addresses for selected or all VLANs (active and inactive VLANs).

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call up the command with the following parameters:

```
show vlan learning params [vlan <vlan-range>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vlan	Keyword for a VLAN or VLAN range	-
vlan-range	Number of the addressed VLAN or VLAN range	1 ... 4094 Enter the range limits with a hyphen or a space.

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

Result

The settings for the automatic learning of addresses are displayed.

7.1.1.4 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 41)".

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

Result

The information about the ports is displayed.

7.1.1.5 show vlan protocols-group

Description

This command displays the table with the protocol group entries.

Requirement

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 vlan protocols-group
```

Result

The table of protocol groups is 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 base bridge-mode

Description

With this command, you configure whether or not the device forwards frames with VLAN tags transparently (IEEE 802.1D/VLAN-unaware mode) or takes VLAN information into account (IEEE 802.1Q/VLAN-aware mode).

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
base bridge-mode {dot1d-bridge|dot1q-vlan}
```

The parameters have the following meaning:

Parameter	Description	Range of values / notes
dot1d-bridge	Sets the mode "VLAN-unaware" for the device. VLAN tags are not taken into account or changed but are forwarded transparently.	-
dot1q-vlan	Sets the mode "VLAN-aware" for the device. VLAN information is taken into account.	-

Result

The device mode is configured.

Further notes

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

7.1.2.2 interface range

Description

With this command, you can put several interfaces or the interfaces of VLANs together and configure them together. The configurations are valid for all interfaces of the specified range.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call up the command with the following parameters:

```
interface range
(
  {<interface-type> <0/a-b,0/c,...>}
  {vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>}
)
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
interface-type	Keyword for an interface	Enter a valid interface.
0/a-b, 0/c,...	Module no. and port no. of the interface	
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094
vlan-id	Number of the addressed VLAN	2 ... 4094

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

If you want to address several VLANs with this command, you must insert a blank before and after the hyphen, for example `interface range vlan 5 - 10`.

Result

The interfaces or interfaces of VLANs were put together to form an interface range.

The command prompt is as follows:

```
cli (config-if-vlan-range) #
```

The configuration commands you enter in a mode apply to all interfaces of this area.

Further notes

With the `no interface range` command, you remove VLANs from this range or break it up.

7.1.2.3 no interface range

Description

With this command, you remove the interfaces or interfaces of VLANs from the interface range or break it up if you first remove all previously added interfaces.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no interface range vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094
vlan-id	Number of the addressed VLAN	2 ... 4094

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

If you address several VLANs, you must insert a blank before and after the hyphen, for example `no interface range vlan 5 - 10`.

Result

The VLANs have been removed from the specified interface area.

Further notes

With the `interface range` command, you can put several interfaces or VLANs together to be able to configure them together.

7.1.2.4 map protocol

Description

With this command, you assign a protocol to a protocol 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:

```
map protocol
    {ip | ipv6 | novell | netbios | appletalk | other <aa:aa>}
    enet-v2 protocols-group <group-id (1-100)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ip	Internet Protocol v4	HEX 08:00
ipv6	Internet protocol v6	HEX 86:dd
novell	Novell Netware protocol	HEX 81:38
netbios	Netbios via TCP/IP	HEX f0:f0
appletalk	Appletalk	HEX 80:9b
other	Other protocol.	enter the hexadecimal protocol value. <ul style="list-style-type: none">• other: aa:aa• IPV6: 86:DD• LLDP: 88:CC• PTP IEEE1588: 88:F7• EAP (802.1X): 88:8E
enet-v2	Frame structure is Ethernet II	-
protocols-group	Keyword for a protocol group	-
group-id	Number of the group	decimal 1 ... 100

Result

The protocol group is created.

Further notes

You delete the protocol group with the `no map protocol` command.

You can display the status of this function and other information with the `show vlan protocols-group` command.

7.1.2.5 no map protocol

Description

With this command, you delete a protocol from all protocol groups.

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 map protocol  
    {ip | ipv6 | novell | netbios | appletalk | other <aa:aa>}  
enet-v2
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ip	Internet Protocol v4	HEX 08:00
ipv6	Internet protocol v6	HEX 86:dd
novell	Novell Netware protocol	HEX 81:38
netbios	Netbios via TCP/IP	HEX f0:f0
appletalk	Appletalk	HEX 80:9b
other	Other protocol.	enter the hexadecimal protocol value. <ul style="list-style-type: none">• other: aa:aa• IPV6: 86:DD• LLDP: 88:CC• PTP IEEE1588: 88:F7• EAP (802.1X): 88:8E
enet-v2	Frame structure is Ethernet II	-

Result

The protocol is removed from all protocol groups.

Further notes

You create the protocol group with the `map protocol` command.

You can display the status of this function and other information with the `show vlan protocols-group` command.

7.1.2.6 no protocol-vlan

Description

With this command, you disable the protocol-based classification on all interfaces.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
no protocol-vlan
```

Result

The classification is disabled.

Further notes

You enable the setting with the `protocol-vlan` command.

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

7.1.2.7 protocol-vlan

Description

With this command, you enable the protocol-based classification on all interfaces.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
protocol-vlan
```

7.1 VLAN

Result

The classification is enabled.

Further notes

You disable the setting with the `no protocol-vlan` command.

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

7.1.2.8 subnet-vlan

Description

With this command, you enable IPv4 subnet-based VLAN on all interfaces.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
subnet-vlan
```

Result

The classification is enabled.

Further notes

You disable the setting with the `no subnet-vlan` command.

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

You configure IPv4 subnet-based VLAN with the `map subnet` command.

7.1.2.9 no subnet-vlan

Description

With this command, you disable IPv4 subnet-based VLAN on all interfaces.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
no subnet-vlan
```

Result

The setting is disabled.

Further notes

You enable the setting with the `subnet-vlan` command.

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

7.1.2.10 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 16 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) #
```

7.1 VLAN

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

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 can display information about the VLAN with the `show vlan` command.

7.1.2.11 no vlan

Description

With this command, you delete a VLAN on the device.

Requirement

- The VLAN must not be assigned to a physical port.
- You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameter:

```
no vlan <vlan-id(1-4094)>
```

Parameter	Description	Range of values / note
vlan-id	Number of the addressed VLAN	1 ... 4094

The VLAN with number 1 cannot be deleted.

Result

The VLAN is deleted

Further notes

With the `vlan` command, you create a VLAN on the device.

You can display information about the VLAN with the `show vlan` command.

7.1.3 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.

These commands are available in the Interface Configuration mode of the Ethernet interfaces. For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

7.1.3.1 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 the Interface configuration mode.
- The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
mtu <frame-size(90-1500)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
frame-size	Size of the MTU in bytes	90 ... 1500 Default: 1500

Result

The setting for the size of the MTU is configured.

Further notes

You can shut down the interface with the `shutdown` command.

You display this setting with the `show interface mtu` command.

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

7.1.3.2 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.

7.1.3.3 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.

7.1.3.4 switchport acceptable-frame-type

Description

With this command, you configure which types of frames the interface accepts.

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}
```

The parameters have the following meaning:

Parameters	Description
all	All frames (with and without VLAN variables) are accepted
tagged	Only frames with VLAN variables are accepted

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

- The function is configured for `all`.

Result

The setting is enabled.

Further notes

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

7.1.3.5 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.

7.1.3.6 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.

7.1.3.7 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.

7.1.3.8 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.

7.1.3.9 no switchport mode

Description

With this command, you reset the operating mode for the switch port to the default.

The default value is Hybrid.

Requirement

- The interface is configured as a switch port.
- You are in the Interface configuration mode.
The command prompt is:

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

Syntax

Call the command without parameters:

```
no switchport mode
```

Result

The setting is reset to the default value.

Further notes

You configure the operating mode with the `switchport mode` command.

You display this setting and other information with the `show vlan port config` command.

You configure the interface as a switch port with the `switchport` command.

7.1.3.10 switchport priority default

Description

With this command, you configure the priority default for the interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
switchport priority default <(0-7)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
-	Value for the priority default	0 ... 7 Default: 0

Result

The setting for the default priority of the interface is configured.

Further notes

You reset the priority default to the original default with the `no switchport priority default` command.

You display this setting and other information with the `show vlan port config` command.

7.1.3.11 no switchport priority default**Description**

With this command, you reset the priority default for the interface to the default value.

The default value is 0.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

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

Syntax

Call the command without parameters:

```
no switchport priority default
```

Result

The setting is reset to the default value.

Further notes

You configure the priority default with the `switchport priority default` command.

You display this setting and other information with the `show vlan port config` command.

7.1.3.12 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 the Interface configuration mode.

The command prompt is as follows:

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

Syntax

Call up 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

Further notes

You can reset the setting to the default with the `no switchport pvid` command.

You configure the VLAN ID with the `switchport access vlan` command.

You display the setting and other information with the `show vlan port config` command.

7.1.3.13 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 the 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.

Further notes

You configure the setting with the `switchport pvid` command.

You configure the VLAN ID with the `switchport access vlan` command.

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

7.1.4 Commands in the VLAN configuration mode

This section describes commands that you can call up in the VLAN Configuration mode.

In global configuration mode, enter the `vlan $$$` command to change to this mode. When doing this, you need to replace the \$\$\$ placeholders with the relevant VLAN ID.

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

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

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

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

7.1.4.1 ip address

Description

With this command, you assign an IP address.

Requirement

You are in the Interface Configuration mode of VLAN.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
ip address <ip-address> [<subnet-mask>| / <prefix-length(0-32)>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
ip-address	IP address	Specify a valid IP address.
subnet-mask	Subnet mask	Enter a valid subnet mask.
prefix-length	Decimal representation of the mask as a number of "1" bits	0 ... 32

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The IP address is assigned.

Note

Effectiveness of the command

The command is effective immediately. If you configure the interface via which you access the device, the connection will be lost!

Further notes

You delete the setting with the `no ip address` command.

7.1.4.2 no ip address

Description

With this command, you delete the assignment of an IP address and disable DHCP.

Requirement

You are in the Interface Configuration mode of VLAN.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
no ip address [{ <ucast_addr> | dhcp }]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
ucast-addr	Value for an IPv4 unicast address	Enter a valid IPv4 unicast address.
dhcp	Specify this parameter if you want to disable the DHCP function explicitly.	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

If DHCP was enabled on this interface, DHCP is now disabled. Any existing dynamically learned IP address will be automatically converted to a static IP address.

If static IP addresses were configured and if no explicit IP address was transferred as a parameter, all static IP addresses will be deleted from this interface.

If a static IP address was specified explicitly, this address is deleted from this interface.

Note

Effectiveness of the command

The command is effective immediately.

If you configure the interface via which you access the device, you can lose the connection!

Further notes

You assign an IP address with the `ip address` or `ip address dhcp` command.

7.1.4.3 name

Description

With this command, you assign a name to the VLAN.

Requirement

You are in the VLAN Configuration mode.

7.1 VLAN

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
name <vlan-name>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
vlan-name	Name that will be assigned to the VLAN	max. 32 characters

Result

The VLAN is assigned a name.

Further notes

You delete name assignment for a VLAN with the `no name` command.

7.1.4.4 no name

Description

With this command, you delete the name assignment for a VLAN.

Requirement

You are in the VLAN configuration mode.

The command prompt is as follows:

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

Syntax

Call the command without parameters:

```
no name
```

Result

The name of the VLAN is deleted.

Further notes

You assign the VLAN a name with the command `name`.

7.1.4.5 ports

Description

With this command, you generate a list that specifies the behavior of the interfaces and replaces the existing VLAN configuration.

- Member ports (tagged ports)

The interface is added permanently to the list of incoming and outgoing connections. Tagged and untagged frames are transferred.

- Untagged Ports

The interface transfers untagged frames. If the VLAN ID (PVID) is set, incoming untagged frames are given a tag with the VLAN ID specified there. If the received frames already contain a VLAN ID, frames are only accepted if their VLAN ID matches the set PVID. With outgoing frames, the tag with the VLAN ID is removed.

- Forbidden Ports

This interface is not used for communication in a VLAN.

The "tagged port" and "untagged port" you specify with this command are used for outgoing data traffic.

Requirement

You are in the VLAN configuration mode.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
ports
(
  [<interface-type><0/a-b,0/c,...>]
  [<interface-type><0/a-b,0/c,...>]
)
[
  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:

Parameter	Description	Values
interface-type	Type or speed of the interface	Specify a valid interface.
0/a-b,0/c,...	a-b and c: Placeholders for numeric identification 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 41)".

Result

The settings are enabled.

Further notes

You display details of the function with the `show vlan` command.

You reset the settings with the `no ports` command.

7.1.4.6 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 41)".

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.

7.1.4.7 tia interface

Description

With this command, you enable or disable the property TIA interface. The TIA interface defines the VLAN on which the PROFINET functionalities are available. This mainly affects the device search with or via DCP.

Requirement

- The interface is enabled.
- You are in the Interface configuration mode of the VLAN interface.
The command prompt is:

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

\$\$\$ stands for the numbering of the interface.

Syntax

Call the command without parameters:

```
tia-interface
```

Result

The TIA interface property is enabled exclusively for the specified VLAN. The function was disabled on the other interfaces.

Further notes

Note that only one VLAN interface can become the TIA interface.

7.2 PPP

This section describes commands relevant for connecting to the WAN.

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 ppp information

Description

This command shows the settings and status of PPP.

Requirement

You are now in the Interface configuration mode xDSL.

The command prompt is as follows:

```
CLI(config-ppp-X) #
```

Syntax

Call the command without parameters:

```
show ppp information
```

Result

The information is 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 interface ppp

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. The name of the selected interface is displayed in the command prompt.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
interface ppp <interface-id>
```

The parameter has the following meaning:

Parameter	Description	Values
interface-id	Module no. and port no. of the interface	Specify a valid interface.

Result

You are in the Interface configuration mode.

The command prompt is as follows:

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

The placeholder `$` is replaced by the following module no. and port no. of the interface:

Further notes

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

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

7.2.3 Commands in the Interface configuration mode

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

In the 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.

7.2.3.1 forced disconnect

Description

With this command you specify whether you want the forced disconnect of your provider to be shifted to a specific time of day.

Requirement

- The "PPPoE Passthrough" function is disabled
- You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-ppp-X) #
```

Syntax

Call up the command with the following parameters:

```
forced disconnect{enabled | disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
enabled	Enables the forced disconnect	-
disabled	Disables the forced disconnect	-

Result

The setting is configured.

Further notes

You configure the time of day with the `forced disconnect time` command.

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

7.2.3.2 forced disconnect time

Description

With this command you specify the time of day to which you want to shift the forced disconnect of the DSL provider. This is only possible if the correct system time is set on the device.

Requirement

You are in the MODEM configuration mode

The command prompt is as follows:

```
cli(config-ppp-X)#
```

Syntax

Call up the command with the following parameters:

```
forced disconnect time <hh:mm:ss>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
-	Time of day	Enter the time of day in the following format: hh:mm:ss

Result

The time is specified:

Further notes

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

You enable the forced disconnect with the `forced disconnect` command.

7.2.3.3 interface vlan

Description

With this command, you specify the interface via which the PPP connection is established.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli (config-ppp-X) #
```

Syntax

Call up the command with the following parameters:

```
interface vlan <vlan-id (1-4094)>
```

The parameters have the following meaning:

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

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The interface is assigned.

Further notes

You display this setting and other information with the `show ppp informations` command.

You enable the PPP connection with the `pool-enable` command.

7.2.3.4 ip address

Description

With this command, you assign an IPv4 address to the interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-ppp-X)#
```

Syntax

Call up the command with the following parameters:

```
ip address <ip-address>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ip-address	IPv4 address for the Interface	Enter a valid IPv4 address

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The IP address is assigned to the PPP interface.

Further 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.

7.2.3.5 ip address dhcp

Description

With this command, the interface obtains the IPv4 address via DHCP.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-ppp-X)#
```

Syntax

Call the command without parameters:

```
ip address dhcp
```

Result

The DHCP assigns the IPv4 address to the 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.

7.2.3.6 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

The command prompt is as follows:

```
cli(config-ppp-X)#
```

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 41)".

Result

The setting is configured.

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.

7.2.3.7 password

Description

With this command, you configure the password.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-ppp-X)#
```

Syntax

Call up the command with the following parameters:

```
password <pw(255)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
pw	Password	Enter the password for the user. You will receive the password from your DSL provider. Maximum of 255 characters

Result

The password is configured.

Further notes

You display this setting and other information with the `show ppp informations` command.

7.2.3.8 shutdown

Description

With this command, you shut down the interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-ppp-X)#
```


Syntax

Call up the command with the following parameters:

```
shutdown [complete]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
without parameters	The interface is shut down but the connection remains.	-
complete	The interface is shut down and the PPP connection is terminated.	-

Result

The WAN interface is disabled.

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

Further notes

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

7.2.3.9 no shutdown

Description

With this command, you enable the WAN interface.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-ppp-X) #
```

Syntax

Call the command without parameter assignment:

```
no shutdown
```

Result

The Interface is shut down.

Further notes

You disable the WAN interface with the `shutdown` command.

7.2.3.10 type ppo-ex

Description

With this command you specify that the PPPoE (Point-to-Point over Ethernet) protocol is used for the PPP connection.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli(config-ppp-X)#
```

Syntax

Call the command without parameter assignment:

```
type ppo-ex
```

Result

The PPPoE protocol is used.

Further notes

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

7.2.3.11 username

Description

With this command, you configure the user name.

Requirement

You are in the Interface configuration mode

The command prompt is as follows:

```
cli (config-ppp-X) #
```

Syntax

Call up the command with the following parameters:

```
username <name (255)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
name	User name	Specify the user name. You will receive the user name from your DSL provider.

Result

The user name is configured.

Further notes

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

You configure the corresponding password with the `password` command.

7.3 Passive Listening

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 passive-listening

Description

This command shows whether or not "passive listening" is enabled.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call up the command with the following parameters:

```
show passive-listening
```

Result

`disabled` is displayed if "passive listening" is disabled. If "passive listening" is enabled, `enabled` is displayed.

7.3.2 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 **passive-listening bpdu-vlan-flood**

Description

With this command you enable forwarding of BPDUs for specific VLANs; in other words to all ports that are members of a VLAN.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
passive-listening bpdu-vlan-flood
```

As default the function is "enabled".

Result

BPDUs for specific VLANs.

Further notes

You disable this function with the `no passive-listening bpdu-vlan-flood` command.

You display the status of "passive listening" with the `show passive-listening` command.

7.3.2.2 **no passive-listening bpdu-vlan-flood**

Description

With this command you enable the flooding of BPDUs to all available ports of the device regardless of the configured VLANs.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
no passive-listening bpdu-vlan-flood
```

Result

BPDU's are flooded to all available ports.

Further notes

You enable this function with the `passive-listening bpdu-vlan-flood` command.

You display the status of "passive listening" with the `show passive-listening` command.

7.3.2.3 passive-listening

Description

This command enables "passive listening".

Requirement

Note

No simultaneous operation with spanning tree

"Passive listening" can only be enabled when spanning tree is disabled.

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
passive-listening
```

Result

The "passive listening" function is enabled.

Further notes

You disable "passive listening" with the `no passive-listening` command.

You display the status of "passive listening" with the `show passive-listening` command.

7.3.2.4 no passive-listening

Description

This command disables "passive listening".

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
no passive-listening
```

Result

The "passive listening" function is disabled.

Further notes

You enable "passive listening" with the `passive-listening` command.

You display the status of "passive listening" with the `show passive-listening` command.

7.4 Spanning Tree

The Spanning Tree Protocol is used to monitor a LAN for redundant connections. These are blocked and reactivated when necessary if there are changes to the network topology.

This section describes the commands of the Spanning Tree Protocol (STP), the Rapid Spanning Tree Protocol (RSTP) and the Multiple Spanning Tree Protocol (MSTP).

Note

Avoiding bad configurations

When using the commands in this section, you should take particular care because a bad configuration of this function can have serious negative affects on the network.

7.4.1 The "show" commands

This section describes commands with which you display various settings.

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

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

7.4.1.1 show spanning-tree

Description

This command shows the settings of the spanning tree function.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```


Syntax

Call up the command with the following parameters:

```
show spanning-tree [{ summary | blockedports | pathcost method }]
```

The parameters have the following meaning:

Parameter	Description
summary	Shows a summary
blockedports	Shows the blocked ports
pathcost method	Shows whether 16-bit (short) or 32 bit (long) values are used in the calculation

Result

The settings for the spanning tree function are displayed.

Further notes

You can show further settings for special aspects of the Spanning Tree Protocol with the following commands:

- `show spanning-tree active`
- `show spanning-tree bridge`
- `show spanning-tree detail`
- `show spanning-tree interface`
- `show spanning-tree root`
- `show spanning-tree mst`

7.4.1.2 show spanning-tree active

Description

This command shows the settings for the active ports of the spanning tree function.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call up the command with the following parameters:

```
show spanning-tree active [detail]
```

The parameter has the following meaning:

Parameter	Description
detail	Shows settings in detail

Result

The settings for the active ports of the spanning tree function are displayed.

7.4.1.3 show spanning-tree bridge

Description

This command shows the settings of the spanning tree function of the bridge.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call up the command with the following parameters:

```
show spanning-tree bridge  
[{ address | forward-time | hello-time | id | max-age | protocol | priority | detail  
}]
```

The parameters have the following meaning:

Parameter	Description
address	Shows the MAC address of the bridge
forward-time	Shows the time that the bridge is in the listening mode when changing from the blocking mode to the learning mode
hello-time	Shows the time after which the bridge sends configuration frames (BPDUs)
id	Shows the ID of the bridge
max-age	Shows the maximum age of the data packet after which it is deleted
protocol	Shows the protocol used
priority	Shows the priority of the bridge
detail	Shows detailed information about the Spanning Tree settings of the bridge

Result

The settings for the spanning tree function of the bridge are displayed.

7.4.1.4 show spanning-tree detail

Description

This command shows the detailed settings of the spanning tree function.

Requirement

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

The command prompt is as follows:

```
cli> OR cli#
```

Syntax

Call the command without parameters:

```
show spanning-tree detail
```

Result

The detailed settings for the spanning tree function are displayed.

7.4.1.5 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 port-fast 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 41)".

Result

The settings of the ports for the spanning tree function are displayed.

7.4.1.6 show spanning-tree interface layer2-gateway-port

Description

This command shows the settings of Layer 2 Gateway Port (L2GP). For example the priority, the MAC address and the status of L2GP are displayed.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call up the command with the following parameters:

```
show spanning-tree interface
[<interface-type><interface-id>]
layer2-gateway-port
```

The parameters have the following meaning:

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The settings for Layer 2 Gateway Port (L2GP) are displayed.

7.4.1.7 show spanning-tree root

Description

This command shows the settings of the root bridge for the spanning tree function.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call up the command with the following parameters:

```
show spanning-tree root
[ {address|cost|forward-time|id|max-age|port|priority|detail} ]
```

The parameters have the following meaning:

Parameter	Description
address	Shows the MAC address of the root bridge
cost	Shows the costs of the connection to the root bridge.
forward-time	Shows the time that the bridge is in the listening mode when changing from the blocking mode to the learning mode
id	Shows the ID of the root bridge
max-age	Shows the maximum age of the data packet after which it is deleted
port	Shows the interface via which the spanning tree is set up

Parameter	Description
priority	Shows the priority of the bridge
detail	Shows detailed information about the root bridge

Result

The settings of the root bridge for the spanning tree function are displayed.

7.4.2 clear spanning-tree detected protocols

Description

With this command, you restart the protocol transmission process on a specific or on all interfaces and force renegotiation of the connection settings with the neighboring devices.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
clear spanning-tree detected protocols  
  [{interface<interface-type><interface-id>}]
```

The parameters have the following meaning:

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

If you do not select any parameters from the parameter list, the process is restarted for all interfaces.

Result

The connection settings for spanning tree are renegotiated.

7.4.3 clear spanning-tree counters

Description

With this command, you reset all the statistical counters of the spanning tree function at the device and port level.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
clear spanning-tree counters
```

Result

The spanning tree counters are reset.

7.4.4 Commands in the global configuration mode

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

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

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

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

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

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

7.4.4.1 spanning-tree

Description

The Spanning Tree Protocol is used to monitor a LAN for redundant connections. These are blocked and reactivated when necessary if there are changes to the network topology.

With this command, you enable the spanning tree function.

Requirement

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.

7.4.4.2 no spanning-tree

Description

With this command, you disable the spanning tree function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no spanning-tree
```

Result

The spanning tree function is disabled.

Further notes

You enable the spanning tree function with the `spanning-tree` command.

You can display the status of this function and other information with the `show spanning-tree detail` command.

You can display information about active ports with the `show spanning-tree active` command.

7.4.4.3 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
<code>forward-time</code>	Keyword for the time after which a port changes its spanning tree status from "Blocking" to "Forwarding"	-
<code>seconds</code>	Time after which the changeover takes place	4 ... 30 Default: 15
<code>hello-time</code>	Keyword for the time after which the bridge sends its configuration BPDUs	-
<code>seconds</code>	Time after which they are sent	1 ... 6 Default: 2

Parameter	Description	Range of values / note
max-age	Keyword for the time after which the information of the BPDUs becomes invalid	-
seconds	Maximum age of the BPDUs in seconds	6 ... 55 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:

- $2 * (\text{forward-time} - 1) \geq \text{max-age}$
 - $\text{max-age} \geq 2 * (\text{hello-time} + 1)$
-

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 time settings are reset.

You display these settings and other information with the commands that start with `show spanning-tree`

7.4.4.4 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 time settings are reset.

The default values are as follows:

Parameter	Default value
forward-time	15 seconds
hello-time	2 seconds
max-age	20 seconds

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no spanning-tree{forward-time|hello-time|max-age}
```

The parameters have the following meaning:

Parameter	Description
forward-time	Time after which a port changes its spanning tree status from "Blocking" to "Forwarding"
hello-time	Time after which the bridge sends its configuration frames (BPDUs)
max-age	Time after which the information of the BPDUs becomes invalid

Result

The selected setting for the time is reset to the default value.

Further notes

You configure the time with the `spanning-tree` command (time settings).

You display these settings and other information with the commands that start with `show spanning-tree`

7.4.5 Commands in the Interface configuration mode

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

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

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

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

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

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

7.4.5.1 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 up the command with the following parameters:

```
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	Range of values/note
<code>cost</code>	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: <ul style="list-style-type: none"> • 200000 for physical interfaces • 199999 for port channels
<code>disable</code>	disables the interface for spanning tree	- Default: The spanning tree function is enabled on the interface
<code>link-type</code>	Connection status of the following network segment	<ul style="list-style-type: none"> • <code>point-to-point</code> • <code>shared</code> Default: <ul style="list-style-type: none"> • <code>point-to-point</code> The connection is configured as <code>full-duplex</code> <ul style="list-style-type: none"> • <code>shared</code> in all other cases
<code>portfast</code>	Enables the PortFast function	- Default: disabled
<code>port-priority</code>	Priority of the interface	0 ... 240 in increments of 16 Default: 128

Note

Configure multiple properties

With each call of the command, you can configure precisely one property.
If you want to configure several properties, call the command several times.

Result

The selected property is configured.

Further notes

You can reset the setting to the default with the `no spanning-tree (properties)` command.

You display these settings and other information with the commands that start with `show spanning-tree ...`

7.4.5.2 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: <ul style="list-style-type: none">• 200000 for physical interfaces• 199999 for port channels
disable	The spanning tree function is enabled on the interface
link-type	<ul style="list-style-type: none">• point-to-point The connection is configured as <code>full-duplex</code> <ul style="list-style-type: none">• shared in all other cases
portfast	disabled
port-priority	128

Requirement

You are in interface configuration mode.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
no spanning-tree {cost|disable|link-type|portfast|port-priority}
```

The parameters have the following meaning:

Parameter	Description
cost	Keyword for the costs of the port for calculating the lowest-cost path.
disable	Enables the interface for spanning tree.
link-type	Connection status of the following network segment
portfast	Disables the PortFast function.
port-priority	Keyword for the priority of the interface

Note**Configure multiple properties**

With each call of the command, you can configure precisely one property.
If you want to configure several properties, call the command several times.

Result

The selected setting was reset to the default value.

Further notes

You configure the setting with the `spanning-tree` command (properties).

You display these settings and other information with the commands that start with `show spanning-tree`

7.4.5.3 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.

7.4.5.4 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.

Network protocols

This part contains the sections that describe the commands for working with the various network protocols.

8.1 IPv4 protocol

This section describes commands of the Internet Protocol (IP) version 4.

8.1.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.1.1.1 show ip dns

Description

This command shows information about the DNS client, for example the status of the DNS client and parameters for querying the DNS server.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show ip dns
```

Result

Information on the DNS client is displayed.

8.1.1.2 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 41)".

Result

The overview of the DCP forwarding behavior is displayed.

8.1.1.3 show dcp server

Description

This command shows whether or not the DCP function is enabled on the device.
If the DCP function is enabled, the read and write permissions are displayed.

Requirement

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

The command prompt is as follows:

```
cli> OR cli#
```

Syntax

Call the command without parameters:

```
show dcp server
```

Result

The overview of the status of the DCP function and access rights is displayed.

8.1.1.4 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}]
```

The parameters have the following meaning:

Parameter	Description	Range of values
ip-address	Shows the information for a specific IP address.	Specify a valid IP address
mask	Defines an address range using the subnet mask.	/8, /16 or /24
connected	Shows the direct connections.	-
static	Shows the static connections.	-

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The routing table is displayed.

8.1.1.5 show ip routing

Description

This command shows whether or not the "routing" function 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 ip routing
```

Result

The routing function is enabled.

8.1.1.6 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.

8.1.1.7 show ip telnet

Description

This command shows the admin status and the port number of the Telnet server.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show ip telnet
```

Result

The admin status and the port number of the Telnet server are displayed.

8.1.2 Commands in the global configuration mode

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

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

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

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

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

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

8.1.2.1 dcp server

Description

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.

8.1.2.2 no dcp server

Description

With this command, you disable the DCP server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no dcp server
```

Result

The DCP server is disabled.

Further notes

You enable and configure the DCP server with the `dcp server` command.

8.1.2.3 ip echo-reply

Description

To check the availability of a network node, packets of the Internet Control Message Protocol (ICMP) can be sent to it. These packets of type 8 request the recipient to send a packet back to the sender (echo reply).

With this command you enable the network node to react to ping queries.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip echo-reply
```

Result

"ICMP echo reply messages" are enabled. The network node reacts to ping queries.

Further notes

You disable the setting with the `no ip echo-reply` command.

8.1.2.4 no ip echo-reply

Description

With this command you stop the network node reacting to ping queries.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip echo-reply
```

Result

"ICMP echo reply messages" are disabled. The network node does not react to ping queries.

Further notes

You change the setting with the `ip echo-reply` command.

8.1.2.5 ip route

Description

With this command, you configure a static entry in the IP routing table.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ip route <prefix> <mask> <next-hop> [<distance (1-255)>] [ interface { vlan <short  
(1-4094)> } ]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
prefix	Specifies the IP address or the address range	specify a valid IP address
mask	Specifies the subnet mask used for prefix. Use decimal notation.	enter a valid subnet mask
next-hop	Specifies the IP address to which the selected addresses will be forwarded.	specify a valid IP address
distance	The value for the administrative distance.	1 ... 255
interface		
vlan	Keyword for a VLAN connection	-
short	Number of the addressed VLAN	1 ... 4094

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The entry in the IP routing table is configured.

Further notes

You delete an entry from the IP routing table with the `no ip route` command.

You display the IP routing table with the `show ip route` command.

8.1.2.6 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	Specifies the IP address or the address range	Enter a valid IPv4 address
mask	Specifies the subnet mask used for prefix. Use decimal notation.	enter a valid subnet mask
next-hop	specifies the IP address to which the selected addresses were forwarded.	Enter a valid IPv4 address

Result

The entry is deleted.

Further 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.

8.1.2.7 ip routing

Description

With this command, you enable the routing function for IPv4.

Note

This command is available only with layer 3. DHCP must not be enabled on any IP interface.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
ip routing
```

Result

The routing function is enabled.

Further notes

You disable the function with the `no ip routing` command.

You display the setting with the `show ip route` command.

8.1.2.8 no ip routing

Description

With this command, you disable IPv4 routing function on the device.

Note

IPv6 routing

If IPv6 routing is enabled on the device, this is also disabled with this function.

Note

This command is available only with layer 3.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ip routing
```

Result

IPv4 routing is disabled.

Further notes

You enable the function with the `ip routing` command.

You display the setting with the `show ip route` command.

8.1.2.9 telnet-server

Description

With this command, you enable the Telnet server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
telnet-server
```

As default the function is "enabled".

Result

The Telnet server is enabled.

Further notes

You disable the Telnet server with the `no telnet-server` command.

8.1.2.10 no telnet-server

Description

With this command, you disable the Telnet server.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli (config) #
```

Syntax

Call the command without parameters:

```
no telnet-server
```

Result

The Telnet server is disabled.

Further notes

You enable the Telnet server with the `telnet-server` command.

8.1.3 Commands in the Interface configuration mode

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

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

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

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

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

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

8.1.3.1 dcp forwarding

Description

With this command, you configure the forwarding behavior of the interface for DCP frames.

Note

PROFINET configuration

Since DCP is a PROFINET protocol, the configuration created here is only effective with the VLAN associated with the TIA interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
dcp forwarding {block|forward}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
block	DCP frames are discarded	-
forward	DCP frames are forwarded	Default: forward

Result

The forwarding behavior of the interface for DCP frames is configured.

8.1.3.2 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 or a router port.

The command prompt is as follows:

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

or with a router port:

```
cli(config-RPort-if-Int$-$)
```

Syntax

Call up the command with the following parameters:

```
ip address <ip-address> {<subnet-mask>|/<prefix-length(0-32)>}[secondary]
```

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	0 ... 32
secondary	Further subnet for this interface	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The IPv4 address is assigned to the VLAN interface or the router port.

Note

Effectiveness of the command

The command is effective immediately.

If you configure the interface via which you access the device, the connection will be lost!

Further notes

You delete the IPv4 address with the `no ip address` command.

You display this setting and other information with the `show ip interface` command.

8.1.3.3 ip address dhcp

Description

With this command, the VLAN interface obtains the IPv4 address via DHCP.

Requirement

You are in the Interface Configuration mode of VLAN.

The command prompt is as follows:

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

Syntax

Call the command without parameters:

```
ip address dhcp
```

Result

The DHCP assigns the IP address to the VLAN interface.

Further notes

You delete the settings with the `no ip address` command.

You display this setting and other information with the `show ip interface` command.

8.1.3.4 no ip address

Description

With this command, you delete the assignment of an IP address to a VLAN interface.

Requirement

You are in the Interface configuration mode of VLAN.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

```
no ip address [{ <ucast_addr>|dhcp}]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
ucast_addr	IP Address of the VLAN interface that will be deleted	enter a valid IP address
dhcp	Specify this parameter if you want to cancel the obtaining of the IP address from a DHCP server.	

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The assignment of the IP address to a VLAN interface is deleted and DHCP is disabled.

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 setting with the `ip address` command.

You display this setting and other information with the `show ip interface` command.

8.2 ARP

This section describes commands of the Address Resolution Protocol (ARP).

8.2.1 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.

8.2.1.1 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 up the command with the following parameters:

```
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	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	
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	-

Parameter	Description	Range of values/note
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 41)".

If you do not select any parameter from the parameter list, all parameters of the ARP table are displayed.

Result

The ARP table is displayed.

8.3 DHCP client

This section describes commands of the Dynamic Host Configuration Protocol (DHCP).

8.3.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.3.1.1 show ip dhcp client

Description

With this command, you display the configuration settings of the DHCP client.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show ip dhcp client
```

Result

The configuration settings of the DHCP client are displayed.

8.3.2 Commands in the global configuration mode

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

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

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

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

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

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

8.3.2.1 ip dhcp config-file-request

Description

If the DHCP config file request option is set, the device requests the TFTP address and the name of a configuration file from the DHCP server. If the device is restarted following the completed download, the configuration settings are read from this file.

With this command, you enable the DHCP config file request option.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ip dhcp config-file-request
```

Result

The DHCP config file request option is enabled.

Further notes

You disable the DHCP config file request option with the `no ip dhcp config-file-request` command.

8.3.2.2 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.

8.3.2.3 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 the 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 | iaaid-duid }
```

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	-
iaaid-duid	The client registers with the IAID (Interface Association Identifier) and the DUID (DHCP Unique Identifier).	-

Result

The registration mode of the DHCP client is configured.

Further notes

You configure the DUID type with the `dhcp duid type` command.

8.3.2.4 dhcp duid type

Description

With this command, you specify the DUID type.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
dhcp duid type {llt | en | ll}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
llt	DUID is based on the link layer address of the interface and a time stamp	-
en	DUID is assigned by the vendor (EN = enterprise number)	-
ll	DUID is based on the link layer address of the interface	-

Result

The DUID type is defined.

8.4 DHCP server

You can operate the device as a DHCP server. This allows IP addresses to be assigned automatically to the connected devices. The IP addresses are either distributed dynamically from an address band (pool) you have specified or a specific IP address is assigned to a particular device.

Both with the dynamic and static assignment a pool is selected based on the following criteria:

1. With the DHCP query option 82 is enabled.

The DHCP server checks whether there is a pool with option 82. You configure this criterion with the `relay-information` command.

2. The DHCP query was received via a relay agent.

The DHCP server checks whether the relay agent is located in the subnet of a pool.

3. The port via which the DHCP query was received is enabled in the Port Range.

The DHCP server checks whether the IP interface of the port is located in the subnet of a pool. You configure this criterion with the `ip address` command.

This section describes commands relevant for configuring the DHCP server.

Requirement

The connected devices are configured so that they obtain the IPv4 address from a DHCP server.

8.4.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.4.1.1 show ip dhcp-server bindings

Description

This command shows the current assignments of IPv4 addresses of the DHCP server.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameter assignment:

```
show ip dhcp-server bindings
```

Result

The information is displayed.

8.4.1.2 show ip dhcp-server pools

Description

The command shows the DHCP server configuration of a specific IPv4 address band or all IPv4 address bands and the corresponding DHCP options.

Requirement

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 dhcp-server pools [pool-id (1-5)]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
pool-id	ID of the addressed IPv4 address band	1 ... 5

Result

The configuration of the DHCP server and the DHCP options is displayed.

8.4.2 Commands in the global configuration mode

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

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

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

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

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

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

8.4.2.1 ip dhcp-server

Description

With this command, you enable the DHCP server on the device.

Note

To avoid conflicts with IPv4 addresses, only one device may be configured as a DHCP server in the network.

Note

Maximum number of IP addresses

The maximum number of IPv4 addresses that the DHCP server supports is 100. In other words, a total of 100 IPv4 addresses (dynamic + static).

With the static assignments, you can create a maximum of 20 entries.

Requirement

- You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
ip dhcp-server
```

Result

The DHCP server is enabled.

Further notes

You disable the DHCP server with the `no ip dhcp-server` command.

8.4.2.2 no ip dhcp-server

Description

With this command, you disable the DHCP server on the device.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no ip dhcp-server
```

Result

The DHCP server is disabled.

Further notes

You enable the DHCP server with the `ip dhcp-server` command.

8.4.2.3 no ip dhcp-server icmp-probe

Description

With this command you disable the function "Probe address with ICMP echo before offer".

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no ip dhcp-server icmp-probe
```

Result

The function is disabled.

Further notes

You enable the function with the `ip dhcp-server icmp-probe` command.

8.4.2.4 ip dhcp-server icmp-probe

Description

With this command you enable the function "Probe address with ICMP echo before offer". The DHCP server checks whether or not the IPv4 address has already been assigned. If no reply is received, the DHCP server can assign the IPv4 address.

Note

With static assignments, this check is not made.

Requirement

You are in the Global Configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
ip dhcp-server icmp-probe
```

Result

The function is enabled.

Further notes

You disable the function with the `no ip dhcp-server icmp-probe` command.

8.4.2.5 ip dhcp-server pool

Description

With this command, you have three options of changing to the DHCPPOOL configuration mode and to assign an interface to the IPv4 address band.

1. If you call the command `ip dhcp-server pool` with the parameter `pool-id (1-8)`, you change to the corresponding DHCPPOOL configuration mode. The corresponding pool ID must have already been created.
2. If you call the `ip dhcp-server pool` command with the parameter `vlan` or `interface-type/interface-id`, an IPv4 address band with the next free pool ID is created and the specified interface assigned directly to it. This is followed by a change to the DHCPPOOL configuration mode. You then configure the other settings in the DHCPPOOL configuration mode.
3. If you call the `ip dhcp-server pool` command without parameters, an IPv4 address band with the next free pool ID is created and you change directly to the corresponding DHCPPOOL configuration mode.

You then configure the interface and the other settings in the DHCPPOOL configuration mode.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ip dhcp-server pool [{ <pool-id (1-8)> | [{ vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }]]]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
pool-id	ID of the addressed IPv4 address band	1 ... 8
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094
interface-type	Type of interface	Specify a valid interface.
interface-id	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The ID of the addressed IPv4 address band is configured.

You are now in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Further notes

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

You delete the entry with the `no ip dhcp-server pool` command.

8.4.2.6 no ip dhcp-server pool

Description

With this command, you delete the required IPv4 address band.

Requirement

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 dhcp-server pool <pool-id (1-8)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
pool-id	ID of the addressed IPv4 address band	1 ... 8

Result

The required IPv4 address band is deleted.

Further notes

You create the IPv4 address band with the `ip dhcp-server pool` command.

8.4.3 Commands in the DHCPPOOL configuration mode

This section describes commands that you can call up in the DHCPPOOL Configuration mode.

In global configuration mode, enter the `ip dhcp-server pool` command to change to this mode.

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

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

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

8.4.3.1 lease-time

Description

With this command, you specify how long the assigned IPv4 address remains valid. When half the period of validity has elapsed, the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
lease-time <seconds (60-31536000)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
seconds	Time until renewal of the assigned IPv4 address in seconds	60 ... 31536000

Result

The time is configured.

Further notes

You display the setting with the `show ip dhcp-server pools` command.

8.4.3.2 network

Description

With this command you configure the IPv4 address band from which the DHCP client receives any IPv4 address.

Note**Maximum number of IP addresses**

The maximum number of IPv4 addresses that the DHCP server supports is 100. In other words, a total of 100 IPv4 addresses (dynamic + static).

With the static assignments, you can create a maximum of 20 entries.

Assignment of IP addresses

The requirement for the assignment is that the IPv4 address of the interface is located within the IPv4 address band. If this is not the case, the interface does not assign any IPv4 addresses

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
network <lower-IP> <upper-IP> { <subnet-mask> | / <prefix-length (1-32)> }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
lower-IP	Start of the IPv4 address band	Enter a valid IPv4 address.
upper-IP	End of the IPv4 address band	Enter a valid IPv4 address.
subnet-mask	Subnet mask of the corresponding subnet	Enter a valid subnet mask
prefix-length	Decimal representation of the mask as a number of "1" bits	1 ... 32

Result

The IPv4 address band is configured. The DHCP options 1, 3, 6, 66 and 67 are created automatically. With the exception of option 1, the options can be deleted.

Note

DHCP options supported

The DHCP options 1, 2, 3, 4, 5, 6, 42, 66, 67 are supported.

Further notes

You display the setting with the `show ip dhcp-server pools` command.

You configure the DHCP options 1, 3, 4, 5, 6, 42 and 66 with the `option (IP address)` command.

You configure the DHCP option 2 with the `option value-hex` command.

You configure the DHCP options 66 and 67 with the `option value-string` command.

You assign an IP address to an interface with the `set interface` command.

You delete the DHCP option with the `no option` command.

8.4.3.3 option (IP address)

Description

With this command you configure the DHCP options 1, 3, 4, 5, 6, 42 and 66. If the DHCP options do not exist, the corresponding entry is created.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
option <option-code> { <ip-address-list> | int-ip }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
option-code	Code of the DHCP option	Enter a valid DHCP option. <ul style="list-style-type: none">• 1 - Subnet mask• 3 - Router• 4 - Time server• 5- Name server• 6 - DNS servers• 42 -NTP server• 66 - TFTP server
ip-address-list	IPv4 address or IPv4 address list	-
int-ip	Uses IPv4 address of the interface that is assigned to the IPv4 address band.	Enter the IPv4 address or the IPv4 address list. Several IPv4 addresses are separated by commas.

Result

The DHCP option is configured.

Further notes

You display the setting with the `show ip dhcp-server pools` command.

You disable the IPv4 address band with the `no pool-enable` command.

You delete the DHCP option with the `no option` command.

You configure the interface with the `set interface` command.

8.4.3.4 option value-hex

Description

With this command, you create DHCP options that contain a hexadecimal value as DHCP parameter. The various DHCP options are defined in RFC 2132.

The exceptions are the DHCP options: 1, 3, 12, 66 and 67. You configure the DHCP options 3, 6 and 66 with the command `option` (IP address) and the DHCP options 12 and 67 with the command `option value-string`.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>) #
```

Syntax

Call up the command with the following parameters:

```
option <option-code> value-hex <dhcp-param>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
option-code	Code of the DHCP option	Enter a valid DHCP option. The following DHCP options are not supported: <ul style="list-style-type: none">• 50 - 60• 255
dhcp-param	DHCP parameter in hexadecimal	Enter a valid hexadecimal value. Format: XXXXX e.g. C0A86402

Result

The DHCP option is configured. In total a maximum of 20 DHCP options are possible.

Further notes

You display the setting with the `show ip dhcp-server-pools` command.

You disable the IPv4 address band with the `no pool-enable` command.

You delete the DHCP option with the `no option` command.

8.4.3.5 option value-string

Description

With this command you configure DHCP options 12, 66 and 67 that contain a string as DHCP parameter. The DHCP options 66 and 67 are created automatically when the IPv4 address band is created.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>) #
```

Syntax

Call up the command with the following parameters:

```
option <option-code> value-string <dhcp-param>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
option-code	Code of the DHCP option	<ul style="list-style-type: none">• 12 - Host name• 66 - TFTP server• 67 - Bootfile name
dhcp-param	Name of the file	Enter the name in the string format.

Result

The DHCP option is configured.

Further notes

You display the setting with the `show ip dhcp-server pools` command.

You delete the DHCP option with the `no option` command.

You configure the DHCP options 3 and 6 with the `option (IP address)` command.

You disable the IPv4 address band with the `no pool-enable` command.

8.4.3.6 no option

Description

With this command, you delete the DHCP option with the specified number.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli (config-dhcp-pool-<ID>) #
```

Syntax

Call up the command with the following parameters:

```
no option <option-code>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
option-code	Code of the DHCP option	Enter a valid DHCP option code. <ul style="list-style-type: none">• 2 - Offset time• 3 - Router• 4 - Time server• 5- Name server• 6 - DNS servers• 42 -NTP server• 66 - TFTP server• 67 - Bootfile name

Result

The specified DHCP option is deleted.

Further notes

You configure the DHCP option with a string with the `option value-string` command.

You configure DHCP options with a hexadecimal value with the `option value-hex` command.

You configure the DHCP options with IPv4 address with the `option (IP-Adresse)` command.

8.4.3.7 pool-enable

Description

With this command you specify that this IPv4 address band will be used.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call the command without parameter assignment:

```
pool-enable
```

Result

The setting is enabled.

Note

If the IPv4 address band is enabled, the following parameters can no longer be edited:

- DHCP options (`option ...`)
 - Static Leases (`static-lease`)
-

Further notes

You display the setting with the `show ip dhcp-server pools` command.

You disable the setting with the `no pool-enable` command.

8.4.3.8 no pool-enable

Description

With this command you specify that this IPv4 address band will not be used.

Note

Deleting DHCP server bindings

If you disable or delete an IPv4 address band or you switch the DHCP server off and on again, the DHCP server bindings are deleted. You display the DHCP server bindings with the `show ip dhcp-server bindings` command.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call the command without parameter assignment:

```
no pool-enable
```

Result

The setting is disabled.

Further notes

You display the setting with the `show ip dhcp-server pools` command.

You enable the setting with the `pool-enable` command.

8.4.3.9 set-interface

Description

With this command, you specify the interface via which the IPv4 addresses are dynamically assigned.

Note

Assignment of IP addresses

When assigning IP addresses from a local address band, the IPv4 address of the interface must be located within the IPv4 address band. If this is not the case, the interface does not assign any IPv4 addresses.

The IP address does not need to be within the IPv4 address band if relay agent information is configured for the address band.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
set-interface {vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }
```

The parameters have the following meaning:

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The interface is assigned. Before the IPv4 address band can be used, it still needs to be activated.

Further notes

You display the setting with the `show ip dhcp-server pools` command.

You enable the IPv4 address band with the `pool-enable` command.

8.4.3.10 static-lease

Description

With this command you specify that certain devices will be assigned a certain IP address. The address assignment is made based on the MAC address, the client ID or the DUID.

Requirement

- The assignment has not yet been created.
- You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>) #
```

Syntax

Call up the command with the following parameters:

```
static-lease {mac <mac-address> | client-id <string> | client-id-duid <hex_str> }  
<ip-address>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
mac	Keyword for a MAC address	-
mac-address	Unicast MAC address	Specify the MAC address. aa:bb:cc:dd:ee:ff
client-id	Keyword for a DHCP client ID	-
string	Freely definable DHCP client ID	Enter the required designation. Maximum of 254 characters
client-id-duid	Keyword for a DUID	-
hex_str	DHCP Unique Identifier	Specify the DUID.
ip-address	Unicast IPv4 address	Enter a valid IPv4 address. The IPv4 address must match the subnet of the IPv4 address band.

Result

The assignment is specified.

Further notes

You display the setting with the `show ip dhcp dhcp-server bindings` command.

You disable the IPv4 address band with the `no pool-enable` command.

You delete the assignment with the `no static-lease` command.

8.4.3.11 no static-lease

Description

With this command, you delete the assignment of an IPv4 address.

Requirement

You are in the DHCPPOOL configuration mode.

The command prompt is as follows:

```
cli(config-dhcp-pool-<ID>)#
```

Syntax

Call up the command with the following parameters:

```
no static-lease { mac <mac-address> | client-id <string> | client-id-duid <hex_str> }
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
mac	Keyword for a MAC address	-
mac-address	Unicast MAC address	Specify the MAC address. aa:bb:cc:dd:ee:ff
client-id	Keyword for a DHCP client ID	-
string	Freely definable DHCP client ID	Enter the required designation.
client-id-duid	Keyword for a DUID	-
hex_str	DHCP Unique Identifier	Specify the DUID.

Result

The assignment is deleted.

Further notes

You configure the assignment with the `static-lease` command.

8.5 DNS

This section describes commands of the Domain Name System (DNS).

8.5.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.5.1.1 show 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.

8.5.1.2 show ddnsclient information

Description

This command shows the configuration of the dynamic DNS client.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show ddnsclient overview
```

Result

The configuration is displayed.

8.5.2 Commands in the global configuration mode

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

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

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

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

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

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

8.5.2.1 **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.

8.5.2.2 **dnsproxy**

Description

With this command, you change to the DNS PROXY 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:

```
dnsproxy
```

Result

You are now in the DNS PROXY configuration mode.

The command prompt is as follows:

```
cli(config-dnsproxy)#
```

Further notes

You exit the DNS PROXY configuration mode with the `end` or `exit` command.

8.5.2.3 ddnsclient

Description

With this command, you change to the DDNS Client configuration mode.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ddnsclient
```

Result

You are now in the DDNS Client configuration mode.

The command prompt is as follows:

```
cli(config-ddnsclient)#
```

Further notes

You exit the DDNS Client configuration mode with the `end` or `exit` command.

8.5.3 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.

8.5.3.1 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	IPv4 address	Enter a valid IPv4 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 `manual` command.

8.5.3.2 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	IPv4 address	Enter the IPv4 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.

8.5.3.3 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.

8.5.3.4 shutdown

Description

With this command, you end 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 ended.

Further notes

You start the DNS client with the `no shutdown` command.

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

8.5.3.5 no shutdown

Description

With this command, you start 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 end the DNS client with the `shutdown` command.

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

8.5.4 Commands in the DNS PROXY configuration mode

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

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

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

8.5.4.1 `cachendomain`

Description

With this command, you enable the caching of NXDOMAIN responses. This means that the domain names that were unknown to the DNS server remain in the cache.

Requirement

You are in the DNS PROXY configuration mode.

The command prompt is as follows:

```
cli(config-dnsproxy)#
```

Syntax

Call the command without parameter assignment:

```
cache nxdomain
```

Result

The setting is enabled.

Further notes

You disable the setting with the `no cachendomain` command.

8.5.4.2 `no cachendomain`

Description

With this command, you disable the caching of NXDOMAIN responses.

Requirement

You are in the DNS PROXY configuration mode.

The command prompt is as follows:

```
cli(config-dnsproxy)#
```

Syntax

Call the command without parameter assignment:

```
no cache nxdomain
```

Result

The setting is disabled.

Further notes

You enable the setting with the `cache nxdomain` command.

8.5.4.3 shutdown

Description

With this command, you disable the proxy of the DNS server.

Requirement

You are in the DNS PROXY configuration mode.

The command prompt is as follows:

```
cli(config-dnsproxy)#
```

Syntax

Call the command without parameter assignment:

```
shutdown
```

Result

The setting is disabled.

Further notes

You enable the setting with the `no shutdown` command.

8.5.4.4 no shutdown

Description

With this command, you enable the proxy of the DNS server.

Requirement

You are in the DNS PROXY configuration mode.

The command prompt is as follows:

```
cli(config-dnsproxy)#
```

Syntax

Call the command without parameter assignment:

```
no shutdown
```

Result

The setting is enabled.

Further notes

You disable the setting with the `shutdown` command.

8.5.5 Commands in the DDNS Client configuration mode

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

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

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

8.5.5.1 service

Description

With this command, you enable the dynamic DNS provider.

Requirement

You are in the DDNS Client configuration mode.

The command prompt is as follows:

```
cli(config-ddnsclient)#
```

Syntax

Call up the command with the following parameters:

```
service {show-services | <index>}
```

The parameters have the following meaning:

Parameter	Description	Range of values
show-services	Lists the available providers.	-
index	Number corresponding to a specific provider.	Specify a valid number.

Result

The specified entry is enabled.

Further notes

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

You disable an entry with the `no service` command.

8.5.5.2 no service

Description

With this command, you disable the dynamic DNS provider.

Requirement

You are in the DDNS Client configuration mode.

The command prompt is as follows:

```
cli(config-ddnsclient)#
```


Syntax

Call up the command with the following parameters:

```
no service {show-services | <index>}
```

The parameters have the following meaning:

Parameter	Description	Range of values
show-services	Lists the available providers.	-
index	Number corresponding to a specific provider.	Specify a valid number.

Result

The specified entry is disabled.

Further notes

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

You enable an entry with the `no service` command.

8.5.5.3 userhost

Description

With this command, you configure the host name that you have agreed with your dynamic DDNS provider for the device, e.g. example.no-ip.com.

Requirement

You are in the DDNS Client configuration mode.

The command prompt is as follows:

```
cli(config-ddnsclient)#
```

Syntax

Call up the command with the following parameters:

```
userhost {show-services | <index> <host>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
show-services	Lists the available providers.	-
index	Number corresponding to a specific provider.	Specify a valid number.
host	Host name	Specify the agreed host name.

Result

The host name is configured.

Further notes

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

You configure the user name with the `username` command.

You configure the password with the `password` command.

8.5.5.4 username

Description

With this command, you configure the user name with which the device logs on to the dynamic DNS server.

Requirement

You are in the DDNS Client configuration mode.

The command prompt is as follows:

```
cli(config-ddnsclient)#
```

Syntax

Call up the command with the following parameters:

```
username {show-services | <index> <username>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
show-services	Lists the available providers.	-
index	Number corresponding to a specific provider.	Specify a valid number.
username	User names	Specify the negotiated user name.

Result

The user name is configured.

Further notes

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

You configure the password with the `password` command.

8.5.5.5 password

Description

With this command, you configure the password with which the device logs on to the dynamic DNS server.

Requirement

You are in the DDNS Client configuration mode.

The command prompt is as follows:

```
cli(config-ddnsclient)#
```

Syntax

Call up the command with the following parameters:

```
password {show-services | <index> <password>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
show-services	Lists the available providers.	-
index	Number corresponding to a specific provider.	Specify a valid number.
password	Password	Enter the negotiated password.

Result

The password is configured.

Further notes

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

You configure the user name with the `username` command.

8.6 SNMP

This section describes commands of the Simple Network Management Protocol (SNMP).

Example of a configuration

IP configuration

Define the IP address of the device that is suitable for the SNMP trap receiver used.

Execute the following commands:

```
configure terminal
int vlan 1
no ip address
ip address 192.168.1.1 255.255.255.0
end
```

Trap configuration forr SNMPv2c notifications

To configure the sending of SNMP traps, an SBMP community is required.

This community is used along with other SNMP parameters to send traps to a trap recipient.

The selection of the traps recipient is made using tags that are set when SNMP notifications are called.

Execute the following commands:

```
configure terminal
snmp community index v2trapindex name public security v2secname
snmp targetaddr trapringer param pav2c ipv4 192.168.1.254 taglist publictrapv2tag
snmp targetparams pav2c user v2secname security-model v2c message-processing v2c
snmp notify testnotify tag publictrapv2tag type trap
end
```

Event configuration

Enable the sending of traps.

Execute the following commands:

```
configure terminal
events
client config trap
end
```

For system messages all configured SNMP notification are always called.

With RMOB events. the SNMP notifications to be called must be configured explicitly, see section "RMON".

8.6.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.6.1.1 show snmp

Description

This command shows the status information of SNMP.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp
```

Result

The status information is displayed.

8.6.1.2 show snmp community

Description

This command shows the details of the configured of SNMP communities.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp community
```

Result

The details of the configured SNMP communities are displayed.

8.6.1.3 **show snmp engineID**

Description

This command shows the SNMP identification number of the device.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp engineID
```

Result

The SNMP identification number of the device is displayed.

8.6.1.4 **show snmp filter**

Description

This command shows the configured SNMP filters.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp filter
```

Result

The configured SNMP filters are displayed.

8.6.1.5 show snmp group**Description**

This command shows the configured SNMP groups.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp group
```

Result

The configured SNMP groups are displayed.

8.6.1.6 show snmp group access**Description**

This command shows the rights of the configured SNMP groups.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp group access
```

Result

The rights of the configured SNMP groups are displayed.

8.6.1.7 **show snmp inform statistics**

Description

This command shows the statistics of the Inform Messages.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp inform statistics
```

Result

The statistics of the Inform Messages are displayed.

8.6.1.8 **show snmp notif**

Description

With this command, you display the configured SNMP notification types.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```


Syntax

Call the command without parameters:

```
show snmp notif
```

Result

The configured SNMP notification types are displayed.

8.6.1.9 show snmp targetaddr**Description**

This command shows the configured SNMP target addresses.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp targetaddr
```

Result

The configured SNMP target addresses are displayed.

8.6.1.10 show snmp targetparam**Description**

This command shows the configured SNMP target parameters.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp targetparam
```

Result

The configured SNMP target parameters are displayed.

8.6.1.11 **show snmp tcp**

Description

This command shows the configuration for SNMP via TCP.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp tcp
```

Result

The configuration for SNMP via TCP is displayed.

8.6.1.12 **show snmp user**

Description

This command shows the settings for the SNMP users.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp user
```

Result

The settings for the SNMP users are displayed.

8.6.1.13 show snmp viewtree

Description

This command shows the settings for the SNMP tree view.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show snmp viewtree
```

Result

The settings for the SNMP tree view are displayed.

8.6.2 Commands in the global configuration mode

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

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

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

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

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

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

8.6.2.1 snmpagent

Description

With this command, you enable the SNMP agent function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
snmpagent
```

Result

The SNMP agent function is enabled.

Further notes

You disable the SNMP agent function with the `no snmpagent` command.

8.6.2.2 no snmpagent

Description

With this command, you disable the SNMP agent function.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no snmpagent
```

Result

The SNMP agent function is disabled.

Further notes

You enable the SNMP agent function with the `snmpagent` command.

8.6.2.3 snmp agent version**Description**

With this command, you configure whether all SNMP queries or only SNMPv3 queries are processed.

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 agent version {v3only|all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
v3only	Only SNMPv3 queries are processed	-
all	All SNMP queries are processed	Default: all

Result

The setting is configured.

8.6.2.4 snmp access**Description**

With this command, you configure the access to 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 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	<ul style="list-style-type: none"> v1 v2c v3
Authentication	Selects the authentication method.	<ul style="list-style-type: none"> auth Enables MD5 or SHA as authentication method noauth No authentication priv Enables authentication and encryption
read	The data can be read. Keyword	<ul style="list-style-type: none"> ReadView none
write	The data can be read and written Keyword	<ul style="list-style-type: none"> WriteView none
notify	Changes can be sent as a tag. Keyword	<ul style="list-style-type: none"> NotifyView none
Storage Type	Specifies whether the settings remain following a restart.	<ul style="list-style-type: none"> 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.

Further notes

You delete the access to an SNMP group with the `no snmp access` command.

You display the configured SNMP groups with the `show snmp group` command.

You display the access configurations for SNMP groups with the `show snmp group access` command.

You display the configured SNMP tree views with the `show snmp viewtree` command.

8.6.2.5 no snmp access

Description

With this command, you delete the access to 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 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	<ul style="list-style-type: none">v1v2cv3
Authentication	Selects the authentication method.	<ul style="list-style-type: none">authnoauthpriv

Result

The access to an SNMP group is deleted.

Further notes

You configure the setting with the `snmp access` command.

You display the configured SNMP groups with the `show snmp group` command.

You display the access configurations for SNMP groups with the `show snmp group access` command.

You display the configured SNMP tree views with the `show snmp viewtree` command.

8.6.2.6 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.	<ul style="list-style-type: none">• : The settings are lost after a restart• : The settings are retained after a restart

If optional parameters are not specified when configuring a community, the default values apply.

Note**Community string**

For security reasons, do not use the standard values "public" or "private". Change the community strings following the initial installation.

The recommended minimum length for community strings is 6 characters.

Result

The settings are configured.

Additional notes

You delete the details of an SNMP community with the `no snmp community index` command.

You show the details of an SNMP community with the `show snmp community` command.

You show the status information of the SNMP communication with the `show snmp` command.

8.6.2.7 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.

8.6.2.8 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	<ul style="list-style-type: none">includedexcluded
-	specifies whether the settings remain following a restart:	<ul style="list-style-type: none">volatile (volatile): The default settings are used after a restartnonvolatile (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.

8.6.2.9 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.

8.6.2.10 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.	<ul style="list-style-type: none">v1v2cv3
Storage type	Specifies whether the settings remain following a restart.	<ul style="list-style-type: none">volatile : The settings are lost after a restartnonvolatile : The settings are retained after a restart.

If optional parameters are not specified when configuring a group, the default values apply.

Result

The details of the group are configured.

Further notes

You delete the details of an SNMP group with the `no snmp group` command.

You display the created SNMP groups with the `show snmp group` command.

You display the created SNMP users with the `show snmp user` command.

8.6.2.11 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.	<ul style="list-style-type: none">v1v2cv3

Result

The details of the group are deleted.

Further notes

You change the details of an SNMP group with the `snmp group` command.

You display the created SNMP groups with the `show snmp group` command.

You display the created SNMP users with the `show snmp user` command.

8.6.2.12 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	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">: The settings are lost after a restart: The settings are retained after a restart

Result

The details of the SNMP notifications are configured.

Further notes

You delete the details of an SNMP notification with the `no snmp notify` command.

You display the configured SNMP notifications with the `show snmp notif` command.

You display the configured SNMP target addresses with the `show snmp targetaddr` command.

8.6.2.13 no snmp notify

Description

With this command, you delete the details of the SNMP notifications.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no snmp notify <NotifyName>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
NotifyName	Name of the notification	max. 32 characters

Result

The details of the SNMP notifications are deleted.

Further notes

You change the details of an SNMP group with the `snmp notify` command.

You display the configured SNMP notifications with the `show snmp notif` command.

You display the configured SNMP target addresses with the `show snmp targetaddr` command.

8.6.2.14 snmp targetaddr

Description

With this command, you configure the SNMP target address.

Requirement

The SNMP target parameters are configured.

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
snmp targetaddr <TargetAddressName> param <ParamName> {ipv4<IPAddress>}
[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
TargetAddressName	Name of the target address	max. 32 characters
param	Keyword for the parameter name	-
ParamName	Name of the destination address or the designation of the parameter name	max. 32 characters
ipv4	Keyword for an IPv4 address	-
IPAddress	Value for an IPv4 unicast address	Enter a valid IPv4 unicast 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 target address for SNMP.	Specify the tag identifier.
none	No tag identifier	-
Storage Type	Specifies whether the settings remain following a restart.	<ul style="list-style-type: none"> 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 names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

If optional parameters are not specified when configuring, the following defaults apply:

Parameter	Default value
taglist	snmp
Storage Type	volatile
port	162

Result

The SNMP target address is configured.

Further notes

You delete the SNMP target address with the `no snmp targetaddr` command.

You display the SNMP target address with the `show snmp targetaddr` command.

You configure the SNMP target parameters with the `snmp targetparams` command.

You display the SNMP target parameters with the `show snmp targetparam` command.

8.6.2.15 no snmp targetaddr

Description

With this command, you delete the SNMP target address.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no snmp targetaddr <TargetAddressName>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
TargetAddressName	SNMP target address	max. 32 characters

Result

The SNMP target address is deleted.

Further notes

You change the SNMP target address with the `snmp targetaddr` command.

You display the SNMP target address with the `show snmp targetaddr` command.

8.6.2.16 snmp targetparams

Description

With this command, you configure 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:

```
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

Parameter	Description	Range of values / note
<code>security-model</code>	Specifies which SNMP version is used. With SNMPv3 a security level (authentication, encryption) can also be configured.	<ul style="list-style-type: none"> • SNMP version <ul style="list-style-type: none"> – v1 – v2c – v3 • Security level for v3 <ul style="list-style-type: none"> – auth Authentication enabled / no encryption enabled – noauth No authentication enabled, no encryption enabled – priv Authentication enabled / encryption enabled
<code>message-processing</code>	Specifies which SNMP version is used for processing the messages and whether the settings remain following a restart.	<ul style="list-style-type: none"> • SNMP version <ul style="list-style-type: none"> – v1 – v2c – v3 • Settings after the restart <ul style="list-style-type: none"> – : The settings are lost after a restart – : The settings are retained after a restart

Keywords need to be specified.

If optional parameters are not specified when configuring, the default values apply.

Result

The SNMP target parameters are configured.

Further notes

You delete the SNMP target parameters with the `no snmp targetparams` command.

You display settings of this function with the `show snmp targetparam` command.

You configure the user profile with the `snmp user` command.

You display the list of users with the `show snmp user` command.

8.6.2.17 no snmp targetparams

Description

With this command, you delete the SNMP target parameters.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no snmp targetparams <ParamName>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
ParamName	Name of the SNMP parameter	max. 32 characters

Result

The SNMP target parameters are deleted.

Further notes

You change the SNMP target parameters with the `snmp targetparams` command.

You display settings of this function with the `show targetparam` command.

8.6.2.18 snmp v1-v2 readonly

Description

With this command, you block write access for SNMPv1 and SNMPv2 PDUs.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
snmp v1-v2 readonly
```

Result

Write access for SNMPv1 and SNMPv2 PDUs is blocked.

Further notes

You release write access for SNMPv1 and SNMPv2 PDUs with the `no snmp v1-v2 readonly` command.

8.6.2.19 no snmp v1-v2 readonly**Description**

With this command, you enable write access for SNMPv1 and SNMPv2 PDUs.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no snmp v1-v2 readonly
```

Result

Write access for SNMPv1 and SNMPv2 PDUs is enabled.

Further notes

You block write access for SNMPv1 and SNMPv2 PDUs with the `snmp v1-v2 readonly` command.

8.6.2.20 snmp user

Description

With this command, you configure 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:

```
snmp user <UserName> [auth {md5|sha} <passwd> [priv DES <passwd>]]  
[{volatile|nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
UserName	Name of the user	max. 32 characters
auth	Specifies that authentication takes place and which algorithm is used	<ul style="list-style-type: none">md5 (Message Digest 5)sha (Secure Hash Algorithm) Default: No authentication
passwd	Password for authentication	max. 32 characters
priv DES	Specifies that there is encryption.	- Default: No encryption
passwd	Value for the password of the encryption	max. 32 characters
Storage type	Specifies whether the settings remain following a restart.	<ul style="list-style-type: none">volatile: The default settings are used after a restart.nonvolatile: The saved settings are used after a restart.

If optional parameters are not specified when configuring an SNMP user, the default values apply.

Result

The details of an SNMP user are configured.

Further notes

You delete the settings with the `no snmp user` command.

You display the configured users with the `show snmp user` command.

8.6.2.21 no snmp user

Description

With this command, you delete the details of an SNMP user.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no snmp user <UserName>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
UserName	Name of the user	max. 32 characters

Result

The details of an SNMP user are deleted.

Further notes

You change the settings with the `snmp user` command.

You display the configured users with the `show snmp user` command.

8.6.2.22 snmp view

Description

With this command, you configure an SNMP view.

Requirement

- An SNMP group has been created
- The access to the group is configured with `snmp access`
- You are in the Global Configuration mode.
The command prompt is:
`cli(config)#`

Syntax

Call up the command with the following parameters:

```
snmp view <ViewName> <OIDTree> [mask<OIDMask>] {included|excluded}  
      [{volatile|nonvolatile}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ViewName	Name of the SNMP view	max. 32 characters
OIDTree	Object ID	Path information of the MIB tree
mask	Keyword for the OID mask	-
OIDMask	Mask that filters access to the elements of the MIB tree	A series of "0" and "1" separated by dots in keeping with the path information of the MIB tree
View type	Specifies whether the filtered elements are used or excluded.	<ul style="list-style-type: none">• <code>included</code> (Default)• <code>excluded</code>
Storage type	Specifies whether the settings remain following a restart.	<ul style="list-style-type: none">• <code>volatile</code>: The settings are lost after a restart• <code>nonvolatile</code>: 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.

Further notes

You delete the view with the `no snmp view` command.

You display the configured SNMP tree views with the `show snmp viewtree` command.

You display the access rights of the SNMP groups with the `show snmp group access` command.

You configure the access rights of the SNMP groups with the `snmp access` command.

8.6.2.23 no snmp view

Description

With this command, you delete an SNMP view.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
no snmp view <ViewName> <OIDTree>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ViewName	Name of the view	max. 32 characters
OIDTree	Object ID	Path information of the MIB tree

Result

The SNMP view is deleted.

Further notes

You configure a view with the `snmp view` command.

You display the configured SNMP tree views with the `show snmp viewtree` command.

8.7 HTTP server

This section describes commands of the Hypertext Transfer Protocol (HTTP).

8.7.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.7.1.1 show ip http server status

Description

This command shows the status of the HTTP server.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show ip http server status
```

Result

The status of the HTTP server is displayed.

8.7.2 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.

8.7.2.1 ip http

Description

With this command, you enable HTTP 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:

```
ip http
```

As default the function is "enabled".

Result

HTTP 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.

You deactivate HTTP on the device with the `no ip http` command.

8.7.2.2 no ip http

Description

With this command, you disable the access via HTTP. You can only access the WBM of the device using HTTPS.

Requirement

You are in the 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.

Further notes

You can display the setting of this function and other information with the `show ip http server status` command.

You enable HTTP with the `ip http` command.

8.8 HTTPS server

This section describes commands of the Hypertext Transfer Protocol Secure (HTTPS).

8.8.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.8.1.1 `show ip http secure server status`

Description

This command shows the status of the HTTPS server.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show ip http secure server status
```

Result

The status, cipher suite and version of the HTTPS server are displayed.

8.8.1.2 `show ssl server-cert`

Description

This command shows the SSL server certificate.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show ssl server-cert
```

Result

The SSL server certificate is displayed.

8.8.2 Commands in the Global Configuration mode

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

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

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

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

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

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

8.8.2.1 ip http secure minimum tls-version

Description

With this command, you define which version of TLS is used at least.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
ip http secure minimum tls-version {v10 | v11 | v12}
```

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	Factory setting
v12	TLS as of version 1.2 can be used	-

Result

HTTP is enabled on the device.

Further notes

You can display the setting of this function and other information with the `show ip http secure server status` command.

8.8.2.2 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.

8.9 Proxy server

This section describes commands for the proxy server.

8.9.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.9.1.1 show proxyserver table

Description

This command shows the configuration of the proxy server.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
show proxyserver table
```

Result

The configuration is displayed.

8.9.2 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.

8.9.2.1 proxyserver

Description

With this command, you change to the PROXYSERVER 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:

```
proxyserver
```

Result

You are now in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv)#
```

Further notes

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

8.9.3 Commands in the PROXYSERVER configuration mode

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

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

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

8.9.3.1 **srv name**

Description

With this command, you create a proxy server entry. You assign a name and configure the parameters.

Requirement

You are in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv)#
```

Syntax

Call up the command with the following parameters:

```
srv name <name(128)> type {http|socks} port <num(0-65535)> auth {basic|ntlm|none}  
[addr <ip_addr|dns(255)>] [user <string(255)>] [pw <string(255)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Proxy server name	Specify a unique name for the proxy server. Maximum of 128 characters
type	Keyword the type of the proxy server	-
http	Proxy server only for access using HTTP	-
socks	Universal proxy server	-
port	Keyword for port	-
num	Port number	0 ... 65535 Specify the port on which the proxy service runs.
auth	Keyword for the authentication method	-
basic	Standard authentication. User name and password are sent unencrypted	-
ntlm	Authentication according to the NTML standard (Windows user logon)	-
none	No authentication	-
addr	Keyword for IPv4 address	-
ip_addr	IPv4 address	Enter the IPv4 address of the proxy server.
dns	DNS host name	Enter the DNS host name of the proxy server.
user	Keyword for a user name	-

Parameter	Description	Range of values / note
string	Name	Specify the user name for access to the proxy server. Maximum of 255 characters
pw	Keyword for a password	-
string	Password	Specify the password for access to the proxy server. Maximum of 255 characters

Result

The proxy server is configured.

Further notes

You delete this proxy server with the `no srv` command.

You change the parameters with the `srv name...` commands.

You display this setting and other information with the `show proxyserver table` command.

8.9.3.2 no srv

Description

With this command, you delete a specific proxy server or all proxy servers.

Requirement

- The corresponding proxy server name has been created and is not being used anywhere.
- You are in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv)#
```

Syntax

Call up the command with the following parameters:

```
no srv {name <string(128)> | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Keyword for proxy server name	-
string	Proxy server name	Specify a valid proxy server name. Maximum of 128 characters
all	Deletes all proxy servers	-

Result

The specified proxy server is deleted.

Further notes

You create the proxy server with the `srv name` command.

You display the available proxy server names with the `srv show-names` command.

8.9.3.3 `srv name addr`

Description

With this command, you change the address of the proxy server.

Requirement

- The proxy server name has been created.
- You are in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv)#
```

Syntax

Call up the command with the following parameters:

```
srv name <string(128)> addr <ip_addr|dns(50)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
<code>string</code>	Proxy server name	Specify the proxy server name. Maximum of 128 characters
<code>ip_addr</code>	IPv4 address	Enter the IPv4 address of the proxy server.
<code>dns</code>	DNS host name	Enter the DNS host name of the proxy server. Maximum of 50 characters

Result

The IPv4 address of the proxy server has been changed.

Further notes

You display the available proxy server names with the `srv show-names` command.

You create the proxy server with the `srv name` command.

8.9.3.4 `srv name auth`

Description

With this command, you change the authentication method of the proxy server.

Requirement

- The proxy server name has been created.
- You are in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv)#
```

Syntax

Call up the command with the following parameters:

```
srv name <string(128)> auth <none|basic|ntlm>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
string	Proxy server name	Specify the proxy server name. Maximum of 128 characters
none	No authentication	-
basic	Standard authentication The user name and password are sent unencrypted.	-
ntlm	Authentication according to the NTLM standard (Windows user logon)	-

Result

The authentication method has been changed.

Further notes

You display the available proxy server names with the `srv show-names` command.

You create the proxy server with the `srv name` command.

8.9.3.5 `srv name port`

Description

With this command, you change the port of the proxy server.

Requirement

- The proxy server name has been created.
- You are in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv) #
```

Syntax

Call up the command with the following parameters:

```
srv name <string(128)> port <number(0-65535)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
<code>string</code>	Proxy server name	Specify the proxy server name. Maximum of 128 characters
Port	Port number	Specify the port number on which the proxy service runs. 0 - 65535

Result

The port has been changed.

Further notes

You display the available proxy server names with the `srv show-names` command.

You create the proxy server with the `srv name` command.

8.9.3.6 `srv name pw`

Description

With this command, you change the password for access to the proxy server.

Requirement

- When selecting the authentication method `basic` is used.
- The proxy server name has been created.
- You are in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv)#
```

Syntax

Call up the command with the following parameters:

```
srv set name <string(255)> pw <name(255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
string	Proxy server name	Specify the proxy server name. Maximum of 128 characters
pw	Password	Specify the changed password for access to the proxy server. Maximum of 255 characters

Result

The password is changed.

Further notes

You display the available proxy server names with the `srv show-names` command.

You create the proxy server with the `srv name` command.

8.9.3.7 `srv name type`

Description

With this command, you change the type of the proxy server.

Requirement

- The proxy server name has been created.
- You are in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv)#
```

Syntax

Call up the command with the following parameters:

```
srv name <string(128)> type <http|socks>
```


The parameters have the following meaning:

Parameter	Description	Range of values / note
string	Proxy server name	Specify the proxy server name. Maximum of 128 characters
http	Universal proxy server	-
socks	Keyword for port	-

Result

The type of the proxy server has been changed.

Further notes

You display the available proxy server names with the `srv show-names` command.

You create the proxy server with the `srv name` command.

8.9.3.8 `srv name user`

Description

With this command, you change the user name for access to the proxy server.

Requirement

- When selecting the authentication method `basic` is used.
- The proxy server name has been created.
- You are in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv)#
```

Syntax

Call up the command with the following parameters:

```
srv name <string(128)> user <name(255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
string	Proxy server name	Specify the proxy server name. Maximum of 128 characters
name	User name	Specify the user name for access to the proxy server. Maximum of 255 characters.

Result

The user name has been changed.

Further notes

You display the available proxy server names with the `srv show-names` command.

You create the proxy server with the `srv name` command.

8.9.3.9 `srv show-names`

Description

With this command, you display the available proxy server names.

Requirement

You are in the PROXYSERVER configuration mode.

The command prompt is as follows:

```
cli(config-proxysrv)#
```

Syntax

Call the command without parameter assignment:

```
srv show-names
```

Result

The proxy server names are listed.

Further notes

You create a proxy server with the `srv name` command.

8.10 SMTP client

This section describes commands of the Simple Mail Transfer Protocol (SMTP).

8.10.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.10.1.1 `show 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.

8.10.1.2 `show events sender email`

Description

This command shows the configured e-mail sender 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 parameters:

```
show events sender email
```

Result

The configured e-mail sender address is displayed.

8.10.1.3 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.

8.10.2 Commands in the Events configuration mode

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

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

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

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

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

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

8.10.2.1 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.

8.10.2.2 smtp-server

Description

With this command, you change to the SMTP server configuration mode. There are two options to do this:

- Create new

If there is no entry with this address yet, a new SMTP server entry is created and a switch to the SMTP server configuration mode takes place. In this mode, you configure the other settings of the SMTP server.

- Change configuration

If the entry already exists, a switch to the SMTP configuration mode takes place. In this mode, you can change the settings of the SMTP server.

Requirement

You are in the EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
smtp-server { ipv4 <ucast_addr> | fqdn-name <FQDN> }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ipv4	Keyword for an IPv4 address	-
ucast_addr	IPv4 address of the SMTP server	Enter a valid IPv4 unicast address.
fqdn-name	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters

For information on addresses and interfaces, refer to the section "Addresses and interface names (Page 41)".

Result

An entry for the SMTP server is created.

You are now in the SMTP server configuration mode.

The command prompt is as follows:

```
cli(events-smtp-server)#
```

Further notes

You delete the SMTP server entry with the `no smtp-server` command.

You display the configuration of the SMTP server with the `show events smtp-server` command.

8.10.2.3 no smtp-server

Description

With this command, you delete an SMTP server entry.

Requirement

You are in the EVENTS configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
no smtp-server { ipv4 <ucast_addr> | fqdn-name <FQDN> }>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ipv4	Keyword for an IPv4 address	-
ucast_addr	IPv4 address of the SMTP server	Enter a valid IPv4 unicast address.
fqdn-name	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters

For information on addresses and interfaces, refer to the section "Addresses and interface names (Page 41)".

Result

The SMTP server entry is deleted.

Further notes

You configure an SMTP server entry with the `smtp-server` command.

8.10.3 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.

8.10.3.1 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.
password	Keyword for a password	-
password	Password	Enter the password used for authentication on the SMTP server.

Result

The user data is configured.

Further notes

You delete the user data with the `no auth username` command.

You display this setting with the `show events smtp-server` command.

8.10.3.2 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.

8.10.3.3 port

Description

With this command, you configure the port via which the SMTP server can be reached.

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:

```
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

Result

The SMTP port is configured.

Further notes

You display this setting with the `show events smtp-server` command.

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

8.10.3.4 no port

Description

With this command, you reset the SMTP port to the default.
The default value is 25.

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 port
```

Result

The SMTP port is reset to the default value.

Further notes

You configure the setting with the `port` command.
You display this setting with the `show events smtp-server` command.

8.10.3.5 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.

8.10.3.6 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.

8.10.3.7 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.

8.10.3.8 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.

8.10.3.9 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.

8.10.3.10 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.

8.10.3.11 test

Description

You send a test e-mail to the configured recipients with this command.

Requirement

You are in the SMTP server configuration mode.

The command prompt is as follows:

```
cli (events-smtp-server) #
```

Syntax

Call the command without parameters:

```
test
```

Result

A test e-mail was sent to the configured recipients. The test result is shown in the console output. If sending was not successful, the message contains possible causes.

8.11 SSH server

This section describes commands of the Secure Shell (SSH) Server.

8.11.1 The "show" commands

This section describes commands with which you display various settings.

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

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

8.11.1.1 show ip ssh

Description

This command shows the settings of the SSH server.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show ip ssh
```

Result

The settings for the SSH server are displayed.

8.11.2 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.

8.11.2.1 ssh-server

Description

With this command, you enable the SSH protocol on the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
ssh-server
```

As default the function is "enabled".

Result

The SSH protocol is enabled on the device.

Further notes

You disable the SSH protocol with the `no ssh-server` command.

8.11.2.2 no ssh-server

Description

With this command, you disable the SSH protocol on the device.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameters:

```
no ssh-server
```

Result

The SSH protocol is disabled on the device.

Further notes

You enable the SSH protocol with the `ssh-server` command.

Load control

This part contains the sections describing the functions for controlling and balancing network load.

9.1 Flow control

The flow control function monitors the incoming data traffic of a port. If there is overload ("Congestion", "Overflow") it sends a signal to the connection partner. If the flow control function receives a signal at the sending end, it stops the data transmission to avoid loss of data.

This section describes commands of the flow control function.

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 flow-control

Description

This command shows the settings of the flow control function.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call up the command with the following parameters:

```
show flow-control [interface <interface-type><interface-id>]
```

The parameters have the following meaning:

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

If you do not select any parameters from the parameter list, the information for the router will be displayed.

Result

The settings of the flow control function are displayed.

9.1.2 Commands in the interface configuration mode

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

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

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

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

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

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

9.1.2.1 flowcontrol

Description

The flow control function monitors a connection at the receiving end to make sure that not more data is received than can be processed. If flow control detects a threat of data overflow, the partner at the sending end is sent a signal to stop transmitting.

With this command, you configure the flow control function for an interface.

Requirement

You are in the Interface configuration mode.

The command prompt is as follows:

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

Syntax

Call up the command with the following parameters:

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

The parameters have the following meaning:

Parameter	Description	Range of values / note
on	Enables the function	You can only enable or disable flow control when the "Auto negotiation" function is turned off. Afterwards you can enable "Auto negotiation" again.
off	Disables the function	-

Result

The settings for the flow control function are configured.

Further notes

You can display the status of this function with the `show flow-control` command.

You disable "Auto negotiation" with the `no negotiation` command.

You enable "Auto negotiation" with the `negotiation` command.

9.2 Dynamic MAC aging

The section describes commands with which the aging of dynamically learned entries is configured in a MAC address list.

9.2.1 The "show" commands

This section describes commands with which you display various settings.

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

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

9.2.1.1 show 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.

9.2.1.2 show mac-address-table aging-status

Description

This command shows whether or not MAC aging is enabled.

Requirement

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

The command prompt is as follows:

```
cli> OR cli#
```

Syntax

Call the command without parameters:

```
show mac-address-table aging-status
```

Result

The status of the MAC aging is displayed.

9.2.2 Commands in the global configuration mode

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

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

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

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

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

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

9.2.2.1 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.

9.2.2.2 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.

9.2.2.3 mac-address-table aging-time

Description

With this command, you configure the aging of a dynamically learned entry in the MAC address list.

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:

```
mac-address-table aging-time <seconds(15-630)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
seconds	Life of the entry in seconds	15 ... 630 Default: 300 Enter the period of time in seconds in steps of 15. When you input the Aging Time, note that the WBM rounds to correct values. If you enter a value that cannot be divided by 15, the value is automatically rounded down.

Result

The value of the aging of a dynamically learned entry is configured.

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.

Layer 3 functions

10.1 VRRPv3 (IPv4)

This section describes the commands relevant for working with routing with VRRPv3. Version 3 of VRRP is based on version 2.

Note

- Enable routing to be able to use VRRPv3.
 - The commands can only be used in connection with the VLAN interfaces.
-

VRRP and DHCP server

If you want to operate a DHCP server on the devices of a VRRP group, the DHCP server must be configured on the master router. Backup routers do not react to DHCP queries. Make sure that the master router is statically configured and that after a failure, becomes the master of the VRRP group again.

10.1.1 clear vrrp3 statistics

Description

With this command, you reset the counters to zero.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
clear vrrp3 statistics
```

Result

The counters are reset.

Further notes

You display the table with the commands `show vrrp3 interface` and `show vrrp3 interface - vrid`.

10.1.2 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.

10.1.2.1 show vrrp3

Description

This command shows the settings of a virtual router.

Requirement

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 vrrp3 [interface vlan <vlan-id(1-4094)> <VrId(1-255)>]  
[{{brief|detail|statistics}}]
```

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
VrId	ID of the virtual router	1 ... 255
brief	shows brief information on VRRP	-
detail	shows detailed information on VRRP.	-
statistics	shows the statistics of the VRRP protocol	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The settings of the virtual router are displayed.

10.1.2.2 show vrrp3 interface

Description

This command shows the settings of VRRP3 for the 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 vrrp3 interface [vlan <vlan-id(1-4094)>] [{brief|detail|statistics}]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vlan	Keyword for a VLAN connection	-
VlanId	Number of the addressed VLAN	1 ... 4094
brief	shows brief information on VRRP	-
detail	shows detailed information on VRRP.	-
statistics	shows the statistics of the VRRP protocol	-

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The settings for the interface are displayed.

10.1.2.3 show vrrp3 track

Description

With this command, you display the configured interface tracking.

Requirement

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 vrrp3 track
```

Result

The configured interface tracking is displayed.

10.1.3 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.

10.1.3.1 router vrrp3

Description

With this command, you enable routing with VRRPv3 and change to the VRRP3 Router 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:

```
router vrrp3
```

Result

Routing with VRRP3 is enabled.

You are now in the VRRP3 Router configuration mode.

The command prompt is as follows:

```
cli (config-vrrp-v3) #
```

Further notes

You disable routing with VRRP with the `no router vrrp3` command.

10.1.3.2 no router vrrp3

Description

With this command, you disable routing with VRRPv3.

Note

This command is available only with layer 3.

Requirement

You are in the Global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call the command without parameter assignment:

```
no router vrrp3
```

Result

Routing with VRRPv3 is disabled.

Further notes

You enable routing with VRRPv3 with the `router vrrp3` command.

10.1.4 Commands in the VRRP3 Router configuration mode

This section describes commands that you can call up in the VRRP3 Router configuration mode.

In the Global configuration mode, enter the `router vrrp3` command to change to this mode.

- If you exit the VRRP3 Router configuration mode with the `exit` command, you return to the Global configuration mode.
- If you exit the VRRP3 Router 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 VRRP3 Router configuration mode.

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

10.1.4.1 interface

Description

With this command, you decide the interface for which you want to assign parameters in the VRRP3 Router configuration mode.

There you can edit the settings for a VRRP3 interface. You select the VRRP3 interface with the parameters of this command.

Requirement

You are in the VRRP3 Router configuration mode.

The command prompt is as follows:

```
cli (config-vrrp-v3) #
```


Syntax

Call up the command with the following parameters:

```
interface vlan <vlan-id(1-4094)>
```

The parameters have the following meaning:

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

You are now in the VRRP3 Interface configuration mode.

The command prompt is as follows:

```
cli (config-vrrp-v3-if-$$$) #
```

Further notes

You exit the VRRP3 Interface configuration mode with the `end` or `exit` command.

You delete a VRRP3 interface with the `no interface` command.

You display the status and the configuration of the VRRP3 interfaces with the `show vrrp3` or `show vrrp3 interface` command.

10.1.4.2 no interface

Description

With this command, you delete a VRRP3 interface.

Requirement

You are in the VRRP3 Router configuration mode.

The command prompt is as follows:

```
cli (config-vrrp-v3) #
```

Syntax

Call up the command with the following parameters:

```
no interface vlan <vlan-id(1-4094)>
```

The parameters have the following meaning:

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

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The VRRP3 interface has been deleted.

Further notes

You configure a VRRP3 interface with the `interface` command.

You display the status and the configuration of the VRRP3 interface with the `show vrrp3` or `show vrrp3 interface` command.

10.1.4.3 track interface

Description

With this command, you configure the tracking of interfaces.

When the link of one or more tracked interfaces changes from "up" to "down", the priority of the assigned VRRP interface is reduced. When the link of the interface changes back from "down" to "up", the original priority of the VRRP interface is restored.

Requirement

You are in the VRRP Router configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3)#
```

Syntax

Call up the command with the following parameters:

```
track <group-index> interface { {vlan <vlan-id (1-4094)> | {ppp | usb} <intf-num(0-4)>} | <interface-type> <interface-id> }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
group-index	ID of the interface tracking	-
vlan	Keyword for a VLAN connection	-

Parameter	Description	Range of values / note
vlan-id	Number of the addressed VLAN	1 ... 4094
ppp	WAN interface EGPRS, GPRS, UMTS	-
usb	WAN interface LTE	-
intf-num	Number of the addressed interface	0 ... 4
interface-type	Type of interface	Specify a valid interface.
interface-id	Module no. and port no. of the interface	

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The selected interface is monitored.

Further notes

You delete an interface tracking with the `no interface interface` command.

You display the configured interface tracking with the `show vrrp track` command.

You assign a VRRP interface to an interface tracking with the `vrrp track decrement` command.

You configure the value by which the priority is reduced with the command `vrrp track decrement`.

With the `track links` command you configure how many of the monitored interfaces need to change their status before the priority of the assigned VRRP interface is changed.

10.1.4.4 no track interface

Description

With this command, you delete the tracking of interfaces.

Requirement

You are in the VRRP Router configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3)#
```

Syntax

Call up the command with the following parameters:

```
no track <group-index> interface { {vlan <vlan-id (1-4094)> | {ppp | usb} <intf-  
num(0-4)>}} | <interface-type> <interface-id> }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
group-index	ID of the interface tracking	-
vlan	Keyword for a VLAN connection	-
vlan-id	Number of the addressed VLAN	1 ... 4094
ppp	WAN interface EGPRS, GPRS, UMTS	-
usb	WAN interface LTE	-
intf-num	Number of the addressed interface	0 ... 4
interface-type	Type of interface	Specify 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 41)".

Result

Interface tracking is deleted.

Further notes

You configure an interface tracking with the `track interface` command.

You display the configured interface tracking with the `show vrrp track` command.

10.1.4.5 track links

Description

With this command you define how many tracked interfaces need to change to the "down" status, before the priority of the assigned VRRP interface is changed.

Requirement

You are in the VRRP Router configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3)#
```

Syntax

Call up the command with the following parameters:

```
track <group-index> links <links-to-track(1-255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
group-index	ID of the interface tracking	-
links-to-track	Number of interfaces	1 ... 255

Result

The number of tracked interfaces is defined.

Further notes

You delete the configuration with the `no track links` command.

You configure the tracking of interfaces with the `track interface` command.

You display the configured number of tracked interfaces with the `show vrrp track` command.

10.1.4.6 no track links

Description

With this command, you delete the the number of tracked interfaces.

Requirement

You are in the VRRP Router configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3)#
```

Syntax

Call up the command with the following parameters:

```
no track <group-index> links
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
group-index	ID of the interface tracking	-

Result

The number of tracked interfaces is deleted.

Further notes

You configure the number of tracked interfaces with the `track links` command.

You display the configured number of tracked interfaces with the `show vrrp track` command.

10.1.4.7 vrrp vrid-track

Description

With this command, you enable VRID tracking.

When enabled, all VRRP instances are monitored. If the status of a VRRP instance changes to "Initialize", the priority of all VRRP instances is reduced to the value "1".

If the status of a VRRP instance changes, the original priority of all VRRP instances is restored.

Requirement

You are in the VRRP Router configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3) #
```

Syntax

Call the command without parameter assignment:

```
vrrp vrid-track
```

Result

VRID tracking is enabled.

Further notes

You disable VRID tracking with the `no vrrp vrid-track` command.

You display configured VRID trackings with the command `show vrrp3` or `show vrrp3 interface` with the parameter `detail`.

10.1.4.8 no vrrp vrid-track

Description

With this command, you disable VRID tracking.

Requirement

You are in the VRRP Router configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3)#
```

Syntax

Call the command without parameter assignment:

```
no vrrp vrid-track
```

Result

VRID tracking is disabled.

Further notes

You enable VRID tracking with the `vrrp vrid-track` command.

You display configured VRID trackings with the command `show vrrp3` or `show vrrp3 interface` with the parameter `detail`.

10.1.5 Commands in the Interface Configuration mode

This section describes the commands relevant for working with routing with VRRPv3. Version 3 of VRRP is based on version 2.

Note

- Enable routing to be able to use VRRPv3.
 - The commands can only be used in connection with the VLAN interfaces.
-

VRRP and DHCP server

If you want to operate a DHCP server on the devices of a VRRP group, the DHCP server must be configured on the master router. Backup routers do not react to DHCP queries. Make sure that the master router is statically configured and that after a failure, becomes the master of the VRRP group again.

10.1.5.1 vrrp associated-ip

Description

With this command, you specify which IP addresses the virtual router monitors.

Requirement

You are in the VRRP3 Interface configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
vrrp <vrid(1-255)> associated-ip ipv4 <ip_addr>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vrid	ID of the virtual router	1 ... 255
ipv4	Keyword for IPv4 address	-
ip_addr	IPv4 address	Enter a valid IPv4 address.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The IP addresses are specified.

Further notes

You configure a VRRP3 interface with the `interface` command.

You remove an IP address with the `no vrrp associated-ip` command.

You display the IP addresses with the `show vrrp3` command.

10.1.5.2 no vrrp associated-ip

Description

With this command, you remove an IP address from the virtual router.

Requirement

You are in the VRRP3 Interface configuration mode.

The command prompt is as follows:

```
cli (config-vrrp-v3-if-$$$) #
```

Syntax

Call up the command with the following parameters:

```
no vrrp <vrid(1-255)> associated-ip ipv4 <ip_addr>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vrid	ID of the virtual router	1 ... 255
ipv4	Keyword for IPv4 address	-
ip_addr	IPv4 address	Enter a valid IPv4 address.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The IP address is removed from the virtual router.

Further notes

You configure a VRRP3 interface with the `interface` command.

You display the IP addresses with the `show vrrp` command.

10.1.5.3 vrrp primary-ip

Description

With this command, you specify the primary IP address specified with the VRRP3 packets as the source address.

Requirement

You are in the VRRP3 Interface configuration mode.

The command prompt is as follows:

```
cli (config-vrrp-v3-if-$$$) #
```

Syntax

Call up the command with the following parameters:

```
vrrp <vrid(1-255)> primary-ip ipv4 <ip_addr>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vrid	ID of the virtual router	1 ... 255
ipv4	Keyword for IPv4 address	-
ip_addr	IPv4 address	Enter a valid IPv4 address.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The primary IP address is specified.

Further notes

You configure a VRRP3 interface with the `interface` command.

You remove the primary IP address with the `no vrrp primary-ip` command.

You show the configuration of the virtual router with the `show vrrp3` command.

10.1.5.4 no vrrp primary-ip

Description

With this command, you remove a primary IP address from the virtual router.

Requirement

You are in the VRRP3 Interface configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no vrrp <vrid(1-255)> primary-ip ipv4 <ip_addr>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
<code>vrid</code>	ID of the virtual router	1 ... 255
<code>ipv4</code>	Keyword for IPv4 address	-
<code>ip_addr</code>	IPv4 address	Enter a valid IPv4 address.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The primary IP address is removed from the virtual router.

Further notes

You configure a VRRP3 interface with the `interface` command.

You assign a primary IP address to a virtual router with the `vrrp primary-ip` command.

You display the IP addresses with the `show vrrp3` command.

10.1.5.5 vrrp priority

Description

With this command, you specify the priority of the virtual router. The current master router is automatically given 255. All other priorities can be distributed freely among the VRRP routers. The higher the priority, the earlier the VRRP router becomes "Master".

Requirement

- An IP address is assigned to the virtual router.
- You are in the VRRP3 Interface configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
vrrp <vrid(1-255)> priority <priority(1-254)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vrid	ID of the virtual router	1 ... 255
priority	Priority of the virtual router	1 ... 254 Default: 1

Result

The priority of the virtual router is specified.

Further notes

You configure a VRRP3 interface with the `interface` command.

You reset the priority to the default with the `no vrrp priority` command.

You assign IP addresses to a virtual router with the `vrrp associated-ip` command.

You display the priority with the `show vrrp3` command.

10.1.5.6 no vrrp priority

Description

With this command, you reset the router priority back to the default value.

Requirement

- An IP address is assigned to the virtual router.
- You are in the VRRP3 Interface configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no vrrp <vrid(1-255)> priority
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vrid	ID of the virtual router	1 ... 255

Result

The priority is reset.

Further notes

You configure a VRRP3 interface with the `interface` command.

You create the priority with the `vrrp priority` command.

You assign IP addresses to a virtual router with the `vrrp associated-ip` command.

You display the priority with the `show vrrp3` command.

10.1.5.7 vrrp timer

Description

With this command, you specify the time interval after which a virtual router with the "Master" status sends an advertisement packet again.

Requirement

- An IP address is assigned to the virtual router.
- You are in the VRRP3 Interface configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
vrrp <vrid(1-255)> timer <interval(10-4095)centiseconds>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vrid	ID of the virtual router	1 ... 255
interval	Time interval in hundredths of seconds	10 ... 4095 Default: 10

Result

The time interval is specified.

Further notes

You configure a VRRP3 interface with the `interface` command.

You enable routing with VRRP3 with the `router vrrp3` command.

You reset the time interval to the default with the `no vrrp timer` command.

You assign IP addresses to a virtual router with the `vrrp associated-ip` command.

You show the interval with the `show vrrp3` command.

10.1.5.8 no vrrp timer

Description

With this command, you reset the time interval to the default value.

Requirement

- Routing with VRRP3 is enabled.
- An IP address is assigned to the virtual router.
- You are in the VRRP3 Interface configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no vrrp <vrid(1-255)> timer <interval(50-4095)centiseconds>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vrid	ID of the virtual router	1 ... 255
interval	Time interval in hundredths of seconds	50 ... 4095

Result

The time interval is reset.

Further notes

You configure a VRRP3 interface with the `interface` command.

You enable routing with VRRP3 with the `router vrrp3` command.

You configure the interval with the `vrrp timer` command.

You assign IP addresses to a virtual router with the `vrrp associated-ip` command.

You show the interval with the `show vrrp3` command.

10.1.5.9 vrrp track decrement

Description

You can use this command to assign interface monitoring to a VRRP interface and set the value by which the priority is reduced.

Requirement

You are in the VRRP Interface configuration mode.

The command prompt is as follows:

```
cli (config-vrrp-v3-if-$$$) #
```

Syntax

Call up the command with the following parameters:

```
vrrp <vrid(1-255)> track <group-index> decrement <integer(1-254)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vrid	ID of the virtual router	1 ... 255
group-index	ID of the interface tracking	-
integer	Value by which priority of the VRRP interface will be reduced	1 ... 254

Result

A VRRP interface is assigned to interface tracking. The value by which the priority will be reduced is defined.

Further notes

You delete the configuration with the `no vrrp track` command.

You display the assignment and value of the priority with the command `show vrrp3` or `show vrrp3 interface` with the parameter `detail`.

You configure the tracking of interfaces with the `track interface` command.

10.1.5.10 no vrrp track

Description

With this command, you delete the assignment of interface tracking to a VRRP interface and the value by which the priority is reduced.

Requirement

You are in the VRRP Interface configuration mode.

The command prompt is as follows:

```
cli(config-vrrp-v3-if-$$$)#
```

Syntax

Call up the command with the following parameters:

```
no vrrp <vrid(1-255)> track
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
vrid	ID of the virtual router	1 ... 255

Result

The assignment and the value by which the priority will be reduced is defined are deleted.

Further notes

You assign a VRRP interface to an interface tracking and configure the value by which the priority is reduced with the command `vrrp track decrement`.

You display the assignment and value of the priority with the command `show vrrp3` or `show vrrp3 interface` with the parameter `detail`.

10.2 NAT

This section describes commands relevant for NAT / NAPT.

10.2.1 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.

10.2.1.1 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.

10.2.1.2 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.

10.2.1.3 show firewallnat netmap

Description

This command shows the configured NETMAP 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 netmap
```

Result

The configured NETMAP rules are displayed.

10.2.1.4 show firewallnat src-nat

Description

This command shows the configured source NAT 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 src-nat
```

Result

The configured source NAT rules are displayed.

10.2.2 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.

10.2.2.1 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.

10.2.3 Commands in the FIREWALL NAT configuration mode

10.2.3.1 Introductory sentence for the FirewallNAT 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.

Available interfaces

As the source and destination interfaces, the following interfaces are available:

Interface		masquerading-nat napt	netmap src-nat	
VLAN	VLANs with configured subnet	x	x	vlan num
PPP	WAN interface	x	x	ppp 2
IPsec VPN	All IPsec VPN connections	-	x	ipseccall
	Specific IPsec VPN connection	-	x	ipsec num
OpenVPN	All OpenVPN connections	-	x	openvpnall
	Specific OpenVPN connection	-	x	openvpn num
SINEMA RC	Connection to SINEMA RC Server	-	x	sinemarcall

x: available

- : not available

10.2.3.2 ipsec connection show-idx

Description

With this command, you show the numbers of the configured IPsec VPN connections.

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:

```
ipsec connection show-idx
```

Result

The entries are listed.

10.2.3.3 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.

10.2.3.4 masquerading

Description

With this command, you enable the rules for IP masquerading on the interface.

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:

```
masquerading {vlan|ppp|usb} <num(0-4094)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vlan	VLAN interface	-
ppp	WAN interface	-
usb		-
num	Number of the addressed VLAN	Specify a valid interface index. 0 ... 4094

For information on identifiers of interfaces, refer to the section "Commands in the FIREWALL NAT configuration mode (Page 412)".

Result

The rules for IP masquerading are enabled on the specified interface.

Further notes

You disable IP masquerading with the `no masquerading` command.

You display the setting with the `show masquerading` command.

10.2.3.5 no masquerading

Description

With this command, you disable the rules for IP masquerading on the interface.

Requirement

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 masquerading {{vlan|ppp|usb} <num(0-4094)>|all-int|show-int}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
vlan	VLAN interface	-
ppp	WAN interface	-
usb		-
num	Number of the addressed VLAN	Specify a valid interface index. 0 ... 4094
all-int	Disables the rules for IP masquerading on all interfaces.	-
show-int	Lists the available interfaces.	-

For information on identifiers of interfaces, refer to the section "Commands in the FIREWALL NAT configuration mode (Page 412)".

Result

The rules for IP masquerading are disabled on the relevant interface.

Further notes

You enable IP masquerading with the `masquerading-nat` command.

10.2.3.6 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.

10.2.3.7 napt type ipv4

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
- 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:

```
napl srcint <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	-
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.
transip	Keyword for the IPv4 address of the node to which this frame will be forwarded	-
ip	IPv4 address	Enter a valid IPv4 address.
dstip	Keyword for the destination IP address	-
ip	IPv4 address	Enter a valid IPv4 address.

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL NAT configuration mode (Page 412)".

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), port 500 (ISAKMP), port 4500 (IPsec Nat-T).

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.

10.2.3.8 no napt**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 <vlan> <num(0-4094)> idx <num(1-200)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
srcint	Keyword for the source interface	-
VLAN	VLAN interface	-

Parameter	Description	Range of values / note
num	Number of the addressed VLAN	0 ... 4094
idx	Number corresponding to a specific NAPT rule. Specify a valid number.	0 ...200

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.

10.2.3.9 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.

10.2.3.10 netmap destination srcint

Description

With this command, you create the NETMAP rule for the address translation of the destination IP address.

Requirement

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:

```
netmap destination srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall>
[<num(0-4094)>] dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>]
type ipv4 srcip <*>|subnet> dstip <subnet> transip <subnet> [auto-fwrules]
[auto-bidirectionalrule]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
srcint	Keyword for the source interface	-
vlan	VLAN interface	-
ipsec ipsecall sinemarcall openvpn openvpnall	Access via VPN tunnel partners that can be reached via SINEMA RC, via all VPN connections (all) or via a certain VPN connection <num>.	-
num	Number of the VLAN interface or the VPN connection	0 ... 4094
dstint	Keyword for the destination interface	-
vlan	VLAN interface	-
ipsec ipsecall sinemarcall openvpn openvpnall	Access to the VPN tunnel partners that can be reached via SINEMA RC, via all VPN connections (all) or via a specific VPN connection <num>.	-
num	Number of the VLAN interface or the VPN connection	0 ... 4094
srcip	Keyword for the source subnet (sender).	-

Parameter	Description	Range of values / note
*	All IP addresses	-
subnet	The subnet can also be a single PC or another subset of the subnet.	Specify the subnet in the CIDR notation.
dstip	Keyword for the destination subnet (recipient)	-
subnet	The subnet can also be a single PC or another subset of the subnet.	Specify the subnet in the CIDR notation.
transip	Keyword for the subnet with which the destination subnet is replaced.	-
subnet	The subnet can also be a single PC or another subset of the subnet.	Specify the subnet in the CIDR notation.
auto-fwrules	The NETMAP rule for the opposite direction is created automatically.	-
auto-bidirectionalrule	The IPv4 firewall rules are created automatically.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL NAT configuration mode (Page 412)".

Note

Firewall rule with destination NAT

Address translation with NAT was already performed before the firewall; the translated addresses are therefore used in the firewall.

ipv4rule

- `srcip <ip|subnet|range>:` Input from "`srcip <*>|subnet>`"
- `dstip <ip|subnet|range>:` Input from "`transip <subnet>`"

Result

The NETMAP rule for the address translation of the destination IP address has been created. During creation, an entry with a unique number (index) is created.

Further notes

You delete a NETMAP rule with the `no netmap` command.

You delete all NETMAP rules with the `no netmap all` command.

You display the numbers of the NETMAP rules with the `netmap show-idx` command.

You display the NETMAP rule with the `show firewallnat netmap-nat` command.

You display the IPv4 firewall rules with the `show firewall ip-rules ipv4` command.

10.2.3.11 netmap show-idx

Description

With this command, you show the numbers of the configured NETMAP 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:

```
netmap show-idx
```

Result

The numbers are listed.

Further notes

You delete a NETMAP rule with the `no netmap` command.

You delete all NETMAP rules with the `no netmap all` command.

You create a NETMAP rule with the commands `netmap source type ipv4` and `netmap destination type ipv4`.

10.2.3.12 netmap source type ipv4

Description

With this command, you create the NETMAP rule for the address translation of the source IP address.

Requirement

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:

```
netmap source srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>]
dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>]
type ipv4 srcip <subnet> transip <subnet> dstip <*<subnet>>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
srcint	Keyword for the source interface	-
vlan	VLAN interface	-
ipsec ipsecall sinemarcall openvpn openvpnall	Access via VPN tunnel partners that can be reached via SINEMA RC, via all VPN connections (all) or via a specific VPN connection <num> .	-
num	Number of the interface or the VPN connection	0 ... 4094
dstint	Keyword for the destination interface	-
vlan	VLAN interface	
ipsec ipsecall sinemarcipsec ipsecall sinemarcall openvpn openvpnall	Access to the VPN tunnel partners that can be reached via SINEMA RC, via all VPN connections (all) or via a specific VPN connection <num>.	-
num	Number of the interface or the VPN connection	0 ... 4094
srcip	Keyword for the source subnet (sender).	-
subnet	The subnet can also be a single PC or another subset of the subnet.	Specify the subnet in the CIDR notation.
transip	Keyword for the subnet with which the source subnet is replaced.	-

Parameter	Description	Range of values / note
subnet	The subnet can also be a single PC or another subset of the subnet.	Specify the subnet in the CIDR notation.
srcip	Keyword for the source subnet (sender).	-
*	All IP addresses	-
subnet	The subnet can also be a single PC or another subset of the subnet.	Specify the subnet in the CIDR notation.
auto-fwrules	The NETMAP rule for the opposite direction is created automatically.	-
auto-bidirectionalrule	The IPv4 firewall rules are created automatically.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL NAT configuration mode (Page 412)".

Note

Firewall rule with source NAT

Address translation with source NAT was only performed after the firewall; the non-translated addresses are therefore used.

ipv4rule

- srcip <ip|subnet|range>: Input from "srcip <*>|subnet>"
- dstip <ip|subnet|range>: Input from "dstip <*>|subnet>"

Result

The NETMAP rule for the address translation of the source IP address has been created. During creation, an entry with a unique number (index) is created.

Further notes

You delete a NETMAP rule with the `no netmap` command.

You delete all NETMAP rules with the `no netmap all` command.

You display the numbers of the NETMAP rules with the `netmap show-idx` command.

You display the NETMAP rule with the `show firewallnat netmap` command.

You display the IPv4 firewall rules with the `show firewall ip-rules ipv4` command.

10.2.3.13 no netmap srcint

Description

With this command, you delete a specific NETMAP rule.

Requirement

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 netmap srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>]
dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<integer(0-4094)>] idx
<integer(1-200)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
srcint	Keyword for the source interface	-
vlan	Type or speed of the interface	-
ipsec ipsecall sinemarcall openvpn openvpnall	Access via VPN tunnel partners that can be reached via SINEMA RC via all VPN connections (all) or via a certain VPN connection <integer> .	-
num	Number of the addressed interface	0 ... 4094
dstint	Keyword for the destination interface	-
vlan	Type or speed of the interface	-
ipsec ipsecall sinemarcall openvpn openvpnall	Access via VPN tunnel partners that can be reached via SINEMA RC via all VPN connections (all) or via a certain VPN connection <integer> .	-
integer	Number of the addressed interface	0 ... 4094
idx	Keyword for the number of the NETMAP rule	-
integer	Number corresponding to a specific NETMAP rule.	Specify a valid number. 0 ... 200

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL NAT configuration mode (Page 412)".

Result

The specified NETMAP rule is deleted.

Further notes

You display the numbers of the NETMAP rules with the `netmap show-idx` command.

You delete all NETMAP rules with the `no netmap all` command.

You create a NETMAP rule with the commands `netmap source type ipv4` and `netmap destination type ipv4`.

10.2.3.14 no netmap all

Description

With this command, you delete all NETMAP 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 netmap all
```

Result

All NETMAP rules are deleted.

Further notes

You create a NETMAP rule with the commands `netmap source type ipv4` and `netmap destination type ipv4`.

10.2.3.15 src-nat show-idx

Description

With this command, you show the numbers of the configured source NAT 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:

```
src-nat show-idx
```

Result

The numbers are listed.

Further notes

You delete a source NAT rule with the `no src-nat.` command

You delete all source NAT rules with the `no src-nat all` command.

You create a source NAT rule with the `src-nat type ipv4` command.

10.2.3.16 src-nat type ipv4**Description**

With this command, you create a rule for source NAT.

Requirement

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:

```
src-nat srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<integer(0-4094)>] dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<integer(0-4094)>] type ipv4 srcip <ip|subnet> dstip <ip|subnet> [transip <ip>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
srcint	Keyword for the source interface	-
vlan	VLAN interface	-
ipsec ipsecall sinemarcall openvpn openvpnall	Access via VPN tunnel partners that can be reached via SINEMA RC via all VPN connections (all) or via a certain VPN connection <integer> .	-
integer	Number of the interface or the VPN connection	0 ... 4094
dstint	Keyword for the destination interface	-
vlan	VLAN interface	-
ipsec ipsecall sinemarcall openvpn openvpnall	Access to the VPN tunnel partners that can be reached via SINEMA RC via all VPN connections (all) or via a certain VPN connection <integer> .	-
integer	Number of the interface or the VPN connection	0 ... 4094

Parameter	Description	Range of values / note
<code>srcip</code>	Keyword for the source IP address	-
<code>ip</code>	IPv4 address or certain IPv4 address range	Enter a valid IPv4 address or an IP address range.
<code>subnet</code>	The subnet can also be a single PC or another subset of the subnet.	Specify the subnet in the CIDR notation.
<code>dstip</code>	Keyword for the destination IP address	-
<code>ip</code>	IPv4 address or certain IPv4 address range	Enter a valid IPv4 address.
<code>subnet</code>	The subnet can also be a single PC or another subset of the subnet.	Specify the subnet in the CIDR notation.
<code>transip</code>	Keyword for the IPv4 address with which the IPv4 address of the source is replaced. Note If you do not use the parameter, the IP address of the selected destination interface is used.	-
<code>ip</code>	If the interface has an IPv4 address, the parameter is optional. In this case, the IPv4 address of the interface is used.	Enter a valid IPv4 address.

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL NAT configuration mode (Page 412)".

Note

Firewall rules with source NAT

If you create a corresponding firewall rule for a source NAT rule, use the entry from "Source IP Subnet" in "IP Rules" for the "Source (Range)". For "Destination (Range)", use the entry from "Destination IP Subnet".

Result

The source NAT rule is created. During creation, an entry with a unique number (index) is created.

Further notes

You delete a source NAT rule with the `no src-nat` command.

You delete all source NAT rules with the `no src-nat all` command.

You display the numbers of the source NAT rules with the `src-nat show-idx` command.

You display the source NAT rule with the `show firewallnat src-nat` command.

10.2.3.17 no src-nat all

Description

With this command, you delete all source NAT 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:

```
src-nat del all
```

Result

The source NAT rules are created.

Further notes

You create a source NAT rule with the `src-nat type ipv4` command.

10.2.3.18 no src-nat

Description

With this command, you delete a specific source NAT rule.

Requirement

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 src-nat srcint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>] dstint <vlan|ipsec|ipsecall|sinemarcall|openvpn|openvpnall> [<num(0-4094)>]  
idx <num(1-200)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
srcint	Keyword for the source interface	-
vlan	VLAN interface	-
ipsec ipsecall sinemarcall openvpn openvpnall	Access via VPN tunnel partners that can be reached via SINEMA RC, via all VPN connections (all) or via a specific VPN connection <num> .	-
num	Number of the interface or the VPN connection	0 ... 4094
dstint	Keyword for the destination interface	-
vlan	VLAN interface	-
ipsec ipsecall sinemarcall openvpn openvpnall	Access to the VPN tunnel partners that can be reached via SINEMA RC, via all VPN connections (all) or via a specific VPN connection <num>.	-
num	Number of the interface or the VPN connection	0 ... 4094
idx	Keyword for the number of the source NAT rule	-
num	Number corresponding to a specific source NAT rule.	Specify a valid number. 0 ... 200

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL NAT configuration mode (Page 412)".

Result

The specified source NAT rule is deleted.

Further notes

You delete all source NAT rules with the `no src-nat all` command.

You create a source NAT rule with the `src-nat type ipv4.` command.

You display the numbers of the source NAT rules with the `src-nat show-idx` command.

Security and authentication

This part contains the sections that describe the access rights and authentication methods.

11.1 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.

11.1.1 The "show" commands

This section describes commands with which you display various settings.

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

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

11.1.1.1 show 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.

11.1.1.2 show radius server

Description

This command shows the RADIUS server configuration.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameters:

```
show radius server [{<ucast_addr> | <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 41)".

If no parameters are specified, all configured RADIUS servers are displayed.

Result

The RADIUS server configuration is displayed.

11.1.2 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.

11.1.2.1 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.

11.1.2.2 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.

11.1.2.3 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.

11.1.2.4 radius-server

Description

With this command, you configure 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:

```
radius-server { ipv4 <ipv4-address> | fqdn-name <FQDN> } [auth-port <portno(1-65535)>] [retransmit <1-5>] [key <secret-key-string>] >] [primary] [test]
```

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
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: empty string
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.	

For information on addresses and interfaces, refer to the section "Addresses and interface names (Page 41)".

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.

11.1.2.5 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>} [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
primary	Identifies the RADIUS server as primary server	-

For information on addresses and interfaces, refer to the section "Addresses and interface names (Page 41)".

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.

11.2 User management

This section describes commands for access as administrator and the configuration of the authentication methods.

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 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.

11.2.1.2 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.

Further notes

You create a role with the `role` command.

You delete a role with the `no role` command.

11.2.1.3 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.

11.2.1.4 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.

11.2.1.5 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.

11.2.2 change password

Description

With this command, you change the password of the logged in user.

Requirement

- You are logged into the device with a local user account
- You are in the User EXEC mode or in the Privileged EXEC mode.

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call up the command with the following parameters:

```
change password <passwd>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
passwd	Value for the password	Enter the password. The entry depends on the password policy. The <code>show password-policy</code> 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.

11.2.3 whoami

Description

This command shows the user name of the logged in user.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
whoami
```

Result

The user name of the logged in user is displayed.

11.2.4 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.

11.2.4.1 loginpage

Description

With this command, you specify the login page with which the WBM starts by default.

Requirement

You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
loginpage {configuration | firewall}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
configuration	Logging into the WBM	-
firewall	Logging into the WBM page for user-specific firewall.	-

Result

The default login page is configured.

11.2.4.2 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 >
```

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

Result

The password policy is specified:

Further notes

You assign a new password with the `user-account` command.

You display the setting with the `show password-policy` command.

11.2.4.3 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: <ul style="list-style-type: none">• It must be unique.• It must be between 1 and 64 characters long.
function-rights	Keyword for the function rights	-
function-rights-value	Value of the function rights	Select the function rights of the role. <ul style="list-style-type: none">• 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.

11.2.4.4 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.

11.2.4.5 user-account

Description

With this command, you specify a new user. You can also change the password/role of an already created user.

Requirement

- The user is logged in with the "admin" role.
- You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
user-account <user-name> password <user-password> role <user-role> [description  
<user-description>] [remote-access {none|additional|only}]
```

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: <ul style="list-style-type: none">• It must be unique.• It must be between 1 and 250 characters long.• The following characters must not be included: \$? " ; : The characters for Space and Delete must also not be included.
password	Keyword for a password	-

Parameter	Description	Range of values / note
user-password	Value for the password	<p>Enter the password.</p> <p>The following characters must not be included:</p> <ul style="list-style-type: none"> • \$? " ; : • The characters for Space and Delete must also not be included. <p>The strength of the password depends on the set password policy.</p> <ul style="list-style-type: none"> • low: Password length: at least 6 characters • high: The password must meet the following conditions: <ul style="list-style-type: none"> – 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	<p>Enter a role.</p> <p>You can choose between system-defined and self-defined roles.</p>
description	Keyword for the description	-
user-description	Content of the description	<p>Enter a description for the user account.</p> <p>The description text can be up to 100 characters long.</p>
remote-access	Remote access	<ul style="list-style-type: none"> • none <p>No remote access. The user is logged in with the rights of the associated role.</p> <ul style="list-style-type: none"> • additional <p>Remote access and rights assigned to the user.</p> <ul style="list-style-type: none"> • only <p>Only remote access, which means no rights other than logging into the WBM page for user-specific firewall.</p>

Note**User names: admin**

You can configure the device with this user name.

If you log in the first time or log in after a "Restore Factory Defaults and Restart", you will be prompted to change the predefined password "admin". You can also rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible.

Result

The new user has been created or the password / role has been changed.

Note**Changes in "Trial" mode**

Even if the device is in "Trial" mode, these changes are saved immediately.

Note

The users preset in the factory as well as logged in users cannot be deleted or changed.

Further notes

You delete a user with the `no user-account` 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.

11.2.4.6 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.

11.2.4.7 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
<code>user-account-ext</code>	Keyword for a user in the table "External User Accounts"	-
<code>user-name-ext</code>	User name	Enter the name for the user. The name must meet the following conditions: <ul style="list-style-type: none">• It must be unique.• It must be between 1 and 250 characters long.
<code>role</code>	Keyword for the role name	-
<code>user-role-ext</code>	Role name	Enter a role. You can choose between system-defined and self-defined roles.
<code>description</code>	Keyword for the description	-
<code>user-ext-description</code>	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.

11.2.4.8 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.

11.2.4.9 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>]
```

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: <ul style="list-style-type: none">• 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.

11.2.4.10 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.

11.2.4.11 username

Description

With this command, you change the password for users with the user name "user" or "admin".

Requirement

- The user is logged in with the "admin" role.
- You are in global configuration mode.

The command prompt is as follows:

```
cli(config)#
```

Syntax

Call up the command with the following parameters:

```
username {user|admin} password <passwd>
```


The parameters have the following meaning:

Parameter	Description	Range of values/note
user	User with the "user" user name.	If you have created a user with the user name "user", you can change the password for this user with this command.
admin	User with the "admin" user name.	If you have not renamed the "admin" user preset in the factory, you can change the password for this user with this command.
password	Keyword for a password	-
passwd	Value for the password	Enter the password. The strength of the password depends on the set password policy: <ul style="list-style-type: none"> • <code>low</code>: Password length: at least 6 characters • <code>high</code>: The password must meet the following conditions: <ul style="list-style-type: none"> – Password length: at least 8 characters – at least 1 uppercase letter – at least 1 special character – at least 1 number

Result

The password is changed.

Note

Changing the password in Trial mode

Even if you change the password in Trial mode, this change is saved immediately.

Further notes

You show the created users with the `show user-accounts` command.

You can also change the passwords with the `user-account` command.

You display the currently valid password policy with the `show password-policy` command.

11.3 Firewall

11.3.1 Introduction to the Firewall section

This section describes commands relevant for the firewall.

11.3.2 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.

11.3.2.1 show firewall icmp-services ipv4

Description

This command shows the configured ICMPv4 services.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewall icmp-services ipv4
```

Result

The configured ICMPv4 services are displayed.

11.3.2.2 show firewall information

Description

This command shows the configuration of the firewall.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewall information
```

Result

The configuration is displayed.

11.3.2.3 show firewall ip-protocols**Description**

This command displays the configured protocols.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewall ip-protocols
```

Result

The configured protocols are displayed.

11.3.2.4 show firewall ip-rules ipv4**Description**

This command shows an overview of the IPv4 firewall rules.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewall ip-rules ipv4
```

Result

The overview of the IPv4 firewall rules is displayed.

11.3.2.5 show firewall ip-services

Description

This command shows the configured IP services.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewall ip-services
```

Result

The configured IP services are displayed.

11.3.2.6 show firewall pre-rules ipv4

Description

This command shows the predefined IPv4 rules available on the interface.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewall pre-rules ipv4
```

Result

The predefined IPv4 rules are displayed.

11.3.2.7 show firewall ruleset**Description**

This command shows the user-defined rule sets.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewall ruleset
```

Result

The user-defined rule sets are displayed.

11.3.2.8 show firewall ruleset assignment**Description**

This command shows the assignment of the rule sets.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show firewall ruleset assignment
```

Result

The assignment is displayed.

11.3.3 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.

11.3.3.1 firewall

Description

With this command, you change to the FIREWALL 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:

```
firewall
```

Result

You are now in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Further notes

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

11.3.4 Commands in the FIREWALL configuration mode

11.3.4.1 Introductory sentence for the Firewall configuration mode

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

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

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

Available interfaces

As the source and destination interfaces, the following interfaces are available:

Interface		prede- fined firewall rules	own firewall rules	
VLAN	VLANs with configured subnet	x	x	vlan integer(0)
PPP (vlan)	WAN interface	x	x	ppp 2
IPsecVPN	All IPsec VPN connections	-	x	IPsecall
	Specific IPsec VPN connection	-	x	IPsec ifnum
Open VPN	All OpenVPN connections			OpenVPNall
	Specific OpenVPN connection	-	x	OpenVPN ifnum
SINEMA RC	Connection to Sinema RC Server	-	x	SinemaRC
Device	Connection to the device	-	x	Device

x: available

- : not available

Communication directions

from	to	Meaning
vlan (1-x)	vlan (1-x)	Access from IP subnet vlan x to IP subnet vlan x. Example: vlan1 (INT) → vlan2 (EXT) Access from the local IP subnet and the device to the external IP subnet.
	ppp 2	Access from the IP subnet to the WAN interface of the device.
	Device	Access from the IP subnet to the device.
	SinemaRC	Access from the IP subnet and the device to the SINEMA RC server.
	IPsecall IPsec ifnum OpenVPNall OpenVPN ifnum	Access from the IP subnet to the VPN tunnel partners that can be reached via all VPN connections ^(all) or via a certain VPN connection (ifnum).
Device	vlan (1-x)	Access from the device to the IP subnet.
	ppp 2	Access from the device to the WAN interface of the device.
	SinemaRC	Access from the device to the SINEMA RC server.
	IPsecall IPsec ifnum OpenVPNall OpenVPN ifnum	Access from the device to the VPN tunnel partners that can be reached via all VPN connections ^(all) or via a certain VPN connection (ifnum).
SinemaRC	vlan (1-x)	Access from the SINEMA RC server to the IP subnet.
	ppp 2	Access from the SINEMA RC server to the WAN interface of the device.
	Device	Access from the SINEMA RC server to the device.
	IPsecall IPsec ifnum OpenVPNall OpenVPN ifnum	Access from the SINEMA RC server to the VPN tunnel partners that can be reached via all VPN connections ^(all) or via a certain VPN connection (ifnum).
IPsecall IPsec ifnum OpenVPNall OpenVPN ifnum	vlan (1-x)	Access via VPN tunnel partners to the IP subnet.
	ppp 2	Access via VPN tunnel partners to the WAN interface of the device.
	Device	Access via VPN tunnel partners to the device.
	SinemaRC	Access via VPN tunnel partners to the SINEMA RC server.
ppp 2	vlan (1-x)	Access from the WAN interface to the IP subnet.
	Device	Access from the WAN interface to the device.
	SinemaRC	Access from the WAN interface to the SINEMA RC server.
	IPsecall IPsec ifnum OpenVPNall OpenVPN ifnum	Access from the WAN interface to the VPN tunnel partners that can be reached via all VPN connections ^(all) or via a certain VPN connection (ifnum).

11.3.4.2 di-input set address

Description

With this command, you configure the IP address or an IP range that is allowed to send IP packets.

Requirement

- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
di-input idx 1 set address <ipaddr>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Number of the digital input	1
address	Keyword for the source.	-
ipaddr	Address that can send IP packets.	<ul style="list-style-type: none">Individual IP address: Specify the IP address.IP range: Specify the range with start address "-" end address, e.g. 192.168.100.10 - 192.168.100.20.All IP addresses: Specify "0.0.0.0/0".

Result

The IP address or the IP range is configured.

Further notes

You display this setting and other information with the `di-input show-idx` command.

11.3.4.3 di-input set ruleset

Description

With this command, you specify which rule set is executed through control of the digital input.

Requirement

- A digital input is configured for the event "Firewall".
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call up the command with the following parameters:

```
di-input idx 1 set ruleset {idx <integer> | name <string>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Number of the digital input	1
ruleset	Specifies which rule set is used.	-
idx	Number corresponding to a specific rule set.	Enter the required number. 1 ... 8
name	Name of the rule set	Enter the required name.

Result

The rule set is assigned to the digital input.

Further notes

You display this assignment with the `di-input show-idx` command.

You configure a rule set with the `ruleset name` command.

You list the available rule sets with the `ruleset show-idx` command.

You configure the IP address that can send IP packets with the `di-input set address` command.

You configure the event with the `event config` command.

11.3.4.4 di-input show-idx

Description

With this command, you can see whether a rule set is assigned to the digital input.

Requirement

- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call the command without parameter assignment:

```
di-input show-idx
```

Result

The assignment is displayed.

Further notes

You configure the assignment to the rule set with the `di-input set ruleset` command.

11.3.4.5 icmp name

Description

With this command, you create an ICMP service. You can also change the ICMP packet type and the code of an already created ICMP service.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
icmp name <string(32)> type <num(0-256)> code <num(0-256)> ver ipv4
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
string	ICMP service name	Enter a unique ICMP service name. Maximum of 32 characters
type	Keyword for the ICMP packet type	-
num	Number corresponding to a specific ICMP packet type.	Enter the required number. Default: 256 = any
code	Keyword for the code of the ICMP packet type	-
num	Number corresponding to a specific code.	Enter the required number. Default: 256
ver	Keyword for the version of the ICMP protocol	-
ipv4	IP Version4	-

Result

The ICMP service is configured.

Further notes

You change the configuration with the `icmp name set type` command.

You display the available service names with the `icmp show-names` command.

You show the available ICMP packet types and codes with the `icmp show-types-codes` command.

You delete this service with the `no icmp` command.

You display this setting and other information with the `show firewall icmp-services ipv4` command.

11.3.4.6 no icmp

Description

With this command, you delete all ICMP services or a specific ICMP service.

Requirement

- The corresponding ICMP service has been created and is not being used anywhere.
- You are in the Firewall configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
no icmp {name <string(255)> | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Keyword for ICMP service name	-
string	ICMP service name	Specify a valid service name. Maximum of 255 characters
all	Deletes all ICMP service names	-

Result

The corresponding ICMP service is deleted.

Further notes

You create the ICMP service with the `icmp name` command.

You display the available service names with the `icmp show-names` command.

You show the available ICMP packet types and codes with the `icmp show-types-codes` command.

11.3.4.7 icmp name set type

Description

With this command, you change the ICMP packet type and the code of an already created ICMP service.

Requirement

- The corresponding ICMP service is has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
icmp name <string(32)> set type <num(0-256)> code <num(0-256)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
string	ICMP service name	Specify a valid service name. Maximum of 32 characters
type	Keyword for the ICMP packet type	-
integer	Number corresponding to a specific ICMP packet type.	Enter the required number.
code	Keyword for the code of the ICMP packet type	-
integer	Number corresponding to a specific code.	Enter the required number. The selection depends on the ICMP packet type.

Result

The ICMP packet type and code have been changed.

Further notes

You create an ICMP service with the `icmp name type` command.

You display the available service names with the `icmp show-names` command.

You show the available ICMP packet types and codes with the `icmp show-types-codes` command.

You delete this service with the `no icmp` command.

You display this setting and other information with the `show firewall icmp-services ipv4` command.

11.3.4.8 icmp show-names

Description

With this command, you display the available ICMP service names.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call the command without parameter assignment:

```
icmp show-names
```

Result

The list is displayed.

Further notes

You create a protocol with the `icmp name` command.

11.3.4.9 icmp show-types-codes

Description

With this command, you display the available ICMP packet types and codes.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call the command without parameter assignment:

```
icmp show-types-codes
```

Result

The list is displayed.

Further notes

You create a protocol with the `icmp name` command.

11.3.4.10 idle timeout icmp**Description**

With this command, you configure the required period for ICMP. If no data exchange takes place, the ICMP connection is terminated automatically when this time has elapsed.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
idle timeout icmp <second(1-21474836)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
second	Interval in seconds	1 ... 21474836

Result

The interval is configured.

Further notes

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

11.3.4.11 idle timeout tcp**Description**

With this command, you configure the required period for TCP. If no data exchange takes place, the TCP connection is terminated automatically when this time has elapsed.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call up the command with the following parameters:

```
idle timeout tcp <second(1-21474836)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
second	Interval in seconds	1 ... 21474836

Result

The interval is configured.

Further notes

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

11.3.4.12 idle timeout udp

Description

With this command, you configure the required period for UDP. If no data exchange takes place, the UDP connection is terminated automatically when this time has elapsed.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call up the command with the following parameters:

```
idle timeout udp <second(1-21474836)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
second	Interval in seconds	1 ... 21474836

Result

The interval is configured.

Further notes

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

11.3.4.13 ipv4rule

Description

With this command, you create your own IPv4 rules for the firewall. These IPv4 firewall rules have a higher priority than the predefined IPv4 firewall rules.

Requirement

- The service name or protocol name has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call up the command with the following parameters:

```
ipv4rule from <iftype|OpenVPN|OpenVPNall|IPsec|IPsecall|SinemaRC|Device> [<ifnum(0-4094)>] to <iftype|OpenVPN|OpenVPNall|IPsec|IPsecall|SinemaRC|Device> [<ifnum(0-4094)>] srcip <ip|subnet|range> dstip <ip|subnet|range> action {drop|acc|rej} [service <all|name(32)>] [log {no|info|war|cri}] [prior <number(0-127)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
from	Keyword for the incoming direction (from)	-
iftype	Interface that sends the IPv4 packet	Specify a valid interface.

Parameter	Description	Range of values / note
OpenVPN OpenVPNall IPsec IPsecall SinemaRC	Access via VPN tunnel partners that can be reached via SINEMA RC via all VPN connections (all) or via a certain VPN connection <integer> .	-
Device	Access from the device	-
ifnum	Number of the interface or the VPN connection	0 ... 4094
to	Keyword for the outgoing direction (to)	
iftype	Interface that receives the IPv4 packets	Specify a valid interface to vlan
OpenVPN OpenVPNall IPsec IPsecall SinemaRC	Access to the VPN tunnel partners that can be reached via SINEMA RC via all VPN connections (all) or via a certain VPN connection <integer> .	-
Device	Access to the device	-
ifnum	Number of the interface or the VPN connection	0 ... 4094
srcip	Keyword for the source	-
ip	IPv4 address	Specify the IP address.
subnet	Subnet	Specify the subnet in the CIDR notation. All IP addresses: Specify " 0.0.0.0/0".
range	IPv4 address range	Enter the IP address range with start address "-" end address, e. g. 192.168.100.10 - 192.168.100.20.
dstip	Keyword for the destination	-
ip	IPv4 address	Specify the IP address.
subnet	Subnet	Specify the subnet in the CIDR notation. All IP addresses: Specify " 0.0.0.0/0".
range	IPv2 address range	Enter the IP address range with start address "-" end address, e.g. 192.168.100.10 - 192.168.100.20.
action	Keyword for the action with incoming IPv4 packets	-
acc	The data packets can pass through.	-
drop	The data packets are discarded without any notification to the sender.	-
rej	The data packets are rejected, and the sender receives a corresponding message.	-
service	Keyword for service or protocol name	-

Parameter	Description	Range of values / note
all	All service or protocol names for which this rule is valid.	-
name	Service or protocol name for which this rule is valid.	Enter a valid name. Maximum of 32 characters
log	Keyword for making entries in the firewall log	-
no	The rule coming into effect is not logged.	-
info	Messages about event severity "information" are logged.	-
war	Messages about event severity "warning" are logged.	-
cri	Messages about event severity "critical" are logged.	-
prior	Keyword for the priority	-
number	Priority	Enter the priority for the IPv4 rule. 0 ... 127

For information on identifiers of interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The IPv4 rule is created. When it is created, the IPv4 rule is automatically given a unique number (index).

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You create a service with the following commands: `icmp name, service name`.

You create a protocol with the `proto name` command.

You change the settings with the commands `ipv4rule` and `set....`

11.3.4.14 ipv4rule del ruleset

Description

With this command, you remove the assignment of the rule set.

Requirement

- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> del ruleset {idx <number(1-5)> | name <string>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128
ruleset	Specifies which rule set is used.	-
idx	Number corresponding to a specific rule set.	Enter the required number. 1 ... 5
name	Name of the rule set	Enter the required name.

Result

The assignment is removed.

Further notes

You display the assignment and other information with the `show firewall ruleset assignment` command.

You configure the assignment of the rule set with the `ipv4rule set ruleset` command.

11.3.4.15 no ipv4 rule

Description

With this command, you delete all IPv4 firewall rules or a specific IPv4 firewall rule.

Requirement

- The corresponding IPv4 firewall rule has been created and is not being used anywhere.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
no ipv4rule {all | idx <integer(1-128)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
all	Deletes all IPv4 rules	-
idx	Keyword for index	-
integer	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128

Result

The corresponding IPv4 firewall rule is deleted.

Further notes

You display the IPv4 firewall rule with the `ipv4rule` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.16 `ipv4rule set action`

Description

With this command, you change the action taken with incoming IPv4 packets.

Requirement

- The IPv4 firewall rule has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> set action {drop|acc|rej}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128
action	Keyword for the action with incoming IPv4 packets	-
acc	The data packets can pass through.	-
drop	The data packets are discarded without any notification to the sender.	-
rej	The data packets are rejected, and the sender receives a corresponding message.	-

Result

The action taken with the corresponding IPv4 firewall rule has been changed.

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.17 ipv4rule set dstip

Description

With this command, you change the destination.

Requirement

- The IPv4 firewall rule has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> set dstip <ip_addr>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128
dstip	Keyword for the destination	-
ip_addr	Address that receives IPv4 packets.	<ul style="list-style-type: none">Individual IP address: Specify the IP address.IP range: Specify the range with the start address "-" end address, e.g. 192.168.100.10 - 192.168.100.20.All IP addresses: Specify "0.0.0.0/0".

Result

The destination of the corresponding IPv4 firewall rule has been changed.

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.18 ipv4rule set from

Description

With this command, you change the outgoing direction.

Requirement

- The IPv4 firewall rule has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```


Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> set from <ifname(50)> [<ifnum(0-4094)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128
from	Keyword for the outgoing direction (from)	-
ifname	Interface that sends the IPv4 packet	Specify a valid interface. Maximum of 50 characters
ifnum	Number of the interface	0 ... 4094

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The outgoing direction of the corresponding IPv4 firewall rule has been changed.

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.19 ipv4rule set log

Description

With this command, you change the making of entries in the firewall log.

Requirement

- The IPv4 firewall rule has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> set log {no|info|war|cri}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128
log	Keyword for making entries in the firewall log	-
no	The rule coming into effect is not logged.	-
info	Messages about event severity "information" are logged.	-
war	Messages about event severity "warning" are logged.	-
cri	Messages about event severity "critical" are logged.	-

Result

Entering in the firewall log has been changed.

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.20 ipv4rule set prior

Description

With this command, you change the priority of the IPv4 firewall rule.

Requirement

- The IPv4 firewall rule has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> set prior <number(0-127)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128
prior	Keyword for the priority	-
number	Priority	Enter the priority for the IPv4 rule. 0 ... 127

Result

The priority of the corresponding IPv4 firewall rule has been changed.

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.21 ipv4rule set ruleset

Description

With this command, you assign a rule set to the IPv4 firewall rule. You can combine multiple IPv4 firewall rules with the rule set.

Requirement

- The IPv4 firewall rule and rule set have been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> set ruleset {idx <number(1-8)> | name <string>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128
ruleset	Specifies which rule set is used.	-
idx	Number corresponding to a specific rule set.	Enter the required number. 1 ... 8
name	Name of the rule set	Enter the required name.

Result

The IPv4 firewall rule is assigned to a rule set.

Further notes

You display this assignment and other information with the `show firewall ruleset assignment` command.

You configure a rule set with the `ruleset name` command.

You list the available IPv4 firewall rules with the `ipv4rule show-rules` command.

You list the available rule sets with the `ruleset show-idx` command.

You remove the assignment of the rule set with the `ipv4rule del ruleset` command.

11.3.4.22 ipv4rule set service

Description

With this command, you change the service or protocol name.

Requirement

- The IPv4 firewall rule has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> set service <name(32)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128
service	Keyword for service or protocol name	-
name	Service or protocol name for which this rule is valid.	Enter a valid name. Maximum of 32 characters

Result

The service or protocol name of the corresponding IPv4 firewall rule has been changed.

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.23 ipv4rule set srcip

Description

With this command, you change the source.

Requirement

- The IPv4 firewall rule has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> set srcip <ip_addr>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 128
srcip	Keyword for the source	
ip_addr	Address that sends IPv4 packets.	<ul style="list-style-type: none">Individual IP address: Specify the IP address.IP range: Specify the range with the start address "-" end address, e.g. 192.168.100.10 - 192.168.100.20.All IP addresses: Specify "0.0.0.0/0".

Result

The source of the corresponding IPv4 firewall rule has been changed.

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.24 ipv4rule set to

Description

With this command, you change the incoming direction (to).

Requirement

- The IPv4 firewall rule has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
ipv4rule idx <number(1-128)> set to <ifname(50)> [<ifnum(0-4094)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific IPv4 rule.	Enter the required number. 1 ... 64
to	Keyword for the incoming direction (to)	-
ifname	Interface that receives the IPv4 packet	Specify a valid interface. Maximum of 50 characters
ifnum	Number of the interface	0 ... 4094

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The incoming direction of the corresponding IPv4 firewall rule has been changed.

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.25 ipv4rule ipsec connection

Description

With this command, you list the firewall rules for the IPsec connections.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call the command without parameter assignment:

```
ipv4rule ipsec connection show-idx
```

Result

The IPv4 firewall rules are listed.

Further notes

You display the IPv4 firewall rule with the `ipv4rule` command.

11.3.4.26 `ipv4rule show interfaces`**Description**

With this command, you list the available source and destination interfaces.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
ipv4rule show {from|to} interfaces
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
<code>from</code>	Lists the source interfaces.	-
<code>to</code>	Lists the destination interfaces.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The interfaces are listed.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.27 `ipv4rule show-rules`

Description

With this command, you display the available IPv4 firewall rules.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call the command without parameter assignment:

```
ipv4rule show-rules
```

Result

The IPv4 firewall rules are listed.

Further notes

You display further information with the `show firewall ip-rules ipv4` command.

You display the IPv4 firewall rule with the `ipv4rule` command.

11.3.4.28 `prerule all ipv4`

Description

With this command, you enable all predefined firewall rules on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call up the command with the following parameters:

```
prerule all ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables all predefined firewall rules on all interfaces.	-
enabled	Enables the predefined firewall rules.	-
disabled	Disables the predefined firewall rules.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

All predefined firewall rules are enabled on the corresponding interface.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.29 prerule cloudconnector ipv4

Description

You can use this command to activate the pre-defined Cloud Connector firewall rule at the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
prerule cloudconnector ipv4 {int <interface-type> <num(0-4094)> | all-int}
{enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The pre-defined Cloud Connector firewall rule is enabled at the corresponding interface.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.30 `prerule dhcp ipv4`

Description

With this command, you enable the predefined firewall rule DHCP on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
prerule dhcp ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule DHCP is enabled on the relevant interface. The DHCP server or the DHCP client can be accessed via the interface.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.31 prerule dns ipv4

Description

With this command, you enable the predefined firewall rule DNS on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
prerule dns ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule DNS is enabled on the relevant interface. DNS queries to the device are possible via the interface.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.32 prerule http ipv4

Description

With this command, you enable the predefined firewall rule HTTP on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
prerule http ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule HTTP is enabled on the relevant interface. The WBM can be accessed using HTTP.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.33 prerule https ipv4

Description

With this command, you enable the predefined firewall rule for HTTPS on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
prerule https ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4049
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule HTTPS is enabled on the relevant interface. The WBM can be accessed using HTTPS.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.34 prerule ipsec ipv4

Description

With this command, you enable the predefined firewall rule IPsec on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
prerule ipsec ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule IPsec is enabled on the relevant interface. IKE (Internet Key Exchange) data transfer from the external network to the device is allowed.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.35 prerule ipv4 show-int

Description

With this command, you list the available interfaces.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call the command without parameter assignment:

```
prerule ipv4 show-int
```


Result

The interfaces are listed.

11.3.4.36 prerule ping ipv4

Description

With this command, you enable the predefined firewall rule Ping on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
prerule ping ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule Ping is enabled on the relevant interface.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.37 prerule snmp ipv4

Description

With this command, you enable the predefined firewall rule SNMP on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
prerule snmp ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule SNMP is enabled on the relevant interface. Incoming SNMP connections are possible via the interface.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.38 prerule ssh ipv4

Description

With this command, you enable the predefined firewall rule SSH on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call up the command with the following parameters:

```
prerule ssh ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule SSH is enabled on the relevant interface. Encrypted access to the CLI is possible.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.39 prerule systime ipv4

Description

With this command, you enable the predefined firewall rule System time on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
prerule systime ipv4 {int <interface-type> <num(0-4094)> | all-int}  
{enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule System time is enabled on the relevant interface.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.40 prerule telnet ipv4

Description

With this command, you enable the predefined firewall rule Telnet on the selected interface.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call up the command with the following parameters:

```
prerule telnet ipv4 {int <interface-type> <num(0-4094)> | all-int} {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
int	Keyword for the interface	-
interface-type	Type or speed of the interface	Specify a valid interface.
num	Interface index	Specify a valid interface index. 0 ... 4094
all-int	Enables the predefined firewall rule on all interfaces.	-
enabled	Enables the predefined firewall rule.	-
disabled	Disables the predefined firewall rule.	-

For information on identifiers of addresses and interfaces, refer to the section "Commands in the FIREWALL configuration mode (Page 463)".

Result

The predefined firewall rule Telnet is enabled on the relevant interface. Unencrypted access to the CLI is possible.

Further notes

You display this setting and other information with the `show firewall pre-rules ipv4` command.

You list the available interfaces with the `prerule ipv4 show-int` command.

11.3.4.41 proto name

Description

With this command, you configure user-defined protocols. You select a protocol name and assign a protocol number to it.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
proto name <name(32)> num <number(1-255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Protocol name	Specify a unique protocol name. Max. 32 characters
num	Protocol number	1 ... 255 Default: 255 Specify a protocol number, e.g. 2. You will find a list of the protocol numbers on the Internet pages of Internet Assigned Numbers Authority (IANA) (https://www.iana.org/).

Result

The protocol is configured. If the optional parameters are not specified, a protocol with this name is created and the default value is used. You can adapt the parameter later.

Further notes

You display this setting and other information with the `show firewall ip-protocols` command.

You delete the protocol with the `no proto.` command.

11.3.4.42 no proto

Description

With this command, you delete all protocols or a specific protocol.

Requirement

- The corresponding protocol has been created and is not being used anywhere.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
no proto {name <string(32)> | all}}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Keyword for a protocol name	-
string	Protocol name	Specify a valid protocol name. Maximum of 32 characters
all	Deletes all protocol names	-

Result

The relevant protocol is deleted.

Further notes

You create a protocol with the `proto name` command.

You display the available protocol names with the `proto show-names` command.

11.3.4.43 proto show-names

Description

With this command, you display the available protocol names.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call the command without parameter assignment:

```
proto show-names
```

Result

The protocol names are listed.

Further notes

You create a protocol with the `proto name` command.

11.3.4.44 ruleset idx

Description

With this command, you can change the configuration of a rule set.

Requirement

- The rule set has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
ruleset idx <number(0-5)> [name <text(128)>] [comment <text(128)>] [timeout <5-480>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific rule set.	Enter the required number. 0 ... 5
name	Keyword for name	-

Parameter	Description	Range of values / note
text	Name of the rule set	Enter the required name. Maximum of 128 characters
comment	Keyword for comment	-
text	Comment	Enter a description of the rule set. Maximum of 128 characters
timeout	Duration of the access	Enter the duration of the access. 5 ... 480 minutes

Result

The configuration is changed.

Further notes

You display this assignment and other information with the `show firewall ruleset assignment` command.

You configure a rule set with the `ruleset name` command.

11.3.4.45 ruleset name

Description

With this command, you create a rule set.

Requirement

- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
ruleset name <text(128)> [timeout <5-480>] [comment <text(128)>]
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Name of the rule set	Enter a unique name. Maximum of 128 characters
comment	Comment	Enter a description of the rule set. Maximum of 128 characters
timeout	Duration of the access	Enter the duration of the access. 5 ... 480 minutes

Result

The rule set has been created.

Further notes

You display this setting and other information with the `show firewall ip-rules ipv4` command.

You obtain the numbers with the `ipv4rule show-rules` command.

11.3.4.46 ruleset show-idx

Description

With this command, you list the available rule sets.

Requirement

- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call the command without parameter assignment:

```
ruleset show-idx
```

Result

The rule sets are listed.

Further notes

You configure a rule set with the `ruleset name` command.

11.3.4.47 no ruleset

Description

With this command, you disable a specific rule set or all existing rule sets.

Requirement

- The corresponding rule set has been created and is not being used anywhere.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
no ruleset {show-idx | idx <number> | name <text(128)> | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
show-idx	Lists the available rule sets.	-
idx	Keyword for index	-
number	Number of the rule set	Enter the number of the rule set to be deleted. 0 ... 5
name	Keyword for name	-
text	Name of the rule set	Enter the name of the rule set to be deleted. Maximum of 128 characters
all	Disables all rule sets.	-

Result

The affected rule set is deleted.

Further notes

You configure a rule set with the `ruleset name` command.

11.3.4.48 service name

Description

With this command, you configure a service. You select a service name and assign the service parameters to it.

Requirement

You are in the Firewall configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
service name <string(32)> proto {udp|tcp} src {all|port <number(0-65535)|range>} dst  
{all|port <number(0-65535)|range>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
string	Service name	Specify a unique service name. Maximum of 32 characters
proto	Keyword for a protocol	-
udp	The service is valid only for UDP frames.	-
tcp	The service is valid only for TCP frames.	Default
src	Keyword for the source	-
all	Applies to all ports.	-
port	Keyword for a port	-
number	Port number	0 ... 65535 Specify the required port.
range	Keyword for a port range	0 ... 65535 Specify the start port and end port, e.g. 10 - 20.
dst	Keyword for the destination	-
all	Applies to all ports.	-
port	Keyword for a port	-
number	Port number	0 ... 65535 Specify the required port.
range	Keyword for a port range	0 ... 65535 Specify the start port and end port, e.g. 10 - 20.

Result

The service is configured.

Further notes

You delete this service with the `no service` command.

You display the service with the `show firewall ip-services` command.

11.3.4.49 no service

Description

With this command, you delete all services or a specific service.

Requirement

- The corresponding service has been created and is not being used anywhere.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
no service {name <string(32)> | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Keyword for service name	-
string	Service name	Specify a valid service name. Maximum of 32 characters
all	Deletes all service names	-

Result

The corresponding service is deleted.

Further notes

You display the available service names with the `service show-names` command.

You create a service with the `service name` command.

You display this setting and other information with the `show firewall ip-services` command.

11.3.4.50 service name set dst

Description

With this command, you change the destination port.

Requirement

- The service name has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
service name <string(32)> set dst {all|port <number(0-65535)|range>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
string	Service name	Specify a valid service name. Maximum of 32 characters
all	Valid for all ports.	-
port	Keyword for a port	-
number	New destination port	0 ... 65535 Specify the required port.
range	New port range	0 ... 65535 Specify the start port and end port, e.g. 10 - 20.

Result

The destination port of the corresponding service has been changed.

Further notes

You display the available service names with the `service show-names` command.

You create the service with the `service name` command.

You display this setting and other information with the `show firewall ip-services` command.

11.3.4.51 service name set prot

Description

With this command, you change the protocol.

Requirement

- The service name has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
service name <string(32)> set proto {udp|tcp}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
string	Service name	Specify a valid service name. Maximum of 32 characters
udp	The service is valid only for UDP frames.	-
tcp	The service is valid only for TCP frames.	-

Result

The protocol of the relevant service has been changed.

Further notes

You display the available service names with the `service show-names` command.

You create the service with the `service name` command.

You display this setting and other information with the `show firewall ip-services` command.

11.3.4.52 service name set src

Description

With this command, you change the source port.

Requirement

- The service name has been created.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
service name <string(32)> set src {all|port <number(0-65535)|range>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
string	Service name	Specify a valid service name. Maximum of 32 characters
all	Applies to all ports.	-
port	Keyword for a port	-
number	Port number	0 ... 65535 Specify the required port.
range	Keyword for a port range	0 ... 65535 Specify the start port and end port, e.g. 10 - 20.

Result

The source port of the corresponding service has been changed.

Further notes

You display the available service names with the `service show-names` command.

You create the service with the `service cr name` command.

You display this setting and other information with the `show firewall ip-services` command.

11.3.4.53 service show-names

Description

With this command, you display the available service names.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call the command without parameter assignment:

```
service show-names
```

Result

The service names are listed.

Further notes

You create a protocol with the `service cr name` command.

11.3.4.54 shutdown

Description

With this command, you disable the firewall.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli (config-fw) #
```

Syntax

Call the command without parameter assignment:

```
shutdown
```

Result

The firewall is disabled.

Further notes

You enable the firewall with the `no shutdown` command.

11.3.4.55 no shutdown

Description

With this command, you enable the firewall.

Requirement

You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call the command without parameter assignment:

```
no shutdown
```

Result

The firewall is enabled.

Further notes

You disable the firewall with the `shutdown` command.

11.3.4.56 useraccount show-idx

Description

With this command, you show the numbers of the configured users with remote access.

Requirement

- The user has remote access.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call the command without parameter assignment:

```
useraccount show-idx
```

Result

The users are listed.

Further notes

You configure remote access with the `user-account` command.

11.3.4.57 useraccount ruleset

Description

With this command, you assign a rule set to a user.

Requirement

- The user has remote access.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw)#
```

Syntax

Call up the command with the following parameters:

```
useraccount {idx <integer> | name <string(128)>} ruleset {idx <integer> | name  
<string>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
integer	Number corresponding to a specific user.	Enter the required number.
name	Keyword for user name	-
string	User names	Enter the required name.
ruleset	Specifies which rule set is used.	-
idx	Number corresponding to a specific rule set.	Enter the required number. 1 ... 8
name	Name of the rule set	Enter the required name.

Result

A rule set is assigned to the user.

Further notes

You configure remote access with the `user-account` command.

You configure a rule set with the `ruleset name` command.

You list the available users with remote access with the `useraccount show-idx` command.

You list the available rule sets with the `ruleset show-idx` command.

11.3.4.58 no useraccount ruleset

Description

With this command, you delete the rule sets assigned for a specific user.

Requirement

- The corresponding rule set has been created and is not being used anywhere.
- You are in the FIREWALL configuration mode.

The command prompt is as follows:

```
cli(config-fw) #
```

Syntax

Call up the command with the following parameters:

```
no useraccount {idx <number> | name <text(128)>} ruleset
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx	Keyword for index	-
number	Number corresponding to a specific user.	Enter the required number. 1 ... 64
name	Keyword for user name	
text	User names	Enter the required name. Maximum of 128 characters

Result

The rule set for the selected user is deleted.

Further notes

You assign a rule set to a user with the `useraccount ruleset` command.

11.4 IPsec VPN

This section describes commands relevant for IPsec.

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 ipsec conn-authentication

Description

This command shows the security settings of the IPsec VPN connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show ipsec conn-authentication
```

Result

The settings are displayed.

11.4.1.2 show ipsec connections

Description

This command shows the configuration of the IPsec VPN connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show ipsec connections
```

Result

The configurations are displayed.

11.4.1.3 show ipsec conn-phase1

Description

This command shows the configuration of the phase 1 of the IPsec VPN connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show ipsec conn-phase1
```

Result

The configurations are displayed.

11.4.1.4 show ipsec conn-phase2

Description

This command shows the configuration of the phase 2 of the IPsec VPN connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show ipsec conn-phase2
```

Result

The configurations are displayed.

11.4.1.5 show ipsec information

Description

This command shows the basic setting of IPsec VPN.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show ipsec information
```

Result

The settings are displayed.

11.4.1.6 show ipsec remoteend

Description

This command shows the configuration of the remote stations (VPN end point).

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show ipsec remoteend
```

Result

The configurations 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 ipsec

Description

With this command, you change to the IPSEC 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:

```
ipsec
```

Result

You are now in the IPSEC configuration mode.

The command prompt is as follows:

```
cli(config-ipsec)#
```

Further notes

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

11.4.3 Commands in the IPSEC configuration mode

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

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

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

11.4.3.1 crl-policy

Description

With this command, you specify whether the validity of the certificates is checked based on the CRL (Certificate Revocation List).

Requirement

You are in the IPSEC configuration mode.

The command prompt is as follows:

```
cli(config-ipsec)#
```

Syntax

Call up the command with the following parameters:

```
CRL-policy {yes|no|ifuri}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
yes	CRL is used	-
no	CRL is not used	-
ifuri	Is only used when a CRLURL is defined.	-

Result

The setting is configured.

Further notes

You display this setting and other information with the show ipsecvpn information command.

11.4.3.2 connection name

Description

With this command, you change to the IPSEC CONNECTION configuration mode. If a suitable VPN connection does not exist, a VPN connection is first created.

Requirement

You are in the IPSEC configuration mode.

The command prompt is as follows:

```
cli(config-ipsec)#
```

Syntax

Call up the command with the following parameters:

```
connection name <name(122)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
name	Name of the VPN connection	Enter the name for the VPN connection. Maximum of 122 characters

Result

You are now in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-conn-X) #
```

Further notes

You exit the IPSEC CONNECTION configuration mode with the `end` or `exit` command.

You delete a VPN connection with the `no connection name` command.

You delete all VPN connections with the `no connection all` command.

11.4.3.3 no connection name

Description

With this command, you delete a specific VPN connection.

Requirement

- The corresponding VPN connection has been created and is not being used anywhere.
- You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-ipsec) #
```

Syntax

Call up the command with the following parameters:

```
no connection name <name(122)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
name	Name of the VPN connection	Enter the name of the VPN connection.

Result

The corresponding VPN connection is deleted.

Further notes

You display the VPN connection with the `connection name` command.

11.4.3.4 no connection all**Description**

With this command, you delete all VPN connections.

Requirement

- The VPN connection have been created and are not being used anywhere.
- You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-ipsec)#
```

Syntax

Call the command without parameter assignment:

```
no connection all
```

Result

All VPN connections are deleted.

Further notes

You display the VPN connection with the `connection name` command.

11.4.3.5 nat-keep-alive**Description**

With this command, you specify the interval at which sign of life frames (keepalives) are sent.

Requirement

You are in the IPSEC configuration mode.

The command prompt is as follows:

```
cli(config-ipsec)#
```

Syntax

Call up the command with the following parameters:

```
nat-keep-alive <sec(1-10000)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
sec	Interval	Enter the required interval. 1 ... 10000 seconds

Result

The interval is configured.

Further notes

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

11.4.3.6 remote-end name

Description

With this command, you change to the IPSEC REMOTE END configuration mode. In this mode, you configure the other settings.

If the matching VPN remote station does not exist, the VPN remote station is first created.

Requirement

You are in the IPSEC configuration mode.

The command prompt is as follows:

```
cli(config-ipsec)#
```

Syntax

Call up the command with the following parameters:

```
remote-end name <name(128)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
name	Name of the VPN remote station	Enter the name for the VPN remote station. Maximum of 128 characters

Result

You are now in the IPSEC REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-ipsec-rmend-X)#
```

X is a placeholder for the name

Further notes

You exit the IPSEC REMOTE END configuration mode with the `end` or `exit` command.

You delete a VPN remote station with the `no remote-end name` command.

You delete all VPN remote stations with the `no remote-end all` command.

11.4.3.7 no remote-end name

Description

With this command, you delete a specific VPN remote station.

Requirement

- The corresponding VPN remote station has been created and is not being used anywhere.
- You are in the IPSEC REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-ipsec)#
```

Syntax

Call up the command with the following parameters:

```
no remote-end name <name(128)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
name	Name of the VPN remote station	Enter the name of the VPN remote station. Maximum of 128 characters

Result

The corresponding VPN remote station is deleted.

Further notes

You create the VPN remote station with the `remote-end name` command.

11.4.3.8 no remote-end all

Description

With this command, you delete all VPN remote stations.

Requirement

- The VPN remote stations have been created and are not being used anywhere.
- You are in the IPSEC REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-ipsec)#
```

Syntax

Call the command without parameter assignment:

```
no remote-end all
```

Result

All VPN remote stations are deleted.

Further notes

You display the VPN remote station with the `remote-end name` command.

11.4.3.9 shutdown

Description

With this command, you disable the IPsec method for VPN.

Requirement

You are in the IPSEC configuration mode.

The command prompt is as follows:

```
cli (config-ipsec) #
```

Syntax

Call the command without parameter assignment:

```
shutdown
```

Result

The IPsec method is disabled.

Further notes

You enable the IPsec method with the `no shutdown` command.

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

11.4.3.10 no shutdown

Description

With this command, you enable the IPsec method for VPN.

Requirement

You are in the IPSEC configuration mode.

The command prompt is as follows:

```
cli (config-ipsec) #
```

Syntax

Call the command without parameter assignment:

```
no shutdown
```

Result

The IPsec method is enabled.

Further notes

You disable the IPsec method with the shutdown command.

You display this setting and other information with the show ipsecvpn information command.

11.4.4 Commands in the IPSEC REMOTE END configuration mode

This section describes commands that you can call up in the IPSEC REMOTE END configuration mode.

In the IPSEC configuration mode, enter the `remote end name` command to change to this mode.

- If you exit the IPSEC REMOTE END configuration mode with the `exit` command, you return to the IPSEC configuration mode.
- If you exit the IPSEC REMOTE END configuration mode with the `end` command, you return to the Privileged EXEC mode.

11.4.4.1 `addr`

Description

With this command, you configure the address of the VPN remote station.

Requirement

You are in the IPSEC REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Call up the command with the following parameters:

```
addr <subnet|dns>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
subnet	IP subnet	<ul style="list-style-type: none">• In Roadwarrior mode Specify the WAN IP address.• In standard mode Enter an IP range from which connections will be accepted. 0.0.0.0/0 means all IP addresses are accepted.
dns	DNS host name	Only in standard mode Specify the DNS host name.

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The address is specified.

Further notes

You configure the mode with the `conn-mode` command.

You display this setting and other information with the `show ipsec remoteend` command.

11.4.4.2 addr-mode

Description

With this command, you specify the type of the remote station address.

Requirement

You are in the IPSEC REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Call up the command with the following parameters:

```
addr-mode <manual|any>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
manual	Accepts the connection from remote stations with a specific address.	<ul style="list-style-type: none">• In Roadwarrior mode Only accepts connections from remote stations with a fixed IP address (/32), fixed IP subnet (CIDR notation), or (D)DNS host name.• In standard mode Only establishes a connection to a specific remote station with a fixed IP address or with (D)DNS host name. Or only accepts a connection from a specific remote station with a fixed IP address or with (D)DNS host name.
any	Accepts the connection from remote stations with any IPv4 address.	Only in Roadwarrior mode

Result

The setting is specified.

Further notes

You configure the mode with the `conn-mode` command.

You configure the IP address with the `addr` command.

You configure the remote subnet with the `subnet` command.

You display this setting and other information with the `show ipsec remoteend` command.

11.4.4.3 conn-mode

Description

With this command, you specify the role the remote stations will adopt.

Requirement

You are in the IPSEC REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Call up the command with the following parameters:

```
conn-mode {roadwarrior|standard}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
roadwarrior	Roadwarrior mode The device accepts VPN connections from remote stations with an unknown address.	-
standard	Standard mode The device establishes a connection to or from a known remote station. The remote station is identified by the IPv4 address or the DDNS hostname.	-

Result

The role is configured.

Further notes

You display this setting and other information with the `show ipsec remoteend` command.

11.4.4.4 subnet

Description

With this command, you configure the remote subnet of the VPN remote station.

Requirement

You are in the IPSEC REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Call up the command with the following parameters:

```
subnet <subnet|dns>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
subnet	IP subnet	Enter the subnet.
dns	DNS name	Specify the DNS host name.

For information on names of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The remote subnet is configured.

Further notes

You display this setting and other information with the `show ipsec remoteend` command.

11.4.4.5 vir-ip

Description

With this command, you specify the subnet from which the remote station is offered a virtual IP address.

Requirement

You are in the IPSEC REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-ipsec-rmend-X)#
```

Syntax

Call up the command with the following parameters:

```
vir-ip ipv4 [<subnet>]
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
subnet	Subnet from which the remote station is offered a virtual IPv4 address	Specify the subnet in CIDR notation.

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The subnet is configured.

Further notes

You display this setting and other information with the `show ipsec remoteend` command.

You disable the setting with the `no vir-ip` command.

11.4.4.6 no vir-ip

Description

With this command, you specify that the remote station is not offered a virtual IPv4 address.

Requirement

You are in the IPSEC REMOTE END configuration mode.

The command prompt is as follows:

```
cli (config-ipsec-rmend-X) #
```

Syntax

Call the command without parameter assignment:

```
no vir-ip
```

Result

The setting is configured.

Further notes

You display this setting and other information with the `show ipsec remoteend` command.

You enable this setting with the `vir-ip` command.

11.4.5 Commands in the IPSEC CONNECTION configuration mode

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

In the IPSEC configuration mode, enter the `connection name` command to change to this mode.

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

11.4.5.1 authentication

Description

With this command, you change to the IPSEC AUTHENTICATION configuration mode.

Requirement

You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-conn-X) #
```

Syntax

Call the command without parameter assignment:

```
authentication
```

Result

You are now in the IPSEC AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-conn-auth) #
```

Further notes

You exit the IPSEC AUTHENTICATION configuration mode with the `end` or `exit` command.

11.4.5.2 k-proto

Description

With this command, you specify whether IKEv2 or IKEv1 will be used.

Requirement

You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-conn-X) #
```

Syntax

Call up the command with the following parameters:

```
k-proto {ikev1|ikev2}
```


The parameters have the following meaning:

Parameter	Description	Range of values / note
IKEv1	Uses IKEv1	-
IKEv2	Uses IKEv2	-

Result

The setting is configured.

Further notes

You display this setting and other information with the `show ipsec connections` command.

11.4.5.3 loc-subnet

Description

With this command, you configure the local subnet.

Requirement

You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-conn-X)#
```

Syntax

Call up the command with the following parameters:

```
loc-subnet <subnet|dns>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
subnet	Local subnet address	Specify the local subnet in CIDR notation. The local network can be a single PC or another sub-set of the local network.

For information on identifiers of addresses and interfaces, refer to the section Interface identifiers and addresses (Page 41).

Result

The local subnet is configured.

Further notes

You display this setting and other information with the `show ipsecvpn connections` command.

11.4.5.4 operation

Description

With this command you specify how the connection is established.

Requirement

You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-conn-X)#
```

Syntax

Call up the command with the following parameters:

```
operation {disabled|start|wait|on-demand|start-di|wait-di}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
disabled	The VPN connection is disabled	-
start	The device attempts to establish a VPN connection to the partner.	-
wait	The device waits for the partner to initiate the connection.	-
on-demand	The VPN connection is established when necessary.	-
start-di	If the event "Digital In" occurs the device attempts to establish a VPN connection to the partner. This is on condition that the event "Digital In" is passed on to the VPN connection.	-
wait-di	If the event "Digital In" occurs, the device waits for the partner to initiate a connection establishment. This is on condition that the event "Digital In" is passed on to the VPN connection.	-

Result

The setting is configured.

Further notes

You display this setting and other information with the `show ipsec connections` command.

11.4.5.5 phase

Description

With this command, you change to the IPSEC PHASE configuration mode.

Requirement

You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-conn-X)#
```

Syntax

Call up the command with the following parameters:

```
phase <num(1-2)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
num	Phase of the VPN connection	<ul style="list-style-type: none">1: Phase 12: Phase 2

Result

You are now in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phsX)#
```

Further notes

You display this setting and other information with the `show ipsec connections` command.

11.4.5.6 rmend name

Description

With this command, you specify the VPN remote station for the IPsec connection.

Requirement

- The VPN remote station has been created.
- You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli (config-conn-X) #
```

Syntax

Call up the command with the following parameters:

```
rmend name <name(128)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
name	Name of the VPN remote station	Enter a valid name. Maximum of 128 characters

Result

The VPN remote station has been configured.

Further notes

You display this setting and other information with the `show ipsec connections` command.

You create the VPN remote station with the `remote-end name` command.

11.4.5.7 timeout

Description

With this command, you configure the interval after which the VPN connection will be terminated. If no packets are sent during this time, the VPN connection is automatically terminated.

Requirement

- The VPN connection is established when necessary (on demand).
- You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli (config-conn-X) #
```

Syntax

Call up the command with the following parameters:

```
timeout <sec(0-1000)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
sec	Period	Enter the period of time in seconds.

Result

The period of time is configured.

Further notes

You display this setting and other information with the `show ipsec connections` command.

You configure the `on demand` setting with the `operation` command.

11.4.5.8 vir-ip

Description

With this command, you specify that during connection establishment a virtual IPv4 address is requested from the VPN remote station.

Requirement

You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-conn-X)#
```

Syntax

Call the command without parameter assignment:

```
vir-ip
```

Result

The setting is enabled.

Further notes

You display this setting and other information with the `show ipsec connections` command.

You disable the requesting of a virtual IPv4 address with the `no vir-ip` command.

11.4.5.9 no vir-ip

Description

With this command, you disable the requesting of a virtual IPv4 address.

Requirement

You are in the IPSEC CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-conn-X)#
```

Syntax

Call the command without parameter assignment:

```
no vir-ip
```

Result

The setting is disabled.

Further notes

You display this setting and other information with the `show ipsec connections` command.

You enable the requesting of a virtual IPv4 address with the `vir-ip` command.

11.4.6 Commands in the IPSEC AUTHENTICATION configuration mode

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

In the IPSEC CONNECTION configuration mode, enter the `authentication` command to change to this mode.

- If you exit the IPSEC AUTHENTICATION configuration mode with the `exit` command, you return to the IPSEC CONNECTION configuration mode.
- If you exit the IPSEC AUTHENTICATION configuration mode with the `end` command, you return to the Privileged EXEC mode.

11.4.6.1 auth cacert

Description

With this command you specify that a CA certificate will be used for authentication.

Requirement

- The certificates are loaded.
- You are in the IPSEC AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-conn-auth)#
```

Syntax

Call up the command with the following parameters:

```
auth cacert <string(255)> localcert <string(255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
cacert	Keyword for CA certificate	
string	Name of the CA certificate	Specify a valid CA certificate.
localcert	Keyword for a device certificate	
string	Name of the device certificate	Specify a valid device certificate.

Result

The setting is configured.

Further notes

You show the loaded certificates with the `show-idx` command.

You display this setting and other information with the `show ipsec conn-authentication` command.

You show the available certificates with the `show-idx` command.

You show the configuration of the IPsec connection with the `show ipsec connections` command.

You remove the authentication with the `no auth` command.

11.4.6.2 auth psk

Description

With this command you specify that a key will be used for authentication.

Requirement

You are in the IPSEC AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-conn-auth)#
```

Syntax

Call up the command with the following parameters:

```
auth psk <string(255)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
string	Value for the key	Specify a valid key.

Result

The key is configured.

Further notes

You display this setting and other information with the `show ipsec conn-authentication` command.

You remove the authentication with the `no auth` command.

11.4.6.3 auth remcert

Description

With this command you specify that the remote station certificate will be used for authentication.

Requirement

- The certificates are loaded.
- You are in the IPSEC AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-conn-auth)#
```

Syntax

Call up the command with the following parameters:

```
auth remcert <string(255)> localcert <string(255)>
```

The parameters have the following meaning:

remcert	Keyword for a remote station certificate	-
string	Name of the remote station certificate	Specify a valid remote station certificate. Maximum of 255 characters
localcert	Keyword for a device certificate	-
string	Name of the device certificate	Specify a valid device certificate. Maximum of 255 characters

Result

The setting is configured.

Further notes

You show the loaded certificates with the `show-idx` command.

You display this setting and other information with the `show ipsec conn-authentication` command.

You remove the authentication with the `no auth` command.

11.4.6.4 no auth

Description

With this command, you delete the authentication method.

Requirement

You are in the IPSEC AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-conn-auth)#
```

Syntax

Call the command without parameter assignment:

```
no auth
```

Result

The authentication method is deleted.

11.4.6.5 local-id

Description

With this command, you configure the local ID.

Requirement

You are in the IPSEC AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-conn-auth)#
```

Syntax

Call up the command with the following parameters:

```
local-id <string(255)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
string	Local ID	Enter the local ID. If you do not specify the local ID, the local ID is read from the device certificate. If you use PSK as the authentication, the WAN IP address is used as the local ID.

Result

The local ID is configured.

Further notes

You display this setting and other information with the `show ipsec conn-authentication` command.

You remove the local ID with the `no local-id` command.

11.4.6.6 no local-id

Description

With this command, you remove the local ID.

Requirement

You are in the IPSEC AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-conn-auth)#
```

Syntax

Call the command without parameter assignment:

```
no local-id
```

Result

The local ID is removed.

Further notes

You display this setting and other information with the `show ipsec conn-authentication` command.

You configure the local ID with the `local-id` command.

11.4.6.7 rem-id

Description

With this command, you configure the remote ID.

Requirement

You are in the IPSEC AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-conn-auth)#
```

Syntax

Call up the command with the following parameters:

```
rem-id <string(255)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
string	Remote ID	Enter the remote ID. If you do not specify the remote ID, the remote ID is read from the device certificate. If you use PSK as the authentication, the WAN IP address is used as the remote ID.

Result

The remote ID is configured.

Further notes

You display this setting and other information with the `show ipsec conn-authentication` command.

You remove the remote ID with the `no rem-id` command.

11.4.6.8 no rem-id

Description

With this command, you remove the remote ID.

Requirement

You are in the IPSEC AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli (config-conn-auth) #
```

Syntax

Call the command without parameter assignment:

```
no rem-id
```

Result

The remote ID is removed.

Further notes

You display this setting and other information with the `show ipsec conn-authentication` command.

You configure the remote ID with the `rem-id` command.

11.4.7 Commands in the IPSEC PHASE1 configuration mode

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

In the IPSEC CONNECTION configuration mode, enter the `phase` command with the parameter `1` to change to this mode.

- If you exit the IPSEC PHASE1 configuration mode with the `exit` command, you return to the IPSEC CONNECTION configuration mode.
- If you exit the IPSEC PHASE1 configuration mode with the `end` command, you return to the Privileged EXEC mode.

11.4.7.1 aggressive

Description

With this command you specify that the aggressive mode will be used.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call the command without parameter assignment:

```
aggressive
```

Result

The setting is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

You disable the aggressive mode with the `no aggressive` command.

11.4.7.2 no aggressive

Description

With this command, you disable the aggressive mode.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call the command without parameter assignment:

```
no aggressive
```

Result

The setting is disabled. The main mode is used.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

You enable the aggressive mode with the `aggressive` command.

11.4.7.3 default-ciphers

Description

With this command, you specify that a preset list (default list) is transferred to the VPN connection partner during connection establishment. The list contains a combination of the three algorithms (Encryption, Authentication, Key Derivation).

To establish a VPN connection, the VPN connection partner must support at least one of these combinations. The combinations depend on the phase and the key exchange method (IKE).

Combination			Phase 1		Phase 2	
Encryption	Authenticat- tion	Key Derivation	IKEv1	IKEv2	IKEv1	IKEv2
AES128	SHA1	DH Group 14	x	x	x	x
AES256	SHA512	DH Group 16	x	x	x	x
AES128 CCM 16	SHA256	DH Group 14	-	x	x	x
AES256 CCM 16	SHA512	DH Group 16	-	x	x	x
AES128	SHA1	none	-	-	x	x
AES256	SHA512	none	-	-	x	x
AES128 CCM 16	SHA256	none	-	-	x	x
AES256 CCM 16	SHA512	none	-	-	x	x

x: is supported

-: is not supported

none: For phase 2, no separate keys are exchanged. This means that Perfect Forward Secrecy (PFS) is disabled.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phsX)#
```

```
X: 1 (Phase 1)
```

```
    2 (Phase 2)
```

Syntax

Call the command without parameter assignment:

```
default-ciphers
```

Result

The default list is used.

Further notes

You display this setting and other information with the `show ipsec conn-phaseX` command.

You disable the use of the default list with the `no default-ciphers` command.

11.4.7.4 no default-ciphers

Description

With this command, you disable the use of the default list.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli (config-conn-phsX) #  
X: 1 (Phase 1)  
    2 (Phase 2)
```

Syntax

Call the command without parameter assignment:

```
no default-ciphers
```

Result

The use of the default list is disabled. The fixed values are used for the phase.

Further notes

You configure the fixed values for phase 1 with the commands `ike-encryption`, `ike-auth` and `ike-keyderivation`.

You configure the fixed values for phase 2 with the commands `esp-encryption`, `esp-auth` and `esp-keyderivation`.

You display this setting and other information with the `show ipsec conn-phase1` or `show ipsec conn-phase2` command.

You enable the use of the default list with the `default-ciphers` command.

11.4.7.5 dpd

Description

With this command, you enable Dead Peer Detection (DPD).

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call the command without parameter assignment:

```
dpd
```

Result

DPD is enabled. Using DPD, it is possible to find out whether the VPN connection still exists or whether it has aborted.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

You disable DPD with the `no dpd` command.

11.4.7.6 no dpd

Description

With this command, you disable DPD.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call the command without parameter assignment:

```
no dpd
```

Result

DPD is disabled.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

You enable DPD with the `dpd` command.

11.4.7.7 dpd-period

Description

With this command, you configure the period after which DPD queries are sent.

Requirement

- DPD is enabled
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call up the command with the following parameters:

```
dpd-period <sec(10-120)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
sec	Period for DPD queries	Enter the period of time in seconds.

Result

The period of time is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

You enable DPD with the `dpd` command.

11.4.7.8 dpd-timeout

Description

With this command, you configure the timeout setting for the VPN connection. If there is no response to the DPD queries, the connection to the remote station is declared to be invalid after this time has elapsed.

Requirement

- DPD is enabled
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call up the command with the following parameters:

```
dpd-timeout <sec(10-1000)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
sec	Period for DPD queries	Enter the period of time in seconds. Note: To avoid unwanted connection breakdowns, set the DPD timeout significantly longer than the DPD period. We recommend setting the DPD timeout at least three times as long as the DPD period.

Result

The period of time is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

You enable DPD with the `dpd` command.

11.4.7.9 ike-auth

Description

With this command, you configure the method for calculating the checksum.

Requirement

- The default list is not used.
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call up the command with the following parameters:

```
ike-auth {md5|sha1|sha256|sha384|sha512}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
md5	Message Digest Algorithm 5	-
sha1	Secure Hash Algorithm 1 with 160 bit hash length	-
sha256	Secure Hash Algorithm 2 with 256 bit hash length	-
sha384	Secure Hash Algorithm 2 with 384 bit hash length	-
sha512	Secure Hash Algorithm 2 with 512 bit hash length	-

Result

The method for configuring the checksum is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

You disable the use of the default list with the `no default-ciphers` command.

11.4.7.10 ike-encryption

Description

With this command, you configure the encryption algorithm.

Requirement

- The default list is not used.
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli (config-conn-phs1) #
```

Syntax

Call up the command with the following parameters:

```
ike-encryption
{3des|aes128cbc|aes192cbc|aes256cbc|aes128ctr|aes192ctr|aes256ctr|aes128ccm16|aes192ccm16|aes256ccm16|aes128gcm16|aes192gcm16|aes256gcm16}
```

The parameters have the following meaning:

Parameter	Description	Phase 1	
		IKEv1	IKEv2
3des	Triple Data Encryption Standard	x	x
aes128cbc	Advanced Encryption Standard with 128 bits	x	x
aes192cbc	Advanced Encryption Standard with 192 bits	x	x
aes256cbc	Advanced Encryption Standard with 256 bits	x	x
aes128ctr	Advanced Encryption Standard with 128 bits in Counter mode	-	x
aes192ctr	Advanced Encryption Standard with 192 bits in Counter mode	-	x
aes256ctr	Advanced Encryption Standard with 256 bits in Counter mode	-	x
aes128ccm16	Advanced Encryption Standard with 128 bits in Counter mode using a 16 byte Integrity Check Value (ICV)	-	x
aes192ccm16	Advanced Encryption Standard with 192 bits in Counter mode using a 16 byte Integrity Check Value (ICV)	-	x
aes256ccm16	Advanced Encryption Standard with 256 bits in Counter mode using a 16 byte Integrity Check Value (ICV)	-	x
aes128gcm16	Advanced Encryption Standard with 128 bits in Galois Counter mode using a 16 byte Integrity Check Value (ICV)	-	x
aes192gcm16	Advanced Encryption Standard with 192 bits in Galois Counter mode using a 16 byte Integrity Check Value (ICV)	-	x
aes256gcm16	Advanced Encryption Standard with 256 bits in Galois Counter mode using a 16 byte Integrity Check Value (ICV)	-	x

x: is supported

-. is not supported

Result

The encryption algorithm is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

You disable the use of the default list with the `no default-ciphers` command.

11.4.7.11 ike-keyderivation

Description

With this command, you configure the required Diffie-Hellmann group (DH) from which a key will be generated.

Requirement

- The default list is not used.
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call up the command with the following parameters:

```
ike-keyderivation {dhgroup <1|2|5|14|15|16|17|18>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
auto	Automatic detection	-
dhgroup	Diffie-Hellmann group (DH)	Specify the required Diffie-Hellmann group (DH). <ul style="list-style-type: none">• 1• 2• 5• 14• 15• 16• 17• 18

Result

The Diffie-Hellmann group (DH) is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

You disable the use of the default list with the `no default-ciphers` command.

11.4.7.12 ike-keytries

Description

With this command, you configure the number of repetitions for a failed connection establishment.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call up the command with the following parameters:

```
ike-keytries <num(0-100)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
num	Period for DPD queries	Enter the required number. With 0 there is no limit to the number of attempts to establish the connection.

Result

The number of times configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

11.4.7.13 ike-lifetime

Description

With this command, you configure a period to specify the lifetime of the agreed keys. When the time expires, the key is renegotiated.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs1)#
```

Syntax

Call up the command with the following parameters:

```
ike-lifetime <min(10-2500000)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
min	Period for DPD queries	Specify the period of time in minutes.

Result

The period of time is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase1` command.

11.4.8 Commands in the IPSEC PHASE2 configuration mode

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

In the IPSEC CONNECTION configuration mode, enter the `phase` command with the parameter `2` to change to this mode.

- If you exit the IPSEC PHASE2 configuration mode with the `exit` command, you return to the IPSEC CONNECTION configuration mode.
- If you exit the IPSEC PHASE2 configuration mode with the `end` command, you return to the Privileged EXEC mode.

11.4.8.1 auto-fwrules

Description

With this command you specify that the firewall rule will be created automatically for the VPN connection.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs2)#
```

Syntax

Call the command without parameter assignment:

```
auto-fwrules
```

Result

The firewall rule is created automatically for the VPN connection.

Further notes

You display this setting and other information with the `show ipsec conn-phase2` command.

You disable the setting with the `no auto-fwrules` command.

11.4.8.2 no auto-fwrules

Description

With this command you specify that the firewall rule will not be created automatically for the VPN connection.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs2)#
```

Syntax

Call the command without parameter assignment:

```
no auto-fwrules
```

Result

The firewall rule is not created automatically for the VPN connection. You need to create the firewall rule manually.

Further notes

You display this setting and other information with the `show ipsec conn-phase2` command.

You enable the setting with the `auto-fwrules` command.

11.4.8.3 default-ciphers

Description

With this command, you specify that a preset list (default list) is transferred to the VPN connection partner during connection establishment. The list contains a combination of the three algorithms (Encryption, Authentication, Key Derivation).

To establish a VPN connection, the VPN connection partner must support at least one of these combinations. The combinations depend on the phase and the key exchange method (IKE).

Combination			Phase 1		Phase 2	
Encryption	Authenticat- tion	Key Derivation	IKEv1	IKEv2	IKEv1	IKEv2
AES128	SHA1	DH Group 14	x	x	x	x
AES256	SHA512	DH Group 16	x	x	x	x
AES128 CCM 16	SHA256	DH Group 14	-	x	x	x
AES256 CCM 16	SHA512	DH Group 16	-	x	x	x
AES128	SHA1	none	-	-	x	x
AES256	SHA512	none	-	-	x	x
AES128 CCM 16	SHA256	none	-	-	x	x
AES256 CCM 16	SHA512	none	-	-	x	x

x: is supported

-: is not supported

none: For phase 2, no separate keys are exchanged. This means that Perfect Forward Secrecy (PFS) is disabled.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli (config-conn-phsX) #
```

```
X: 1 (Phase 1)
    2 (Phase 2)
```

Syntax

Call the command without parameter assignment:

```
default-ciphers
```

Result

The default list is used.

Further notes

You display this setting and other information with the `show ipsec conn-phaseX` command.

You disable the use of the default list with the `no default-ciphers` command.

11.4.8.4 no default-ciphers

Description

With this command, you disable the use of the default list.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phsX)#
X: 1 (Phase 1)
    2 (Phase 2)
```

Syntax

Call the command without parameter assignment:

```
no default-ciphers
```

Result

The use of the default list is disabled. The fixed values are used for the phase.

Further notes

You configure the fixed values for phase 1 with the commands `ike-encryption`, `ike-auth` and `ike-keyderivation`.

You configure the fixed values for phase 2 with the commands `esp-encryption`, `esp-auth` and `esp-keyderivation`.

You display this setting and other information with the `show ipsec conn-phase1` or `show ipsec conn-phase2` command.

You enable the use of the default list with the `default-ciphers` command.

11.4.8.5 esp-auth

Description

With this command, you configure the method for calculating the checksum.

Requirement

- The default list is not used.
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs2)#
```

Syntax

Call up the command with the following parameters:

```
esp-auth md5|sha1|sha256|sha384|sha512}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
md5	Message Digest Algorithm 5	-
sha1	Secure Hash Algorithm 1 with 160 bit hash length	-
sha256	Secure Hash Algorithm 2 with 256 bit hash length	-
sha384	Secure Hash Algorithm 2 with 384 bit hash length	-
sha512	Secure Hash Algorithm 2 with 512 bit hash length	-

Result

The method for configuring the checksum is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase2` command.

You disable the use of the default list with the `no default-ciphers` command.

11.4.8.6 esp-encryption**Description**

With this command, you configure the encryption algorithm.

Requirement

- The default list is not used.
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli (config-conn-phs2) #
```

Syntax

Call up the command with the following parameters:

```
esp-encryption {3des|aes128cbc|aes192cbc|aes256cbc|aes128ctr|aes192ctr|aes256ctr|  
aes128ccm16|aes192ccm16|aes256ccm16|aes128gcm16|aes192gcm16|aes256gcm16}
```

The parameters have the following meaning:

Parameter	Description	Phase 2	
		IKEv1	IKEv2
3des	Triple Data Encryption Standard	x	x
aes128cbc	Advanced Encryption Standard with 128 bits	x	x
aes192cbc	Advanced Encryption Standard with 192 bits	x	x
aes256cbc	Advanced Encryption Standard with 256 bits	x	x
aes128ctr	Advanced Encryption Standard with 128 bits in Counter mode	x	x
aes192ctr	Advanced Encryption Standard with 192 bits in Counter mode	x	x
aes256ctr	Advanced Encryption Standard with 256 bits in Counter mode	x	x
aes128ccm16	Advanced Encryption Standard with 128 bits in Counter mode using a 16 byte Integrity Check Value (ICV)	x	x
aes192ccm16	Advanced Encryption Standard with 192 bits in Counter mode using a 16 byte Integrity Check Value (ICV)	x	x
aes256ccm16	Advanced Encryption Standard with 256 bits in Counter mode using a 16 byte Integrity Check Value (ICV)	x	x
aes128gcm16	Advanced Encryption Standard with 128 bits in Galois Counter mode using a 16 byte Integrity Check Value (ICV)	x	x

Parameter	Description	Phase 2	
		IKEv1	IKEv2
aes192gcm16	Advanced Encryption Standard with 192 bits in Galois Counter mode using a 16 byte Integrity Check Value (ICV)	x	x
aes256gcm16	Advanced Encryption Standard with 256 bits in Galois Counter mode using a 16 byte Integrity Check Value (ICV)	x	x

x: is supported

-: is not supported

Result

The encryption algorithm is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase2` command.

You disable the use of the default list with the `no default-ciphers` command.

11.4.8.7 esp-keyderivation

Description

With this command, you configure the required Diffie-Hellmann group (DH) from which a key will be generated.

Requirement

- The default list is not used.
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs2)#
```

Syntax

Call up the command with the following parameters:

```
esp-keyderivation {none|dhgroup <1|2|5|14|15|16|17|18>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
none	No keys are exchanged and Perfect Forward Secrecy (PFS) is disabled	-
dhgroup	Diffie-Hellmann group (DH)	Specify the required Diffie-Hellmann group (DH). <ul style="list-style-type: none">• 1• 2• 5• 14• 15• 16• 17• 18

Result

The Diffie-Hellmann group (DH) is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase2` command.

You disable the use of the default list with the `no default-ciphers` command.

11.4.8.8 lifebyte

Description

With this command, you configure the data limit to specify the lifetime of the agreed keys. When the data limit is reached, the key is renegotiated.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs2)#
```

Syntax

Call up the command with the following parameters:

```
lifebyte <integer(0-4294967295)>
```


The parameter has the following meaning:

Parameter	Description	Range of values / note
integer	Data limit	Enter the data limit in bytes.

Result

The data limit is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase2` command.

11.4.8.9 lifetime

Description

With this command, you configure a period to specify the lifetime of the agreed keys. When the time expires, the key is renegotiated.

Requirement

You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs2)#
```

Syntax

Call up the command with the following parameters:

```
lifetime <min(10-16666666)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
min	Period	Specify the period of time in minutes.

Result

The period of time is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase2` command.

11.4.8.10 port

Description

With this command, you specify the port via which the VPN tunnel communicates.

Requirement

- The VPN connection region is assigned a VPN remote station.
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs2)#
```

Syntax

Call up the command with the following parameters:

```
port {all|range <number(0-65535)-number(0-65535)>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
all	Applies to all ports.	-
range	Keyword for port range	
number	Port range	Specify the start port. 0 ... 65535
number		Specify the end port. 0 ... 65535

Result

The port or port range is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase2` command.

You assign a VPN remote station to the VPN connection with the `rmend name` command.

11.4.8.11 proto

Description

With this command, you specify the protocol for which the VPN connection is valid.

Requirement

- The VPN connection region is assigned a VPN remote station.
- You are in the IPSEC PHASE configuration mode.

The command prompt is as follows:

```
cli(config-conn-phs2)#
```

Syntax

Call up the command with the following parameters:

```
proto {all|<integer(0-255)>}
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
all	Applies to all protocols.	-
integer	Protocol number	Enter the number for the required protocol. You will find list of the protocol numbers on the Internet pages of iana.org .

Result

The protocol is configured.

Further notes

You display this setting and other information with the `show ipsec conn-phase2` command.

You assign a VPN remote station to the VPN connection with the `rmend name` command.

11.5 Certificates

This section describes commands relevant for certificates.

11.5.1 Commands in the global configuration mode

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

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

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

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

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

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

11.5.1.1 certificate

Description

With this command, you change to the CERT 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:

```
certificate
```

Result

You are now in the CERT configuration mode.

The command prompt is as follows:

```
cli(config-cert)#
```

Further notes

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

11.5.2 Commands in the CERT configuration mode

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

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

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

11.5.2.1 The "show" commands

This section describes commands with which you display various settings.

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

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

show-idx

Description

The command lists the loaded certificates and their indexes.

Requirement

- Certificates are loaded.
- You are in the CERT configuration mode.

The command prompt is as follows:

```
cli(config-cert)#
```

Syntax

Call the command without parameter assignment:

```
show-idx
```

Result

The list is displayed.

show-info

Description

This command shows information on the relevant certificate. e.g. the serial number.

Requirement

- You are in the CERT configuration mode.

The command prompt is as follows:

```
cli(config-cert)#
```

Syntax

Call up the command with the following parameters:

```
show-info idx <number>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
idx	Number corresponding to a specific certificate.	Enter the required number. 1 ... 100

Result

The information on the certificate is displayed.

Further notes

You display the indexes of the certificate with the `show idx` command.

11.5.2.2 cacert

Description

With this command, you specify the corresponding revocation list for a CA certificate.

Requirement

- You are in the CERT configuration mode.

The command prompt is as follows:

```
cli(config-cert)#
```

Syntax

Call up the command with the following parameters:

```
cacert <idx number> uri {first|second} <URL>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
idx number	Number corresponding to a specific certificate.	Enter the required number. 1 ... 100
uri	Keyword for the URL	-
first	Certificate revocation list 1st URL	-
second	Certificate revocation list 2nd URL	-
URL	Enter the URL with which the revocation list can be called up. Enter an alternative URL. If the revocation list cannot be called up using the 1st URL, the alternative URL is used.	Can only be edited if supported by the certificate.

Result

The revocation list for the corresponding CA certificate is specified.

Further notes

You show the available certificates with the `show-idx` command.

You display the use of the certificate with the `show-info` command.

11.5.2.3 del

Description

With this command, you delete a specific certificate or all certificates.

Requirement

- Certificates are loaded and are not being used anywhere.
- You are in the CERT configuration mode.

The command prompt is as follows:

```
cli(config-cert)#
```

Syntax

Call up the command with the following parameters:

```
del { <idx number> | all }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
<code>idx number</code>	Number corresponding to a specific certificate.	Enter the required number. 1 ... 100
<code>all</code>	Deletes all certificates.	---

Result

The relevant certificate is deleted.

Further notes

You load certificates with the `tftp load` command.

You show the available certificates with the `show-idx` command.

You display the use of the certificate with the `show-info` command.

11.5.2.4 passphrase

Description

With this command, you specify the password for the relevant certificate.

Requirement

- You are in the CERT configuration mode.

The command prompt is as follows:

```
cli(config-cert)#
```

Syntax

Call up the command with the following parameters:

```
passphrase <idx number> <key>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
<code>idx number</code>	Number corresponding to a specific certificate.	Enter the required number. 1 ... 100
<code>key</code>	Value for the key	Specify a valid key.

Result

The password for the certificate is specified.

Further notes

You show the password-protected certificates with the command `passphrase show-idx`.

11.5.2.5 passphrase show-idx**Description**

The command lists the certificates that are password protected.

Requirement

- Certificates are loaded.
- You are in the CERT configuration mode.

The command prompt is as follows:

```
cli(config-cert)#
```

Syntax

Call the command without parameter assignment:

```
passphrase show-idx
```

Result

The list is displayed.

Further notes

You configure the password with the `passphrase` command.

11.6 OpenVPN

This section describes commands relevant for OpenVPN client.

11.6.1 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.

11.6.1.1 show openvpn authentication

Description

This command shows the security settings of the OpenVPN connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show openvpn authentication
```

Result

The settings are displayed.

11.6.1.2 show openvpn connections

Description

This command shows the configuration of the OpenVPN connections.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show openvpn connections
```

Result

The configurations are displayed.

11.6.1.3 show openvpn remoteend

Description

This command shows the configuration of the remote stations (VPN end point).

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameter assignment:

```
show openvpn remoteend
```

Result

The configurations are displayed.

11.6.2 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.

11.6.2.1 openvpn

Description

With this command, you change to the OPENVPN 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:

```
openvpn
```

Result

You are now in the OPENVPN configuration mode.

The command prompt is as follows:

```
cli(config-openvpn)#
```

Further notes

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

11.6.3 OPENVPN configuration mode

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

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

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

11.6.3.1 connection name

Description

With this command, you change to the OPENVPN CONNECTION configuration mode. If a suitable OpenVPN connection does not exist, an Open VPN connection is first created.

Requirement

You are in the OPENVPN configuration mode.

The command prompt is as follows:

```
cli(config-openvpn)#
```

Syntax

Call up the command with the following parameters:

```
connection name <string(128)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
string	Name of the OpenVPN connection	Enter the name for the OPENVPN connection. Maximum of 128 characters

Result

You are now in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-ov-conn-X)#
```

Further notes

You exit the OPENVPN CONNECTION configuration mode with the `end` or `exit` command.

You delete all OpenVPN connections with the `no conn name` command.

You show the configuration of the OpenVPN connection with the `show openvpn connctions` command.

11.6.3.2 no conn

Description

With this command, you delete a specific OpenVPN connection or all OpenVPN connections.

Requirement

- The corresponding OpenVPN connection has been created and is not being used anywhere.
- You are in the OPENVPN configuration mode.

The command prompt is as follows:

```
cli(config-openvpn)#
```

Syntax

Call up the command with the following parameters:

```
no conn {name <name(128)> | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Keyword for the OpenVPN connection	-
string	Deletes the specified OpenVPN connection	Enter a valid name. Max. 128 characters
all	Deletes all OpenVPN connections	-

Result

The corresponding OpenVPN connection is deleted.

Further notes

You display the OpenVPN connection with the `connection name` command.

You display the available OpenVPN connections with the `show conn-names` command.

11.6.3.3 remote name

Description

With this command, you change to the OPENVPN REMOTE END configuration mode. In this mode, you configure the other settings.

If the matching OpenVPN partner station does not exist, the OpenVPN partner station is first created.

Requirement

You are in the OPENVPN configuration mode.

The command prompt is as follows:

```
cli (config-openvpn) #
```

Syntax

Call up the command with the following parameters:

```
remote name <name(128)>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
name	Name of the OpenVPN partner station	Enter the name for the OpenVPN partner station. Maximum of 128 characters

Result

You are now in the OPENVPN REMOTE END configuration mode.

The command prompt is as follows:

```
cli (config-openvpn-rm-X) #
```

X is a placeholder for the name

Further notes

You exit the OpenVPN REMOTE END configuration mode with the `end` or `exit` command.

You delete all VPN partner stations with the `no remote` command.

11.6.3.4 no remote

Description

With this command, you delete a specific OpenVPN partner station or all OpenVPN partner stations.

Requirement

- The corresponding OpenVPN partner station has been created and is not being used anywhere.
- You are in the OPENVPN configuration mode.

The command prompt is as follows:

```
cli(config-openvpn)#
```

Syntax

Call up the command with the following parameters:

```
no remote {name <name(128)> | all}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Keyword for the OpenVPN partner station	-
name	Deletes the specified OpenVPN partner station	Enter a valid name. Max. 128 characters
all	Deletes all OpenVPN partner stations	-

Result

The corresponding VPN partner station is deleted.

Further notes

You create an OpenVPN partner station with the `remote name` command.

11.6.3.5 shutdown

Description

With this command, you disable OpenVPN.

Requirement

You are in the OPENVPN configuration mode.

The command prompt is as follows:

```
cli (config-openvpn) #
```

Syntax

Call the command without parameter assignment:

```
shutdown
```

Result

OpenVPN is disabled

Further notes

You enable the OpenVPN with the `no shutdown` command.

11.6.3.6 no shutdown

Description

With this command, you enable OpenVPN.

Requirement

You are in the OPENVPN configuration mode.

The command prompt is as follows:

```
cli (config-openvpn) #
```

Syntax

Call the command without parameter assignment:

```
no shutdown
```

Result

OpenVPN is enabled

Further notes

You disable OpenVPN with the `shutdown` command.

11.6.4 Commands in the OPENVPN REMOTE END configuration mode

This section describes commands that you can call up in the OPENVPN REMOTE END configuration mode.

In the OPENVPN configuration mode, enter the `remote end name` command to change to this mode.

- If you exit the OPENVPN REMOTE END configuration mode with the `exit` command, you return to the OPENVPN configuration mode.
- If you exit the OPENVPN REMOTE END configuration mode with the `end` command, you return to the Privileged EXEC mode.

11.6.4.1 connection

Description

With this command, you specify the OpenVPN connection for the OpenVPN partner station.

Requirement

You are in the OPENVPN REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-rm-X) #
```

Syntax

Call up the command with the following parameters:

```
connection <name>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
name	Name of the OpenVPN connection	Enter a valid name. Maximum of 128 characters

Result

The OpenVPN connection has been changed.

Further notes

You display this setting and other information with the `show openvpn remoteend` command.

11.6.4.2 port

Description

With this command, you specify the port via which the VPN tunnel communicates.

Requirement

You are in the OPENVPN REMOTE END configuration mode.

The command prompt is as follows:

```
cli (config-openvpn-rm-X) #
```

Syntax

Call up the command with the following parameters:

```
port <1-65535>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
-	Port number	Enter a valid port number. 1 ... 65535

Result

The port is specified.

Further notes

You display this setting and other information with the `show openvpn remoteend` command.

11.6.4.3 proto

Description

With this command, you change the protocol that is set.

Requirement

- The proxy server is configured.
- You are in the OPENVPN REMOTE END configuration mode.

The command prompt is as follows:

```
cli (config-openvpn-rm-X) #
```

Syntax

Call up the command with the following parameters:

```
proto {udp|tcp [proxy <string (255)>]}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
udp	UDP protocol	-
tcp	TCP protocol	-
proxy	Keyword for the proxy server with which the OpenVPN tunnel is established to the defined OpenVPN partner.	-
string	Name of the proxy server Provided that the TCP protocol is used and that the proxy server has been created.	Specify the proxy server. Maximum of 255 characters.

Result

The protocol has been changed.

Further notes

You display this setting and other information with the `show openvpn remoteend` command.

11.6.4.4 proxy

Description

With this command you specify whether the OpenVPN tunnel to the defined OpenVPN partner is established via a proxy server.

Requirement

- The proxy server is configured.
- You are in the OPENVPN REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-rm-X)#
```

Syntax

Call up the command with the following parameters:

```
proxy <name>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
name	Proxy server name	Specify the proxy server name. Max. 128 characters

Result

The proxy server via which the connection is established is configured.

Further notes

You display this setting and other information with the `show openvpn remoteend` command.

11.6.4.5 remote-addr

Description

With this command you configure the WAN IP address or the DNS host name of the OpenVPN partner.

Requirement

You are in the OPENVPN REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-rm-X) #
```

Syntax

Call up the command with the following parameters:

```
remote-addr <ipaddr|dns>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ipaddr	WAN IP address	Specify a valid IP address.
dns	DNS host name	Specify the DNS host name.

Result

The address is configured.

Further notes

You display this setting and other information with the `show openvpn remoteend` command.

11.6.4.6 show-context

Description

This command shows the available OpenVPN partner stations.

Requirement

You are in the OPENVPN REMOTE END configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-rm-X) #
```

Syntax

Call the command without parameter assignment:

```
show context
```

Result

The names of the OpenVPN partner stations are listed.

11.6.5 Commands in the OPENVPN CONNECTION configuration mode

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

In the OPENVPN configuration mode, enter the `connection name` command to change to this mode.

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

11.6.5.1 auth-algo

Description

With this command you specify the method for calculating the checksum.

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X)#
```

Syntax

Call up the command with the following parameters:

```
auth-algo {sha1|sha224|sha384|sha256|sha512|md5}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
sha1	Secure Hash Algorithm 1	-
sha224	Secure Hash Algorithm 224	-
sha384	Secure Hash Algorithm 384	-
sha256	Secure Hash Algorithm 256	-
sha512	Secure Hash Algorithm 512	-
md5	Message Digit Algorithm 5	-

Result

The method is specified.

Further notes

You display this setting and other information with the `show openvpn connections` command.

You display the available OpenVPN connections with the `show auth-names` command.

11.6.5.2 authentication

Description

With this command, you change to the OPENVPN AUTHENTICATION configuration mode.

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X) #
```

Syntax

Call the command without parameter assignment:

```
authentication
```

Result

You are now in the OPENVPN AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli((config-openvpn-conn-auth) #
```

Further notes

You exit the OPENVPN AUTHENTICATION configuration mode with the `end` or `exit` command.

11.6.5.3 autoFW

Description

With this command, you configure the setting for the firewall of the OpenVPN connection .

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X) #
```

Syntax

Call up the command with the following parameters:

```
autoFW {enabled|disabled}
```


The parameters have the following meaning:

Parameter	Description	Range of values / note
enabled	The firewall rules are created automatically for the OpenVPN connection.	-
disabled	You will need to create the suitable firewall rules yourself.	-

Result

The setting is configured.

Further notes

You display this setting and other information with the `show openvpn connections` command.

You display the available OpenVPN connections with the `show auth-names` command.

11.6.5.4 encryp-algo

Description

With this command, you configure the encryption algorithm of the OpenVPN connection.

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X) #
```

Syntax

Call up the command with the following parameters:

```
encryp-algo {bfcbc|aes128cbc|aes192cbc|aes256cbc|desede3}
```

The parameters have the following meaning:

Parameter	Description
bfcbc	Blowfish
aes128cbc	Advanced Encryption Standard with 128 bits
aes192cbc	Advanced Encryption Standard with 192 bits
aes256cbc	Advanced Encryption Standard with 256 bits
desede3	DES-EDE3: Data Encryption Standard 192 bit key length

Result

The setting is configured.

Further notes

You display this setting and other information with the `show openvpn connections` command.

You display the available OpenVPN connections with the `show auth-names` command.

11.6.5.5 NAT**Description**

With this command, you configure the "IP masquerading" setting.

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X)#
```

Syntax

Call up the command with the following parameters:

```
NAT {enabled|disabled}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
enabled	Enables the "IP masquerading" setting	-
disabled	Disables the "IP masquerading" setting	-

Result

The setting is configured.

Further notes

You display this setting and other information with the `show openvpn connections` command.

You display the available OpenVPN connections with the `show auth-names` command.

11.6.5.6 operation

Description

With this command you specify how the connection is established.

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X)#
```

Syntax

Call up the command with the following parameters:

```
operation {disabled|start|start-di|start-sms}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
disabled	The VPN connection is disabled.	Default
start	The device attempts to establish a VPN connection to the partner.	-
start-di	If the event "Digital In" occurs the device attempts to establish a VPN connection to the partner. This is on condition that the event "Digital In" is passed on to the VPN connection.	-
start-sms	M874, M876 only When the device receives a command SMS, the device waits until the connection establishment is initiated by the partner. This assumes that the device accepts a command SMS of the class "System" from certain senders.	-

Result

The setting is configured.

Further notes

You display this setting and other information with the `show openvpn connections` command.

You display the available OpenVPN connections with the `show auth-names` command.

11.6.5.7 LZO

Description

With this command, you configure the LZO setting of the OpenVPN connection .

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X)#
```

Syntax

Call up the command with the following parameters:

```
LZO {yes|no|adaptive}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
yes	The data is compressed with the LZO algorithm.	-
no	The data is not compressed.	-
adaptive	Adaptive compression with which the OpenVPN stack regularly checks the compression. When the effect of the compression is slight, the compression is turned off and activated again in a later check.	

Result

The setting is configured.

Further notes

You display this setting and other information with the `show openvpn connections` command.

You display the available OpenVPN connections with the `show auth-names` command.

11.6.5.8 no LZO

Description

With this command, you disable the LZO setting of the OpenVPN connection.

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X)#
```

Syntax

Call the command without parameter assignment:

```
no LZO
```

Result

The LZO setting of the OpenVPN connection is disabled.

Further notes

You configure the LZO setting of the OpenVPN connection with the `LZO` command.

11.6.5.9 show auth-names**Description**

This command displays which method is used to calculate the checksum of which OpenVPN connection.

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X)#
```

Syntax

Call the command without parameter assignment:

```
show auth-names
```

Result

The use is listed.

Further notes

You create an OpenVPN connection with the `connection name` command.

11.6.5.10 show context

Description

This command shows the available OpenVPN connections.

Requirement

You are in the OPENVPN CONNECTION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-X)#
```

Syntax

Call the command without parameter assignment:

```
show context
```

Result

The names of the OpenVPN connections are listed.

Further notes

You create an OpenVPN connection with the `connection name` command.

11.6.6 Commands in the OPENVPN AUTHENTICATION configuration mode

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

In the OPENVPN CONNECTION configuration mode, enter the `authentication` command to change to this mode.

- If you exit the OPENVPN AUTHENTICATION configuration mode with the `exit` command, you return to the OPENVPN CONNECTION configuration mode.
- If you exit the OPENVPN AUTHENTICATION configuration mode with the `end` command, you return to the Privileged EXEC mode.

11.6.6.1 auth

Description

With this command you specify that a certificate will be used for authentication.

Requirement

- The relevant certificate is loaded.
- You are in the OPENVPN AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-auth)#
```

Syntax

Call up the command with the following parameters:

```
auth cacert <name(255)> macert <name(255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
-	Certificate selection	<ul style="list-style-type: none">• <code>cacert</code>: CA certificate• <code>macert</code>: Machine certificate
<code>name</code>	Name of the CA or machine certificate	Specify the certificate name.

Result

The certificate is specified.

Further notes

You display this setting and other information with the `show openvpn authentication` command.

You delete the authentication with the `no auth` command.

11.6.6.2 no auth

Description

With this command, you delete the authentication method.

Requirement

You are in the OPENVPN AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli(config-openvpn-conn-auth) #
```

Syntax

Call the command without parameter assignment:

```
no auth
```

Result

The authentication method is deleted.

11.6.6.3 auth user

Description

With this command, you configure the user name and the password for the CA certificate.

Requirement

You are in the OPENVPN AUTHENTICATION configuration mode.

The command prompt is as follows:

```
cli (config-openvpn-conn-auth) #
```

Syntax

Call up the command with the following parameters:

```
auth cacert <string(255)> user <string(255)> pw <string(255)>
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
cacert	Keyword for CA certificate	-
string	CA certificate	Specify the name of the CA certificate. Maximum of 255 characters
user	Keyword for the user name	-
string	User names	Specify the user name. Maximum of 255 characters
pw	Keyword for the password	-
string	Password	Enter the password. Maximum of 255 characters

Result

The user data is configured.

Further notes

You display this setting and other information with the `show openvpn authentication` command.

You delete the authentication with the `no auth` command.

Diagnostics

The monitoring of the system and error diagnostics are handled in different ways:

- Event and fault handling:
Predefined events generate a message. These messages can be distributed in different ways:
 - Entry in local logs
 - Transfer to the Syslog server
 - Sending as SNMP trap
 - Lighting up of the error LED
 - Switching at the digital output
- Syslog client:
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 The "show" commands

This section describes commands with which you display various settings.

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

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

12.1.1.1 **show 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.

12.1.1.2 **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.

12.1.1.3 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:

Parameter	Description
power	Monitoring of the power supply for power outage
link	Monitoring of the network connections for a change in the connection status

If no parameters are specified, the settings for both error monitoring functions are displayed.

Result

The current configuration of the selected error monitoring function is displayed.

12.1.1.4 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.

12.1.1.5 show fault counter**Description**

This command shows the number of errors since the last startup.

Requirement

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

The command prompt is as follows:

```
cli> or cli#
```

Syntax

Call the command without parameters:

```
show fault counter
```

Result

The number of faults is displayed.

Further notes

You reset the counter for the errors with the `clear fault counter` command.

12.1.1.6 show fwlog

Description

With this command, you show the messages that occurred in the firewall. The messages can be filtered according to the event severity.

Requirement

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 fwlog [{ info | warning | critical }]
```

Parameter

The parameters have the following meaning:

Parameter	Description	Range of values / note
info	Information	-
warning	Warnings	-
critical	Critical messages	-

If you use the command without setting parameters, all messages are displayed.

Result

The content of the firewall log is displayed.

12.1.1.7 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 categories "Information", "Warning" and "Critical" are displayed.
warning	All log entries of the categories "Warning" and "Critical" are displayed.
critical	All log entries of the category "Critical" are displayed.

Result

The content of the logbook is displayed.

12.1.1.8 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.

12.1.1.9 show seclog

Description

With this command, you show the messages that occurred during communication via a secure VPN tunnel. The messages can be filtered according to the event severity.

Requirement

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 seclog [{ info | warning | critical }]
```

Parameter

The parameters have the following meaning:

Parameter	Description	Range of values / note
info	Information	-
warning	Warnings	-
critical	Critical messages	-

If you use the command without setting parameters, all messages are displayed.

Result

The content of the security log is displayed.

12.1.2 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.

12.1.3 clear fwlog**Description**

With this command, you delete the content of the firewall log.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
clear fwlog
```

Result

The content of the firewall log is deleted.

12.1.4 clear logbook

Description

With this command, you delete the content of the logbook.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
clear logbook
```

Result

The content of the logbook is deleted.

12.1.5 clear seclog

Description

With this command, you delete the content of the security log.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call the command without parameters:

```
clear seclog
```

Result

The content of the security log is deleted.

12.1.6 fault report ack

Description

Some errors can be acknowledged and thus removed from the error list, e.g. an error of the event "Cold/warm restart".

With this command, you can acknowledge these errors or remove them from the error list.

Requirement

You are in the Privileged EXEC mode.

The command prompt is as follows:

```
cli#
```

Syntax

Call up the command with the following parameter:

```
fault report ack <fault-state-id>
```

The parameter has the following meaning:

Parameters	Description	Range of values/note
fault-state-id	Error ID	Enter the ID of the error. You determine the ID with the "show events faults status" command.

Result

The error is acknowledged and removed from the error list.

12.1.7 no logging console

Description

With this command, you disable the logging of inputs and outputs to 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 logging function is disabled on the console.

Further notes

You enable the setting with the `logging console` command.

As default the function is "disabled".

12.1.8 logging console

Description

With this command, you enable the logging of inputs and outputs to 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:

```
logging console
```

Result

The logging function is enabled on the console.

Further notes

You disable the setting with the `no logging console` command.

As default the function is "disabled".

12.1.9 Commands in the global configuration mode

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

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

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

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

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

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

12.1.9.1 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`.

12.1.10 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.

12.1.10.1 add log

Description

With this command, you create an entry in the 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>
```

The parameter has the following meaning:

Parameter	Description	Range of values / note
log-entry	Entry in the logbook	max. 150 characters

Result

The entry has been made in the logbook.

12.1.10.2 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-mail

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:

```
client config {syslog|trap|email|all}
```

The parameters have the following meaning:

Parameter	Description
<code>syslog</code>	Enables the client that sends the messages to the Syslog server
<code>trap</code>	Enables the client that sends the SNMP traps
<code>email</code>	Enables the client that sends the e-mails
<code>all</code>	Enables all clients at once

Result

The function of the client selected for the transfer is enabled.

Further 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.

12.1.10.3 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 the 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 transfer is disabled.

Further 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.

12.1.10.4 event config

Description

With this command, you configure which of the various message types of the device will be stored or forwarded.

The following events or message types are available:

- Message if there is cold or warm restart
- Message when there is a status change on a physical interface
- Message if there is an incorrect login
- Message when there is a status change in the power supply
- Message when there is a status change in the error monitoring
- Message when using VPN
- Message when using firewall rules
- Message when changing the connection status
- Message on connection establishment and when the configuration changes
- Message when there is a status change of the digital input.
- Message on error in connection with secure NTP
- Message on persistent saving of configuration
- Message on non-configurable entry in the log table

These messages can be processed by the clients in different ways:

- Entry in the logbook of the device
- Sending the message to the Syslog server of the system
- Sending an e-mail
- Sending an SNMP trap
- Lighting up of the error LED
- Switching at the digital output

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:

```
event config { cold-warmstart | linkchange | authentication-failure | faultstate-
change | security-log | firewall-log | ddns-client-log | system-general-log | system-
connection-status | digital-in | vpn-tunnel | secure-ntp | config-change| service-
information | all} {logtable | syslog | email | trap | faults | sms | digital-out |
vpn-tunnel | 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
faultstate-change	Message when there is a status change in the error monitoring
security-log	Message when using IPsec
firewall-log	Message when using a firewall rule
ddns-client-log	Message when synchronizing the DDNS client with the host name registered with the DDNS provider.
system-general-log	Message on connection establishment and when the configuration changes
system-connection-status	Message when there is a status change of the connection
digital-in	Message when the digital input changes.
vpn-tunnel	Message if VPN changes (IPsec, OpenVPN, SINEMA RC)
secure-ntp	Message when the device receives the system time from a secure NTP server.
config-change	Message on persistent saving of configuration
service-information	Message on non-configurable entry in the log table
all	All messages
logtable	Client that processes the log entries
syslog	Client that sends the messages to the Syslog server
email	Client that sends the e-mails
trap	Client that sends the SNMP traps
faults	Error LED lights up. The setting is possible only for a cold or warm restart.
digital-out	Controls the digital output or signals the status change with the "DO" LED.
firewall	Executes the user-defined rule set.
vpn-tunnel	Controls the VPN connection (establishment/termination).
all	All clients at once

Result

The setting deciding which message of the device is stored or forwarded is configured.

Further notes

You display the status of the events and the clients with the `show events config` command.

You delete the settings with the `no event config` command.

With this command, the clients are not enabled.

To enable the clients, use the `client config` command.

Note

Changing several message types or clients

With each command call, you can only select one message type and one client.

If you want to process several message types or clients, it may be more efficient to first select the `all` option and then disable individual elements.

12.1.10.5 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 the 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 | faultstate-  
change | security-log | firewall-log | ddns-client-log | system-general-log | system-  
connection-status | digital-in | vpn-tunnel | secure-ntp | config-change | service-  
information | all } { logtable | syslog | email | trap | faults | sms | digital-out |  
vpn-tunnel | firewall | 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
faultstate-change	Message when there is a status change in the error monitoring
security-log	Message when using IPsec
firewall-log	Message when using a firewall rule
ddns-client-log	Message when synchronizing the DDNS client with the host name registered with the DDNS provider.
system-general-log	Message on connection establishment and when the configuration changes
system-connection-status	Message when there is a status change of the connection
digital-in	Message when the digital input changes.
vpn-tunnel	Message if VPN changes (IPsec, OpenVPN, SINEMA RC)
secure-ntp	Message when the device receives the system time from a secure NTP server.
config-change	Message on persistent saving of configuration
service-information	Message on non-configurable entry in the log table
all	All messages
logtable	Client that processes the log entries
syslog	Client that sends the messages to the Syslog server
email	Client that sends the e-mails

Parameter	Description
trap	Client that sends the SNMP traps
faults	Error LED lights up. The setting is possible only for a cold or warm restart.
digital-out	Controls the digital output or signals the status change with the "DO" LED.
vpn-tunnel	Controls the VPN connection (establishment/termination).
firewall	Executes the user-defined rule set.
all	All clients at once

Result

The setting deciding which messages of the device are not stored or forwarded is configured.

Further 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.

12.1.10.6 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 the EVENTS Configuration mode.

The command prompt is as follows:

```
cli(config-events)#
```

Syntax

Call up the command with the following parameters:

```
link {up|down}
```

The parameters have the following meaning:

Parameters	Description	Range of values / note
up	Only the establishment of a connection is signaled	-
down	Only a break on a connection is signaled	-

Result

The settings for monitoring the physical network connections have been configured.

Further notes

You can display the current setting with the `show events faults config` command.

You disable the function with the `no link` command.

12.1.10.7 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 the 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}
```

The parameters have the following meaning:

Parameters	Description	Range of values / note
up	The message when establishing a connection is disabled	-
down	The message when a connection is down is disabled	-

Result

The settings for monitoring the physical network connections have been configured.

Further notes

You can display the current setting with the `show events faults config` command.

You enable the function with the `link` command.

12.1.10.8 severity

Description

With this command, you configure the threshold values for the sending of system event notifications.

Requirement

You are in the EVENTS configuration mode.

The command prompt is as follows:

```
cli (config-events) #
```

Syntax

Call up the command with the following parameters:

```
severity {mail | log | syslog } {info | warning | critical }
```

The parameters have the following meaning:

Example

Parameter	Description	Range of values / note
mail	Specifies the threshold value for sending system event messages by e-mail.	-
log	Specifies the threshold value for entering system event messages in the log table.	Default
syslog	Specifies the threshold value for entering system event messages in the Syslog file.	-
info	The messages of all levels are sent or logged.	The messages of all levels are sent or logged.
warning	The message of this level and the "critical" level are sent or logged.	-
critical	Only the messages of this level are sent or logged.	-

Result

The settings 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 config`

12.1.10.9 no severity

Description

With this command, you disable the setting for the threshold values for the sending of system event notifications.

Requirement

You are in the EVENTS Configuration mode.

The command prompt is as follows:

```
cli (config-events) #
```

Syntax

Call up the command with the following parameters:

```
no severity { mail | log | syslog }
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
mail	The setting of the threshold value for sending system event messages by e-mail is disabled.	-
log	The setting of the threshold value for entering system event messages in the log table disabled.	-
syslog	The setting of the threshold value the entering event messages in the Syslog file is disabled.	-

If you do not select any parameters from the parameter list, the default value is used.

Result

The settings for sending system event messages are configured.

Further notes

You enable the setting with the `severity` command.

You display the status of this function and other information `show events severity`.

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 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.

12.2.2.1 syslogserver

Description

With this command, you configure the Syslog server address.

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:

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

The parameters have the following meaning:

Parameter	Description	Range of values / note
ipv4	Keyword for an IP address	-
ucast_addr	Syslog server IPv4 Address	Enter a valid IPv4 address.
fqdn-name	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters
port	Serverport	1 .. 65535 Default: 514

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

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.

Further notes

You disable the setting with the `no syslogserver` command.

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

12.2.2.2 no syslogserver

Description

With this command, you configure the Syslog server address.

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:

```
syslogserver {ipv4 <ucast_addr> | fqdn-name <FQDN>}
```

The parameters have the following meaning:

Parameter	Description	Range of values / note
ipv4	Keyword for an IP address	-
ucast_addr	Syslog server IPv4 Address	Enter a valid IPv4 address.
fqdn-name	Keyword for a domain name	-
FQDN	Domain name (Fully Qualified Domain Name)	Maximum of 100 characters

For information on identifiers of addresses and interfaces, refer to the section "Interface identifiers and addresses (Page 41)".

Result

The settings for the Syslog server are disabled.

Further notes

You enable the setting with the `syslogserver` command.

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

Index

A

- add log, 615
- addr, 147, 530
- Address of the gateway, 44
- addr-mode, 531
- aggressive, 550
 - no aggressive, 551
- alias, 80
 - no alias, 81
- auth, 598
 - no auth, 600
- auth cacert, 543
 - no auth, 546
- auth psk
 - no auth, 546
- auth psk, 544
- auth remcert, 545
 - no auth, 546
- auth user, 601
 - no auth, 600
- auth username
 - no auth username, 368
- auth usernamet, 367
- auth-algo, 591
- authentication, 536, 591
- autoenrollment interval, 148
- autoFW, 592
- autofwnat, 149
 - no autofwnat, 151
- auto-fwrules, 562
 - no auto-fwrules, 562
- auto-save, 109
 - no auto-save, 110

B

- base bridge mode, 198

C

- cacert, 574
- cachenxdomain, 309
 - no cachenxdomain, 309
- certificate, 572
- change password, 443

- clear counters, 66
- clear fault counter, 609
- clear fwlog, 610
- clear history, 55
- clear line vty, 67
- clear logbook, 611
- clear screen, 45
- clear seclog, 611
- clear spanning-tree counters, 247
- clear spanning-tree detected protocols, 246
- clear vrrp3 statistics, 387
- CLI commands
 - Symbolic representation, 40
- cli-console-timeout, 76
 - no cli-console-timeout, 77
- configure terminal, 67
- connection, 586
- connection name, 523, 581
 - no conn name, 582
 - no connection all, 525
 - no connection name, 524
- connection type, 150
- conn-mode, 532
- coordinates height, 72
- coordinates latitude, 72
- coordinates longitude, 73
- crl-policy, 522

D

- das delete, 116
- das discover interface, 112
- das mac blink, 115
- das mac ip, 114
- das mac name, 113
- dcp forwarding, 270
- dcp server, 262
 - no dcp server, 263
- ddnsclient, 304
- default-ciphers, 552, 563
 - no default-ciphers, 553, 564
- del (Certificate), 575
- delete, 94
- device id, 152
- device pw, 153
- digital output close, 131
- digital output open, 132
- di-input set address, 465

- di-input set ruleset, 466
- di-input show-idx, 467
- disable, 68
- dnsclient, 303
- dnsproxy, 303
- do, 46
- dpd, 554
 - no dpd, 554
- dpd-period, 555
- dpd-timeout, 556
- duplex, 82
 - no duplex, 83

E

- enable, 69
- encryp-algo, 593
- esp-auth, 565
- esp-encryption, 566
- esp-keyderivation, 567
- event config, 618
 - no event config, 621
- events, 614
- exit, 48

F

- factoryclean, 125
- fault report ack, 612
- firewall, 353, 462
- firewallnat, 411
- firmware-on-plug, 124
 - no firmware-on-plug, 124
- flowcontrol, 381
- forced disconnect, 227
- forced disconnect time, 228

G

- Glossary, 4
- grep, 51

H

- help, 49

I

- icmp name
 - no icmp, 469

- icmp name set type, 469
- icmp name type, 467
- icmp show-names, 471
- icmp show-types-codes, 471
- idle timeout icmp, 472
- idle timeout tcp, 472
- idle timeout udp, 473
- ike-auth, 557
- ike-encryption, 557
- ike-keyderivation, 559
- ike-keytries, 560
- ike-lifetime, 560
- interface, 74
 - no interface, 75
- interface (VRRP3), 392
 - no interface, 393
- interface ppp, 226
- interface range, 199
 - no interface range, 200
- interface vlan, 229
- interval, 143
- ip address, 217, 229, 230, 271, 272
 - no ip address, 231, 273
- ip dhcp client mode, 279, 280
- ip dhcp config-file-request, 277
 - no ip dhcp config-file-request, 278
- ip dhcp-server, 283
 - no ip dhcp-server, 284
- ip dhcp-server icmp-probe, 286
 - no ip dhcp-server icmp-probe, 285
- ip dhcp-server pool
 - no ip dhcp-server pool, 288
- ip dhcp-server pool, 287
- ip echo-reply, 263
 - no ip echo-reply, 264
- ip http, 347, 350
 - no ip http, 348
- ip http https redirection, 351
- ip route, 265
 - no ip route, 266
- ip routing, 267
- ipsec, 522
- ipsec connection show-idx, 412
- IPv4
 - Notation, 43
 - IPv4 address, 43
 - ipv4rule, 474, 480
 - no ipv4rule, 477
 - ipv4rule ipsec connection, 487
 - ipv4rule set, 486
 - ipv4rule set action, 477, 478
 - ipv4rule set dstip, 479

- ipv4rule set log, 481
- ipv4rule set prior, 482
- ipv4rule set ruleset, 483
- ipv4rule set service, 484
- ipv4rule set srcip, 485
- ipv4rule show interfaces, 488
- ipv4rule show-rules, 489
- ipv6 unicast-routing, 268

K

- k-proto, 536

L

- lease time, 289
- lifebyte, 568
- lifetime, 569
- link, 622
 - no link, 623
- lldp, 83
 - no lldp, 84
- load tftp, 91
- loadsave, 93
- local-id, 546
 - no local-id, 547
- loc-subnet, 537
- login authentication, 435
- loginpage, 445
- logon, 136
 - no logon, 136
- logon idx authority, 137
- logon idx fragment, 138
- logon idx path, 139
- logon idx query, 140
- logon show-idx, 141
- logout, 70
- LZO, 596

M

- mac-address-table aging, 384
 - no mac-address-table aging, 385
- mac-address-table aging-time, 386
- manual srv, 305
 - no manual srv, 306
- map protocol, 201
 - no map protocol, 202
- masquerading, 414
 - no masquerading, 415
- masquerading show-idx, 413

- mtu, 207

N

- name, 219
 - no name, 220
- napt show-idx, 416
- napt type ipv4, 416
 - no napt, 418
 - no napt all, 419
- NAT, 594
- nat-keep-alive, 525
- negotiation, 85
 - no negotiation, 86
- netmap destination type ipv4, 420
 - no netmap, 425
 - no netmap all, 426
- netmap show-idx, 422
- netmap source type ipv4, 423
 - no netmap, 425
 - no netmap all, 426
- network, 290
- no ip address, 218
- no login authentication, 436
- no LZO, 596
- no passive listening, 239
- no passive-listening bpdu-vlan-flood, 237
- no role, 448
- no sinema, 119
- no snmp filterprofile, 331
- no user-account-ext, 454
- no user-group, 455
- ntp, 171
- ntp secure, 175
 - no ntp secure, 176
- ntp server, 179
 - no ntp server, 179
- ntp server id, 172
 - no ntp server id, 173
- ntp server interface, 180
 - no ntp server interface, 182
- ntp server secure, 174
- ntp server secure interface, 183
 - no ntp server secure interface, 184
- ntp time diff, 176

O

- openvpn, 580
- operation, 538, 595

- option, 291
 - no option, 295
- option value-hex, 293
- option value-string, 294
 - no option, 295, 295

P

- panel-button control-restart, 160
 - no panel-button-restart, 161
- passive listening, 238
- passive-listening bpdu-vlan-flood, 237
- passphrase, 576
- passphrase show-idx, 577
- password, 102, 232, 315
 - no password, 103
- password policy, 446
- phase, 539
- ping, 70
- plug, 122
- pool-enable, 296
 - no pool-enable, 297
- port, 154, 369, 570, 587
 - no port, 370
- ports, 221
 - no ports, 222
- prerule all ipv4, 489
- prerule cloudconnector ipv4, 490
- prerule dhcp ipv4, 491
- prerule dns ipv4, 492
- prerule http ipv4, 493
- prerule https ipv4, 494
- prerule ipsec ipv4, 495
- prerule ipv4 show-int, 496
- prerule ping ipv4, 497
- prerule snmpm ipv4, 498
- prerule ssh ipv4, 499
- prerule systime ipv4, 500
- prerule telnet ipv4, 501
- presetplug, 123
- proto, 571, 587
- proto name, 502
 - no proto, 503
- proto show-names, 503
- protocol-vlan, 203
 - no protocol-vlan, 203
- proxy, 155, 588
 - no proxy, 156
- proxyserver, 353

R

- radius authorization-mode, 436
- radius server, 437
 - no radius-server, 439
- Range of values for IPv4 address, 43
- receiver-address, 370
 - no receiver-address, 371
- rem-id, 548
- rem-id
 - no rem-id, 549
- remote name, 583
 - no remote, 584
- remote-addr, 589
- remote-end name, 526
 - no remote-end all, 528
 - no remote-end name, 527
- restart, 104
- rmend name, 539
- role, 441, 447
- router vrrp3, 391
 - no router vrrp3, 391
- ruleset
 - no ruleset, 507
- ruleset name, 505
- ruleset show-idx, 506
- ruleset idx, 504

S

- save filetype, 92
- Scope of the manual, 3
- security, 372
 - no security, 372
- send test mail, 365
- sender-address, 373
 - no sender address, 374
- serv name
 - no srv, 355
- server type, 306
- service, 312
 - no service, 312
- Service & Support, 4
- service name, 508
 - no service, 509
- service name set dst, 510
- service name set prot, 511
- service name set src, 512
- service show-names, 513
- set-interface, 298
- severity, 624
 - no severity, 625

sftp filename, 98
sftp load, 99
sftp save, 100
sftp server, 101
show auth-names, 597
show cli-console-timeout, 58
show context, 590, 598
show coordinates, 58
show das info, 111
show dcp forwarding, 258
show dcp server, 259
show ddnsclient overview, 302
show device information, 59
show digital input, 130
show digital output, 131
show dnsclient information, 301
show dst info, 163
show events config, 604
show events faults config, 605
show events faults status, 605
show events sender email, 363
show events severity, 604
show events smtp-port, 364
show events smtp-server, 363
show events syslogserver, 626
show fault counter, 606
show firewall icmp-services ipv4, 458
show firewall information, 458
show firewall ip-protocols, 459
show firewall ip-rules ipv4, 459
show firewall ip-services, 460
show firewall pre-rules ipv4, 460
show firewall ruleset, 461
show firewall ruleset assignment, 461
show firewallnat masquerading, 409
show firewallnat napt, 409
show firewallnat netmap, 410
show firewallnat src-nat, 410
show flow-control, 379
show fwlog, 607
show history, 56
show in, 61
show interface mtu, 61
show interfaces, 60
show interfaces ... counters, 62
show ip arp, 274
show ip dhcp client, 276
show ip dhcp server pools, 282
show ip dhcp-server bindings, 282
show ip dns, 257
show ip http secure server status, 349
show ip http server status, 346
show ip interface, 64
show ip route, 259
show ip routing, 260
show ip ssh, 376
show ip static route, 261
show ip telnet, 261
show ipsec conn-authentication, 518
show ipsec connections, 519
show ipsec conn-phase1, 519
show ipsec conn-phase2, 520
show ipsec information, 520
show ipsec remoteend, 521
show lldp neighbors, 63
show lldp status, 63
show loadsave files, 89
show loadsave sftp, 90
show loadsave tftp, 90
show logbook, 607
show mac-address-table aging-status, 383
show mac-address-table aging-time, 382
show ntp info, 170
show ntp server info, 178
show openvpn authentication, 578
show openvpn connections, 579
show openvpn remoteend, 579
show passive-listening, 236
show password-policy, 440
show plug, 121
show power-line-state, 608
show ppp information, 225
show proxyserver table, 352
show radius server, 434
show radius statistics, 433
show running-config, 106
show seclog, 609
show sinema, 117
show sinemarc, 145
show snmp, 317
show snmp community, 317
show snmp engineID, 318
show snmp filter, 318
show snmp group, 319
show snmp group access, 319
show snmp inform statistics, 320
show snmp notif, 320
show snmp targetaddr, 321
show snmp targetparam, 321
show snmp tcp, 322
show snmp user, 322
show snmp viewtree, 323
show snmp broadcast-mode status, 185
show snmp status, 186

- show snmp unicast-mode status, 186
- show spanning-tree, 240
- show spanning-tree active, 241
- show spanning-tree bridge, 242
- show spanning-tree detail, 243
- show spanning-tree interface, 243
- show spanning-tree interface layer2-gateway-port, 244
- show spanning-tree root, 245
- show srs, 133
- show srs overview, 134
- show ssl server-cert, 349
- show time, 164
- show user-accounts, 441
- show user-groups, 442
- show users, 443
- show versions, 65
- show vlan, 193
- show vlan device info, 194
- show vlan learning params, 195
- show vlan port config, 196
- show vlan protocols-group, 197
- show vrrp3, 388
- show vrrp3 interface, 389
- show vrrp3 track, 390
- show web-session-timeout, 127
- show-idx, 573
- show-info (Certificate), 574
- shutdown
 - no shutdown (DNS Proxy), 311
 - no shutdown (DNS-Client), 308
 - no shutdown (Firewall), 514
 - no shutdown (IPsec), 529
 - no shutdown (OpenVPN), 585
 - no shutdown (PPP), 233
 - no shutdown (SINEMA RC), 157
 - no shutdown (SRS), 142
 - shutdown (DNS Proxy), 310
 - shutdown (DNS-Client), 307
 - shutdown (Firewall), 513
 - shutdown (IPsec), 529
 - shutdown (OpenVPN), 584
 - shutdown (PPP), 232
 - shutdown (SINEMA RC), 156
 - shutdown (SRS), 141
- shutdown complete, 86, 208
 - no shutdown, 87, 209
- SIMATIC NET glossary, 4
- SIMATIC NET manual, 4
- sinema, 118
- sinemarc, 146
- smtp-server
 - no smtp-server, 366
- snmp
 - client config, 616
 - no client config, 617
 - snmp access, 325
 - no snmp access, 327
 - snmp agent version, 325
 - snmp community index, 328
 - no snmp community index, 329
 - snmp filterprofile, 330
 - snmp group, 332
 - no snmp group, 333
 - snmp notify, 334
 - no snmp notify, 335
 - snmp targetaddr, 335
 - no snmp targetaddr, 337
 - snmp targetparams, 338
 - no snmp targetparams, 340
 - snmp user, 342
 - no snmp user, 343
 - snmp v1-v2 readonly, 340
 - no snmp v1-v2 readonly, 341
 - snmp view, 343
 - no snmp view, 345
 - snmpagent, 324
 - no snmpagent, 324
- snmp, 187
- snmp client addressing-mode, 192
- snmp time diff, 188
- snmp unicast-server, 189
 - no snmp unicast-server, 191
- spanning-tree, 247
 - no spanning-tree, 248
- spanning-tree (properties), 252
 - no spanning-tree, 254
- spanning-tree (time settings), 249
 - no spanning-tree, 250
- spanning-tree auto-edge, 255
 - no spanning-tree auto-edge, 256
- speed, 88
- src-nat show-idx, 427
- src-nat type ipv4, 428
 - no src-nat, 430
 - no src-nat all, 430
- srs, 135
- srv name, 354
- srv name addr, 356
- srv name auth, 357
- srv name port, 358
- srv name pw, 359
- srv name type, 360
- srv name user, 361
- srv show-names, 362

- ssh-server, 377
 - no ssh-server, 378
- static-lease, 299
 - no static-lease, 300
- subnet, 533
- Subnet mask, 43
- subnet-vlan, 204
 - no subnet-vlan, 205
- switchport acceptable-frame-type, 209
 - no switchport acceptable-frame-type, 210
- switchport ingress-filter, 211
 - no switchport ingress-filter, 212
- switchport mode, 212
 - no switchport mode, 213
- switchport priority default, 214
 - no switchport priority default, 215
- switchport pvid, 216
 - no switchport pvid, 216
- syslogserver, 627
 - no syslogserver, 628
- system contact, 78
- system location, 78
- system name, 79

T

- telnet-server, 268
 - no telnet-server, 269
- test, 375
- tftp filename, 95
- tftp load, 96
- tftp save, 97
- tftp server, 97
 - Downloading, 91
- tftp/sftp server
 - Saving, 92
- time, 165
- time dst date, 166
 - no time dst, 168
- time dst recurring, 167
- time set, 169
- timeout, 540
- track interface, 394
 - no track interface, 395
- track links, 396
 - no track links, 397
- Training, 4
- type ppo-ex, 234

U

- user-account, 449
 - no user-account, 451
- useraccount ruleset
 - no useraccount ruleset, 517
- user-account ruleset, 516
- useraccount show-idx, 515
- user-account-ext, 452
- user-group, 454
- userhost, 313
- username, 235, 314, 456

V

- validate cert, 144
- verification cacert, 158
- verification fingerprint, 159
- vir-ip, 534, 541
 - no vir-ip, 535, 542
- vlan, 205
 - no vlan, 206
- vrrp associated-ip (VRRP3), 400
 - no vrrp associated-ip, 400
- vrrp ipv4 (VRRP3)
 - no vrrp ipv4, 402
- vrrp primary-ip (VRRP3), 401
- vrrp priority (VRRP3), 403
 - no vrrp priority, 404
- vrrp timer (VRRP3), 405
 - no vrrp-timer, 406
- vrrp track decrement, 407
 - no vrrp track, 408
- vrrp vrid-track, 398
 - no vrrp vrid-track, 399

W

- web-session-timeout, 128
 - no web-session-timeout, 129
- whoami, 444
- write, 125
- write startup-config, 108

