

SIEMENS

SIMATIC NET

Industrial Ethernet Switches Web User Interface (Web UI) SINEC OS V2.2

Configuration Manual

For SCALANCE XCH-300, XCM-300, XRH-300 and
XRM-300

10/2022


C79000-G8976-C497-04


Preface	1
Introduction	2
User Interface	3
Getting started	4
Device management	5
System administration	6
Security	7
Interface management	8
IP Address Assignment	9
Network redundancy	10
Network discovery and management	11
Traffic control and classification	12
Time settings	13
Multicast filtering	14
Diagnostics	15
Troubleshooting	16


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.

Table of contents

1	Preface	17
1.1	Security Disclaimer	17
1.2	Firmware/Software Support	17
1.3	Open source	17
1.4	Trademarks	18
1.5	Related documents	18
1.6	Training	19
1.7	Customer support	19
2	Introduction	21
2.1	Features and benefits	21
2.2	Security recommendations	24
2.3	Configuration limits	27
2.4	Available services	29
2.5	Access rights	30
2.6	Device configuration	32
2.7	Supported functions	33
2.8	Supported Internet browsers	35
3	User Interface	37
3.1	User interface	37
3.1.1	Login page	37
3.1.2	Start page	39
3.1.3	Status bar	40
3.1.4	Online help	41
3.1.4.1	Opening the online help	42
3.1.4.2	Structure of the online help	43
3.1.4.3	Searching in the online help	44
3.2	Configuration transactions	45
3.2.1	Select a configuration mode	45
3.2.2	Displaying configuration changes	45
3.2.3	Checking Configuration Changes	47
3.2.4	Disabling a function	47
3.2.5	Committing configuration changes (Commit)	47
3.2.5.1	Check and commit configuration changes in a single step	48
3.2.5.2	Commit checked configuration changes	48
3.2.6	Resolving configuration conflicts	48
3.2.7	Deleting Individual Configuration Changes	49
3.2.8	Discarding All Configuration Changes	49

3.2.9	Showing saved configurations	50
3.2.10	Restoring a Configuration (Rollback)	50
3.3	Basic operation	51
3.3.1	Working with tables	51
3.3.1.1	Add a new row	51
3.3.1.2	Select a row	51
3.3.1.3	Delete a row	52
3.3.1.4	Configuring Parameters for All Rows of a Column at the Same Time	52
3.3.1.5	Performing Actions for all Rows of a Table at the Same Time	52
3.3.1.6	Editable and read-only cells	53
3.3.1.7	Define the number of entries to be displayed	53
3.3.1.8	Tables with multiple pages	53
3.3.2	Switching to the Start Page	54
3.3.3	Multiple Selection in Drop-Down Lists	54
3.3.4	Loading and saving files via a remote server	54
3.3.5	Specifying a duration	56
3.3.6	Optical Feedback Messages	58
3.3.7	Adapting the Page Layout	59
3.3.8	Operating the Web UI with the Keyboard	59
3.4	Configuration of the user interfaces	59
3.4.1	Understanding user interface configuration	60
3.4.2	Configuring the NETCONF user interface	61
3.4.2.1	Enabling the NETCONF user interface	61
3.4.2.2	Changing the inactivity timeout for NETCONF sessions	62
3.4.2.3	Configuring a server endpoint for NETCONF	62
3.4.2.4	Changing the SSH Key Exchange Method for a NETCONF Server Endpoint	63
3.4.2.5	Enabling a server endpoint for NETCONF	64
3.4.3	Configuring the CLI user interface	64
3.4.3.1	Changing the inactivity timeout for CLI sessions	65
3.4.3.2	Configuring a server endpoint for the CLI	66
3.4.3.3	Changing the SSH Key Exchange Method for a CLI Server Endpoint	66
3.4.3.4	Enabling a server endpoint for the CLI	67
3.4.4	Configuring the Web user interface	68
3.4.4.1	Enabling the Web user interface	68
3.4.4.2	Changing the inactivity timeout for Web UI sessions	69
3.4.4.3	Configuring an HTTP server endpoint for the Web UI	70
3.4.4.4	Enabling an HTTP server endpoint for the Web UI	70
3.4.4.5	Configuring an HTTPS server endpoint for the Web UI	71
3.4.4.6	Enabling an HTTPS server endpoint for the Web UI	72
3.4.4.7	Using a user-defined HTTPS certificate	72
4	Getting started	73
4.1	Accessing the Web UI via a network connection	73
4.2	Login	74
4.2.1	Default user profiles and passwords	74
4.2.2	Logging in to a device with default settings	74
4.2.3	Logging in to a configured device	75
4.3	Logout	76
4.4	Basic settings	76
4.4.1	Configuring basic settings	76

4.4.1.1	Changing the host name.....	76
4.4.1.2	Specifying the device location.....	77
4.4.1.3	Specifying the contact person for the device.....	77
4.4.1.4	Configuring the default gateway manually.....	77
4.4.2	Displaying the default gateway.....	78
5	Device management.....	79
5.1	Restarting and shutting down the device.....	79
5.1.1	Understanding restarting and shutting down the device.....	79
5.1.1.1	Canceling a command.....	79
5.1.1.2	Exiting sessions.....	79
5.1.1.3	Taking configuration changes into account.....	80
5.1.2	Restarting the device.....	80
5.2	Resetting the device to default settings.....	80
5.3	Decommissioning the device.....	81
5.4	Firmware.....	82
5.4.1	Understanding firmware management.....	82
5.4.2	Displaying the current firmware version.....	83
5.4.3	Obtaining a firmware package.....	83
5.4.4	Upgrading the firmware.....	83
5.4.4.1	Loading a newer firmware file from a local client PC.....	84
5.4.4.2	Loading a newer firmware file from a remote server.....	84
5.4.5	Downgrading the firmware.....	86
5.4.5.1	Loading an older firmware file from a local client PC.....	86
5.4.5.2	Loading an older firmware file from a remote server.....	87
5.4.6	Rejecting a Loaded Firmware File.....	88
5.4.7	Activating the backup firmware.....	88
5.5	Device hardware.....	89
5.5.1	Listing Hardware Components.....	89
5.6	Configuration file.....	90
5.6.1	Saving the Current Configuration as File on a Local Client PC.....	91
5.6.2	Saving the Current Configuration as File on a Remote Server.....	92
5.6.3	Loading a Configuration File from a Local Client PC.....	93
5.6.4	Loading a Configuration File from a Remote Server.....	95
5.6.5	Displaying the header information of a configuration file.....	96
5.7	Open Source Software Information.....	97
5.7.1	Saving OSS Information on a Local Client PC.....	98
5.7.2	Saving OSS Information on a Remote Server.....	98
5.8	Operator panel.....	98
5.8.1	Understanding the operator panel.....	99
5.8.1.1	LEDs.....	99
5.8.1.2	"A" LED.....	99
5.8.1.3	LEDs "DM1" and "DM2".....	99
5.8.1.4	LEDs "L1" and "L2".....	99
5.8.1.5	"P" LEDs.....	100
5.8.1.6	Button.....	101
5.8.2	Monitoring the operating state of the device.....	101
5.8.3	Setting the display mode.....	102

5.9	Signaling contact	102
5.9.1	Signaling contact	102
5.9.2	Setting the signaling contact mode	103
5.10	Button functions	103
5.10.1	Understanding the button functions.....	103
5.10.1.1	Resetting the device to default settings with the button (in the startup phase).....	104
5.10.1.2	Resetting the device to default settings with the button (during operation).....	104
5.10.1.3	Loading a firmware file via TFTP.....	105
5.10.2	Enabling the 'Reset to default settings' button function.....	106
5.11	Configuration and License PLUG	107
5.11.1	Understanding the CLP.....	107
5.11.1.1	Device replacement	107
5.11.1.2	Modes	108
5.11.1.3	Firmware on CLP.....	108
5.11.1.4	Memory areas.....	109
5.11.1.5	Related events	109
5.11.2	Saving firmware on the CLP.....	110
5.11.3	Saving the device configuration on the CLP.....	110
5.11.4	Deleting the Data of the CLP.....	110
5.11.5	Resetting the CLP	111
5.11.6	Showing the status of the CLP.....	111
6	System administration.....	113
6.1	Password policy	113
6.1.1	Configuring the password policy.....	113
6.1.1.1	Configuring the minimum number of characters.....	114
6.1.1.2	Configuring the maximum number of characters	114
6.1.1.3	Configuring the condition for numbers	114
6.1.1.4	Configuring the condition for lowercase letters	115
6.1.1.5	Configuring the condition for uppercase letters	115
6.1.1.6	Configuring the condition for special characters.....	116
6.1.1.7	Enabling the password policy	116
6.1.2	Displaying the password policy.....	116
6.2	User administration	117
6.2.1	Case sensitivity in user names	117
6.2.2	Configuring users.....	117
6.2.2.1	Configuring a new user	118
6.2.2.2	Enabling the assignment of a new password	119
6.2.2.3	Changing the password of a user.....	120
6.2.2.4	Changing the user profile of a user	121
6.2.3	Monitoring Users	122
6.2.3.1	Displaying active users	122
6.2.3.2	Displaying user details.....	122
6.3	Preparing the device for troubleshooting	123
6.3.1	Saving debug information.....	123
6.3.1.1	Saving debug information on a local client PC.....	123
6.3.1.2	Saving Debug Information on a Remote Server.....	123
6.3.2	Enabling the Debug user account.....	124

7	Security	125
7.1	Security	125
7.2	Brute-force attack prevention	125
7.2.1	Understanding BFA Prevention	125
7.2.1.1	How the prevention mechanism works	125
7.2.1.2	Related events	126
7.2.2	Configuring BFA prevention	126
7.2.2.1	Changing the auto-reset timer	126
7.2.2.2	Changing the maximum number of failed login attempts	127
7.2.2.3	Changing the time between failed login attempts	127
7.2.2.4	Enabling BFA prevention	128
7.2.3	Unblocking a user or IP address	128
7.2.4	Monitoring BFA prevention	128
7.3	Security-relevant events	129
7.3.1	Understanding security-relevant events	129
7.3.1.1	SIEM system	130
7.3.1.2	Structure of an event message	131
7.3.1.3	Variables in event messages	132
7.3.2	Monitoring security-relevant events	134
7.3.2.1	Identification and authentication of human users	134
7.3.2.2	Identification and authentication of devices	137
7.3.2.3	User account management	138
7.3.2.4	Unsuccessful login attempts	140
7.3.2.5	Session lock	140
7.3.2.6	Limiting the number of simultaneous sessions	141
7.3.2.7	Configuration changes	141
7.3.2.8	Communication integrity	142
7.3.2.9	Software and information integrity	142
7.3.2.10	Session integrity	142
7.3.2.11	Protection from denial-of-service (DoS) attacks	143
7.3.2.12	Protection of check information	143
7.3.2.13	Restoration of the automation system	143
7.4	Keys and certificates	144
7.4.1	Understanding keys and certificates	144
7.4.1.1	Key method	145
7.4.1.2	Default key pairs	145
7.4.1.3	Certificates	146
7.4.1.4	Certificates from an official certificate authority	146
7.4.1.5	Self-signed certificates	146
7.4.1.6	Certificate chain	147
7.4.1.7	Signatures	147
7.4.1.8	Storage locations	148
7.4.1.9	Access rules	148
7.4.1.10	Related events	149
7.4.2	Managing the keystore	149
7.4.2.1	Importing a key pair from a local client PC	149
7.4.2.2	Importing a key pair from a remote server	151
7.4.3	Managing the truststore	152
7.4.3.1	Importing a certificate from a local client PC	153
7.4.3.2	Importing a certificate from a remote server	154

7.4.4	Monitoring certificates	155
7.4.4.1	Displaying key pairs in the keystore	155
7.4.4.2	Displaying certificates in the keystore	155
7.4.4.3	Displaying certificates in the truststore	156
7.4.4.4	Displays known hosts.....	156
7.5	User authentication	157
7.5.1	Understanding User Authentication.....	157
7.5.1.1	Authentication mode	157
7.5.1.2	RADIUS Authentication	158
7.5.2	Configuring user authentication	159
7.5.3	Configuring RADIUS Authentication	159
7.5.3.1	Configuring a RADIUS server profile	159
7.5.3.2	Testing a RADIUS server connection	161
7.5.4	Selecting the user authentication mode	161
7.5.5	Monitoring User Authentication	162
7.5.5.1	Displaying RADIUS statistics	162
7.6	Management Access Control List (ACL).....	162
7.6.1	Understanding management ACLs	163
7.6.2	Configuring the management ACL.....	163
7.6.2.1	Adding a rule	164
7.6.2.2	Restricting access based on VLAN interface	165
7.6.2.3	Restricting access based on user interface	165
7.6.2.4	Enabling the management ACL	166
7.6.3	Configuration examples	166
7.6.3.1	Creating an authorized manager for a range of remote hosts	166
8	Interface management.....	169
8.1	Interfaces	169
8.1.1	Understanding interfaces.....	169
8.1.1.1	Interface naming conventions.....	170
8.1.1.2	Auto-negotiation	170
8.1.1.3	Duplex communication	170
8.1.1.4	Controller protection through Link Fault Indication (LFI)	171
8.1.1.5	Flow control	172
8.1.1.6	Function Extender Interface (FEI) ports.....	173
8.1.1.7	SFP Transceiver Ports.....	173
8.1.2	Configuring bridge ports	175
8.1.2.1	Adding a description for a bridge port	176
8.1.2.2	Enabling auto-negotiation.....	176
8.1.2.3	Selecting the bridge port speed.....	177
8.1.2.4	Selecting the duplex mode.....	178
8.1.2.5	Enabling downshift for gigabit interfaces	179
8.1.2.6	Enabling link up/down traps.....	179
8.1.2.7	Enabling Smart SFP (for SFP ports only).....	179
8.1.2.8	Enabling a bridge port.....	180
8.1.3	Configuring VLAN interfaces	180
8.1.3.1	Adding a VLAN interface	180
8.1.3.2	Adding a description for a VLAN interface.....	181
8.1.3.3	Configuring the MTU size	181
8.1.3.4	Enabling link up/down traps.....	181
8.1.3.5	Enabling a VLAN interface.....	182

8.1.4	Resetting a bridge port.....	182
8.1.5	Monitoring interfaces.....	182
8.1.5.1	Displaying bridge ports	182
8.1.5.2	Displaying VLAN interfaces.....	183
8.1.5.3	Displaying receive/transmit statistics for all interfaces	184
8.1.5.4	Displaying receive/transmit statistics for only bridge ports	184
8.1.5.5	Monitoring SFP Transceivers.....	186
8.2	MAC address table	187
8.2.1	Understanding the MAC address table	187
8.2.1.1	Dynamic MAC entries.....	187
8.2.1.2	Static MAC entries.....	188
8.2.2	Configuring the MAC address table	188
8.2.2.1	Configuring the MAC address aging time	188
8.2.2.2	Enabling MAC address aging on link failure.....	189
8.2.3	Configuring static MAC filtering entries	189
8.2.3.1	Adding a static MAC filtering entry	189
8.2.3.2	Assigning a traffic class queue	190
8.2.4	Monitoring the MAC address table.....	191
8.2.4.1	Displaying the MAC address table	191
8.2.4.2	Clearing dynamic MAC addresses	191
9	IP Address Assignment	193
9.1	Static IP address assignment.....	193
9.1.1	Configuring a static IPv4 address	193
9.1.2	Listing the IPv4 address configuration.....	193
9.2	Static DNS.....	194
9.2.1	Understanding DNS	194
9.2.1.1	Basic terms for DNS.....	194
9.2.1.2	DNS communication	195
9.2.2	Configuring DNS	196
9.2.2.1	Configuring a DNS server	196
9.2.2.2	Configuring a search domain.....	197
9.2.3	Displaying the DNS configuration	197
9.3	DHCP.....	197
9.3.1	Configuring the device as a DHCP client.....	198
9.3.1.1	Enabling a DHCP client interface	198
9.3.1.2	Requesting a lease time	198
9.3.1.3	Changing the client ID of an interface	199
9.3.1.4	Including the hostname in DHCP messages	200
9.3.1.5	Requesting a Configuration File from the DHCP Server	200
9.3.2	Showing the configuration data of DHCP client interfaces	202
10	Network redundancy	203
10.1	Spanning Tree Protocol (STP).....	203
10.1.1	Understanding STP.....	203
10.1.1.1	Rapid Spanning Tree Protocol (RSTP).....	203
10.1.1.2	RSTP Applications.....	207
10.1.1.3	Enhanced Rapid Spanning Tree Protocol (eRSTP).....	211
10.1.1.4	Multiple Spanning Tree Protocol (MSTP)	212
10.1.1.5	Related events	217
10.1.2	Configuring STP Globally	217

10.1.2.1	Enabling STP.....	218
10.1.2.2	Selecting the STP version	218
10.1.2.3	Selecting the bridge priority	219
10.1.2.4	Configuring the Hello time	219
10.1.2.5	Configuring the maximum aging time	220
10.1.2.6	Configuring the transmit hold count.....	221
10.1.2.7	Configuring the forward delay.....	221
10.1.3	Configuring STP for Bridge Ports	221
10.1.3.1	Enabling STP for a bridge port	222
10.1.3.2	Configuring the bridge port cost.....	222
10.1.3.3	Selecting the bridge port priority.....	223
10.1.3.4	Selecting the edge port state.....	224
10.1.3.5	Selecting the bridge port link type.....	225
10.1.3.6	Restricting the role of a bridge port	225
10.1.3.7	Preventing a bridge port from forwarding TCNs	226
10.1.4	Configuring eRSTP.....	227
10.1.4.1	Selecting the maximum network diameter	227
10.1.4.2	Configuring the BPDU Guard Timeout	228
10.1.4.3	Selecting the Fast Root Failover mechanism.....	229
10.1.4.4	Enabling IEEE 802.1w interoperability	229
10.1.5	Configuring MSTP	230
10.1.5.1	Selecting the maximum number of hops	230
10.1.5.2	Adding the region name	230
10.1.5.3	Configuring the region revision level	230
10.1.6	Configuring Multiple Spanning Tree Instances (MSTIs)	231
10.1.6.1	Creating an MSTI	232
10.1.6.2	Selecting the bridge priority	232
10.1.6.3	Mapping a VLAN to an MSTI	233
10.1.6.4	Configuring the bridge port priority for an MSTI.....	233
10.1.6.5	Configuring the MSTI cost for a bridge port.....	234
10.1.7	Monitoring STP	235
10.1.7.1	Displaying the status of STP.....	235
10.1.7.2	Displaying the status of STP per bridge port.....	236
10.1.7.3	Displaying MSTP region information	237
10.1.7.4	Displaying the status of an MSTI.....	237
10.1.7.5	Displaying the status of an MSTI per bridge port	238
10.1.8	Configuration Examples	239
10.1.8.1	A basic MSTP configuration	240
10.2	Loop Detection	241
10.2.1	Understanding the detection of network loops	241
10.2.1.1	Port modes	242
10.2.1.2	Types of network loops	243
10.2.1.3	VLAN mode	243
10.2.1.4	Related events	243
10.2.2	Configuring the detection of network loops	244
10.2.2.1	Configuring bridge ports for the detection of network loops.....	245
10.2.2.2	Configuring the send interval	245
10.2.2.3	Defining the limit for the detection of a local network loop	245
10.2.2.4	Configuring the reaction to local network loops	246
10.2.2.5	Configuring the reaction to remote network loops	247
10.2.2.6	Configuring the duration for disabling a bridge port.....	247
10.2.2.7	Enabling VLAN mode	248

10.2.2.8	Enabling Loop Detection	248
10.2.2.9	Resetting a bridge port manually after detection of a network loop.....	249
10.2.3	Showing the status of Loop Detection	249
10.3	Device Level Ring	250
10.3.1	Understanding DLR	250
10.3.1.1	Ring Supervisor.....	250
10.3.1.2	Ring Nodes	251
10.3.1.3	DLR Frames.....	251
10.3.1.4	DLR Network.....	253
10.3.2	Configuring DLR.....	254
10.3.2.1	Selecting the DLR VLAN.....	254
10.3.2.2	Selecting the DLR Ports	255
10.3.2.3	Enabling DLR	255
10.3.3	Monitoring DLR.....	255
10.3.4	Configuration examples	257
10.3.4.1	Using DLR in VLAN 0	257
11	Network discovery and management	259
11.1	LLDP	259
11.1.1	Configuring the sending and receiving of LLDPDUs for a bridge port.....	259
11.1.2	Monitoring the LLDP information of neighbor devices.....	259
11.2	DCP	260
11.2.1	Understanding DCP.....	260
11.2.2	Configuring DCP.....	260
11.2.2.1	Configuring the access rights of DCP.....	261
11.2.2.2	Configuring the sending of DCP frames for a bridge port.....	263
11.3	PROFINET.....	263
11.3.1	Understanding PROFINET	264
11.3.1.1	PROFINET components.....	264
11.3.1.2	Device Addressing.....	266
11.3.1.3	PROFINET communication.....	266
11.3.1.4	PROFINET relations	267
11.3.1.5	I&M data.....	267
11.3.1.6	GSD file.....	268
11.3.2	Configuring PROFINET	268
11.3.2.1	Configuring the TIA interface.....	268
11.3.2.2	Configuring PROFINET runtime mode	269
11.3.2.3	Saving the GSD File on a Local Client PC	269
11.3.2.4	Saving the GSD File on a Remote Server	269
11.3.3	Monitoring PROFINET.....	270
11.3.3.1	Displaying the current PROFINET runtime mode.....	270
11.3.3.2	Monitoring the connection to a PROFINET controller.....	270
11.3.3.3	Monitoring the TIA interface	271
11.3.3.4	Displaying the I&M data	271
11.3.3.5	Displaying the PROFINET device name	272
11.4	EtherNet/IP	272
11.4.1	Understanding EtherNet/IP Protocol.....	272
11.4.1.1	Common Industrial Protocol.....	273
11.4.1.2	Message Types.....	273
11.4.1.3	Producer-Consumer Relationship.....	273

11.4.1.4	Object Model	273
11.4.1.5	Supported Objects	274
11.4.1.6	Electronic Data Sheet	274
11.4.2	Configuring EtherNet/IP.....	274
11.4.2.1	Configuring the Management Interface	275
11.4.2.2	Enabling EtherNet/IP	275
11.4.2.3	Saving the EDS File on a Local Client PC.....	275
11.4.2.4	Saving the EDS File on a Remote Server	276
11.5	ARP.....	276
11.5.1	Understanding ARP	276
11.5.2	Displaying the ARP table summary	277
11.6	SNMP	278
11.6.1	Configuring the SNMP agent	278
11.6.1.1	Configuring the SNMP versions the SNMP agent supports	279
11.6.1.2	Configuring a server endpoint for SNMP	279
11.6.1.3	Enabling a server endpoint for SNMP.....	280
11.6.1.4	Enabling the SNMP agent.....	280
11.6.2	Changing the name of an SNMP community.....	281
11.6.3	Changing the IP address of an SNMP target	281
11.6.4	Changing the port of an SNMP target	281
11.6.5	Displaying the engine ID	282
12	Traffic control and classification	283
12.1	Rate limiting	283
12.1.1	Understanding rate limiting	283
12.1.2	Configuring rate limiting	284
12.1.2.1	Determining interface capabilities	284
12.1.2.2	Selecting the type of frames to limit.....	286
12.1.2.3	Selecting the rate limit.....	287
12.1.2.4	Enabling rate limiting.....	287
12.1.3	Configuration examples	287
12.1.3.1	Limiting the rate of traffic.....	287
12.2	VLANs	288
12.2.1	Understanding VLANs	288
12.2.1.1	How VLANs are created.....	289
12.2.1.2	VLAN-aware and VLAN-unaware modes	289
12.2.1.3	Tagged vs. untagged frames	290
12.2.1.4	Access and trunk ports	292
12.2.1.5	Native VLAN vs. default VLAN	292
12.2.1.6	Ingress filtering	292
12.2.1.7	Ingress and egress rules	293
12.2.1.8	GARP VLAN Registration Protocol (GVRP)	294
12.2.1.9	Forbidden VLANs	294
12.2.1.10	VLAN-0-Tunnel mode	294
12.2.1.11	Advantages and disadvantages of using VLANs	295
12.2.2	Configuring VLANs.....	296
12.2.2.1	Adding or modifying a static VLAN	296
12.2.2.2	Enabling VLAN-0-Tunnel mode.....	297
12.2.3	Configuring VLAN settings for bridge ports	297
12.2.3.1	Selecting the port membership type.....	298
12.2.3.2	Configuring the port VLAN ID	298

12.2.3.3	Selecting the frame types accepted	299
12.2.3.4	Enabling PVID tagging on egress traffic.....	299
12.2.3.5	Enabling ingress filtering	300
12.2.3.6	Restricting VLAN membership	300
12.3	Traffic classes	301
12.3.1	Understanding traffic classes	301
12.3.1.1	Traffic class queues	302
12.3.1.2	Weighting algorithms.....	302
12.3.1.3	Default mapping	303
12.3.1.4	Prioritization of ingress frames	304
12.3.1.5	Priority regeneration	305
12.3.2	Configuring traffic classes.....	305
12.3.2.1	Configuring the default priority	306
12.3.2.2	Mapping a PCP value to a traffic class.....	306
12.3.2.3	Mapping a DSCP tag to a traffic class	307
12.3.2.4	Configuring trust mode	307
12.3.2.5	Assigning different priorities to traffic on egress.....	308
12.3.3	Configuration examples	309
12.3.3.1	Prioritizing all frames	309
12.3.3.2	Prioritizing select frames	310
13	Time settings	313
13.1	Showing the date and the system time	313
13.2	Configuring the date and the system time	313
13.3	Using the date and the system time of the client PC.....	314
13.4	Configuring the time zone.....	314
13.5	NTP	314
13.5.1	Understanding NTP	314
13.5.1.1	Stratum Number	315
13.5.1.2	NTP Server	316
13.5.1.3	NTP Client.....	316
13.5.2	Configuring NTP.....	316
13.5.2.1	Configuring an NTP server.....	317
13.5.2.2	Enabling an NTP server	317
13.5.2.3	Configuring the NTP version	317
13.5.2.4	Configuring the polling interval	318
13.5.2.5	Enabling iBurst.....	318
13.5.2.6	Enabling Burst	319
13.5.2.7	Enabling NTP	319
13.5.3	Displaying the NTP configuration.....	319
13.6	PTP	320
13.6.1	Understanding PTP.....	320
13.6.1.1	Supported clock types	320
13.6.1.2	PTP messages	320
13.6.1.3	PTP domains	321
13.6.1.4	PTP profiles	321
13.6.1.5	Best Master Clock Algorithm (BMCA)	322
13.6.1.6	Transparent clocks	323
13.6.2	Configuring PTP	324

13.6.2.1	Defining the PTP domain	324
13.6.2.2	Enabling PTP for a bridge port	324
13.6.2.3	Enabling PTP globally	324
13.6.3	Monitoring PTP	325
13.6.3.1	Displaying the peer mean path delay	325
14	Multicast filtering	327
14.1	Static multicast groups	327
14.1.1	Configuring static multicast groups	327
14.1.1.1	Adding a static multicast group	327
14.1.1.2	Selecting the traffic class for a static multicast group	328
14.1.1.3	Assigning a forwarding port to a static multicast group	328
14.2	GMRP	328
14.2.1	Understanding GMRP	328
14.2.1.1	Joining/leaving multicast groups with GMRP	329
14.2.1.2	GARP attribute types	329
14.2.2	Configuring GMRP	330
14.2.2.1	Enabling GMRP	330
14.2.2.2	Selecting the GMRP mode per bridge port	330
14.2.2.3	Configuring a delay before leaving a multicast group	331
14.2.2.4	Enabling topology change flooding	331
14.2.3	Configuration examples	331
14.2.3.1	Establishing membership with multicast groups using GMRP	331
14.3	IGMP snooping	333
14.3.1	Understanding IGMP snooping	333
14.3.1.1	IGMP modes	333
14.3.1.2	Filtering/pruning multicast traffic	334
14.3.1.3	IGMP snooping querier	334
14.3.1.4	IGMP snooping rules	334
14.3.2	Configuring IGMP snooping	335
14.3.2.1	Enabling IGMP snooping	335
14.3.2.2	Selecting the IGMP version	336
14.3.2.3	Selecting the IGMP mode	336
14.3.2.4	Configuring the IGMP query interval	337
14.3.2.5	Enabling topology change flooding	337
14.3.2.6	Enabling IGMP snooping per VLAN	337
14.3.3	Configuring multicast router forwarding	338
14.3.3.1	Enabling multicast router forwarding	338
14.3.3.2	Configuring a multicast router interface	338
14.3.4	Monitoring IGMP snooping	338
14.3.4.1	Displaying the status of learned multicast groups	339
14.4	Multicast filtering database	339
15	Diagnostics	341
15.1	Diagnostics	341
15.2	System status	341
15.2.1	Displaying the system boot time	341
15.2.2	Displaying the system up time	341
15.3	System logging	341
15.3.1	Understanding system logging	342

15.3.1.1	Structure of a syslog entry.....	342
15.3.1.2	Severity levels	342
15.3.1.3	Syslog facilities	343
15.3.1.4	Remote logging	343
15.3.1.5	Event filtering	343
15.3.2	Configuring remote system logging	344
15.3.2.1	Configuring remote system logging	344
15.3.2.2	Adding a remote syslog server profile	344
15.3.2.3	Defining a filtering rule for a remote syslog server.....	345
15.3.3	Monitoring the system log	346
15.3.3.1	Displaying the logbook.....	346
15.3.3.2	Displaying remote logging servers.....	347
15.3.3.3	Clearing the logbook.....	347
15.4	Event management.....	347
15.4.1	Understanding event management	347
15.4.1.1	Severity levels	348
15.4.1.2	Resources and events.....	348
15.4.1.3	Alarms	350
15.4.2	Configuring events.....	358
15.4.3	Monitoring alarms	358
15.4.3.1	Listing active alarms.....	358
15.4.3.2	Clearing and acknowledging alarms	359
15.5	SMTP	360
15.5.1	Understanding SMTP.....	360
15.5.1.1	SMTP client and server exchanges	361
15.5.1.2	E-mail message format.....	361
15.5.2	Configuring SMTP	362
15.5.2.1	Adding e-mail recipients.....	362
15.5.2.2	Testing the SMTP server connection	363
15.5.2.3	Enabling SMTP	363
15.5.3	Configuring the SMTP account	363
15.5.3.1	Configuring the account e-mail address	364
15.5.3.2	Adding a description for the account	364
15.5.4	Configuring the SMTP server	364
15.5.4.1	Configuring the SMTP server profile	364
15.5.4.2	Configuring the delay for SMTP responses	365
15.5.5	Configuring SMTP authentication	365
15.5.5.1	Configuring the SMTP user	366
15.5.5.2	Enabling SMTP authentication.....	366
15.5.6	Configuration examples	366
15.5.6.1	Configuring SMTP to send event notifications	366
15.6	Traffic mirroring	367
15.6.1	Understanding traffic mirroring	368
15.6.1.1	Traffic mirroring sessions.....	368
15.6.1.2	Traffic mirroring sources and destinations.....	368
15.6.1.3	Deploying traffic mirroring	369
15.6.2	Configuring traffic mirroring.....	369
15.6.2.1	Selecting a traffic source	369
15.6.2.2	Configuring the mirroring destination.....	371
15.6.2.3	Enabling traffic mirroring	371
15.6.3	Configuration examples	372

15.6.3.1	Configuring traffic mirroring across a Layer 2 network.....	372
15.6.3.2	Configuring remote traffic mirroring	373
15.7	Cable diagnostics	373
15.7.1	Running a cable diagnostic test	373
15.7.2	Displaying cable diagnostics results	374
16	Troubleshooting.....	377
16.1	The device is in a restart loop	377

Preface

This document describes how to configure and manage SINEC OS. It is intended for use by network technical support personnel familiar with the operation of networks. It is also recommended for use by network and system planners, system programmers, and line technicians.

1.1 Security Disclaimer

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.

Additional information on industrial security measures that may be implemented, can be found at the following address: (<http://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 made available and that only 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 at the following address: (<https://www.siemens.com/cert>).

1.2 Firmware/Software Support

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

1.3 Open source

SINEC OS is based on Linux®. Linux is made available under the terms of the GNU General Public License Version 2.0 (<https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html>).

SINEC OS contains additional open source software. For license conditions, refer to the associated **License Conditions** document.

For more information, refer to "Open Source Software Information (Page 97)".

1.4 Trademarks

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

- RUGGEDCOM
- SCALANCE
- SINEC

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

1.5 Related documents

The following additional documents may be of interest. Unless specified otherwise, the documents are available in the Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/15247>).

Note

The listed documents are the documents that were available at the time of publication. Newer versions of these documents or the associated products may be available. Additional information is available in the SIOS or contact your Siemens customer service.

Product notes

Product notes are available online in the SIOS (<https://support.industry.siemens.com/cs/ww/en/ps/15247>).

Manuals

Document title	Link
SINEC OS CLI Configuration Manual	Visit (https://support.industry.siemens.com/cs/de/en/ps/15296/man)
SCALANCE XCM-300 Operating Instructions	Visit (https://support.industry.siemens.com/cs/de/en/ps/15296/man)
SCALANCE XRM-300 Operating Instructions	Visit
"SIMATIC NET Network management SINEMA Server" Operating Instructions	Visit (https://support.industry.siemens.com/cs/ww/en/view/109748925)
"SIMATIC NET Network management SINEC PNI" Operating Instructions	Visit (https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=en-US)
"SIMATIC NET: Network management Diagnostics and configuration with SNMP" Diagnostics Manual	Visit (https://support.industry.siemens.com/cs/ww/en/view/103949062)

1.6 Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application requirements.

Siemens' Educational Services team thrives on providing customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure.

Siemens' unique mix of IT and telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit Training Services (<https://support.industry.siemens.com/cs/ww/en/sc/2226>) or contact a Siemens Sales representative.

1.7 Customer support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support using any of the following methods:



Online

Visit (<https://www.siemens.com/automation/support-request>) to submit a Support Request (SR) or check the status of an existing SR.



Telephone

Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit (<https://www.automation.siemens.com/aspa-db/en/automation-technology/Pages/default.aspx>).



Mobile app

Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

- Access Siemens' extensive library of support documentation, including FAQs and manuals
- Submit SRs or check on the status of an existing SR
- Contact a local Siemens representative from Sales, Technical Support, Training, etc.
- Ask questions or share knowledge with fellow Siemens customers and the support community

Introduction

Welcome to the SINEC OS Web UI Configuration Manual. This document details how to configure your device via the SINEC OS Web user interface.

Note

The SINEC OS Web user interface provides limited configuration options and overview of select features. Full configuration and operational information is available via the Command Line Interface (CLI). As such, this document only describes the limited features available through the Web user interface.

For information about fully configuring SINEC OS, including concepts and procedures, refer to the **SINEC OS CLI Configuration Manual**.

2.1 Features and benefits

The following describes the many features available under SINEC OS and their benefits:

- **Cyber security**

Cyber security is critical for many industries where advanced automation and communications networks play a crucial role in mission critical applications. SINEC OS includes the following security features to address security issues at the local area network level:

Passwords	Multi-level user passwords secure against unauthorized configuration updates
SSH/SSL	Extends capability of password protection to add encryption of passwords and data as they traverse the network
Enable/disable interfaces	Capability to block traffic at specific interfaces
VLAN (IEEE 802.1Q)	Logically segregates traffic between predefined interfaces
SNMPv3	Encrypted authentication and access security
IEC 62443-4-1	Developed under a Secure Development Lifecycle (SDL) process in compliance with IEC 62443-4-1 and certified by TÜV SÜD
HTTPS	For secure access to the Web User Interface (UI)
SFTP	For the secure transfer of files
Management ACL	Restrict management access to select remote hosts
RADIUS	Provides UDP-based user authentication via remote authentication servers

- **Command Line Interface (CLI)**

A CLI, used in conjunction with a remote shell, allows for automated data retrieval, configuration updates, and firmware updates. A powerful Telecom Standard style CLI allows expert users to selectively retrieve or manipulate any available parameter.

- **Web User Interface (Web UI)**

SINEC OS offers a graphical user interface for configuration and monitoring via a standard Internet browser.
- **NETCONF**

The NETCONF (NETwork CONFiguration) protocol allows you to remotely monitor and configure SINEC OS devices over SSH using Extensible Markup Language (XML). It features various operations for editing and querying configuration and operational data on a SINEC OS device (or NETCONF server) from a NETCONF client that operates on your PC. NETCONF operates on a simple Remote Procedure Call (RPC) layer. Individual RPC commands are exchanged between the NETCONF server and client in XML format. Communications are session-based, allowing a user to lock individual configuration datastores while they are editing a device. NETCONF can be used for directly editing and querying a device, or incorporated into scripted commands. For more information about using NETCONF, refer to the "NETCONF for SINEC OS Reference Manual". For information about how to configure NETCONF sessions in SINEC OS, refer to "Configuring the NETCONF user interface (Page 61)".
- **Simple Network Management Protocol (SNMP)**

SNMP provides a standardized method for network management stations to interrogate devices from different vendors. SINEC OS supports v1, v2c and v3. SNMPv3 is generally recommended, as it provides security features (e.g. authentication and privacy) not present in earlier SNMP versions. SINEC OS also supports numerous standard MIBs (Management Information Base) allowing for easy integration with any Network Management System (NMS). A feature of SNMP supported by SINEC OS is the ability to generate traps upon system events.
- **PROFINET**

PROFINET (Process Field Network) meets all requirements of process automation and provides the basis for plants in the process industry. As an open standard for fieldbus communication, PROFINET combines the advantages of the tried-and-tested PROFIBUS DP fieldbus standard with those of the Industrial Ethernet network standard. PROFINET defines a cross-manufacturer communication, automation and engineering model for industrial automation. With line, ring, tree and star topologies as well as multicontroller networks, PROFINET offers individual options for the network architecture.
- **EtherNet/IP (EIP)**

EtherNet/IP is an open fieldbus standard based on the Common Industrial Protocol (CIP) application protocol for use in the industrial environment and for time-critical applications. In addition to CIP, EtherNet/IP also supports standard Ethernet, the Internet protocol, TCP and UDP. This compatibility with established protocols enables simple integration of EtherNet/IP in networks. EtherNet/IP creates consistency from the office network to the plant to be controlled.
- **Device Level Ring (DLR)**

Device Level Ring is a Layer 2 redundancy method for EtherNet/IP. This makes it possible to establish ring topologies with EtherNet/IP. When the communication chain is interrupted, communication over a redundant path is maintained.

- **Virtual Local Area Networks (VLANs)**

VLANs allow the segregation of a physical network into separate logical networks with independent broadcast domains. A measure of security is provided since hosts can only access other hosts on the same VLAN and traffic storms are isolated. SINEC OS supports IEEE 802.1Q tagged Ethernet frames and VLAN trunks. Interface-based classification allows devices to be assigned to the correct VLAN. Additional GVRP support is available to simplify the configuration of switches on the VLAN.
- **Traffic classes**

Traffic classes organize inbound frames based on their assigned priority and map them to traffic class queues where they are staged for forwarding. Frames with a specific priority can be mapped to a high priority queue where they are forwarded before those in the next queue. This can be used to reduce the effects of latency and jitter on real-time, system critical applications.
- **Network Time Protocol (NTP)**

NTP automatically synchronizes the internal clock of all NTP-enabled devices on the network. This allows for the correlation of time stamped events for troubleshooting.
- **SIMATIC time synchronization**

The SIMATIC method for time synchronization allows the device to synchronize its system time with other SIMATIC components in the local Industrial Ethernet subnet.
- **Daylight saving time**

Configure the system time to adjust automatically when your chosen time zone supports daylight saving time.
- **Rate limiting**

Rate limiting, or port rate limiting, limits the flow of traffic through specific interfaces. This can be essential when managing precious network bandwidth for service providers. It also provides edge security for Denial of Service (DoS) attacks.
- **Discovery and Basic Configuration Protocol (DCP)**

DCP is used by PROFINET to remotely set the station name and IP address of the device. It is useful in applications that do not include a DHCP server.
- **Dynamic Host Communication Protocol (DHCP)**

DHCP allows for the quick integration and configuration of devices on the network. DHCP-enabled devices automatically receive their TCP/IP configuration settings from a central DHCP server when they are connected to the network.
- **Interface configuration and status**

Speed, duplex, auto-negotiation, flow control and other settings can be configured for individual bridge ports. This allows the device to establish proper links with devices that do not negotiate or have non-standard settings.
- **Interface statistics**

Continuously updating statistics are available per interface, detailing counters for frames (ingress and egress) and frame bytes, as well as detailed error figures.
- **Event logging and alarms**

All significant events are recorded to a non-volatile system log, which allows for forensic troubleshooting. Events include link failure and recovery, unauthorized access, and self-test diagnostics among others. Alarms provide a snapshot of recent events that have yet to be acknowledged by the network administrator. An external hardware relay can be de-energized during the presence of critical alarms, allowing an external controller to react if desired.

2.2 Security recommendations

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

General

- Periodically audit the device to make sure it complies with these recommendations and/or any internal security policies.
- Backup the device configuration to an external server following the initial setup and after each major configuration change.
- Evaluate the security of your site and use a cell protection concept with suitable products. For more information, visit Industrial Security Website (<https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html>).
- Review the user documentation for other Siemens products used along with the device for further security recommendations.
- Use remote system logging to forward system logs to a central logging server. Make sure the server is within the protected network and check the logs regularly to identify potential security breaches/vulnerabilities. For more information, refer to "Configuring remote system logging (Page 344)".

Authentication

NOTICE
Accessibility hazard - risk of data loss
Do not misplace passwords for the device. Access to the device can only be restored by resetting it to factory defaults, which will remove all configuration data.

- Each device has a default **admin** profile with administrator access rights. During commissioning, this profile should be replaced by a unique, user-defined profile that is assigned the admin role. At least one user profile with the admin role is required.
- Replace the default passwords for all user accounts, access modes and applications (where applicable) before the device is deployed.
- Use strong passwords. Avoid weak passwords (e.g. password1, 123456789, abcdefgh) or repeated characters (e.g. abcabc). This recommendation also applies to symmetric passwords/keys configured on the device.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Do not re-use passwords across different user names and systems.
- Record passwords in a safe, secure, off-line location for future retrieval should they be misplaced.
- Change passwords regularly and often.
- When RADIUS is utilized for user authentication, make sure all communications are within the security perimeter or protected by a secure channel.

- Be aware of any link layer protocols that do not provide any inherent authentication between endpoints, such as ARP in IPv4. A malicious entity could exploit weaknesses in these protocols to attack hosts, switches, and routers connected to your Layer 2 network, for example, by poisoning the ARP caches of systems within the subnet and subsequently intercepting traffic. Appropriate safeguards against non-secure Layer 2 protocols, such as securing physical access to the local network and using secure higher layer protocols, should be taken to prevent unauthorized access to the network.
- Take precautions to protect your 2FA authenticator devices/applications. This includes maintaining individual possession of authenticators, not sharing authenticators with others, and immediately reporting lost or compromised authenticators.

Certificates and keys

- Immediately change all certificates and keys upon suspicion of a security breach.
- SSH and SSL keys are accessible to admin users. Make sure to take appropriate precautions when shipping the device beyond the boundaries of the trusted environment:
 - Replace the SSH and SSL keys with throwaway keys prior to shipping.
 - Take the existing SSH and SSL keys out of service. When the device returns, create and program new keys for the device.
- Use password-protected certificates that are in PKCS #12 format.
- Use certificates with a key length of 4096 bits.
- Before returning the device to Siemens for repair, replace the current certificates and keys with temporary throwaway certificates and keys that can be destroyed upon the device's return.
- Verify certificates and fingerprints on the server and client to prevent Man-in-the-Middle (MitM) attacks.

Physical/remote access

- Only operate the devices in a protected network area. Attackers cannot access internal data from outside when the internal and external network are disconnected.
- Restrict physical access to the device to only trusted personnel. A malicious user in possession of the device's removable media could extract critical information, such as certificates, keys, etc. (user passwords are protected by hash codes), or reprogram the media.
- Control access to the serial console to the same degree as any physical access to the device.
- It is highly recommended to keep Brute Force Attack (BFA) protection enabled to prevent a third-party from obtaining unauthorized access to the device.
For more information, refer to "Brute-force attack prevention (Page 125)".
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communications.
- When securely connecting to a server (e.g. in the case of a secure upgrade), make sure the server side is configured with strong ciphers and protocols.
- Terminate management connections (e.g. HTTP, HTTPS, SSH, etc.) properly.
- Make sure the device is fully decommissioned before taking the device out of service.
For more information, refer to "Decommissioning the device (Page 81)".

Secure/non-secure protocols

- Use secure protocols when access to the device is not prevented by physical protection measures.
- Disable or limit the use of non-secure protocols. While some protocols are secure (e.g. HTTPS, SSH, 802.1X, etc.), others were not designed for secure applications (e.g. SNMPv1/v2c, RSTP, etc.).
Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the device/network.
- If non-secure protocols and services are required, make sure the device is operated within a protected network area.
- When a secure alternative is available for a protocol, use the secure version instead. For example:
 - Use HTTPS instead of HTTP
 - Use SNMPv3 instead of SNMPv1/v2c
- Avoid or limit use of the following:
 - Non-authenticated and unencrypted protocols
 - Link Layer Discovery Protocol (LLDP)
- After commissioning the device, access rights for the Discovery and basic Configuration Protocol (DCP) are automatically set to read-only. If your environment does not require DCP, it is recommended to disable it fully.
For more information, refer to "Configuring the access rights of DCP (Page 261)".

Hardware/software

- Limit critical applications and access to management services to private networks. Connecting a SINEC OS device to the Internet is possible. However, the utmost care should be taken to protect the device and the network behind it using secure means, such as a firewall and IPsec.
- Whenever possible, use VLANs to protect against Denial of Service (DoS) attacks and unauthorized access.
- Select services are enabled by default in SINEC OS. It is recommended to only enable the minimum services that are required for your setup.
For more information about available services, "Available services (Page 29)".
- Use the latest Web browser version compatible with SINEC OS to make sure the most secure ciphers available are employed. Additionally, 1/n-1 record splitting is enabled in the latest Web browser versions of Mozilla Firefox, Google Chrome and Microsoft Edge, and mitigates against attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (e.g. BEAST).
- Make sure the latest firmware version is installed, including all security-related patches. For the latest information on security patches for Siemens products, visit the Industrial Security (<https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html>) website or the ProductCert Security Advisories (<https://www.siemens.com/global/en/home/products/services/cert.html>) website. Updates to the Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.

- Only enable services that will be used on the device, including physical ports. Unused physical ports could potentially be used to gain access to the network behind the device.
- For optimal security, use the authentication and encryption mechanisms in SNMPv3 whenever possible, and apply strong passwords.
- Configuration files can be downloaded from the device. Make sure configuration files are properly protected. For instance, digitally sign and encrypt the files, store them in a secure place, and only transfer configuration files via secure communication channels. Configuration files can be password-protected when downloaded. For information about protecting a configuration file with a password, refer to "Saving the Current Configuration as File on a Remote Server (Page 92)".
- When using SNMP (Simple Network Management Protocol):
 - Configure SNMP to raise a trap upon authentication failures. For more information, refer to "SNMP (Page 278)".
 - Make sure the default community strings are changed to unique values.
 - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when necessary.
 - Whenever possible, prevent write access.

2.3 Configuration limits

The following defines the limits of each feature in SINEC OS:

Security

Feature		Limit
Keys and certificates	Key pairs	5
	Certificates per key pair	2
	Certificate bags	2
	Certificates per certificate bag	5
	Key bags	5
	Known hosts per key bag	5
Management ACL	Rule entries	64

System administration

Feature		Limit
Users	Number of users	30
Sessions	Number of CLI sessions	8
	Number of NETCONF sessions	4
	Number of SNMP sessions	4
	Number of Web user interface sessions	4
	Buffer size (bytes) per SSH Session	16834

IP address assignment

Feature		Limit
DNS	Number of DNS servers	3
	Number of DNS domains	6
DHCP	Number of DHCP clients	1
Static IPv4 addresses	Static IPv4 addresses per VLAN	1

Interface management

Feature		Limit
MAC addresses	Number of static unicast MAC filtering entries	256
MAC address table	Number of Dynamically Learned MAC Addresses	4096
VLAN interfaces	Number of Layer 3 interfaces	17

Network discovery and management

Feature		Limit
SNMP	Number of target parameters	16
	Number of targets	16
	Number of traps	16
	Number of communities	16
	Number of views	16
	Number of groups	16
	Number of users	16
ARP	Number of ARP entries	512

Traffic control and classification

Feature		Limit
VLANs	Number of Layer 2 VLANs	255
	Available VLAN IDs	1 - 4094
Traffic classes	Number of priority-to-traffic-class mappings per queue	8
	Number of DSCP-to-traffic-class mappings per queue	64

Time services

Feature		Limit
NTP	Number of NTP servers	1

Multicast filtering

Feature		Limit
General	Number of system installed multicast streams	1023
IGMP	Number of Layer 2 IGMP group forwarding entries	256
	Number of Layer 3 IGMP group membership entries	1024
GMRP	Number of learned multicast groups	1024

Diagnostics

Feature		Limit
System log	Number of logbook log entries	1000
	Number of remote syslog servers	5
SMTP	Number of SMTP servers	1
	Number of e-mail recipients	20

2.4 Available services

The following is a list of all available protocols or services and their ports through which the device can be accessed, including the following information:

- **Service**
The service supported by the device.
- **Protocol**
The protocol used by the service.
- **Port number**
The port number assigned to the service.
- **Default status**
The default state of the service (i.e. Open, Closed, Active)
- **Configurable service**
Specifies whether or not the service can be configured.
- **Configurable port number**
Specifies whether the port number is configurable.
- **Authentication**
Specifies whether an authentication of the communication partner takes place or whether an authentication can be configured.
- **Encryption**
Specifies whether the transfer is encrypted or whether the encryption is configurable.

Service	Protocol	Port number	Default status	Configurable service	Configurable port number	Authentication	Encryption
DHCP	UDP	66/67	Open	✓	-	-	-
DNS	UDP/TCP	53	Closed	✓	-	-	-

Service	Protocol	Port number	Default status	Configurable service	Configurable port number	Authentication	Encryption
EtherNet/IP	UDP	2222 and four ports in the range of 49152 to 65535	Closed	✓	-	-	-
	TCP	44818	Closed	✓	-	-	-
FTP	TCP	21/23	Closed	✓	-	✓	-
HTTP	TCP	80	Open	✓	✓	-	-
HTTPS	TCP	443	Open	✓	✓	✓	✓
NTP	UDP	123	Closed	✓	-	-	-
PROFINET	UDP	34964 and two ports in the range of 49152 to 65535	Open	-	-	-	-
PTP	UDP	319/320	Closed	✓	-	-	-
RADIUS	UDP	1812	Closed	✓	✓	-	-
Secure Syslog	TCP	6514	Closed	✓	✓	✓	✓
SFTP	TCP	22	Closed	✓	✓	✓	✓
SNMP trap	TCP	162	Closed	✓	-	-	-
SNMPv1/v2c	UDP	161	Closed	✓	✓	-	-
SNMPv3	UDP	161	Closed	✓	✓	Configurable	Configurable
SSH	TCP	22	Open	✓	✓	✓	✓
SSH/NETCONF	TCP	830	Open	✓	✓	✓	✓
Syslog	UDP	514	Closed	✓	✓	-	-
TFTP	UDP	69	Closed	✓	-	-	-

2.5 Access rights

A user profile defining the access rights to the functions of the device is assigned to users. The access rights apply equally to all user interfaces.

Users with the **Admin** user profile have full read and write access to the device functions. Users with the **Guest** user profile have limited access rights.

The following access rights are available:

- **Read (R)** - A user can view the configuration.
- **Create (C)** - A user can create new configurations.
- **Update (U)** - A user can change existing configurations.
- **Delete (D)** - A user can delete configurations.

- **Execute (E)** - A user can execute commands.
- **No** - A user has no access rights.

The following table shows the **fundamental access rights** of the user profiles. Deviations are listed in separate tables.

	Access rights per user profile	
	Admin	Guest
All actions	E	No
All configuration data	R/C/U/D	R
All operative data	R	R

The following table shows deviations for **actions**. The entry "-" indicates that there is no deviation from the fundamental access rights.

Activity	Access rights per user profile	
	Admin	Guest
Logging in with the Debug user account	No	-
Pinging an IP address/host (Ping)	-	E
Determining the data path to a host (Traceroute)	-	E

The following table shows deviations for **configuration data**. The entry "-" indicates that there is no deviation from the fundamental access rights.

Activity	Permitted path	Access rights per user profile	
		Admin	Guest
Configuring own user account	/system/authentication/user{OWN}	-	R/U
Configuring local users	/system/authentication/user	-	No
Configuring the Debug user account	/system/authentication/allow-debug-user	-	No
Configuring SNMPv3 users (USM)	/snmp/usm/local/user	-	No
Configuring SNMP communities	/snmp/community	-	No
Configuring SNMP access rights (VACM)	/snmp/vacm	-	No
Configuring certificates	/keystore	-	No

The following table shows deviations for **operative data**. The entry "-" indicates that there is no deviation from the fundamental access rights.

Activity	Permitted path	Access rights per user profile	
		Admin	Guest
Monitoring BFA prevention	/system/authentication/brute-force-prevention	-	No

2.6 Device configuration

SINEC OS supports a two-stage configuration concept in which the current configuration on the device remains unchanged until you commit the configuration changes. For this purpose, SINEC OS has two data memories:

- **Running data memory**
The running data memory contains the configuration with which the device is currently running.
- **Candidate data memory**
A copy of the running configuration is saved in the candidate data memory. You can create, add, delete and change configurations without influencing the running configuration of the device. When you commit the configuration changes, the configuration is moved from the candidate data memory into the running data memory and thus to the running configuration.

A typical configuration session

To be able to configure the device, you must be logged on with write permissions and be in configuration mode. For more information on the configuration mode, refer to "Select a configuration mode (Page 45)".

In a configuration session, you can make one or more changes to the configuration. The configuration changes are initially inactive and are stored in the candidate data memory. The running configuration remains unaffected by this.

You can list the configuration changes and the current configuration on this configuration level. You can also display how the target configuration would look after being committed. For more information, refer to "Displaying configuration changes (Page 45)".

Configuration limits

The configuration limits described apply to the configuration in the running data memory. For more information, refer to "Configuration limits (Page 27)".

The configuration limits are expanded as follows in the candidate data memory: Limit value * 2. This is displayed for DNS servers as an example in the following table:

Function	Limit value	
	Running data memory	Candidate data memory
Number of DNS servers	3	6

The expanded configuration limits allow an entire configuration to be exchanged. You can add and configure 3 new DNS servers with 3 existing DNS servers before you need to delete the existing DNS servers. If you exceed the limit value in the candidate data memory, you receive the following error message:

Candidate configuration limit exceeded

To be able to commit the configuration changes, the limit values of the running data memory must be observed. Otherwise, in the example of DNS servers, the following error message is output:

too many '/system/dns-resolver/server', 6 configured, at most 3 must be configured

Committing configuration changes

To transfer the configuration changes to the current configuration, you must explicitly commit them. You have various options for committing configuration changes. For more information, refer to "Committing configuration changes (Commit) (Page 47)".

Before you commit the configuration changes, you can verify whether there are conflicts with the current configuration.

When configuration changes are committed successfully, the following steps are run through:

1. A time stamp is created to back up and restore the configuration that was running before the change was made.
2. An entry is created in the configuration process.
3. A log entry is created.
4. The configuration changes are integrated in the running configuration. Users who are logged in at the same time are informed about the configuration changes.

If conflicts occur when the configuration changes are committed, none of the changes are applied. The running configuration remains unchanged. You can list the conflicts with the **Validate** command, see also "Checking Configuration Changes (Page 47)".

Restore configurations (Rollback)

You can restore configuration values that were overwritten and thus undo changes that have been committed before. For more information, refer to "Restoring a Configuration (Rollback) (Page 50)".


































































2.7 Supported functions

You can only configure and display certain functions via the Web UI. For all other functions, you use the SINEC OS Command Line Interface (CLI).

The following table provides an overview of the functions that are available via the Web UI:

○ Not supported, ◐ partially supported, ● fully supported

Function	Web UI	CLI
Configuration of the user interfaces	◐	●
Basic settings	●	●
Firmware	◐	●
Device hardware	◐	●
Configuration file	●	●
Signaling contact	●	●
Button functions	●	●
Configuration License PLUG	●	●
Password policy	●	●
User administration	●	●

Function	Web UI	CLI
Debug		
Protection from brute force attacks		
Keys and certificates		
User authentication		
Bridge ports		
VLAN interfaces		
MAC address table		
Static IP address assignment		
Static DNS		
DHCP		
Spanning Tree Protocol		
Loop Detection		
LLDP		
DCP		
PROFINET		
ARP		
SNMP		
Rate limiting		
VLANs		
Traffic classes		
Date and system time		
Time change and daylight saving		
NTP		
SIMATIC time		
PTP		
Static multicast groups		
GMRP		
IGMP snooping		
Database for the multicast filtering		
System status		
Event management		
Ping		
Traceroute		

Function	Web UI	CLI
System logging	●	●
SMTP	●	●
Traffic mirroring	●	●
Cable diagnostics	●	●

2.8 Supported Internet browsers

The SINEC OS Web UI has been tested with the following Internet browsers:

Internet browser	Version
Google Chrome	77
Mozilla Firefox	70
Mozilla Firefox ESR	68

Note

Use of Microsoft Internet Explorer not approved

The SINEC OS Web UI has not been approved for use with Microsoft Internet Explorer. Only use the SINEC OS Web UI with the Internet browsers listed above.

User Interface

This section describes how you use the SINEC OS Web User Interface (Web UI).

3.1 User interface

This section describes the structure of the graphical user interface of the Web UI.

3.1.1 Login page

The following graphic shows the login page.



Figure 3-1 Login page of the SINEC OS Web UI

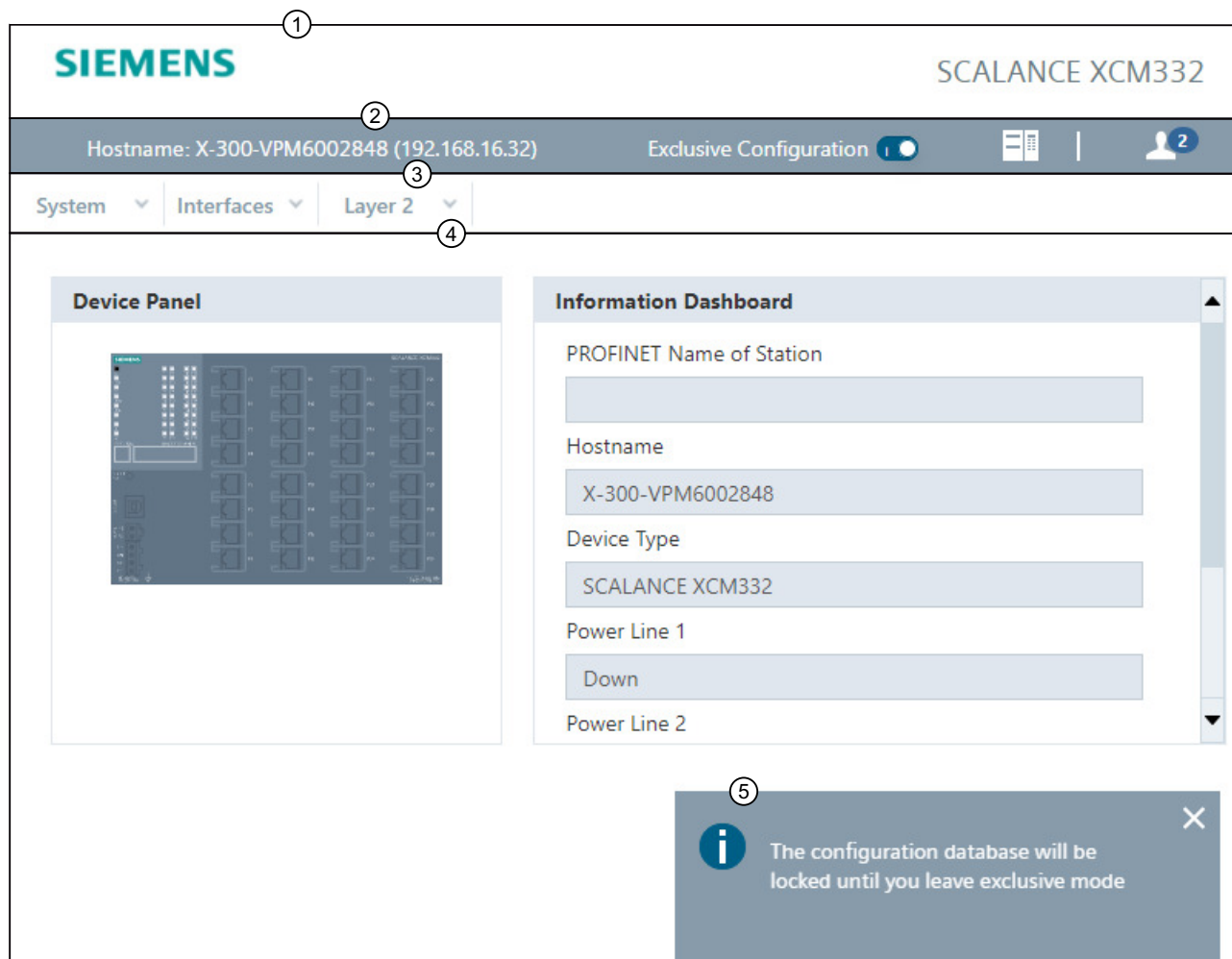
3.1 User interface

The following elements are available to you on the login page:

- **Welcome to SINEC OS**
For more information on logging into the Web UI, see "Login (Page 74)".
- **Support**
When you click the **Support** link, the Siemens Industry Online Support page is opened in a new tab.

3.1.2 Start page

Once you have logged in successfully, you are on the start page. The following graphic shows the individual areas of the Web UI using the start page as an example.



- ① Header
- ② Status bar
- ③ Navigation bar
- ④ Content area
- ⑤ Messages

Figure 3-2 Start page of the SINEC OS Web UI



3.1 User interface






The following table describes the areas of the Web UI.

	Area	Description
①	Header	The following elements are available to you in the header: <ul style="list-style-type: none"> • Logo of Siemens AG When you click on SIEMENS logo, you load the start page of the Web UI. • Name of the device The device name shows the device to which you are connected. You cannot change the device name.
②	Status bar	For more information, refer to "Status bar (Page 40)".
③	Navigation bar	Various menus are available to you in the navigation bar. Click the individual menus to display the submenus. The submenus contain pages on which you can verify and change the device configuration. These pages are displayed in the content area.
④	Content area	The information and configuration pages are displayed in the content area.
⑤	Messages	Messages are displayed in the bottom right margin of the Web UI. The symbols indicate whether these are notes or confirmation prompts.

3.1.3 Status bar

The following functions are available to you in the status bar:

Name	Icon		Description
Hostname	-		The host name is a label that facilitates the identification of a device in a network. The host name also forms the CLI input prompt (e.g. localhost#). For more information on host names, refer to "Changing the host name (Page 76)".
IP address	-		The IP address of the default VLAN (VLAN 1) is displayed in brackets after the host name.
Firmware version	-		The firmware version that is active on the device is shown after the IP address. Example: SINEC OS V02.01.00.00
Exclusive Configuration		Disabled (Default)	You enable or disable the exclusive configuration using the slider: <ul style="list-style-type: none"> • Disabled The shared configuration mode is active. • Enabled The exclusive configuration mode is active. For more information on the configuration mode, refer to "Select a configuration mode (Page 45)".
		Enabled	

Name	Icon		Description
Configuration transactions		No configuration changes (Default)	When you click this icon, the area for configuration transactions is displayed in the content area in the right-side margin of the browser window. This area contains two tabs: Commit and History . The Commit tab is opened by default. The information and configuration pages remain available.
		With uncommitted configuration changes	
		An error occurred while checking or committing the configuration changes.	As soon as you change the current configuration of the device, these changes are displayed on the symbol of the configuration transactions. You can make multiple changes before committing them. The number indicates how many changes have been made since the last time changes were committed.
		The configuration changes are valid.	
User profile			<p>When you click this icon, the following information is displayed:</p> <ul style="list-style-type: none"> • Username - Name of the logged-in user • IP Address - IP address of the client PC via which the user accesses the Web UI • System Time - Current system time • Session Timer - Timer after which the user is automatically logged out If the user does not use the Web UI, the Web UI session is automatically ended after 15 minutes. You can change or disable the timeout. • Log in/out Messages - When the function is enabled, messages are displayed when users log in or out of the device. This also applies to access via SNMP. When the function is disabled, these messages are not displayed. • Logout - Button to log out <p>The number indicates how many users are logged in to the device.</p>
Online help			<p>When you click the book icon, the start page of the online help opens in a new browser tab.</p> <p>Click Begin to open the online help.</p> <p>For more information, refer to "Online help (Page 41)".</p>

3.1.4 Online help

The structure and basic operation of the online help are described in this section.

3.1 User interface

3.1.4.1 Opening the online help

To open the online help, follow these steps:

1. Click on the book icon in the status bar on the right.
The start page of the online help is opened in a new browser tab.
2. Click **Begin**.
You get to the content area of the online help. By default, the table of contents is shown in the **display area** on the left. The **Preface** section is selected and opened in the table of contents. The content of the section is shown on the right.

3.1.4.2 Structure of the online help

The online help consists of the following areas:









- **Header**

The following information is available in the header:

- The Siemens AG logo in the top left
When you click on the SIEMENS logo, you load the start page of the online help.
- The document title on the top right
The document title specifies the version of SINEC OS for which the online help is valid.

- **Control bar**

The control bar contains the following functions:

Name	Icon	Description
Hide		Hides the left part of the display area. Only active when the left part of the display area is displayed.
Show		Shows the left part of the display area. Only active when the left part of the display area is hidden.
Prev		You can navigate in your section structure with this and the next icon. Jumps to the section that you had selected previously.
Next		Jumps to the section that you had selected next. Only active after you have jumped back to a previously selected section.
Settings		Opens the list of settings in the left part of the display area. You can set whether the section numbers are displayed or not.
Selecting the language		Opens the list of available languages in the left part of the display area. In this version, English is available.
Search		Opens the search in the left part of the display area. The search has the following operator controls: <ul style="list-style-type: none"> • An input box for search terms • A drop-down list that defines the searched area <ul style="list-style-type: none"> – Entire document Searches the entire document – Current structure Only searches the section that is currently selected in the table of contents • An Info icon that provides information on the current search situation, for example that multiple words separated by spaces are treated as searches.
Back to table of contents		If settings, language selection or search is displayed, you can get back to the table of contents with this icon.

All settings are temporary. When you close the online help, the settings are lost, even if the browser window remains open. The online help does not save any cookies.

3.1 User interface

- **Display area**

The display area is divided into the following sections:

- The table of contents is shown on the left by default. Settings, language selection or search can also be shown here through operation. You can also hide this part.
- The content of the section selected in the left area is shown on the right. The following functions are available:

Name	Icon	Description
Go back		Goes back to the previous section.
Go forward		Goes to the next section.
Section-in-section link		If this icon is displayed next to a link, you can show the content of the linked section at this point. The linked section is separated by a thin frame. You can only show a limited number of sections at a time.
		Hides the contents of the linked section again.
Zoom		With some graphics, this icon appears in the top right corner when you move the mouse over the graphic. Opens a larger view of the graphic. You can zoom in or out on the graphic with the magnifying glass symbols or the mouse wheel.
		Closes the zoomed view of the graphic.

- **Footer**

The footer contains links to general Siemens information.

3.1.4.3 Searching in the online help

To search in the online help, follow these steps:

1. Open the search.
2. [Optional] Change the searched area. The entire document is searched by default.
3. Click in the input box and enter a search term. As soon as you start to type, matching search terms from the online help appear. The search results are updated continuously. To apply and adapt a search term in the input box, click . To search for multiple words separated by spaces, use double quotes ("").
4. To start the search, click on a search term or click on next to the input box. Instead of the search terms, the sections in which the search term occurs are listed.
5. Click on the section to show its contents. The list of sections continues to be shown. The search term is highlighted in orange.
6. [Optional] To delete a search term from the input box, click

3.2 Configuration transactions

This section describes how to manage the configuration transactions. Configuration transactions refers to all activities in connection with configuration changes, for example, verify, confirm or discard configuration changes.

3.2.1 Select a configuration mode

For the configuration you can switch between a shared or an exclusive configuration mode:

- **Shared configuration mode**
Multiple users can access the device. All changes are hidden from other users until committed.
The changes must be committed so that they are applied to the active configuration.
This mode is active as default.
- **Exclusive configuration mode**
Only one user can enable exclusive configuration on a device. Other users can access the device at the same time. As long as one user has enabled exclusive configuration, the other users cannot apply their changes.
All changes in the exclusive configuration session are hidden from other users until committed. The changes must be committed so that they are applied to the active configuration.
As soon as an exclusive configuration session is ended by manual logout, a timeout or a connection termination, the lock is removed.
If you enable or disable exclusive configuration with pending changes, a query as to whether you want to discard the changes appears in the message area.

For more information on changing the configuration mode, refer to "Status bar (Page 40)".


3.2.2 Displaying configuration changes

To show uncommitted configuration changes, follow these steps:

1. Click the button for **configuration transactions** in the status bar.
The area for configuration transactions is displayed in the content area on the right-side margin of the browser window. The information and configuration pages remain available.
2. Go to the **Commit** tab.

3.2 Configuration transactions

The table displays the following information:

Parameter	Description
Component	Shows the path to the page on which the change was made. Click the path to get to the page.
Operation	Shows the change that was made. Possible values include: <ul style="list-style-type: none"> • created - The element was created. • deleted - The element was deleted. • value_set - The element was changed. • default_set - The element was reset to its default setting.
New Value	Shows the new value after the change.
Old Value	Shows the old value before the change.
Validation	Shows whether the change is valid. Possible values include: <ul style="list-style-type: none"> • Blue check mark - The change was successfully checked against the corresponding data type and is correct. • Green check mark - The change was successfully checked against the existing configuration and is correct. • Red exclamation mark - The change is not valid. The check against the data type or the existing configuration failed. For more information, refer to "Optical Feedback Messages (Page 58)".
Conflict	If conflicts occur when you commit configuration changes, the Validation column changes to Conflict and the configuration changes in conflict are shown with a red exclamation mark. The following error message is output: There is a configuration conflict with another user. It can be resolved with 'Mark as Resolved' operation. Conflicting User: admin For more information on resolving conflicts, refer to "Resolving configuration conflicts (Page 48)". After conflicts have been resolved, the Conflict column changes back to Validation and a red exclamation mark becomes a blue checkmark.
Last column 	You can delete individual configuration changes with the delete icon in the last column.

3.2.3 Checking Configuration Changes

Follow these steps to check the configuration changes:

1. Click the button for **configuration transactions** in the status bar.
2. Go to the **Commit** tab.
3. Click **Validate** in the submenu of the **Commit** button.
Options include:
 - There are no conflicts between the current configuration and configuration changes. The valid changes are marked with a green checkmark. You can commit the changes. For more information, refer to "Commit checked configuration changes (Page 48)".
 - There are conflicts between the current configuration and configuration changes. The device outputs the first conflict found. The invalid changes are identified by a red exclamation mark.

3.2.4 Disabling a function

To disable a function in the Web UI, do the following:

1. Navigate to a function.
2. Change the corresponding parameter to **Disabled**.
3. Commit the change.

3.2.5 Committing configuration changes (Commit)

To commit configuration changes, follow these steps:

1. Click the button for **configuration transactions** in the status bar.
2. Go to the **Commit** tab.
3. Use the **Commit** button.

You do not have to commit every configuration change immediately. You can make several configuration changes and commit them collectively.

When you commit configuration changes, an identifier is assigned to the commitment. You can use this identifier to view the changes in the CLI and restore the previous configuration. The identifier is provided automatically in the Web UI.

You have various options for committing configuration changes.

Note

If the device shuts down or power supply is lost while you commit configuration changes, check the configuration changes as soon as the device can be reached again.

3.2 Configuration transactions

3.2.5.1 Check and commit configuration changes in a single step

To check and commit configuration changes in a single step, do the following:

1. Click the button for **configuration transactions** in the status bar.
2. Go to the **Commit** tab.
3. Click **Commit** to check and commit the changes in a single step.
Options include:
 - There are no conflicts between the current configuration and configuration changes. The configuration changes are committed together with an automatically generated identifier.
 - There are conflicts between the current configuration and configuration changes. The device outputs the first conflict found. The invalid changes are identified by a red exclamation mark.

3.2.5.2 Commit checked configuration changes

To commit configuration changes that have already been checked, do the following:

1. Click the button for **configuration transactions** in the status bar.
2. Go to the **Commit** tab.
3. Check the changes.
For more information, refer to "Checking Configuration Changes (Page 47)".
4. To commit the changes, click **Commit Only** in the submenu of the **Commit** button. The current configuration changes are committed together with an automatically generated identifier.

3.2.6 Resolving configuration conflicts



When configuration changes are committed (in the Configuration transactions area, Commit tab), conflicts can occur between sessions.

Example

In this example, the host name "localhost" is configured for a device.

The host name is changed via a CLI session and, at the same time, via a Web UI session. The value "sec01" is configured in the CLI session and the value "switch02" is configured in the Web UI session.

In the CLI session, the change is committed first and the host name is thus changed into "sec01". If the Web UI session wants to commit its changes, an error message is output and configuration changes in conflict are shown with a red exclamation mark.

Component	Operation	New Value	Old Value	Conflict	
System Information > Host-name	value_set	switch02	localhost		


For more information, refer to "Displaying configuration changes (Page 45)".

In a Web UI session, there are the following ways to resolve configuration conflicts.

Overwriting the configuration change

To overwrite the change of the other session with your configured value, follow these steps:

1. Click **Mark as Resolved** in the submenu of the **Commit** button.
The conflict is resolved.

Component	Operation	New Value	Old Value	Validation	
System Information > Host-name	value_set	switch02	sec01	✓	

2. Commit the configuration changes with **Commit**.
Your changes are applied.
In the example described, the value of the Web UI session would be configured for the host name: "switch02".

Retaining the value of the other session

To apply the value of the other session, click the delete icon in the last column of the conflict row.

The row with the configuration change that is in conflict is deleted.

In the example described, the value of the CLI session would be configured for the host name: "sec01".

Note

You can also resolve the conflict by discarding your configuration changes with **Abort**.

Note that all your uncommitted configuration changes are lost in this case.

3.2.7 Deleting Individual Configuration Changes

Proceed as follows to delete individual configuration changes:

1. Click the button for **configuration transactions** in the status bar.
2. Go to the **Commit** tab.
3. In the row of the change, click the delete icon in the last column.

3.2.8 Discarding All Configuration Changes

Proceed as follows to discard the configuration changes:

1. Click the button for **configuration transactions** in the status bar.
2. Go to the **Commit** tab.
3. Click the **Abort** button.

3.2.9 Showing saved configurations

Before you commit configuration changes, a time stamp is created to save the configuration running before the change. This creates a continuous list of configurations that you can restore. The configuration before the last committed change appears in the list with the number "0".

The device saves a limited number of configurations. After the maximum number of old configurations has been reached, the oldest configuration in the list is deleted when saving a new configuration.

To show saved configurations, follow these steps:

1. Click the button for **configuration transactions** in the status bar.
The area for configuration transactions is displayed in the content area on the right-side margin of the browser window. The information and configuration pages remain available.
2. Go to the **History** tab.

The table displays the following information:

Parameter	Description
First column	You can select a row with the icon.
Number	Shows the number of saved configurations. The larger the number, the older the configuration.
User	Shows the user that committed the configuration changes.
Via	Shows the user interface via which the change was committed and the configuration was saved.
Time Stamp	Shows the date and time at which the configuration was saved.
Label	Shows a user-defined label that was specified when the configuration changes were committed. A label can only be assigned via the CLI.
Comment	Shows a user-defined comment that was specified when the configuration changes were committed. A comment can only be assigned via the CLI.

3.2.10 Restoring a Configuration (Rollback)

When you restore a configuration, the running configuration is reset to an older version.

Note

After downloading a firmware file with a deviating firmware version, all saved configuration versions are deleted. The current configuration is retained and is not changed.

To restore a configuration, follow these steps:

1. Click the button for **configuration transactions** in the status bar.
2. Go to the **History** tab.
The table displays saved configurations that you can restore.
For more information, refer to "Showing saved configurations (Page 50)".

3. Select a configuration and select which configuration(s) you want to restore.
Options include:

Option	Description
Selective	Default Only the changes of the selected configuration are undone. The selected row is highlighted in blue.
Cumulative	All changes made since committing the selected configuration are undone. All affected rows are highlighted in blue, from the configuration with the number 0 to the selected configuration.

4. Click **Load Rollback**.
5. Go to the **Commit** tab.
6. Commit the change(s).

3.3 Basic operation

This section describes the basic operation of the Web UI.

3.3.1 Working with tables

Many configurations in the Web UI are organized in tables. This section describes how to work with tables in the Web UI.

3.3.1.1 Add a new row

To add a new row, do the following:

1. Click the **Add** button.
2. [Optional] Configure the parameters of the row.
3. Commit the changes.

3.3.1.2 Select a row

To select a row, click on the check mark in the first column. A selected row is highlighted in blue.

To cancel the selection, click again on the check mark in the first column.

3.3 Basic operation

3.3.1.3 Delete a row

To delete a row, do the following:

1. Select the row you want to delete.
2. Click the **Delete** button.
3. Commit the change.

3.3.1.4 Configuring Parameters for All Rows of a Column at the Same Time

Some tables have a first row with the keyword **All**. The configurations that you make and confirm in the first row are applied for all subsequent rows.

You can select an entry from the drop-down list or enter a value in an input box. In the row **All**, drop-down lists show the text **Select....** Input boxes are empty in the row **All**.

If a configuration for a row is not possible, a red exclamation mark is shown and an error message is output.

Example

In this example, two parameters for loop detection are configured.

To configure parameters for all rows of a table at the same time, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
The table under **Loop Detection** has a first row with the entry **All** in the first column **Interface**.
2. In the first row under **Transmission State**, select the desired entry in the drop-down list.
The selection is applied for all bridge ports. In each row, a blue checkmark is displayed next to the drop-down box.
3. Enter the desired value in the first row under **Transmission Interval**.
The value is applied for all bridge ports. In each row, a blue checkmark is displayed next to the input box.
4. Commit the changes.

3.3.1.5 Performing Actions for all Rows of a Table at the Same Time

Some tables have a first row with the keyword **All**. If this row contains a button, the corresponding action is executed for all subsequent rows.

Example

In this example, loop detection is manually reset for all bridge ports.

To reset all bridge ports at the same time, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
The table under **Loop Detection** has a first row with the entry **All** in the first column **Interface**.
2. Click **Reset** in the last column of the first row.
All bridge ports are reset. In each row, a green checkmark is displayed next to the button.

3.3.1.6 Editable and read-only cells

Editable and read-only cells differ visually with respect to their border.

Editable cells have a border. In the following example, the cells of the **Description**, **Link Up/Down Trap** and **Interface State** columns are editable.

Read-only cells have no border. In the following example, the cells of the **Interface** and **Operational Status** columns are read-only.

Interface	Description	Link Up/Down Trap	Interface State	Operational Status
ethernet0/1		Enabled ▾	Enabled ▾	down
ethernet0/2		Disabled ▾	Enabled ▾	up

Figure 3-3 Editable and read-only cells

3.3.1.7 Define the number of entries to be displayed

There are static tables with a fixed number of entries, e.g. tables with interfaces. The number of physical interfaces of a device is defined.

Dynamic tables vary with respect to the number of entries, e.g. tables with VLANs and the logfile.

Static and dynamic entries are combined in some tables. A table with interface statistics contains both the fixed number of physical interfaces and the varying number of created VLANs.

If a table contains more than 25 entries, the following information is displayed in the bottom right margin of the table:

- How many table entries are currently displayed (e.g. 1 -25 of 29 items)
- How many entries the table contains in total (e.g. 1 -25 of 29 items)

To define the number of displayed entries, select the corresponding number under **items per page** in the bottom right margin of the table.

You can display 25, 50 or 100 entries. To display all entries, select **All**. With large tables, it may take some time until all entries are displayed. For this reason, a confirmation prompt appears.

In static tables, 50 entries are displayed by default.

In dynamic tables and mixed forms, 25 entries are displayed by default.





3.3.1.8 Tables with multiple pages

If a table contains more entries than can be displayed on one page, the entries continue on a new page.

The following information is displayed in the bottom left margin of the table:

- Which page of the table is currently being displayed (e.g. 1/3)
- How many pages the table contains in total (e.g. 1/3)

With the following buttons, you can navigate between the pages of the table.

Button	Description
	You get to the next page with this button.
	You get to the last page with this button.
	You get to the previous page with this button.
	You get to the first page with this button.

3.3.2 Switching to the Start Page

Click on the SIEMENS logo on the left in the header to switch to the start page.

3.3.3 Multiple Selection in Drop-Down Lists

There are various types of drop-down lists. In some drop-down lists, you can only select one of the displayed entries, e.g. Enabled or Disabled. However, if you are selecting interfaces or VLANs, for example, multiple selection is possible in some drop-down lists. You can recognize these drop-down lists by the following entry in the default state: 0 item selected.

Open the drop-down list and select or deselect as many entries as you like.

The selected entries are displayed in the original order in which they are listed. If the field is not big enough to show all selected entries, they are truncated with "...". When you hover over the field with the mouse, all selected entries are displayed in a tooltip.

To select multiple entries at the same time, click the field and enter a range. For example, if you want to select VLANs 3, 4, 5 and 6, enter "3-6" and then press **Enter** to confirm. This function is not available for interfaces.

Some drop-down lists are expandable. For example, you can specify VLANs 6-10 as a range, even though VLAN 10 does not yet exist. However, the entries are not created automatically. You need to create the corresponding entries yourself.

To deselect all selected entries at the same time, click the top entry "-".

3.3.4 Loading and saving files via a remote server

You can load and save files via a remote server.

The following information is required for loading and saving via a remote server:

- **Protocol**

The following protocols are supported:

- FTP

- SFTP

To establish a connection to an SFTP server, the fingerprint of the public key must be stored in the truststore of the device.

There is a security prompt on the first connection establishment with an SFTP server.

When you confirm this prompt, the device automatically saves the fingerprint of the public key in the truststore. The SFTP server is verified from then on. A security prompt no longer occurs when connections to this SFTP server are established.

- TFTP

Note

Because TFTP is not a TCP-based protocol, errors can occur during file transfers.

If you experience file transfer errors, configure the TFTP server parameters with the following values:

- TFTP timeout: 300 seconds
 - TFTP retransmissions: 100
-

- HTTP

- **User name and password**

The user name and password depend on the protocol:

- With the FTP and SFTP protocols, you need to specify user name and password.
- With HTTP the information is not necessarily required.
- With TFTP the information is not available.

- **Port**

You only need to specify the port if the default port is not to be used:

Protocol	Default port
FTP	TCP port 21
SFTP	TCP port 22
TFTP	UDP port 69
HTTP	TCP port 80

- **Path to the file including the file name**

With the SFTP protocol, you need to specify the entire path up to the file on the remote server.

To load or save a file via a remote server, do the following:

1. Navigate to the appropriate page in the Web UI, for example, **System » Load & Save » Firmware**.
2. Select a protocol under **Protocol**.
3. Enter the IP address of the server under **Server Address / FQDN**.

3.3 Basic operation

4. [Optional] Under **Server Port**, change the port if the remote server does not use the default port.
5. [Optional] If you have selected the option **FTP, SFTP** or **HTTP** under **Protocol**, enter the user name under **Server User**.
6. [Optional] If you have selected the option **FTP, SFTP** or **HTTP** under **Protocol**, enter the password under **Server Password**.
7. Under **File Path / File Name**, enter the path to the file and the file name.
8. [Optional] Under **File Protection**, you can save the file in protected mode.
Options include:

Option	Description
Disabled	Default The file is saved without further options.
Enabled	The file is saved in protected mode. In protected mode, the saved file is given a checksum. The checksum ensures that the saved file can only be downloaded to a device again if it was not changed. The device verifies the checksum when the saved file is downloaded. If the file has been changed, the checksum is no longer correct and the file is not downloaded.

9. [Optional] If you have selected the option **Enabled** under **File Protection**, assign a password under **File Password**.
Condition:
 - Must be between 1 and 255 characters long
 - All standard characters are allowed, plus the following special characters:
\$ % & () * + , - . / : < = > @ [] ^ _ { } ~
10. [Optional] If you have assigned a password under **File Password**, repeat the password under **File Password-Confirm**.
11. Click **Load** or **Save**.
When saving on a local client PC, it depends on the browser settings whether the file is saved directly to a specified folder or if you first see a prompt in which you can select the storage location.

3.3.5 Specifying a duration

To specify a duration, combine the required parts of a time specification (from year to second) with the appropriate separator.

The format of the duration is **nYnMnDnhnmns**.

The individual time specifications and separators are defined as follows:

- **nY** - Indicates the number of years.
- **nM** - Indicates the number of months.
- **nD** - Indicates the number of days.
- **nh** - Indicates the number of hours.

- **nm** - Indicates the number of minutes.
- **ns** - Indicates the number of seconds.

The following is defined for the calculation:

- 30 days correspond to 1 month
- This results in 2592000 seconds per month
(seconds per day * 30)

You must observe the following rules when entering a duration:

- There must be at least one time specification with separators.
- No spaces are used between the time specifications.
- The order of the time entries is fixed.
- If a time specification has the value "0", the time specification including separator can be omitted.
- The time specifications are positive integers. The seconds specification may contain decimal places.
- To represent negative durations, a minus sign is prefixed to the entire duration.

Positive examples

The following table shows correctly entered durations.

Duration	Description
2Y5M6D12h33m15s	2 years, 5 months, 6 days, 12 hours, 33 minutes, 15 seconds
2D35m	2 days, 35 minutes
1m30.5s	1 minute, 30.5 seconds
-6M	Minus 6 months
20M	20 months (The number of months is not limited to 12.)








Negative examples

The following table shows invalid durations.

Duration	Description
	An empty entry is not allowed.
1M2Y	The order of the time entries must be observed.
1.5m	Decimal places are only allowed for seconds.
1Y-6M	The minus sign must be in the first position.

3.3.6 Optical Feedback Messages

The Web UI provides the following optical feedback on inputs, configurations etc.

Optical feedback message	Description
	All fields have a blue border.
	<p>Load symbol</p> <p>An input is being checked.</p>
	<p>Blue check mark</p> <p>An input was successfully checked against the corresponding data type and is correct.</p> <p>The check is carried out immediately during the input.</p> <p>Only correct configuration changes are added to the candidate list.</p> <p>Example</p> <p>In this example, the system time was entered with an invalid format: "2020-3-25 9:00"</p> <p>The check against the data type failed. A red exclamation mark and an error message are output.</p> <p>Example</p> <p>In this example, the system time was entered with a valid format: "2020-03-25 09:00:00"</p> <p>The check against the data type is successful. A blue check mark is displayed.</p>
	<p>Green check mark</p> <p>An input was successfully checked against the existing configuration and is correct.</p> <p>To start the check, use the Validate function in the configuration transactions area. For more information, refer to "Checking Configuration Changes (Page 47)".</p> <p>Only valid configuration changes can be committed.</p>
	<p>Red exclamation mark</p> <p>An input is not valid. The check against the data type or the existing configuration failed.</p>
	<p>Note</p> <p>Notes are displayed in the bottom right margin of the Web UI. Only one note is displayed at any time. A new note replaces the existing note.</p> <p>A note is only displayed until you click the close icon in the top right corner of the note.</p>
	<p>Confirmation prompt</p> <p>Confirmation prompts are displayed in the bottom right margin of the Web UI if a decision is required of the user.</p> <p>A confirmation prompt is displayed until you respond with Yes or No. The action that triggered the confirmation prompt is only performed or canceled after your response.</p>

Optical feedback message	Description
	Truncated interface texts If the available space for an interface text is not big enough, the text is truncated with "...". This applies to headings and fields.
	Tooltips When you hover over the field with the mouse, the truncated text is displayed as tooltip.

3.3.7 Adapting the Page Layout

When the area for the configuration transactions is open, you can adapt the page layout of the content area.

Use the slider to adjust the division between the information/configuration pages and the configuration transactions area.

3.3.8 Operating the Web UI with the Keyboard

Depending on the browser, some key combinations may vary.

Action	Key/Shortcut
Jump to next item	Tab key
Operate a button	Enter
Select or clear a check box	Space bar
Navigate through the entries of a drop-down list	Up and down arrows
Jump to the previous selected page	[Alt] + [left arrow]
Jump to the next selected page	[Alt] + [right arrow]
Copy selected content	[Ctrl] + [C]
Paste selected content	[Ctrl] + [V]
Cut selected content	[Ctrl] + [X]

3.4 Configuration of the user interfaces

This section describes the administration of the SINEC OS user interfaces CLI, Web UI and NETCONF.

3.4 Configuration of the user interfaces

For more information on the SNMP user interface, refer to "SNMP (Page 278)".

For each user interface, you can configure the state (enabled or disabled), the inactivity timeout, and the protocol settings (e.g. IP address and port, SSH or TLS keys used).

3.4.1 Understanding user interface configuration

The server configuration is implemented in SINEC OS via endpoints. An endpoint is defined as an independent instance of a server service.

By default, server endpoints are pre-defined in SINEC OS for the following user interfaces and protocols:

- CLI SSH
- Web UI HTTP
- Web UI HTTPS
- NETCONF SSH
- SNMP

For more information on configuring the SNMP user interface, refer to "Configuring the SNMP agent (Page 278)".

Only one server endpoint can be defined per user interface and protocol.

Note

The pre-defined endpoints cannot be renamed or deleted. You cannot create any further endpoints.

The following tables contain the default settings of the endpoints.

CLI SSH

Endpoint	Default
Name	default
Endpoint enabled	Yes
IP address	0.0.0.0
Port	22

Web UI HTTP

Endpoint	Default
Name	unsecure
Endpoint enabled	No
IP address	0.0.0.0
Port	80

Web UI HTTPS

Endpoint	Default
Name	secure
Endpoint enabled	Yes
IP address	0.0.0.0
Port	443

NETCONF SSH

Endpoint	Default
Name	default
Endpoint enabled	Yes
IP address	0.0.0.0
Port	830

3.4.2 Configuring the NETCONF user interface

To configure the NETCONF user interface, do the following:

1. Enable the NETCONF user interface.
For more information, refer to "Enabling the NETCONF user interface (Page 61)".
2. [Optional] Change the inactivity timeout for NETCONF sessions.
For more information, refer to "Changing the inactivity timeout for NETCONF sessions (Page 62)".
3. Configure a server endpoint for NETCONF.
For more information, refer to "Configuring a server endpoint for NETCONF (Page 62)".
4. Configure the SSH key exchange method for a NETCONF server endpoint.
For more information, refer to "Changing the SSH Key Exchange Method for a NETCONF Server Endpoint (Page 63)".
5. Enable a server endpoint for NETCONF.
For more information, refer to "Enabling a server endpoint for NETCONF (Page 64)".

3.4.2.1 Enabling the NETCONF user interface

The NETCONF user interface is enabled by default.

Only users with the **Admin** user profile can enable the NETCONF user interface.

To enable the NETCONF user interface, do the following:

1. Navigate to **System » Management Services » Overview**.
2. Under **NETCONF**, change **Status** to **Enabled**.
3. Commit the change.

3.4 Configuration of the user interfaces

3.4.2.2 Changing the inactivity timeout for NETCONF sessions

The inactivity timeout indicates the time for which a NETCONF session remains open in case of inactivity. Once the inactivity timeout expires, the server automatically terminates the NETCONF session.

Note

When you change the inactivity timeout, the change only affects new NETCONF sessions. The inactivity timeout is not changed for existing NETCONF sessions.

Only users with the **Admin** user profile can change the inactivity timeout.

To change the inactivity timeout for NETCONF sessions, follow these steps:

1. Navigate to **System » Management Services » Overview**.
2. Under **NETCONF**, change **Idle Timeout**.
Conditions:
 - Formatted as nYnMnDnhnmns, where n is a user-defined number
 - Minimum 0 seconds (0s)
 - Maximum 49 days 17 hours 2 minutes 47 seconds (49D17h2m47s)

Default: 5 m (5 minutes)

If you set the value to **0 s**, automatic logout is disabled.

If you set the value **1M** (1 month), the device calculates the inactivity timeout as follows: 365 days/12 months. Accordingly, a value of 30.4167 days is configured.

3. Commit the change.

3.4.2.3 Configuring a server endpoint for NETCONF

Configure the local IP address and the port via which a server endpoint processes NETCONF requests.

NOTICE
Configuration hazard - risk of connection loss
If the device is assigned its IP address dynamically via DHCP, not the following: If the IP address that the device receives via DHCP does not match the IP address that you configured for the NETCONF server endpoint, the device cannot be reached via the NETCONF server endpoint. You have the following options to prevent connection loss: <ul style="list-style-type: none">• Allows client request on all local addresses (default IP address: 0.0.0.0).• Assign a static IP address for the device.• Make sure that the same IP address is always assigned via DHCP.

Only users with the **Admin** user profile can configure a server endpoint.

To configure a server endpoint, do the following:

1. Navigate to **System » Management Services » Overview**.
The available server endpoints for NETCONF are displayed under **NETCONF » Endpoint**.
2. Under **Endpoint**, select an endpoint. In the **TCP Port** column, change the port over which NETCONF requests are being processed.
Conditions:
 - The number 830
 - A number between 1024 and 49151
 - A number between 49500 and 65535Default: 830
3. Under **Endpoint**, select an endpoint. In the **IP Address** column, change the IP address over which NETCONF requests are being processed.
Default: 0.0.0.0
The default IP address allows client requests on all local addresses.
4. Commit the changes.

3.4.2.4 Changing the SSH Key Exchange Method for a NETCONF Server Endpoint

When an SSH connection is established, key exchange takes place to generate and exchange shared session keys for authentication and encryption.

The key strength is determined by the key exchange method. The higher the number of the Diffie-Hellman group, the stronger and more secure the key is. However, a stronger key requires more computing time and performance.

Note

You can find an assignment of the elliptical curves to Diffie-Hellman groups here:

Internet Key Exchange Version 2 (IKEv2) Parameters (<https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-8>)

Section **Transform Type 4 - Diffie-Hellman Group Transform IDs**

Only users with the **Admin** user profile can configure the SSH key exchange method.

To change the SSH key exchange method for a NETCONF server endpoint, do the following:

1. Navigate to **System » Management Services » Transport Security**.
2. Under **Cipher Selection for NETCONF**, click **Add**.
A new row is added to the table.

3.4 Configuration of the user interfaces

3. Select an SSH key exchange method under **Cipher Selection**.
Options include:
 - curve448-sha512
For more information, refer to RFC8731 (<https://www.ietf.org/rfc/rfc8731.html>)
 - curve25519-sha256
For more information, refer to RFC8731 (<https://www.ietf.org/rfc/rfc8731.html>)
 - diffie-hellman-group14-sha1
For more information, refer to RFC4253 (<https://www.ietf.org/rfc/rfc4253.html>)
 - diffie-hellman-group16-sha512
For more information, refer to RFC8268 (<https://www.ietf.org/rfc/rfc8268.html>)
 - ecdh-sha2-nistp256
For more information, refer to RFC5656 (<https://www.ietf.org/rfc/rfc5656.html>)
 - ecdh-sha2-nistp384
For more information, refer to RFC5656 (<https://www.ietf.org/rfc/rfc5656.html>)
 - ecdh-sha2-nistp521
For more information, refer to RFC5656 (<https://www.ietf.org/rfc/rfc5656.html>)

Default:

 - curve25519-sha256
 - diffie-hellman-group16-sha512
 - ecdh-sha2-nistp256
4. Commit the change.

3.4.2.5 Enabling a server endpoint for NETCONF

The server endpoint for NETCONF is enabled by default.

Only users with the **Admin** user profile can enable a server endpoint.

To enable a server endpoint for NETCONF, do the following:

1. Navigate to **System » Management Services » Overview**.
The available server endpoints for NETCONF are displayed under **NETCONF » Endpoint**.
2. Under **Endpoint**, select an endpoint and change **Status** to **Enabled**.
3. Commit the change.

3.4.3 Configuring the CLI user interface

To configure the CLI user interface, do the following:

1. [Optional] Change the inactivity timeout for CLI sessions.
For more information, refer to "Changing the inactivity timeout for CLI sessions (Page 65)".
2. Configure a server endpoint for the CLI.
For more information, refer to "Configuring a server endpoint for the CLI (Page 66)".

3. Configure the SSH key exchange method for a CLI server endpoint.
For more information, refer to "Changing the SSH Key Exchange Method for a CLI Server Endpoint (Page 66)".
4. Enable a server endpoint for the CLI.
For more information, refer to "Enabling a server endpoint for the CLI (Page 67)".

3.4.3.1 Changing the inactivity timeout for CLI sessions

The inactivity timeout indicates the time for which a CLI session remains open in case of inactivity. Once the inactivity timeout expires, the server automatically terminates the CLI session. The value also applies to sessions where you access the CLI through a serial connection.

Note

With this command, you change the inactivity timeout globally for all CLI sessions. You can overwrite the global timeout for local CLI sessions. For more information about configuring local CLI sessions, refer to the **SINEC OS CLI Configuration Manual**.

Note

When you change the inactivity timeout, the change only affects new CLI sessions. The inactivity timeout is not changed for existing CLI sessions.

Only users with the **Admin** user profile can change the inactivity timeout.

To change the inactivity timeout globally for CLI sessions, follow these steps:

1. Navigate to **System » Management Services » Overview**.
2. Under **CLI**, change **Idle Timeout**.

Conditions:

- Formatted as nYnMnDnhnmns, where n is a user-defined number
- Minimum 0 seconds (0s)
- Maximum 49 days 17 hours 2 minutes 47 seconds (49D17h2m47s)

Default: 15m (15 minutes)

If you set the value to **0 s**, automatic logout is disabled.

If you set the value **1M** (1 month), the device calculates the inactivity timeout as follows: 365 days/12 months. Accordingly, a value of 30.4167 days is configured.

3. Commit the change.

3.4.3.2 Configuring a server endpoint for the CLI

Configure the local IP address and the port via which a server endpoint processes CLI requests.

NOTICE
Configuration hazard - risk of connection loss
If the device is assigned its IP address dynamically via DHCP, not the following: If the IP address that the device receives via DHCP does not match the IP address that you configured for the NETCONF server endpoint, the device cannot be reached via the NETCONF server endpoint. You have the following options to prevent connection loss:
<ul style="list-style-type: none">• Allows client request on all local addresses (default IP address: 0.0.0.0).• Assign a static IP address for the device.• Make sure that the same IP address is always assigned via DHCP.

Only users with the **Admin** user profile can configure a server endpoint.

To configure a server endpoint, do the following:

1. Navigate to **System » Management Services » Overview**.
The available server endpoints for CLI are displayed under **CLI » Endpoint**.
2. Under **Endpoint**, select an endpoint. In the **TCP Port** column, change the port over which CLI requests are being processed.
Conditions:
 - The number 22
 - A number between 1024 and 49151
 - A number between 49500 and 65535Default: 22
3. Under **Endpoint**, change **IP Address** for the selected endpoint to the IP address over which NETCONF requests will be processed.
Default: 0.0.0.0
The default IP address allows client requests on all local addresses.
4. Commit the changes.

3.4.3.3 Changing the SSH Key Exchange Method for a CLI Server Endpoint

When an SSH connection is established, key exchange takes place to generate and exchange shared session keys for authentication and encryption.

The key strength is determined by the key exchange method. The higher the number of the Diffie-Hellman group, the stronger and more secure the key is. However, a stronger key requires more computing time and performance.

Note

You can find an assignment of the elliptical curves to Diffie-Hellman groups here:

Internet Key Exchange Version 2 (IKEv2) Parameters (<https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-8>)

Section Transform Type 4 - Diffie-Hellman Group Transform IDs

Only users with the **Admin** user profile can configure the SSH key exchange method.

To change the SSH key exchange method for a CLI server endpoint, do the following:

1. Navigate to **System » Management Services » Transport Security**.
 2. Under **Cipher Selection for CLI**, click **Add**.
A new row is added to the table.
 3. Select an SSH key exchange method under **Cipher Selection**.
Options include:
 - curve448-sha512
For more information, refer to RFC8731 (<https://www.ietf.org/rfc/rfc8731.html>)
 - curve25519-sha256
For more information, refer to RFC8731 (<https://www.ietf.org/rfc/rfc8731.html>)
 - diffie-hellman-group14-sha1
For more information, refer to RFC4253 (<https://www.ietf.org/rfc/rfc4253.html>)
 - diffie-hellman-group16-sha512
For more information, refer to RFC8268 (<https://www.ietf.org/rfc/rfc8268.html>)
 - ecdh-sha2-nistp256
For more information, refer to RFC5656 (<https://www.ietf.org/rfc/rfc5656.html>)
 - ecdh-sha2-nistp384
For more information, refer to RFC5656 (<https://www.ietf.org/rfc/rfc5656.html>)
 - ecdh-sha2-nistp521
For more information, refer to RFC5656 (<https://www.ietf.org/rfc/rfc5656.html>)
- Default:
- curve25519-sha256
 - diffie-hellman-group16-sha512
 - ecdh-sha2-nistp256
4. Commit the change.

3.4.3.4 Enabling a server endpoint for the CLI

The server endpoint for the CLI is enabled by default.

3.4 Configuration of the user interfaces

Only users with the **Admin** user profile can enable a server endpoint.

Note

If you disable the server endpoint for the CLI, you can continue to access the CLI via a serial connection.

To enable a server endpoint for the CLI, do the following:

1. Navigate to **System » Management Services » Overview**.
The available server endpoints for CLI are displayed under **CLI » Endpoint**.
2. Under **Endpoint**, select an endpoint and change **Status** to **Enabled**.
3. Commit the change.

3.4.4 Configuring the Web user interface

To configure the Web user interface, do the following:

1. Enable the Web user interface.
For more information, refer to "Enabling the Web user interface (Page 68)".
2. [Optional] Change the inactivity timeout for Web UI sessions.
For more information, refer to "Changing the inactivity timeout for Web UI sessions (Page 69)".
3. Configure an HTTP server endpoint for the Web UI.
For more information, refer to "Configuring an HTTP server endpoint for the Web UI (Page 70)".
4. Enable an HTTP server endpoint for the Web UI.
For more information, refer to "Enabling an HTTP server endpoint for the Web UI (Page 70)".
5. Configure an HTTPS server endpoint for the Web UI.
For more information, refer to "Configuring an HTTPS server endpoint for the Web UI (Page 71)".
6. Enable an HTTPS server endpoint for the Web UI.
For more information, refer to "Enabling an HTTPS server endpoint for the Web UI (Page 72)".
7. [Optional] Reference a user-defined HTTPS certificate.
For more information, refer to "Using a user-defined HTTPS certificate (Page 72)".

3.4.4.1 Enabling the Web user interface

The Web user interface is enabled by default.

Only users with the **Admin** user profile can enable the Web user interface.

To enable the Web user interface, do the following:

1. Navigate to **System » Management Services » Overview**.
2. Under **WebUI (HTTP/HTTPS)**, change **Status** to **Enabled**.
3. Commit the change.

3.4.4.2 Changing the inactivity timeout for Web UI sessions

The inactivity timeout indicates the time for which a Web UI session remains open in case of inactivity. Once the inactivity timeout expires, the server automatically terminates the Web UI session.

Note

When you change the inactivity timeout, the change only affects new Web UI sessions. The inactivity timeout is not changed for existing Web UI sessions.

Only users with the **Admin** user profile can change the inactivity timeout.

To change the inactivity timeout for Web UI sessions, follow these steps:

1. Navigate to **System » Management Services » Overview**.
2. Under **WebUI (HTTP/HTTPS)** change **Idle Timeout**.
Conditions:
 - Formatted as nYnMnDnHnmns, where n is a user-defined number
 - Minimum 0 seconds (0s)
 - Maximum 49 days 17 hours 2 minutes 47 seconds (49D17h2m47s)

Default: 15m (15 minutes)

If you set the value to **0 s**, automatic logout is disabled.

If you set the value **1M** (1 month), the device calculates the inactivity timeout as follows: 365 days/12 months. Accordingly, a value of 30.4167 days is configured.

3. Commit the change.

3.4.4.3 Configuring an HTTP server endpoint for the Web UI

Configure the local IP address and the port via which an HTTP server endpoint processes Web UI requests.

NOTICE
Configuration hazard - risk of connection loss
If the device is assigned its IP address dynamically via DHCP, not the following: If the IP address that the device receives via DHCP does not match the IP address that you configured for the NETCONF server endpoint, the device cannot be reached via the NETCONF server endpoint. You have the following options to prevent connection loss:
<ul style="list-style-type: none">• Allows client request on all local addresses (default IP address: 0.0.0.0).• Assign a static IP address for the device.• Make sure that the same IP address is always assigned via DHCP.

Only users with the **Admin** user profile can configure a server endpoint.

To configure an HTTP server endpoint, do the following:

1. Navigate to **System >> Management Services >> Overview**.
The available HTTP server endpoints for SNMP are displayed under **WebUI (HTTP/HTTPS) >> Endpoint**.
2. Under **Endpoint**, change **TCP Port** for the selected HTTP server endpoint to the port that will process Web UI requests.
Conditions:
 - The number 80
 - A number between 1024 and 49151
 - A number between 49500 and 65535Default: 80
3. Under **Endpoint**, change **IP Address** for the selected HTTP server endpoint to the IP address over which Web UI requests will be processed.
Default: 0.0.0.0
The default IP address allows client requests on all local addresses.
4. Commit the changes.

3.4.4.4 Enabling an HTTP server endpoint for the Web UI

By default, no HTTP server endpoint for the Web UI is enabled.

Only users with the **Admin** user profile can enable a server endpoint.

To enable an HTTP server endpoint for the Web UI, do the following:

1. Navigate to **System » Management Services » Overview**.
The available HTTP server endpoints for SNMP are displayed under **WebUI (HTTP/HTTPS) » Endpoint**.
2. Under **Endpoint**, select an HTTP server endpoint and change the **Status** to **Enabled**.
3. Commit the change.

3.4.4.5 Configuring an HTTPS server endpoint for the Web UI

Configure the local IP address and the port via which an HTTPS server endpoint processes Web UI requests.

NOTICE

Configuration hazard - risk of connection loss

If the device is assigned its IP address dynamically via DHCP, not the following:

If the IP address that the device receives via DHCP does not match the IP address that you configured for the NETCONF server endpoint, the device cannot be reached via the NETCONF server endpoint.

You have the following options to prevent connection loss:

- Allows client request on all local addresses (default IP address: 0.0.0.0).
- Assign a static IP address for the device.
- Make sure that the same IP address is always assigned via DHCP.

Only users with the **Admin** user profile can configure a server endpoint.

To configure an HTTPS server endpoint, do the following:

1. Navigate to **System » Management Services » Overview**.
The available HTTPS server endpoints are displayed under **WebUI (HTTP/HTTPS) » Endpoint**.
2. Under **Endpoint**, change **TCP Port** for the selected HTTPS server endpoint to the port that will receive Web UI requests.
Conditions:
 - The number 443
 - A number between 1024 and 49151
 - A number between 49500 and 65535Default: 443
3. Under **Endpoint**, change **IP Address** for the selected HTTPS server endpoint to the IP address over which Web UI requests will be processed.
Default: 0.0.0.0
The default IP address allows client requests on all local addresses.
4. Commit the changes.

3.4.4.6 Enabling an HTTPS server endpoint for the Web UI

An HTTPS server endpoint for the Web UI is enabled by default.

Only users with the **Admin** user profile can enable a server endpoint.

To enable an HTTPS server endpoint for the Web UI, do the following:

1. Navigate to **System » Management Services » Overview**.
The available HTTPS server endpoints for SNMP are displayed under **WebUI (HTTP/HTTPS) » Endpoint**.
2. Under **Endpoint**, select an HTTPS server endpoint and change the **Status** to **Enabled**.
3. Commit the change.

3.4.4.7 Using a user-defined HTTPS certificate

The HTTPS certificate certifies the identity of the device and controls the encrypted data exchange.

To be able to use a user-defined HTTPS certificate, the certificate must be present in the keystore. For more information, refer to "Keys and certificates (Page 144)".

It is strongly recommended you create your own HTTPS certificates and make them available. It is recommended you use HTTPS certificates signed either by a reliable external or by an internal certificate authority.

To use an HTTPS certificate, do the following:

1. Navigate to **System » Management Services » Transport Security**.
2. Under **Keystore Reference of TLS Certificate and Key for HTTPS Endpoint**, select the name of a key pair under **Asymmetric Key**.
3. Under **Certificate**, select the name of a certificate or a certificate chain.
4. Commit the change.
To apply the loaded certificate, you must restart the HTTPS server endpoint.
5. Navigate to **System » Management Services » Overview**.
The available HTTPS server endpoints are displayed under **WebUI (HTTP/HTTPS) » Endpoint**.
6. To activate the certificate, restart the device.
For more information, refer to "Restarting the device (Page 80)".
When the restart is complete, the login page is displayed.
7. Log in.
For more information, refer to "Logging in to a configured device (Page 75)".

Getting started

This chapter describes basic steps that should be performed during the initial commissioning of the device. Tasks include connecting to the device, accessing the user interface, and configuring a basic network.

4.1 Accessing the Web UI via a network connection

To access the Web UI (Web user interface), establish a remote connection between a client PC and a device via the network.

The device has an integrated HTTP/HTTPS server for this purpose. If you address a device using an Internet browser, it returns HTML pages to the client PC depending on the user input.

Requirements

- The device has an IP address.

Note

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

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

Note

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

- Access via HTTP(S) is activated on the device.
- An Internet browser is available on the client PC.
- JavaScript is activated in the Internet browser.
- The Internet browser must not be configured in such a way that it reloads the page from the server each time the page is accessed. Other mechanisms ensure the dynamic page contents are up to date.
- If you are using a firewall, enable the corresponding ports.

Protocol	TCP port
HTTP	80
HTTPS	443

Establishing a connection to a device

To access the Web UI, do the following:


1. Open an Internet browser.
2. In the address box of the Internet browser, enter the IP address or the URL of the device.
3. Press **Enter**.
If there is a problem-free connection to the device, the login page of the Web UI is displayed.
4. Log in.
For more information, refer to "Login (Page 74)".

4.2 Login

This section describes the various methods for logging into SINEC OS.

4.2.1 Default user profiles and passwords

The following default user profiles and passwords are pre-configured in SINEC OS:

 CAUTION
Security hazard - risk of unauthorized access and/or exploitation
To prevent unauthorized access, change the default passwords before commissioning the device. For more information, refer to "Changing the password of a user (Page 120)".

Profile	Password
admin	admin

4.2.2 Logging in to a device with default settings

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

1. Establish a connection to the device and call the Web UI.
The login page of the Web UI is displayed.
For more information, refer to "Accessing the Web UI via a network connection (Page 73)".
2. Click **Username** and enter the factory default user name.
For more information, refer to "Default user profiles and passwords (Page 74)".
3. Click **Password** and enter the factory default password.

4. Click **Sign In** or press **Enter**.
The device verifies the entries. As optical feedback, a load symbol appears beside the fields on the right.
 - If the entries are correct, two further input boxes appear. You are prompted to change the factory default password.
Continue to the next action step.
 - If the entries are incorrect, a red exclamation mark appears to the right of the fields and an error message is displayed. Repeat the last steps.
5. Click **New Password** and assign a new password.
You can enter a password as follows:
 - As hash password
If a password starts with one of the following character combinations, it is viewed as a hash password and saved in this form: \$1\$ (MD5), \$5\$ (SHA-256) or \$6\$ (SHA-512)
 - As plain text password
If a password begins with a character combination other than \$1\$, \$5\$ or \$6\$, it is viewed as a plain text password and converted by the device using the hash algorithm SHA-512. If a password starts with the character combination \$0\$, it is also considered a plaintext password. Use this combination of characters if you want to configure a password that begins with the character \$.
Example: \$0\$\$siemens123

Conditions:

 - Must be between 6 and 255 characters long
 - All standard characters are allowed, plus the following special characters:
\$ % & () * + , - . / : < = > @ [] ^ _ { } ~
6. Click **Confirm Password** and enter the new password again.
7. Click **Change Password** or press **Enter**.
The device verifies the entries. As optical feedback, a load symbol appears beside the fields on the right.
 - If the entries are correct, a green check mark appears briefly to the right of the fields. To activate the changes, the Web UI session is automatically reloaded after a few seconds. Log in with the user name and the new password.
 - If the entries are incorrect, a red exclamation mark appears to the right of the fields and an error message is displayed. Repeat the last steps.

4.2.3 Logging in to a configured device

When you log in to a configured device, do the following:

1. Establish a connection to the device and call the Web UI.
The login page of the Web UI is displayed.
For more information, refer to "Accessing the Web UI via a network connection (Page 73)".
2. Click **Username** and enter the user name.

3. Click **Password** and enter the corresponding password.
4. Click **Sign In** or press **Enter**.
The device verifies the entries. As optical feedback, a load symbol appears beside the fields on the right.
 - If the entries are correct, a green check mark appears briefly to the right of the fields and the start page of the Web UI is displayed.
 - If the entries are incorrect, a red exclamation mark appears to the right of the fields and an error message is displayed. Repeat the last steps.

4.3 Logout

Proceed as follows to log out:

1. Click the button for the **user profile** in the status bar.
2. Click the button **Logout**.

4.4 Basic settings

This section describes the basic configuration steps that should be performed when first commissioning the device.

4.4.1 Configuring basic settings

To configure the basic settings for the device, do the following:

1. Change the host name for the device.
For more information, refer to "Changing the host name (Page 76)".
2. Specify the physical location of the device.
For more information, refer to "Specifying the device location (Page 77)".
3. Specify a contact person for the device.
For more information, refer to "Specifying the contact person for the device (Page 77)".
4. [Optional] Define the default gateway manually.
For more information, refer to "Configuring the default gateway manually (Page 77)".

4.4.1.1 Changing the host name

The host name is a label that helps identify the device on the network. The host name also forms the CLI prompt (e.g. localhost#).

The host name can be either a single domain label or a Fully Qualified Domain Name (FQDN).

Note

The default hostname is in the form of { **Device Family Name** }-{ **Serial Number**}.

To change the host name, do the following:

1. Navigate to **System** » **Information & State**.
2. Under **System Information**, enter the host name for the device under **Hostname**.
Conditions:
 - Must be between 1 and 253 characters long
 - Must not contain spaces
3. Commit the change.

4.4.1.2 Specifying the device location

Specify the location of the device to help administrators to find the physical location of the device.

To specify where the device is located, do the following:

1. Navigate to **System** » **Information & State**.
2. Under **System Information**, enter a description of the location under **Location**.
Condition:
 - Must be between 1 and 255 characters long
3. Commit the change.

4.4.1.3 Specifying the contact person for the device

Specify a contact person to provide a point of contact for other users. This can be the device owner or a system administrator.

To specify a contact person, do the following:

1. Navigate to **System** » **Information & State**.
2. Under **System Information**, enter the name of the contact person (e.g. "Winston Smith (wsmith@company.com)") under **Contact**.
Condition:
 - Must be between 0 and 255 characters long
3. Commit the change.

4.4.1.4 Configuring the default gateway manually

All IP packets for which no other routing information has been found are forwarded to the default gateway. The default gateway forwards all IP packets whose destination address is located in a different subnet than the device.

The IP address of the default gateway can be configured for the device manually or via a network management protocol (e.g. DHCP).

No default gateway is configured for the device as standard.

To configure the default gateway manually, do the following:

1. Navigate to **Interfaces » IP Interfaces**.
2. Enter the IP address of the default gateway under **IPv4 Default Gateway** in the **Default Gateway Address (Static)** field.
Condition:
 - The specified IPv4 address must be in an active subnet.
3. Commit the change.

4.4.2 Displaying the default gateway

The IP address of the default gateway can be configured for the device manually or via a network management protocol (e.g. DHCP). If the device gateway was configured using both methods, the dynamic assignment via DHCP has a higher priority.

To display the default gateway, navigate to **Interfaces » IP Interfaces**.

The IP address of the default gateway used by the device is displayed under **IPv4 Default Gateway** in the **Default Gateway Address** field.

Device management

This chapter describes how to manage device hardware, including rebooting or shutting down the device, managing firmware, and managing configuration files.

5.1 Restarting and shutting down the device

This section describes how you restart and shut down the device.

5.1.1 Understanding restarting and shutting down the device

This section describes the effects restarting and shutting down the device has on open sessions, running actions and configuration changes.

5.1.1.1 Canceling a command

The device will reject a command for restart or shutdown of the device if a firmware file is in the process of being downloaded to the device.

When the device rejects a command, an error message is output and an entry is created in the logbook.

A user cannot prevent the device from being restarted or shut down by another user.

5.1.1.2 Exiting sessions

When the command is being executed via an interactive user interface (CLI/Web UI) and additional sessions are active, the user executing the command is informed and prompted to commit the command. When the user commits the command, all active sessions – except for the user's session – are exited. The session of the user executing the command is exited according to the timeout settings of the device.

In the case of non-interactive user interfaces (NETCONF), the command is executed without being committed and all sessions are exited.

New sessions are blocked to ensure the configuration is not changed after the command has been executed.

Example

In this example, the device is restarted via the CLI and another session is active.

```
localhost# system restart
Are you sure you want to restart the device? [no,yes] yes
There are 1 other active user session(s) which would be killed. Are
you sure you want to continue? [no,yes] yes
```

5.1.1.3 Taking configuration changes into account

When a user has committed configuration changes (`commit`), this action is complete. Temporary configuration changes (`confirmed commit`) are reset.

5.1.2 Restarting the device

During a restart, the device is reinitialized, the internal firmware is reloaded, and the device runs a self-test. The settings of the start configuration are retained, e.g. the IP address of the device. The learned entries in the address table are deleted. You can leave the browser window open while the device restarts. After the restart, you need to log in again.

Note

If you restart the device while it is connected to a SCALANCE LPE, the SCALANCE LPE is also restarted.

To restart the device, do the following:

1. Navigate to **System** » **Restart** » **Restart**.
2. Under **Restart System**, click **Restart**.
3. Respond to the confirmation prompt with **Yes**.
The device restarts. When the restart is complete, the login page is displayed.
To cancel the restart, answer the security prompt with **No**.
4. Log in.
For more information, refer to "Login (Page 74)".

5.2 Resetting the device to default settings

NOTICE
Connection hazard - risk of communication failure
Depending on the configuration of your network, a reset device can cause circular frames and thus the loss of data traffic.

NOTICE
Configuration hazard - risk of data loss
If a CLP is inserted in the device, the CLP is also reset to default settings. Licenses stored on the CLP are retained.

Note

When you reset the device to the default settings, all configurations are deleted, including:

- The IP address
- The created user
- The passwords
- The user-defined keys and certificates

Following this, the device can only be reached via the serial interface.

If you assign an IP address to the device via DHCP or DCP (e.g. SINEC PNI), you can access the CLI and Web UI of the device via a network connection with a preset user profile.

Note

If you reset the device to default settings while it is connected to a SCALANCE LPE, this has no effect on the configuration of the SCALANCE LPE. When the device is restarted, the SCALANCE LPE is also restarted.

To reset the device to default settings, do the following:

1. Navigate to **System » Restart » Restore Defaults & Restart**.
2. Under **Restore Defaults & Restart**, click **Restart**.
3. Respond to the confirmation prompt with **Yes**.
The device restarts with default settings. When the restart is complete, the login page is displayed.
To cancel the reset to default settings, answer the security prompt with **No**.
4. Log in.
For more information, refer to "Logging in to a device with default settings (Page 74)".

5.3 Decommissioning the device

Before taking the device out of service, either permanently or for maintenance by a third-party, make sure the device has been fully decommissioned. This includes removing any sensitive, proprietary information.

Note

If the device is being decommissioned for the purpose of disposal, refer to the Installation Manual for details on how to properly dispose of the device.

To decommission the device, do the following:

1. Obtain a copy of the firmware currently installed on the device.
For more information, refer to "Obtaining a firmware package (Page 83)".
2. Reload the current firmware and reset the configuration settings to their default factory values. This must be done twice to make sure any proprietary information is erased from both partitions.
For more information about loading the firmware and resetting the configuration settings, refer to "Downgrading the firmware (Page 86)".
3. Shut down the device.
For more information, refer to the **SINEC OS CLI Configuration Manual**.

5.4 Firmware

This section describes how to change the version of the firmware installed on the device.

Note

If you switch from one firmware version of SINEC OS to another version, always observe the documentation for the version currently installed on the device. The instructions for different versions may not be the same.

The following descriptions only apply to the SINEC OS version for which they were written. For information on the SINEC OS version see the title page and footers of the document.

Note

Always note the requirements and restrictions published for a firmware version. You can find a list of the SINEC OS firmware publications in the SIOS.

5.4.1 Understanding firmware management

Firmware versions are managed via two partitions. One partition is always active (running firmware) while the other is always inactive (backup firmware). For this reason, two firmware versions are always saved on the device.

Firmware changes are always performed on the inactive partition. The active partition is locked by the system for firmware changes and therefore remains active after a firmware change. In this way, operability is guaranteed and system interruptions are avoided, e.g. if loading the firmware was not successful.

The updated partition is not activated until after a restart. The previously used partition becomes inactive and is available as backup.

When you restart the device after a firmware change, the current version of the configuration database is saved along with the previously active firmware. When you enable a backup firmware, the associated configuration database is restored as well.

5.4.2 Displaying the current firmware version

To display the current firmware version, navigate to the start page.

The following information is displayed under **Information Dashboard**:

Parameter	Description
Running Firmware	Installed firmware version that is active on the device
Backup Firmware	Installed firmware version that is inactive on the device

Alternatively, navigate to **System » Load & Save » Firmware**. The following information is displayed in addition under **Firmware Information**.

Parameter	Description
Running Firmware After Restart	Installed firmware version that is active after the next restart of the device
Bootloader	Installed version of the bootloader running on the device

5.4.3 Obtaining a firmware package

By default, valid firmware packages are available for download in the Siemens Industry Online Support (SIOS (<https://support.industry.siemens.com/cs/de/en/ps/15296/dl>)). Alternatively, you can also request firmware packages from the Siemens customer service.

To download a firmware package via SIOS, do the following:

1. Download the firmware package as described in SIOS. The firmware package is provided as ZIP file and contains:
 - A firmware file
The name of the firmware file indicates the version number (e.g. V02.00.00.00). This version number is made up as follows:
<Identification_letter><Function_level>.<Product_version>.<Service Pack>.<Hotfix>
 - Associated licensing terms
2. Save the firmware file locally on your client PC or on a server.
Depending on the user interface via which you load the firmware file, different options are available to you.
3. Extract the contents of the compressed file and make sure the content is not changed.
4. Depending on the firmware version, you are either performing a firmware upgrade or downgrade.
For the further procedure, see "Upgrading the firmware (Page 83)" or "Downgrading the firmware (Page 86)".

5.4.4 Upgrading the firmware

You can load a firmware file from a local client PC or a remote server.

5.4.4.1 Loading a newer firmware file from a local client PC

NOTICE
Electrical danger - Danger of a device fault due to loss of the power supply
If the power supply to the device is lost while a firmware file is being loaded, an error state can occur. Do not disconnect the device from the power supply while a firmware file is being loaded.

Note

You have the following options to cancel or undo a firmware change:

- If you have not restarted the device yet, you can reject the loaded firmware file. For more information, refer to "Rejecting a Loaded Firmware File (Page 88)".
 - When you have restarted the device, you can activate the backup firmware. For more information, refer to "Activating the backup firmware (Page 88)".
-

To load a firmware file from a local client PC, do the following:

1. Navigate to **System » Load & Save » Firmware**.
2. Under **Load Firmware from Local PC** in the **Firmware File** field, open a dialog window to select a file using the button.
3. Select the relevant firmware file via the dialog and click **Open**.
4. Click **Load** to load the firmware file.
The progress of the load process is displayed under **Firmware Load Progress**.
 - A load symbol is displayed while the firmware is being downloaded.
 - When the firmware has been downloaded successfully, a green check mark appears to the right of the field.
 - If an error has occurred during loading, a red exclamation mark appears to the right of the field and an error message is displayed.

While the firmware file is loading, you can cancel the load process with the **Abort** button.

5. To activate the updated firmware, restart the device.
For more information, refer to "Restarting the device (Page 80)".
The device restarts with the updated firmware. When the restart is complete, the login page is displayed.
6. Log in.
For more information, refer to "Logging in to a configured device (Page 75)".
7. [Optional] Verify the firmware version.
For more information, refer to "Displaying the current firmware version (Page 83)".

5.4.4.2 Loading a newer firmware file from a remote server

You can load a firmware file from a remote server.

Requirements

- You have configured a server accordingly.
- The firmware file (.sfw) is located on the server.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.

Loading a firmware file into the device

NOTICE
Electrical danger - Danger of a device fault due to loss of the power supply
If the power supply to the device is lost while a firmware file is being loaded, an error state can occur. Do not disconnect the device from the power supply while a firmware file is being loaded.

Note

You have the following options to cancel or undo a firmware change:

- If you have not restarted the device yet, you can reject the loaded firmware file.
For more information, refer to "Rejecting a Loaded Firmware File (Page 88)".
- When you have restarted the device, you can activate the backup firmware.
For more information, refer to "Activating the backup firmware (Page 88)".

To load a firmware file via a remote server, do the following:

1. Navigate to **System » Load & Save » Firmware**.
2. You configure the settings for the remote server under **Load Firmware from Remote Server**.
For more information on loading files via a remote server, see "Loading and saving files via a remote server (Page 54)".
3. Click **Load** to load the firmware file.
 - A load symbol is displayed while the firmware is being downloaded.
 - When the firmware has been downloaded successfully, a green check mark appears to the right of the field.
 - If an error has occurred during loading, a red exclamation mark appears to the right of the field and an error message is displayed.
4. To activate the updated firmware, restart the device.
For more information, refer to "Restarting the device (Page 80)".
The device restarts with the updated firmware. When the restart is complete, the login page is displayed.
5. Log in.
For more information, refer to "Logging in to a configured device (Page 75)".
6. [Optional] Verify the firmware version.
For more information, refer to "Displaying the current firmware version (Page 83)".

5.4.5 Downgrading the firmware

You can load a firmware file from a local client PC or a remote server.

5.4.5.1 Loading an older firmware file from a local client PC

NOTICE
Electrical danger - Danger of a device fault due to loss of the power supply
If the power supply to the device is lost while a firmware file is being loaded, an error state can occur. Do not disconnect the device from the power supply while a firmware file is being loaded.

Note

You have the following options to cancel or undo a firmware change:

- If you have not restarted the device yet, you can reject the loaded firmware file. For more information, refer to "Rejecting a Loaded Firmware File (Page 88)".
- When you have restarted the device, you can activate the backup firmware. For more information, refer to "Activating the backup firmware (Page 88)".

To load a firmware file from a local client PC, do the following:

1. Navigate to **System** » **Load & save** » **Firmware**.
2. Under **Load Firmware from Local PC** in the **Firmware File** field, open a dialog window to select a file using the button.
3. Select the relevant firmware file via the dialog and click **Open**.
4. Click **Load** to load the firmware file.
The progress of the load process is displayed under **Firmware Load Progress**.
 - A load symbol is displayed while the firmware is being downloaded.
 - When the firmware has been downloaded successfully, a green check mark appears to the right of the field.
 - If an error has occurred during loading, a red exclamation mark appears to the right of the field and an error message is displayed.

While the firmware file is loading, you can cancel the load process with the **Abort** button.

5. To activate the updated firmware, reset the device to its default settings.
For more information, refer to "Resetting the device to default settings (Page 80)".
The device restarts with the updated firmware and default settings. When the restart is complete, the login page is displayed.
6. Log in.
For more information, refer to "Logging in to a device with default settings (Page 74)".
7. [Optional] Verify the firmware version.
For more information, refer to "Displaying the current firmware version (Page 83)".

5.4.5.2 Loading an older firmware file from a remote server

You can load a firmware file from a remote server.

Requirements

- You have configured a server accordingly.
- The firmware file (.sfw) is located on the server.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.

Loading a firmware file into the device

NOTICE

Electrical danger - Danger of a device fault due to loss of the power supply

If the power supply to the device is lost while a firmware file is being loaded, an error state can occur. Do not disconnect the device from the power supply while a firmware file is being loaded.

Note

You have the following options to cancel or undo a firmware change:

- If you have not restarted the device yet, you can reject the loaded firmware file. For more information, refer to "Rejecting a Loaded Firmware File (Page 88)".
- When you have restarted the device, you can activate the backup firmware. For more information, refer to "Activating the backup firmware (Page 88)".

To load a firmware file via a remote server, do the following:

1. Navigate to **System » Load & Save » Firmware**.
2. You configure the settings for the remote server under **Load Firmware from Remote Server**.
For more information on loading files via a remote server, see "Loading and saving files via a remote server (Page 54)".
3. Click **Load** to load the firmware file.
 - A load symbol is displayed while the firmware is being downloaded.
 - When the firmware has been downloaded successfully, a green check mark appears to the right of the field.
 - If an error has occurred during loading, a red exclamation mark appears to the right of the field and an error message is displayed.
4. To activate the updated firmware, reset the device to its default settings.
For more information, refer to "Resetting the device to default settings (Page 80)".
The device restarts with the updated firmware and default settings. When the restart is complete, the login page is displayed.

5. Log in.
For more information, refer to "Logging in to a device with default settings (Page 74)".
6. [Optional] Verify the firmware version.
For more information, refer to "Displaying the current firmware version (Page 83)".

5.4.6 Rejecting a Loaded Firmware File

If you reject a loaded firmware file, the previously used firmware remains active after a restart. The updated firmware remains inactive.

The **Decline** button is inactive by default. The button is only active if a loaded firmware can be rejected.

Note

You can only reject a firmware file if you have not yet restarted the device after loading a firmware file.

To reject a firmware file, do the following:

1. Navigate to **System » Load & Save » Firmware**.
2. To reject the loaded firmware, click **Decline** under **Firmware Information**.

Note

No confirmation prompt

The firmware file is rejected directly. There is no confirmation prompt.

5.4.7 Activating the backup firmware

When you activate the backup firmware, the currently active firmware (running firmware) becomes inactive.

You cannot activate the backup firmware in the following cases:

- When you change the configuration after loading a firmware file and commit the configuration changes.
- When you have activated new firmware by resetting the device to default settings. You need to assign a new password after the reset to default settings. This is considered a committed configuration change.
- When a CLP is inserted in the device.

Note

You can only activate the backup firmware if you have restarted the device after loading a firmware file.

If you have not restarted the device yet, you can reject the loaded firmware file. For more information, refer to "Rejecting a Loaded Firmware File (Page 88)".

To activate the backup firmware, do the following:

1. Navigate to **System » Load & Save » Firmware**.
2. To activate the backup firmware, click **Rollback** under **Firmware Information**. The associated configuration database is restored together with the backup firmware.

Note**No confirmation prompt**

The backup firmware is activated directly. There is no confirmation prompt.

3. To activate the updated firmware, restart the device. For more information, refer to "Restarting the device (Page 80)". The device restarts with the backup firmware. When the restart is complete, the login page is displayed.
4. Log in. For more information, refer to "Logging in to a configured device (Page 75)".
5. [Optional] Verify the firmware version to ensure the previously inactive firmware version (Backup Firmware) is now active (Running Firmware). For more information, refer to "Displaying the current firmware version (Page 83)".

5.5 Device hardware

This section describes how to determine the hardware profile of the device.

5.5.1 Listing Hardware Components

To list the hardware components installed on your device, navigate to **System » Hardware » Hardware Information**.

The following information is displayed under **Hardware Information**:

Parameter	Description
Component Name	A unique name of the component
Class	The type of the component
Description	A description of the component
Parent	The higher-level component
Hardware Revision	The hardware version

Parameter	Description
Serial Number	The serial number of the hardware
Operational State	The operational state of the component Options include: <ul style="list-style-type: none"> • enabled - The component is ready for operation. • disabled - The component was disabled.
Status	Additional information on the current status of the component Options include: <ul style="list-style-type: none"> • OFF - The component is switched off. • ON - The component is switched on. • OPEN - The component is open. Applies to all relay components (signaling contact). • CLOSE - The component is closed. Applies to all relay components (signaling contact). • { Color } - The color of the component. Applies to LED components.
Article Number	Article number (order number)

5.6 Configuration file

Configuration parameters for SINEC OS can be saved and loaded.

You can save your device configuration and store it as a backup copy.

You can load these backup copies directly into the same device to restore an earlier configuration. If the need arises or an error occurs, a backup copy enables quick and easy device replacement without new configuration of the replacement device.

The prerequisite for the transfer of a configuration file to a replacement device is that the configuration file was saved by a compatible device type (same article number).

When you load the configuration of a failed network component to a compatible replacement device, the replacement device applies the configuration immediately. Note the following:

- If the IP configuration is obtained via DHCP, you need to re-configure the DHCP server accordingly.
- If the configuration includes functions based on MAC addresses, you need to adapt them accordingly.

5.6.1 Saving the Current Configuration as File on a Local Client PC

Note

If you change the saved configuration file and load it to a device again, this can result in unintended behavior or a communication failure.

Saved configuration files should only be changed by experienced users.

To save the current configuration of the device on a local PC, do the following:

1. Make sure that the Web UI is not in exclusive configuration mode.
For more information, refer to section "Status bar (Page 40)".
2. Make sure that no other user has enabled the exclusive configuration.
For more information, refer to section "Displaying active users (Page 122)".
3. Navigate to **System » Load & Save » Configuration**.
4. [Optional] Under **Save Configuration to Local PC**, you can save the configuration in protected mode under **File Protection**.
Options include:

Option	Description
Disabled	Default The configuration is saved without further options.
Enabled	The configuration is saved in protected mode. In protected mode, the saved file is given a checksum. The checksum ensures that the saved file can only be downloaded to a device again if it was not changed. The device verifies the checksum when the saved file is downloaded. If the file has been changed, the checksum is no longer correct and the file is not downloaded.

5. [Optional] If you have selected the option **Enabled** under **File Protection**, assign a password under **File Password**.
Condition:
 - Must be between 1 and 255 characters long
 - All standard characters are allowed, plus the following special characters:
\$ % & () * + , - . / : < = > @ [] ^ _ { } ~

6. [Optional] If you have assigned a password under **File Password**, repeat the password under **File Password-Confirm**.
7. Click **Save**.
It depends on the browser settings whether the file is saved directly to a specified folder or if you will first see a prompt in which you can select the storage location.

Note

Wait until the save operation is complete before making changes to the device configuration.

While the configuration is being saved, a load symbol appears beside the button on the right.

- When the save operation is complete, a green check mark appears.
- If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

The configuration is saved in XML format.

5.6.2 Saving the Current Configuration as File on a Remote Server

You can save the current configuration of the device on a remote server.

Requirements

- You have configured a server accordingly.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.

Saving the configuration

Note

If you change the saved configuration file and load it to a device again, this can result in unintended behavior or a communication failure.

Saved configuration files should only be changed by experienced users.

To save the current configuration of the device on a remote server as a file, do the following:

1. Make sure that the Web UI is not in exclusive configuration mode.
For more information, refer to section "Status bar (Page 40)".
2. Make sure that no other user has enabled the exclusive configuration.
For more information, refer to section "Displaying active users (Page 122)".
3. Navigate to **System » Load & Save » Configuration**.
4. Under **Load/Save Configuration from/to Remote Server**, select the **Save** option for the **Action** parameter.

5. Configure the settings for the remote server.
For more information on saving files via a remote server, see "Loading and saving files via a remote server (Page 54)".
6. Click **Save**.

Note

Wait until the save operation is complete before making changes to the device configuration.

While the configuration is being saved, a load symbol appears beside the button on the right.

- When the save operation is complete, a green check mark appears.
- If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

The configuration is saved in XML format.

5.6.3 Loading a Configuration File from a Local Client PC

You can load a configuration file from a local client PC.

Requirements

- The configuration file was saved by a SINEC OS device.
- The configuration file was saved by a compatible device type (same article number).
- SINEC OS firmware version 2.0 or higher was installed on the device by which the configuration file was saved.

Invalid configurations are rejected with a corresponding error message.

Loading a configuration file**NOTICE****Configuration hazard – risk of communication failure**

When you load a configuration file to a device, this can result in unintended behavior or a communication failure.

To prevent unintended behavior, reset the device to its default settings. After the reset, the device can only be reached via the serial interface. If you assign an IP address to the device via DHCP or DCP (e.g. SINEC PNI), you can access the CLI and Web UI of the device via a network connection with a preset user profile.

For more information on resetting the device, refer to "Resetting the device to default settings (Page 80)".

Note

If you change the saved configuration file and load it to a device again, this can result in unintended behavior or a communication failure.

Saved configuration files should only be changed by experienced users.

To load a configuration file from a local PC into the device, follow these steps:

1. Make sure that the Web UI is not in exclusive configuration mode.
For more information, refer to section "Status bar (Page 40)".
2. Make sure that no other user has enabled the exclusive configuration.
For more information, refer to section "Displaying active users (Page 122)".
3. Navigate to **System » Load & Save » Configuration**.
4. Under **Load Configuration from Local PC**, select the load behavior under **Mode**.
Options include:

Option	Description
Replace	Default This parameter deletes the parameters of the running configuration contained in the configuration file and replaces them with the contents of the configuration file. Parameters of the currently running configuration are only replaced if the corresponding parameters are contained in the configuration file.
Merge	With this parameter, the contents of the configuration file are merged with the currently running configuration. Parameters of the currently running configuration are only merged if the corresponding parameters are contained in the configuration file.

5. [Optional] If the configuration was saved in protected mode, select the option **Enabled** under **File Protection**.
6. [Optional] If the configuration was saved in protected mode, a password was assigned. You need the corresponding password to load the configuration.
Enter the password under **File Password**.
7. Under **Configuration File**, open a dialog window to select a file using the button.
8. Select the corresponding file via the dialog and click **Open**.
9. Click **Load** to load the configuration file.

Note

Wait until the load operation is complete before making changes to the device configuration.

While the configuration is being loaded, a load symbol appears beside the button on the right.

- When the load operation is complete, a green check mark appears.
- If the load operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

5.6.4 Loading a Configuration File from a Remote Server

You can load a configuration file from a remote server.

Requirements

- You have configured a server accordingly.
- The configuration file (.xml) is on the server.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.
- The configuration file was saved by a SINEC OS device.
- The configuration file was saved by a compatible device type (same article number).
- SINEC OS firmware version 2.0 or higher was installed on the device by which the configuration file was saved.

Invalid configurations are rejected with a corresponding error message.

Loading a configuration file

NOTICE

Configuration hazard – risk of communication failure

When you load a configuration file to a device, this can result in unintended behavior or a communication failure.

To prevent unintended behavior, reset the device to its default settings. After the reset, the device can only be reached via the serial interface. If you assign an IP address to the device via DHCP or DCP (e.g. SINEC PNI), you can access the CLI and Web UI of the device via a network connection with a preset user profile.

For more information on resetting the device, refer to "Resetting the device to default settings (Page 80)".

Note

If you change the saved configuration file and load it to a device again, this can result in unintended behavior or a communication failure.

Saved configuration files should only be changed by experienced users.

To load a configuration file from a remote server into the device, follow these steps:

1. Make sure that the Web UI is not in exclusive configuration mode.
For more information, refer to section "Status bar (Page 40)".
2. Make sure that no other user has enabled the exclusive configuration.
For more information, refer to section "Displaying active users (Page 122)".
3. Navigate to **System » Load & Save » Configuration**.
4. Under **Load/Save Configuration from/to Remote Server**, select the **Load** option for the **Action** parameter.

5. Select the load behavior under **Mode**.
Options include:

Option	Description
Replace	Default This parameter deletes the parameters of the running configuration contained in the configuration file and replaces them with the contents of the configuration file. Parameters of the currently running configuration are only replaced if the corresponding parameters are contained in the configuration file.
Merge	With this parameter, the contents of the configuration file are merged with the currently running configuration. Parameters of the currently running configuration are only merged if the corresponding parameters are contained in the configuration file.

6. Configure the settings for the remote server.
For more information on loading files via a remote server, see "Loading and saving files via a remote server (Page 54)".
7. [Optional] If the configuration was saved in protected mode, select the option **Enabled** under **File Protection**.
8. [Optional] If the configuration was saved in protected mode, a password was assigned. You need the corresponding password to load the configuration.
Enter the password under **File Password**.
9. Click **Load**.

Note

Wait until the load operation is complete before making changes to the device configuration.

While the configuration is being loaded, a load symbol appears beside the button on the right.

- When the load operation is complete, a green check mark appears.
- If the load operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

5.6.5 Displaying the header information of a configuration file

To display the header information of a configuration file, do the following:

1. Make sure that the Web UI is not in exclusive configuration mode.
For more information, refer to section "Status bar (Page 40)".
2. Navigate to **System » Load & Save » Configuration**.
3. Under **Load/Save Configuration from/to Remote Server**, select the **Load** option for the **Action** parameter.
4. Configure the settings for the remote server.
For more information on loading files via a remote server, see "Loading and saving files via a remote server (Page 54)".

5. [Optional] If the configuration was saved in protected mode, select the option **Enabled** under **File Protection**.
6. [Optional] If the configuration was saved in protected mode, a password was assigned. You need the corresponding password to load the configuration. Enter the password under **File Password**.
7. Click **View Info**.
 - While the header information is being loaded, a load symbol appears beside the button on the right.
 - If the operation has been completed successfully, the header information of a configuration file is displayed under the button.
 - If the operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

Description

The following information is shown:

Parameter	Description
Backup Time	Date and time at which the configuration file was saved
Backup By	User who saved the configuration file
Device Type	Device name
Serial Number	Serial number of the hardware
Article Number	Article number (order number)
Hardware Revision	Hardware version
Firmware Version	Firmware version that is active on the device
Hostname	Configured hostname
Checksum	Checksum of the configuration file

5.7 Open Source Software Information

The open source software (OSS) information is saved as PDF file. The file contains copyright notes on the third-party software, especially open source software, contained in this product as well as applicable license conditions for this type of third-party software.

Read the information on open source software carefully before using the product.

The OSS information is saved in the device and stored on the supplied data carrier.

5.7.1 Saving OSS Information on a Local Client PC

To save the OSS information on a local PC, do the following:

1. Navigate to **System » Load & Save » OSS Information**.
2. Under **Save Open Source Software (OSS) Information to Local PC**, click **Save**.
It depends on the browser settings whether the file is saved directly to a specified folder or if you will first see a prompt in which you can select the storage location.
As optical feedback, a load symbol appears beside the button on the right.
 - When the save operation is complete, a green check mark appears.
 - If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

5.7.2 Saving OSS Information on a Remote Server

You can save the OSS information on a remote server.

Requirements

- You have configured a server accordingly.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.

Saving the OSS information

To save the OSS information on a remote server, do the following:

1. Navigate to **System » Load & Save » OSS Information**.
2. You configure the settings for the remote server under **Save Open Source Software (OSS) Information to Remote Server**.
For more information on loading and saving files via a remote server, see "Loading and saving files via a remote server (Page 54)".
3. Click **Save**.
As optical feedback, a load symbol appears beside the button on the right.
 - When the save operation is complete, a green check mark appears.
 - If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

5.8 Operator panel

Depending on the device location, direct access to the device may not always be possible. The Web UI therefore displays a simulated operator panel.

A view of the device with the operator panel is displayed on the start page of the Web UI under **Device Panel**.

5.8.1 Understanding the operator panel

The operator panel of the device includes the light-emitting diodes (LEDs) and the button.

5.8.1.1 LEDs

Each device has one or more LEDs that provide information on the operating state of the device. Without direct access to the device, you can monitor the current device state by using the LED simulation in the Web UI.

The display is updated every 5 seconds.

The individual LEDs are described below.

5.8.1.2 "A" LED

LED "A" (alarm LED) indicates the fault status of the device.

Meaning during device startup

LED color	LED status	Meaning during device startup
-	Off	Device startup was completed successfully.
Red	On	Device startup is not complete yet.

Meaning during operation

LED color	LED status	Meaning during operation
-	Off	The device is operating free of errors.
Red	On	The device has detected a problem.

5.8.1.3 LEDs "DM1" and "DM2"

The "DM1" and "DM2" LEDs indicate which display mode is set.

There are 4 display modes (A, B, C and D). Display mode A is the default mode.

LED color	LED status		Meaning
	DM1 LED	DM2 LED	
-	Off		Display mode A
Green	On	Off	Display mode B
Green	Off	On	Display mode C
Green	On		Display mode D

5.8.1.4 LEDs "L1" and "L2"

The "L1" and "L2" LEDs indicate the current state of the power supply at connectors L1 and L2.

The meaning of the "L1" and "L2" LEDs depends on the set display mode, see section "LEDs "DM1" and "DM2" (Page 99)".

Meaning in display modes A, B and C

In the display modes A, B and C, the "L1" and "L2" LEDs tell you whether the power supply is connected.

L1/L2 LED		L1/L2 connector
LED color	LED status	
-	Off	No external power supply connected
Green	On	Power supply connected to L1/L2

Meaning in display mode D

In the current version, the display mode D does not display any information.

5.8.1.5 "P" LEDs

The port LEDs "P1", "P2" etc. show information about the corresponding ports.

The meaning of the Port LEDs depends on the set display mode, see section "LEDs "DM1" and "DM2" (Page 99)".

Meaning in display mode A

In display mode A, the port LEDs indicate whether a valid link exists.

LED color	LED status	Meaning
-	Off	No valid link on the port (e.g. the communication partner is switched off or the cable is not connected) or the link is present but the port is switched off by management. In this state, no data is sent or received via the port.
Green	On	Link exists and port in normal status. In this state, the port can receive and send data.
	Flashes once per period*	Link exists and port in "Blocking" status. In this state, the port only receives management data (no user data).
	Flashes four times per period*	Link exists and is in the "Monitor Port" status. In this state, the data traffic of another port is mirrored to this port.
Yellow	Flashing / lit	Receiving data at port

* 1 period \cong 2.5 seconds

Meaning in display mode B

In display mode B, the port LEDs indicate the transmission speed.

LED color	LED status	Meaning
-	Off	Port operating at 10 Mbps
Green	On	Port operating at 100 Mbps
	Flashes once per period*	Port operating at 10 Gbps

LED color	LED status	Meaning
Yellow	On	Port works at 1 Gbps
	Flashes twice per period*	Port works at 2.5 Gbps
	Flashes five times per period*	Port works at 5 Gbps

* 1 period \triangleq 2.5 seconds

When the transfer settings of a port are permanently set (autonegotiation disabled) and a connection error occurs, the port LED will still show the set transmission rate. When autonegotiation is enabled, the port LED will go off in case of a connection error.

Meaning in display mode C

In display mode C, the port LEDs indicate the mode.

LED color	LED status	Meaning
-	Off	Port operating in half duplex mode
Green	On	Port operating in full duplex mode

Meaning in display mode D

In the current version, the display mode D does not display any information.

5.8.1.6 Button

Each device has a button. Without direct access to the device, you can operate the button with the mouse via the operator panel in the Web UI.

Note

You can not use all functions of the button via the simulated button in the Web UI. You can only set the display mode in the Web UI.

The button is shown in orange in the operator panel.

For more information on the functions of the button, refer to "Button functions (Page 103)".

5.8.2 Monitoring the operating state of the device

To monitor the operating state of the device via the operator panel, do the following:

1. [Optional] Set the display mode.
For more information, refer to "Setting the display mode (Page 102)".
2. Verify the state or the desired setting using the LEDs.
The LEDs show the current display mode, the status of the ports and the power supply (modules) as well as the error state.
For more information, refer to "LEDs (Page 99)".

5.8.3 Setting the display mode

To set the display mode, press the button as follows:

Pressing the button starting at display mode A	LED status		Display mode
	DM1	DM2	
-	Off		Display mode A
Press once	On	Off	Display mode B
Press twice	Off	On	Display mode C
Press three times	On		Display mode D

Depending on the set display mode, the "L1", "L2" LEDs and the port LEDs show different information.

If you do not press the button for longer than 1 minute, the device automatically changes to display mode A.

5.9 Signaling contact

5.9.1 Signaling contact

The signaling contact is an event-driven or manually controlled failsafe alarm relay. Individual alarms can be configured to trigger the relay when the associated event occurs. The relay can also be fixed in an open or closed state.

Manually controlling the relay may be useful to:

- Verify the failsafe relay is properly connected following the installation of the device
- Verify the open/close state is caused by the device itself or some other hardware
- Keep the relay in an open/close state while troubleshooting a network issue

5.9.2 Setting the signaling contact mode

To define the signaling contact mode, do the following:

1. Navigate to **System » Events » Signaling Contact**.
2. Under **Signaling Contact Mode**, select a mode under **Signaling Contact Mode**.
Options include:

Option	Description
Event Driven	Default The signaling contact is controlled by alarms that are configured to open or close the relay when a specific event occurs.
Open	The signaling contact is always open.
Closed	The signaling contact is always closed

3. Commit the change.

5.10 Button functions

The device has a button with the following functions:

- **Reset the device to default settings**
Please note that the button function distinguishes between the startup phase and running operation.
For more information, refer to "Resetting the device to default settings with the button (in the startup phase) (Page 104)" and "Resetting the device to default settings with the button (during operation) (Page 104)".
- **Load a firmware file via TFTP**
For more information, refer to "Loading a firmware file via TFTP (Page 105)".
- **Setting the display mode**
The display mode is used for diagnostics of the device. Depending on the set display mode, the LEDs of the device show different information and indicate the state of the device.
For more information, refer to "Setting the display mode (Page 102)".
For more information on the display modes, refer to "LEDs "DM1" and "DM2" (Page 99)".

5.10.1 Understanding the button functions

The functions of the button are described in greater detail in this section.

5.10.1.1 Resetting the device to default settings with the button (in the startup phase)

NOTICE
Connection hazard - risk of communication failure Depending on the configuration of your network, a reset device can cause circular frames and thus the loss of data traffic.

NOTICE
Configuration hazard - risk of data loss If a CLP is inserted in the device, the CLP is also reset to default settings.

Note

When you reset the device to the default settings, all configurations are deleted, including:

- The IP address
- The created user
- The passwords
- The user-defined keys and certificates

Following this, the device can only be reached via the serial interface.

If you assign an IP address to the device via DHCP or DCP (e.g. SINEC PNI), you can access the CLI and Web UI of the device via a network connection with a preset user profile.

To reset the device to default settings in the startup phase, do the following:

1. Turn off the power to the device.
2. Press the button and reconnect the power supply to the device while holding down the button.
3. Hold down the button until the red alarm LED **A** stops flashing and is permanently lit.
4. Release the button and wait until the alarm LED **A** goes off again.
The device starts automatically with the default settings.

5.10.1.2 Resetting the device to default settings with the button (during operation)

NOTICE
Connection hazard - risk of communication failure Depending on the configuration of your network, a reset device can cause circular frames and thus the loss of data traffic.

NOTICE**Configuration hazard - risk of data loss**

If a CLP is inserted in the device, the CLP is also reset to default settings.

Note

When you reset the device to the default settings, all configurations are deleted, including:

- The IP address
- The created user
- The passwords
- The user-defined keys and certificates

Following this, the device can only be reached via the serial interface.

If you assign an IP address to the device via DHCP or DCP (e.g. SINEC PNI), you can access the CLI and Web UI of the device via a network connection with a preset user profile.

Requirements

- The device is in operation.
- The **Reset to default settings** button function is enabled.
You can enable or disable this button function. For more information, refer to "Enabling the 'Reset to default settings' button function (Page 106)".

Resetting the device to default settings

To reset the device to default settings during operation, do the following:

1. Switch to display mode **A**.
Display mode **A** is active if the LEDs **DM1** and **DM2** are unlit.
If the **DM1** and **DM2** LEDs are lit or flashing, press the button briefly several times until the LEDs are off.
If you do not press the button for longer than 1 minute, the device automatically changes to display mode **A**.
2. Hold down the button for 12 seconds.

Note

If you release the button before the 12 seconds have elapsed, the operation is canceled.

3. Release the button after 12 seconds.
The device restarts with default settings.

5.10.1.3 Loading a firmware file via TFTP

While the device is starting, you can switch to update mode with the button. In this mode, the device initializes the network connection, starts the DHCP client and the TFTP server and can receive files such as firmware files.

If the device cannot be reached via CLI and Web UI, you can restart the device and load a firmware file into the device in update mode via TFTP.

Note

This section describes the procedure based on the example of Microsoft Windows.

To load a firmware file via TFTP into the device, do the following:

1. Turn off the power to the device.
2. Press the button and reconnect the power supply to the device while holding down the button.
3. Hold down the button until the red alarm LED **A** starts to flash.
4. Release the button as long as the red alarm LED **A** is still flashing.

Note

This time only lasts a few seconds.

The bootloader of the device waits in this status for a firmware file that you can load by TFTP.

5. Connect a client PC to a port of the device with an Ethernet cable.
6. Assign an IP address to the device using DHCP or SINEC PNI.
7. Open the Windows command prompt on the client PC.
8. In the Windows command prompt, change to the directory containing the firmware file and execute the following command:

```
tftp -i < IP address > put < firmware file >
```

Note

You enable TFTP in Microsoft Windows as follows:

Control Panel » Programs and Features » Turn Windows features on or off » TFTP client

9. Once the firmware file has been transferred completely to the device and validated, the device restarts automatically. This may take several minutes.

5.10.2 Enabling the 'Reset to default settings' button function

You can reset the device to its default settings using the button.

The **Reset to default settings** button function is enabled by default.

NOTICE**Security risk - Danger of unauthorized access and/or misuse**

Note that configuration only applies to the function during operation of the device.

If you disable the **Reset to default settings** button function, the button function is only disabled during operation. The button function is still active in the startup phase. The button function is only disabled after the configuration has been loaded.

Users with malicious intent can exploit this to disrupt your network and access the device.

To enable the **Reset to default settings** button function, do the following:

1. Navigate to **System » Hardware » SELECT / SET Button**.
2. Under **SELECT / SET Button**, change **Restore Factory Defaults** to **Enabled**.
3. Commit the change.

5.11 Configuration and License PLUG

The Configuration and License PLUG (CLP) is a USB storage medium for backing up and exchanging data and licenses.

The CLP has a USB type C interface and can be used with the following devices that have a corresponding interface:

- Siemens products
- Personal computers (PCs), such as desktop PCs, tablet PCs, laptops, or smartphones

5.11.1 Understanding the CLP

The CLP is used for automatic backup of configuration data. If the need arises or an error occurs, it enables quick and easy device replacement without new configuration of the replacement device.

5.11.1.1 Device replacement

Requirements for transferring the configuration to a replacement device:

- The data was written to the CLP by a compatible device type (same article number).
- The firmware version on the replacement device is the same or newer than the firmware version of the device that wrote to the CLP last.
To ensure this, the firmware can be saved together with the configuration on the CLP. For more information, refer to "Firmware on CLP (Page 108)".

If you insert the CLP of a failed network component into a compatible replacement device, the replacement device automatically boots up with the same configuration as the failed device. Note the following:

- If the IP configuration is obtained via DHCP, you need to re-configure the DHCP server accordingly.
- If the configuration includes functions based on MAC addresses, you need to adapt them accordingly.

5.11.1.2 Modes

Devices with a CLP slot support the following operating modes:

- **Without CLP**
The device saves the configuration data in the internal memory. This mode is active when no CLP is inserted.
- **With CLP**
In the startup phase:
 - When an CLP **with no data** (default setting) is plugged into a device, the device automatically saves its configuration data on the CLP during the startup phase. After that, it behaves like a CLP with data.
 - If a CLP **with data** is plugged into a device, the device automatically adopts the configuration of the CLP during the startup phase.

During operation:

- During operation, changes to the configuration are saved on the CLP and in the internal memory.
- The configuration data of the device is stored in a secured memory area of the CLP. This secured memory area can only be accessed via the authentication of the Siemens device.
- The device checks whether a CLP is inserted at one second intervals. If the device detects that the CLP has been removed, it restarts automatically.

NOTICE
Operating risk - Danger of data loss
Only pull and plug the CLP when the device is de-energized.

- The device signals deviations from normal operation of the CLP (e.g. incompatible data, incorrect operation or malfunctions) via the existing diagnostics mechanisms (e.g. LEDs or user interfaces).

5.11.1.3 Firmware on CLP

In addition to a compatible device type, the version of the firmware is also relevant for a successful device replacement via CLP.

The transfer of the configuration to a replacement device only works if the firmware version on the replacement device is the same or newer than that of the failed device. A device with older firmware does not accept the CLP and starts with the configuration from its internal memory.

A device can therefore store not only its configuration but also its current firmware on the CLP. You can configure whether or not the firmware should be saved on the CLP:

- If the function is enabled, the device saves its current firmware on the CLP. When the firmware file is updated on the device, the updated version is also saved on the CLP.
- When the function is disabled, the firmware is deleted from the CLP.
- When the setting is changed, the device responds directly and saves or deletes the firmware from the CLP.

In the startup phase, the device does not check whether the function is enabled or disabled. If the data of the plugged CLP is compatible and the CLP contains valid but different firmware, the firmware of the CLP is transferred to the device.

5.11.1.4 Memory areas

A CLP has memory areas for different file types:

- **Open memory area**
The public memory area can be accessed by any device. A connected device can change the file system and have read and write access to files in the memory area.
- **Secured memory area**
Only Siemens devices can access the secured memory area after successful authentication. To prevent unauthorized access, configuration data is stored in the secured memory area.
- **Memory area for licenses**
A separate secured memory area for licenses. Only Siemens devices can access the area after a successful authentication.

5.11.1.5 Related events

The following events relating to the CLP are recorded directly in the Syslog.

Event	Severity	Syslog message
EventNoCPlugFound	Info	No CLP found. Internal flash memory used.
EventEmptyCPlugFound	Info	Empty CLP found.
EventCPlugAutoFormat	Info	CLP auto format request.
EventCPlugAccepted	Info	CLP accepted.
EventErrorCPlugFound	Critical	CLP defective.
EventCPlugPluggedOff	Critical	CLP removed at runtime.
EventCPlugDiffType	Critical	CLP has different device type.
EventCPlugCrcError	Critical	CLP has CRC Error.
StateCPlugNotAccepted	Critical	CLP not accepted.
StateCPlugUnmounted	Info	CLP interface unmounted – restart required.

5.11.2 Saving firmware on the CLP

You can configure whether or not to store the firmware of the device on the CLP and keep it in sync. If you change the setting, the device responds directly.

- If you enable the function, the device saves the current firmware on the CLP.
- If you disable the function, the device deletes the firmware from the CLP.

The function is enabled by default.

To enable the function, do the following:

1. Navigate to **System** » **CLP**.
2. Under **Configuration & License Plug (CLP)**, change **Firmware on CLP** to **Enabled**.
3. Commit the change.

5.11.3 Saving the device configuration on the CLP

You can delete all saved data of the CLP and replace it with the current device configuration.

To format the CLP and save the current device configuration, do the following:

1. Navigate to **System** » **CLP**.
2. Under **Configuration & License Plug (CLP)**, click **Format & Write**.
3. Respond to the confirmation prompt with **Yes**.
The device deletes all saved data of the CLP and saves the current device configuration.
To cancel the operation, answer the security prompt with **No**.

5.11.4 Deleting the Data of the CLP

You can delete all saved data from the CLP, apart from the saved licenses.

To delete the data from the CLP, follow these steps:

1. Navigate to **System** » **CLP**.
2. Under **Configuration & License Plug (CLP)**, click **Clean**.
3. Respond to the confirmation prompt with **Yes**.
The device deletes all saved data of the CLP, except the licenses.
To cancel the operation, answer the security prompt with **No**.

5.11.5 Resetting the CLP

You can delete all saved data of the CLP, including licenses, and reset the CLP to default settings.

Note

To delete all data except stored licenses, use **Clean** or reset the device to its default settings. For more information, refer to "Deleting the Data of the CLP (Page 110)" and "Resetting the device to default settings (Page 80)".

To reset the CLP to default settings, do the following:

1. Navigate to **System** » **CLP**.
2. Under **Configuration & License Plug (CLP)**, click **Restore**.
3. Respond to the confirmation prompt with **Yes**.
The device deletes all saved data of the CLP and resets it to the default settings.
To cancel the operation, answer the security prompt with **No**.

5.11.6 Showing the status of the CLP

To show the status of the CLP, navigate to **System** » **CLP**.

The following information is displayed under **Configuration & License Plug (CLP)**.

Parameter	Description
CLP Configuration State	Shows the status of the CLP. Options include: <ul style="list-style-type: none"> • CLP not present - There is no CLP plugged into the device. • Accepted - There is a CLP with a valid and suitable configuration in the device. • Not accepted - There is a CLP in the device. The CLP contains an invalid or incompatible configuration. • Factory - There is a CLP in the device. The CLP does not contain a configuration. This status is also displayed when the CLP was formatted during operation.
Device Group	Shows the product line of the device from which the CLP was used in the previous operation.
Device Type	Shows the device type of the device from which the CLP was used in the previous operation.
Filesystem	Shows the type of file system on the CLP.
Filesystem Size MB	Shows the maximum storage capacity of the file system on the CLP.
Filesystem Usage MB	Shows the memory utilization of the file system of the CLP.

Parameter	Description
Info String	Shows additional information about the device that used the CLP previously, for example, article number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the Not accepted status, further information on the cause of the problem is displayed.
Firmware on CLP	If the function is enabled (Enabled), the firmware is stored on the CLP.
Firmware on CLP State	Shows whether firmware is stored on the CLP (Firmware present) or not (Firmware not present).

System administration

This chapter describes how to perform various administrative tasks, such as define users, configure alarms, and manage system files.

6.1 Password policy

SINEC OS uses a system-wide password policy for local user authentication. The password policy consists of configurable conditions that must be fulfilled when configuring passwords.

By default, a password must fulfill the following conditions:

- It must be between 8 and 255 characters long
- It must contain at least 1 number

Only users with the **Admin** user profile can change the password policy.

When a condition is disabled, these characters may still be included in a password. However, they are not mandatory.

6.1.1 Configuring the password policy

To change the password policy, do the following:

1. [Optional] Configure the minimum number of characters that must be included in a password.
For more information, refer to "Configuring the minimum number of characters (Page 114)".
2. [Optional] Configure the maximum number of characters that may be included in a password.
For more information, refer to "Configuring the maximum number of characters (Page 114)".
3. [Optional] Configure that a password must include at least one number.
For more information, refer to "Configuring the condition for numbers (Page 114)".
4. [Optional] Configure that a password must include at least one lowercase letter.
For more information, refer to "Configuring the condition for lowercase letters (Page 115)".
5. [Optional] Configure that a password must include at least one uppercase letter.
For more information, refer to "Configuring the condition for uppercase letters (Page 115)".
6. [Optional] Configure that a password must include at least one special character.
For more information, refer to "Configuring the condition for special characters (Page 116)".
7. Enable the password policy.
For more information, refer to "Enabling the password policy (Page 116)".

6.1 Password policy

6.1.1.1 Configuring the minimum number of characters

To configure the minimum number of characters, do the following:

1. Navigate to **System » Security » User Management**.
2. Under **Password Policy** in the **Minimum Length** field, configure the minimum number of characters that must be included in a password.
Condition:
 - A number between 1 and 255Default: 8
3. Commit the change.

6.1.1.2 Configuring the maximum number of characters

To configure the maximum number of characters, do the following:

1. Navigate to **System » Security » User Management**.
2. Under **Password Policy** in the **Maximum Length** field, configure the maximum number of characters that may be included in a password.
Condition:
 - A number between 4 and 255The value range starts at 4 to prevent invalid password policies when all conditions are enabled:
 - At least 1 number
 - At least 1 lowercase letter
 - At least 1 uppercase letter
 - At least 1 special characterDefault: 255
3. Commit the change.

6.1.1.3 Configuring the condition for numbers

By default, a password must include at least one number.

To configure whether a password has to contain numbers, do the following:

1. Navigate to **System » Security » User Management**.
2. Under **Password Policy** in the **Number** field, configure whether a password has to contain numbers.
Options include:

Option	Description
Required	Default A password must contain at least 1 number.
Not Required	A password does not need to contain any numbers.

3. Commit the change.

6.1.1.4 Configuring the condition for lowercase letters

By default, passwords are not required to contain any lowercase letters.

To configure whether a password has to contain lowercase letters, do the following:

1. Navigate to **System » Security » User Management**.
2. Under **Password Policy** in the **Lowercase** field, configure whether a password has to contain lowercase letters.
Options include:

Option	Description
Not Required	Default A password does not need to contain any lowercase letters.
Required	A password must contain at least 1 lowercase letter.

3. Commit the change.

6.1.1.5 Configuring the condition for uppercase letters

By default, passwords are not required to contain any uppercase letters.

To configure whether a password has to contain uppercase letters, do the following:

1. Navigate to **System » Security » User Management**.
2. Under **Password Policy** in the **Uppercase** field, configure whether a password has to contain uppercase letters.
Options include:

Option	Description
Not Required	Default A password does not need to contain any uppercase letters.
Required	A password must contain at least 1 uppercase letter.

3. Commit the change.

6.1.1.6 Configuring the condition for special characters

By default, passwords are not required to contain any special characters.

The following special characters are permitted: # \$ % & () * + , - . / : < = > @ [] ^ _ { } ~

To configure whether a password has to contain special characters, do the following:

1. Navigate to **System » Security » User Management**.
2. Under **Password Policy** in the **Special Character** field, configure whether a password has to contain special characters.

Options include:

Option	Description
Not Required	Default A password does not need to contain any special characters.
Required	A password must contain at least 1 special character.

3. Commit the change.

6.1.1.7 Enabling the password policy

By default, the password policy is enabled.

When the password policy is disabled, the only condition is that a password must include at least one character.

To enable the password policy, do the following:

1. Navigate to **System » Security » User Management**.
2. Under **Password Policy**, change **Status** to **Enabled**.
3. Commit the change.

6.1.2 Displaying the password policy

To display the active password policy, navigate to **System » Security » User Management**.

The following information is displayed under **Password Policy**:

Parameter	Description
Status	Specifies whether the password policy is enabled. When the password policy is disabled (Disabled), the only condition is that a password must contain at least one character. Other configured conditions do not need to be met.
Maximum Length	Specifies the maximum number of characters in a password.
Minimum Length	Specifies the minimum number of characters in a password.
Number	Specifies whether numbers must be used.
Special Character	Specifies whether special characters must be used.
Lowercase	Specifies whether lowercase letters must be used.
Uppercase	Specifies whether uppercase letters must be used.

6.2 User administration

You can configure multiple users and assign a user profile to each of them.

The following user profiles can be configured locally on the device in SINEC OS:

- **Admin**
- **Guest**

Different access rights are assigned to each profile. The access rights enable users to change settings and run various commands or prevent them from doing so.

For more information, refer to "Access rights (Page 30)".

6.2.1 Case sensitivity in user names

In SINEC OS, uppercase and lowercase letters are not distinguished in user names (case-insensitive).

user1 and **User1** are only two different spellings of the same user name. Therefore, the following applies:

- When a user with the name **user1** is created, another user with the name **User1** cannot be created.
- When a user with the name **user1** is created, this user can log in using different spellings of the user name, such as **user1**, **User1** or **USER1**. The user profile and password of the created user **user1** are in effect for all spellings.

SINEC OS takes uppercase/lowercase into account for user names when saving. A user name is saved exactly as it was defined when it was created. This spelling is also used in outputs, for example, in the CLI with the `show running-config system authentication user` command or in the Web UI under **System >> Security >> User Management**.

6.2.2 Configuring users

To create a new user, follow these steps:

1. Create a new user and assign this user a password and a user profile.

Note

By default, new users need to assign a new password on initial login.

You can disable this function when configuring a new user.

For more information, refer to "Configuring a new user (Page 118)".

2. [Optional] Enable that a user needs to assign a new password on the next login.
For more information, refer to "Enabling the assignment of a new password (Page 119)".

3. [Optional] Change the password of a user.
For more information, refer to "Changing the password of a user (Page 120)".
4. [Optional] Change the user profile of a user.
For more information, refer to "Changing the user profile of a user (Page 121)".

6.2.2.1 Configuring a new user

Only users with the **Admin** user profile can configure a new user.

To create a new user, follow these steps:

1. Navigate to **System » Security » User Management**.
2. Under **User Management**, click **Add**.
A new row is added to the table.
3. Enter a user name under **Username**.
You can only edit the user name directly after adding the new row. As soon as the field is no longer active, the user name is write-protected. If you want to change the user name, you need to delete the user and re-configure it.
Conditions:
 - Must be unique
 - Must be between 1 and 250 characters long
 - All standard characters are allowed, plus the following special characters: _ -
4. Assign a user profile to the user under **Role**.
Options include:

Option	Description
Admin	Users with the Admin user profile have read and write access to the device functions.
Guest	Users with the Guest user profile have read access to the device functions and can change their own password.

5. Assign a password for the user under **Password**.

You can enter a password as follows:

- As hash password
If a password starts with one of the following character combinations, it is viewed as a hash password and saved in this form:

Character combinations	Hash algorithm
\$1\$	MD5
\$5\$	SHA-256
\$6\$	SHA-512

- As plain text password
If a password begins with a character combination other than \$1\$, \$5\$ or \$6\$, it is viewed as a plain text password and converted by the device using the hash algorithm SHA-512. If a password starts with the character combination \$0\$, it is also considered a plaintext password. Use this combination of characters if you want to configure a password that begins with the character \$.
Example: \$0\$\$iemens123

Conditions:

- Must be between 8 and 255 characters long
- Must contain at least 1 number
- All standard characters are allowed, plus the following special characters:
\$ % & () * + , - . / : < = > @ [] ^ _ { } ~

Note any deviating conditions due to the configurable password policy. For more information, refer to "Displaying the password policy (Page 116)".

6. Enter the password again under **Password Confirm**.

7. Commit the changes.

6.2.2.2 Enabling the assignment of a new password

When this function is enabled, it has the effect that a user needs to assign a new password on the next login.

The function for a new user is enabled by default. The function is automatically disabled after the password change and is therefore disabled by default for existing users.

The table below shows the effects of the function on new and existing users:

Use case	Function enabled	Function disabled
New user	<p>The function for a new user is enabled by default.</p> <p>The user is prompted to change the password on initial login.</p> <p>The function is automatically disabled after the password change.</p> <p>To activate the changes, the Web UI session is automatically closed after a few seconds. The user must log in again with the new password</p>	<p>The function was disabled when a new user was configured.</p> <p>The new user is not prompted to change the password on the initial login.</p>
Existing user	<p>The function was enabled for an existing user.</p> <p>If the user has active sessions, they will be closed after a few seconds and the password change will be forced.</p> <p>The user is prompted to change the password on the next login.</p> <p>The function is automatically disabled after the password change.</p> <p>To activate the changes, the Web UI session is automatically closed after a few seconds. The user must log in again with the new password</p>	<p>The function for existing users is disabled by default, because it is automatically disabled after the password change.</p>

Note

When you load a configuration file in which the function is enabled, this has the same effects.

To enable the assignment of a new password, follow these steps:

1. Navigate to **System » Security » User Management**.
2. Under **User Management**, change the parameter **Change of Password Required** to **Enabled**.
3. Commit the changes.

6.2.2.3 Changing the password of a user

Users with the **Admin** user profile can change the passwords for all users.

Users with the **Guest** user profile can only change their own password.

To change the password, follow these steps:

1. Navigate to **System » Security » User Management**.
2. Under **User Management** in the **Password** column, change the parameter for the user. You can enter a password as follows:
 - As hash password
If a password starts with one of the following character combinations, it is viewed as a hash password and saved in this form:

Character combinations	Hash algorithm
\$1\$	MD5
\$5\$	SHA-256
\$6\$	SHA-512

- As plain text password
If a password begins with a character combination other than \$1\$, \$5\$ or \$6\$, it is viewed as a plain text password and converted by the device using the hash algorithm SHA-512. If a password starts with the character combination \$0\$, it is also considered a plaintext password. Use this combination of characters if you want to configure a password that begins with the character \$.
Example: \$0\$\$iemens123

Conditions:

- Must be between 8 and 255 characters long
- Must contain at least 1 number
- All standard characters are allowed, plus the following special characters:
\$ % & () * + , - . / : < = > @ [] ^ _ { } ~

Note any deviating conditions due to the configurable password policy. For more information, refer to "Displaying the password policy (Page 116)".

3. Enter the password again under **Password Confirm**.
4. Commit the changes.

6.2.2.4 Changing the user profile of a user

Users with the **Admin** user profile can change the user profile of users.

To change the user profile, follow these steps:

1. Navigate to **System » Security » User Management**.
2. Under **User Management** in the **Role** column, change the user profile for the user. Options include:

Option	Description
Admin	Users with the Admin user profile have read and write access to the device functions.
Guest	Users with the Guest user profile have read access to the device functions and can change their own password.

3. Commit the changes.

6.2.3 Monitoring Users

Users logged on to the device are monitored by SINEC OS and can be displayed. If you are logged on with the `admin` user profile, you can monitor users, log them off and send them messages.

6.2.3.1 Displaying active users

If you are logged on with the **Admin** user profile, you can show which users are logged on to the device.

To show which users are currently logged on to the device, navigate to **System » Security » User Management**.

The following information is displayed under **User Sessions**:

Parameter	Description
Session	Number of the session Your own session is marked with a *.
User	User name
From	The IP address with which the user is logged on
Context / Context - Protocol	User interface and protocol via which the user is logged on
Date	Date or time at which the user logged on
Mode	Mode which the user is in Possible values include: <ul style="list-style-type: none">• operational - The user is in operational mode.• config-terminal - The user is in the shared configuration mode.• config-exclusive - The user is in the exclusive configuration mode.

6.2.3.2 Displaying user details

To display the configuration of all users, navigate to **System » Security » User Management**.

The following information is displayed under **User Management**:

Parameter	Description
Username	Displays the user name.
Role	Displays the user profile of the user.
Password	The password is masked.
Password Confirm	
Change of Password Required	Shows whether the user will be prompted on the next login to assign a new password.

6.3 Preparing the device for troubleshooting

To remedy a fault, a Siemens service technician temporarily needs access to the device (debug user account) and/or debug information.

This section describes how you prepare the device for servicing so that your Siemens service technician can optimally support you in troubleshooting.

6.3.1 Saving debug information

The debug information is saved as a ZIP file. The device always saves only one file. When a serious error occurs, the device automatically generates a file with the corresponding debug information.

The ZIP file is protected by a password. The password is device-specific and is only known to your Siemens service technician. Save the debug information and forward it to your Siemens service technician.

You can save the debug information on a local client PC or on a remote server.

6.3.1.1 Saving debug information on a local client PC

To save a ZIP file with debug information on a local PC, do the following:

1. Navigate to **System » Load & Save » Service Files**.
2. Under **Save Service File to Local PC**, select the **Debug Information** option for the **File Type** parameter.
3. Click **Save**.
4. If the debug information has been saved before, there will be a query.
Options include:
 - **Yes** - No new ZIP file is generated. The existing ZIP file is transferred.
 - **No** - A new ZIP file with current debug information is generated and transferred. The existing ZIP file is overwritten.

It depends on the browser settings whether the file is saved directly to a specified folder or if you will first see a prompt in which you can select the storage location.
As optical feedback, a load symbol appears beside the button on the right.

- When the save operation is complete, a green check mark appears.
- If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

6.3.1.2 Saving Debug Information on a Remote Server

You can save the debug information on a remote server.

6.3 Preparing the device for troubleshooting

Requirements

- You have configured a server accordingly.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.

Saving debug information

To save a ZIP file with debug information on a remote server, do the following:

1. Navigate to **System » Load & Save » Service Files**.
2. Under **Save Service File to Remote Server**, select the **Debug Information** option for the **File Type** parameter.
3. Configure the settings for the remote server.
For more information on loading and saving files via a remote server, see "Loading and saving files via a remote server (Page 54)".
4. Click **Save**.
5. If the debug information has been saved before, there will be a query.
Options include:
 - **Yes** - No new ZIP file is generated. The existing ZIP file is transferred.
 - **No** - A new ZIP file with current debug information is generated and transferred. The existing ZIP file is overwritten.

As optical feedback, a load symbol appears beside the button on the right.

- When the save operation is complete, a green check mark appears.
- If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

6.3.2 Enabling the Debug user account

The Debug user account allows your Siemens service technician to access your device for a certain period of time. Only users with the **Admin** user profile can activate the user account. The Debug user account remains active until the account is disabled or the device is shut down.

By default, the Debug user account is disabled.

You can only enable the Debug user account via the CLI.

For more information, refer to the **SINEC OS CLI Configuration Manual**.

Security

7.1 Security

This chapter describes the security features available. Make sure the device and network are properly protected from malicious attacks by reviewing/updating the default security settings.

Note

For general recommendations on how to secure the device, refer to "Security recommendations (Page 24)".

7.2 Brute-force attack prevention

SINEC OS includes a protection mechanism to protect against local and remote Brute-Force Attacks (BFAs) via the CLI, Web UI, SNMP, and NETCONF user interfaces. The mechanism monitors the number of failed login attempts for each unique username and IP address. After a certain number of failed attempts, the username or IP address will be blocked for a period of time.

7.2.1 Understanding BFA Prevention

In a Brute-Force Attack, a malicious user attempts to gain access to a device by repeatedly trying a variety of random usernames, passwords, and SNMP community names until they gain access.

SINEC OS attempts to prevent Brute-Force Attacks from succeeding by blocking unique usernames and IP addresses that have repeatedly failed to login.

7.2.1.1 How the prevention mechanism works

When a user or service fails to log in to the device, their username or IP address is added to a list. The BFA prevention mechanism then begins to track the following:

- The time since the last failed login attempt
This is a configurable time period. If the user/service attempts to log in again within this time period and fails, the number of failed log in attempts is increased.
- The number of failed login attempts
This is a configurable parameter. The user/service is blocked if the number of failed log in attempts reaches the set limit.

If a user or service logs in successfully before reaching the maximum number of failed log in attempts, all counters are reset.

7.2 Brute-force attack prevention

User's and services tha exceed the maximum number of failed log in attempts are blocked for a configurable period of time. If a blocked user/service attempts to log in again before the time period has expired, the block is renewed and the timer resets.

A user is unblocked when:

- The timer expires
- When the block is reset manually by an admin user via SINEC OS
- When the device is rebooted

7.2.1.2 Related events

The following events are triggered by the BFA Prevention mechanism and recorded directly in the syslog.

Event	Severity	Syslog Message
User blocked	Warning	User "{ username }" account is locked for { duration } minutes after { count } unsuccessful login attempts.
IP blocked	Warning	IP { IP address } is locked for { duration } minutes after { count } unsuccessful login attempts

7.2.2 Configuring BFA prevention

To configure BFA prevention, do the following:

1. [Optional] Change the reset timer to control how long users and IP addresses are blocked. For more information, refer to "Changing the auto-reset timer (Page 126)".
2. [Optional] Change the maximum number of failed login attempts before users and IP addresses are blocked. For more information, refer to "Changing the maximum number of failed login attempts (Page 127)".
3. [Optional] Change the time between failed login attempts before the counter resets. For more information, refer to "Changing the time between failed login attempts (Page 127)".
4. Enable BFA prevention. For more information, refer to "Enabling BFA prevention (Page 128)".

7.2.2.1 Changing the auto-reset timer

The auto-reset timer unblocks previously blocked users and IP addresses after a certain amount of time.

To set the maximum amount of time that must pass between when a user/IP address is blocked and when it is unblocked, do the following:

1. Navigate to **System » Security » Brute Force Prevention**.
2. Under **Brute Force Prevention**, configure **Auto-Reset Timer**.
Conditions:
 - Formatted as nYnMnDnHnMns, where n is a user-defined number
 - Minimum 0 seconds
 - Maximum 255 minutes (15300 seconds)Default: 10m
3. Commit the change.

7.2.2.2 Changing the maximum number of failed login attempts

When a user or IP address attempts to log in after a previous failed attempt and the timer has not yet expired, a counter is incremented.

You can set a separate limit for users and IP addresses. When the counter for a user or IP address reaches the set limit, they are automatically blocked.

To change the number of maximum number of failed log in attempts, do the following:

1. Navigate to **System » Security » Brute Force Prevention**.
2. Under **Brute Force Prevention**, configure either **User Specific Login Attempts** or **IP Specific Login Attempts**.
Condition:
 - A number between 0 and 255Default: 10
3. Commit the change.

7.2.2.3 Changing the time between failed login attempts

SINEC OS sets a limit on how much time can expire between each failed log in attempt. If a user or IP address fails to log in, the timer begins. If the user or IP address attempts to log in again within this time period and fails, the number of failed log in attempts for that user/IP address is increased.

7.2 Brute-force attack prevention

To change the time between failed log in attempts, do the following:

1. Navigate to **System » Security » Brute Force Prevention**.
2. Under **Brute Force Prevention**, configure **Trigger Interval**.
Conditions:
 - Formatted as nYnMnDnhnmns, where n is a user-defined number
 - Minimum 5 minutes (300 seconds)
 - Maximum 255 minutes (15300 seconds)Default: 5m
3. Commit the change.

7.2.2.4 Enabling BFA prevention

To enable the BFA prevention mechanism, do the following:

Note

BFA prevention is enabled by default.

1. Navigate to **System » Security » Brute Force Prevention**.
2. Under **Brute Force Prevention**, change **Brute Force Prevention** to **Enabled**.
3. Commit the change.

7.2.3 Unblocking a user or IP address

Username and addresses can be unblocked manually.

To unblock a username or IP address that is currently blocked, do the following:

1. Navigate to **System » Security » Brute Force Prevention**.
2. Under **Brute Force Prevention - State Information**, locate the blocked username or IP address and then click **Reset**.

7.2.4 Monitoring BFA prevention

To review which usernames and/or IP addresses are currently being monitored by the BFA protection mechanism, navigate to **System » Security » Brute Force Prevention**.

Separate tables for users and IP addresses detail the following under **Brute Force Prevention - State Information**:

Parameter	Description
Username	The user or community name that is currently monitored. Note that unknown users, such as those authenticated via RADIUS, are listed as "Unknown User".
IP Address	The IP address that is currently monitored.
Failed Logins	The current number of failed login attempts.
Time Since Last Failed	The time (formatted as nYnMnDnhnmns) since the last failed login attempt .
Blocked	The time (formatted as nYnMnDnhnmns) until the block is removed.

Example

Username	Failed Logins	Time Since Last Failed	Blocked
Unknown User	10	4m18s	22s
admin	0	0s	0s

IP Address	Failed Logins	Time Since Last Failed	Blocked
172.30.142.156	1	18s	0s
172.30.142.244	3	2m6s	0s

7.3 Security-relevant events

To meet the requirements of the leading security standard used in the industrial environment, IEC 62443, you must completely log all user activities, among other things. One important prerequisite is the generation and provision of the corresponding security-relevant events.

7.3.1 Understanding security-relevant events

Security-relevant events are generated by various components (e.g. IE switches, Industrial PCs, servers, network components and controllers) and contain information regarding, for example, the activities executed by various users (e.g. login attempts and configuration changes).

SINEC OS devices generate event messages and save these locally as a system log. The event messages can also be forwarded to one or multiple central logging instances. A logging instance can be a Syslog server (e.g. SINEC INS) or a Security Information and Event Management (SIEM) system.

For more information on the system log, refer to "System logging (Page 341)".

7.3.1.1 SIEM system

A SIEM system can be used to collect security-relevant event messages, analyze them and report critical events. This can be done for individual devices or an entire network.

Use a SIEM system to collect event messages centrally and detect a fault based on interrelated events.

The following figure shows a SIEM system and involved components.

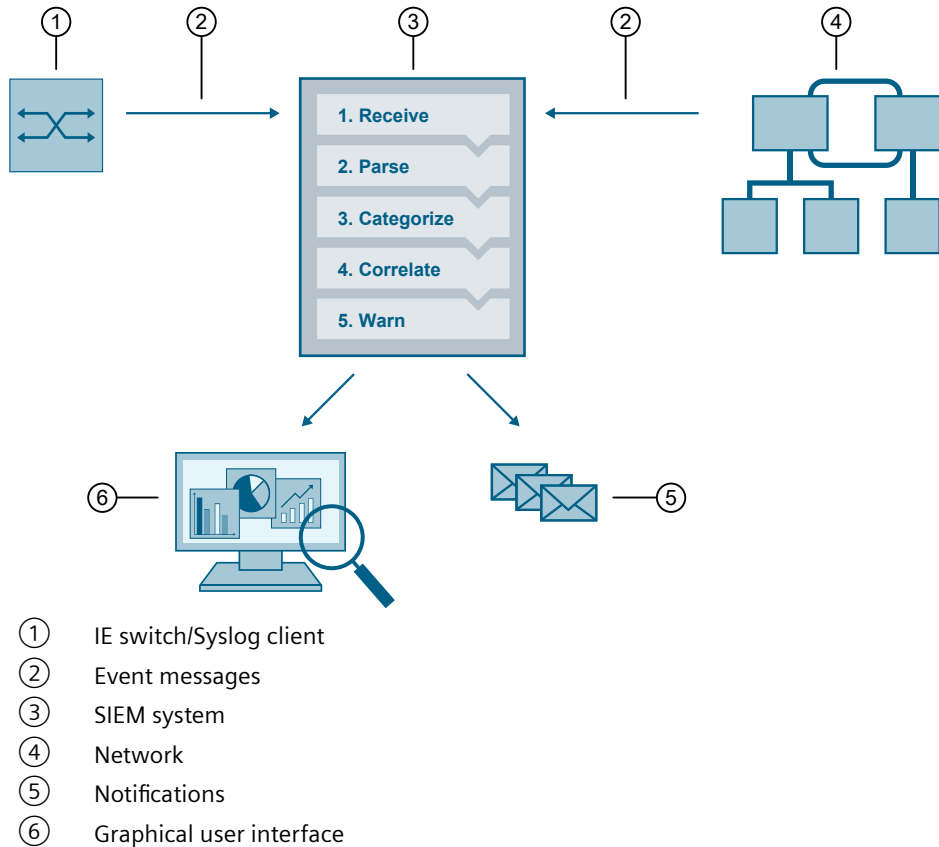


Figure 7-1 SIEM system

A SIEM system processes event messages as follows:

1. **Receive**
An implemented Syslog server receives the event messages from various devices, network components, etc.
2. **Parse**
The SIEM system evaluates the event messages and links each event message to a generalized SIEM-specific event.
For a SIEM system to process event messages, their syntax must be known and compatible. To meet this requirement, the SINEC OS devices follow the IEC 62443 standard.
For more information on the syntax of the event messages, refer to "Variables in event messages (Page 132)".

3. Categorize

The generalized event messages are grouped into categories and saved in the SIEM database. Such categories are, for example, failed login attempts, configuration changes and other potentially malicious activities.

4. Correlate

The SIEM system establishes relations between the event messages. This allows the SIEM system to detect abnormalities (e.g. unusual patterns and trends) that may indicate security-relevant activities.

5. Warn

When potential security-relevant events are identified, the SIEM system generates corresponding security warnings. These can be output via a graphical user interface or sent as notifications.

7.3.1.2 Structure of an event message

Security-relevant event messages are forwarded to a logging instance with the following information:

Element	Description
HEADER	
PRI	Priority of the event message The priority is composed of the following elements: <ul style="list-style-type: none"> Severity Severity of the message For more information on the severity, see "Severity levels (Page 348)". Facility Origin of the message For security-relevant events, the origin is always local0.
VERSION	Version number of the Syslog specification
TIMESTAMP	Time stamp of the event message according to RFC 3339 Example: 2010-01-01T02:03:15+02:00
HOSTNAME	Sender of the event message with FQDN, host name or IP address IPv4 address according to RFC 1035: Bytes in decimal representation: XXX.XXX.XXX.XXX "-" is output if information is missing.
STRUCTURED-DATA	

Element	Description
timeQuality	<p>Information on the system time</p> <p>Example: [timeQuality tzKnown="0" isSynced="0"]</p> <p>The tzKnown parameter indicates whether the sender knows its time zone.</p> <p>Options include:</p> <ul style="list-style-type: none"> Value "1" = The time zone is known. Value "0" = The time zone is unknown. <p>The isSynced parameter specifies whether the source device is synchronized with a reliable external time source, e.g. via NTP.</p> <p>Options include:</p> <ul style="list-style-type: none"> Value "1" = The system time is synchronized. Value "0" = The system time is not synchronized.
MSG	
MESSAGE	Event message as ASCII string in English

Note

For more information on the structure of the event messages and on the meaning of the parameters, see RFC 5424 (<https://tools.ietf.org/html/rfc5424>).

7.3.1.3 Variables in event messages

In each event message, the { **MESSAGE** } element contains variables that are filled dynamically by the data of the respective event. These variables are displayed in curly brackets before the tables in section "Monitoring security-relevant events (Page 134)" (e.g. {Protocol}).

Note

The list of variables is not complete. Only variables that are relevant for the integration of a SIEM system are listed.

The following variables can be found in the { **MESSAGE** } element of a security-relevant event message:

Variable	Description	Example
IP address	Source or destination IP address according to RFC1035 or RFC4291 paragraph 2.2 Format for IPv4: %d.%d.%d.%d	192.168.1.105 2001:DB8::8:800:200C:417A
Dest mac	Destination MAC address Format: %02x:%02x:%02x:%02x:%02x:%02x	00:0C:29:2F:09:B3
Src mac	Source MAC address Format: %02x:%02x:%02x:%02x:%02x:%02x	00:0C:29:2F:09:B3
Src port	Source port Range of values: 0 ... 65535 Format: %d	2345

Variable	Description	Example
Dest port	Destination port Range of values: 0 ... 65535 Format: %d	80
Protocol	Name of the service that generated an event or of the Layer 4 protocol used. Possible values: WBM UDP TCP SSH Console PNIO NET-CONF 802.1X RADIUS DCP IP All Format: %s	TCP
User name	String without spaces that identifies an authenticated user by name. Format: %s	maier
Group	String without spaces that identifies a group based on a name. Format: %s	it-service
Local interface	Symbolic name of a local interface Format: %s	Console
Destination user name	Identifies a user based on a name. The user is linked to the destination of the event. Format: %s	Peter.Maier
Role	Symbolic name for the group role Format: %s	Administrator
Time minute Timeout	Time in minutes Format: %d	44
Time second	Time in seconds Format: %d	44
Failed login count	Number of failed login attempts Format: %d	10
Max sessions	Maximum number of sessions Format: %d	10
Version	Version information without spaces Format: %s	V1.0.3SP1
Firewall rule	String for a firewall rule set with spaces Format: %s	Rule1
Subject	String for the subject in the certificate Used as part of the certificate-based authentication. The string can contain spaces and Unicode characters. Format: (%s) or (%s %s) Format: (%S) or (%S %S) for UTF8 code	(Peter Maier)

7.3 Security-relevant events

Variable	Description	Example
Config detail	String with spaces for the configuration Format: %s	VLAN
License key	String that represents an ALM license or an article number in the case of a CLP Format: %s	SISLSOXTST0100

7.3.2 Monitoring security-relevant events

This section describes the security-relevant event messages. The categorization of the messages is based on the IEC 62443 standard.

7.3.2.1 Identification and authentication of human users

The following event messages provide information about successful and failed login attempts made by users.

{Local interface}: User {User name} logged in.

Example	Console: User admin logged in.
Explanation	A user has successfully logged in to the SINEC OS device via a local interface. In the example, the "admin" user successfully logged in via the console interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: Service account logged in.

Example	Console: Service account logged in.
Explanation	A user has successfully logged in to the SINEC OS device via a local interface with the Debug user account. In the example, the Debug user account was successfully logged in via the console interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: User {User name} failed to log in.

Example	Console: User admin failed to log in.
Explanation	The login attempt of a user via a local interface of the SINEC OS device failed. In the example, the login attempt of the "admin" user via the console interface failed.
Severity	Error

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: Service account failed to log in.

Example	Console: Service account failed to log in.
Explanation	The login attempt with the Debug user account via a local interface of the SINEC OS device failed. In the example, the login attempt with the Debug user account via the console interface failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} logged in from {IP address}.

Example	SSH: User admin logged in from 192.168.0.1.
Explanation	A user has successfully logged in to the SINEC OS device via a network interface. In the example, the "admin" user successfully logged in from the network address "192.168.0.1".
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: Service account logged in from {IP address}.

Example	SSH: Service account logged in from 192.168.0.1.
Explanation	A user has successfully logged in to the SINEC OS device via a network interface with the Debug user account. In the example, the Debug user account was successfully logged in from the network address "192.168.0.1".
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} failed to log in from {IP address}.

Example	SSH: User admin failed to log in from 192.168.0.1.
Explanation	The login attempt of a user to the SINEC OS device via a network interface failed. In the example, the login attempt of the "admin" user from the network address "192.168.0.1" failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: Service account failed to login from {IP address}.

Example	SSH: Service account failed to login from 192.168.0.1.
Explanation	The login attempt with the Debug user account to the SINEC OS device via a network interface failed. In the example, the login attempt with the Debug user account from the network address "192.168.0.1" failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: User {User name} logged out.

Example	Console: User admin logged out.
Explanation	A user has logged out via a local interface of the SINEC OS device. In the example, the "admin" user logged out manually via the console interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} logged out from {IP address}.

Example	SSH: User admin logged out from 192.168.0.1.
Explanation	A user has logged out of the SINEC OS device via a network interface. In the example, the "admin" user manually logged out from the network address "192.168.0.1".
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: Service account logged out.

Example	Console: Service account logged out.
Explanation	A user logged out the Debug user account via a local interface of the SINEC OS device. In the example, the Debug user account was manually logged out via the console interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: Service account logged out from {IP address}.

Example	SSH: Service account logged out from 192.168.0.1.
Explanation	A user logged out the Debug user account from the SINEC OS device via a network interface. In the example, the Debug user account was logged out manually from the network address "192.168.0.1".
Severity	Info

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: Default user {User name} logged in.

Example	Console: Default user admin logged in.
Explanation	A user has successfully logged in to the SINEC OS device via a local interface with a default user profile and password. In the example, the default user "admin" successfully logged in via the console interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

{Protocol}: Default user {User name} logged in from {IP address}.

Example	SSH: Default user admin logged in from 192.168.0.1.
Explanation	A user has successfully logged in to the SINEC OS device via a network interface with a default user profile and password. In the example, the default user "admin" successfully logged in from the network address "192.168.0.1".
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

{Protocol}: No response from the RADIUS server {IP address}.

Example	RADIUS: No response from the RADIUS server 192.168.1.105.
Explanation	No access to a RADIUS server or a RADIUS server is not responding. In the example, the RADIUS server with the IP address "192.168.1.105" is not responding.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

7.3.2.2 Identification and authentication of devices

The following event messages provide information about successful and failed device accesses.

{Protocol}: Device {Src mac} access granted.

Example	WBM: Device 00:0C:29:2F:09:B3 access granted.
Explanation	Device access is granted due to successful port authentication. In the example, access of the device with the source MAC address "00:0C:29:2F:09:B3" is granted.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: Device {Src mac} access denied.

Example	WBM: Device 00:0C:29:2F:09:B3 access denied.
Explanation	Device access is denied due to unsuccessful port authentication. In the example, access of the device with the source MAC address "00:0C:29:2F:09:B3" is denied.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} successfully established.

Example	WBM: Connection from device 192.168.1.105 subject (Peter Maier) successfully established.
Explanation	The device authentication was successful. In the example, a connection from a device with the IP address "192.168.1.105" to the SINEC OS device was set up successfully.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} failed.

Example	WBM: Connection from device 192.168.1.105 subject (Peter Maier) failed.
Explanation	The device authentication has failed. In the example, no connection could be set up between a device with the IP address "192.168.1.105" and the SINEC OS device.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

7.3.2.3 User account management

The following event messages provide information about activities regarding the user accounts. This includes, for example, creating/deleting user accounts, changing passwords, activating the Debug user account.

{Protocol}: User {User name} has changed the password.

Example	WBM: User admin has changed the password.
Explanation	A user has changed his or her own password. In the example, the "admin" user changed their own password.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} has changed the password of user {Destination user name}.

Example	WBM: User admin has changed the password of user user1.
Explanation	A user has changed the password of another user. In the example, the "admin" user changed the password of the "user1" user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} created user-account {Destination user name} with role {Role}.

Example	WBM: User admin created user-account admin2 with role Administrator.
Explanation	A user has created a user account and has assigned a user profile to the account. In the example, the "admin" user created the "admin2" user account and assigned the "Administrator" user profile to the account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} deleted user-account {Destination user name}.

Example	WBM: User admin deleted user-account admin2.
Explanation	A user has deleted an existing user account. In the example, the "admin" user deleted the "admin2" user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} enabled the service account.

Example	SSH: User admin enabled the service account.
Explanation	A user has enabled the Debug user account. In the example, the "admin" user enabled the Debug user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} disabled the service account.

Example	SSH: User admin disabled the service account.
Explanation	A user has disabled the Debug user account. In the example, the "admin" user disabled the Debug user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

7.3.2.4 Unsuccessful login attempts

The following event messages provide information about failed login attempts and the resulting locks through the brute force attack (BFA) prevention.

{Protocol}: User {User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.

Example	All: User admin account is locked for 10 minutes after 11 unsuccessful login attempts.
Explanation	The BFA prevention has blocked a user for a specific period after too many failed login attempts. In the example, the BFA prevention has blocked the "admin" user for 10 seconds after 11 failed login attempts.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

{Protocol}: {IP address} is temporarily blocked for {Time second} seconds after {Failed login count} unsuccessful login attempts.

Example	All: 192.168.1.105 is temporarily blocked for 600 seconds after 11 unsuccessful login attempts.
Explanation	The BFA prevention has blocked an IP address for a specific period after too many failed login attempts. In the example, the BFA prevention has blocked the IP address "192.168.1.105" for 600 seconds after 11 failed login attempts.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

7.3.2.5 Session lock

The following event messages provide information about closing sessions due to inactivity.

{Protocol}: The session of user {User name} was closed after {Time second} seconds of inactivity.

Example	SSH: The session of user admin was closed after 60 seconds of inactivity.
Explanation	A session was closed due to inactivity. In the example, the session of the "admin" user was closed after 60 seconds of inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

7.3.2.6 Limiting the number of simultaneous sessions

The following event messages provide information about the limiting of simultaneous sessions per interface.

{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.

Example	SSH: The maximum number of 8 concurrent login sessions exceeded.
Explanation	The maximum number of parallel sessions has been exceeded. In the example, the maximum number of 8 simultaneous sessions via SSH was exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

7.3.2.7 Configuration changes

The following event messages provide information about configuration changes made by a user or a protocol.

{Protocol}: User {User name} has changed the configuration.

Example	SSH: User admin has changed the configuration.
Explanation	A user has changed the configuration. In the example, the user "admin" has changed the configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

{Protocol}: User {User name} has changed {Config detail} configuration.

Example	SSH: User admin has changed VLAN configuration.
Explanation	A user has changed specific configuration values. In the example, the "admin" user changed the VLAN configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

{Protocol}: User {User name} has initiated a reset to factory defaults.

Example	SSH: User admin has initiated a reset to factory defaults.
Explanation	A user has initiated a reset to default settings. In the example, the user "admin" has initiated a reset to default settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

{Protocol}: A reset to factory defaults was initiated.

Example	DCP: A reset to factory defaults was initiated.
Explanation	A reset to default settings has been initiated. In the example, DCP initiated a reset to default settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

7.3.2.8 Communication integrity

The following event messages provide information about failed integrity verification during communication.

{Protocol}: Integrity verification failed.

Example	Console: Integrity verification failed.
Explanation	An integrity fault was detected while the communication integrity of a message was being checked. Only certificate-based communication is possible.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.1

7.3.2.9 Software and information integrity

The following event messages provide information about failed integrity verification when loading the firmware.

Firmware integrity verification failed. Backup firmware started.

Example	Firmware integrity verification failed. Backup firmware started.
Explanation	An integrity fault was detected while the firmware integrity was being checked. The backup firmware was loaded.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

7.3.2.10 Session integrity

The following event messages provide information about failed integrity verification during a session.

{Protocol}: Session ID verification failed.

Example	WBM: Session ID verification failed.
Explanation	The session ID is invalid.

Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

7.3.2.11 Protection from denial-of-service (DoS) attacks

The following event messages provide information about the occurrence of a DoS attack.

{Protocol}: Denial-of-Service (DoS) attack detected.

Example	Console: Denial-of-Service (DoS) attack detected.
Explanation	A denial-of-service (DoS) attack was detected.
Severity	Alert
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

7.3.2.12 Protection of check information

The following event messages provide information about the deletion of the local logbook.

{Protocol}: User {User name} has cleared the logging buffer.

Example	SSH: User admin has cleared the logging buffer.
Explanation	A user has deleted the local logbook. In the example, the user "admin" has deleted the local logbook.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.9

7.3.2.13 Restoration of the automation system

The following event messages provide information about the successful or failed activation of the firmware.

{Protocol}: User {User name} activated the firmware {Version}.

Example	WBM: User admin activated the firmware v2.0.
Explanation	A user has successfully activated a firmware version. In the example, the "admin" user successfully activated the "v2.0" firmware version.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: Firmware {Version} was activated.

Example	WBM: Firmware v2.0 was activated.
Explanation	A firmware version has been successfully activated. In the example, the firmware version "v2.0" was successfully activated.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: User {User name} failed to activate firmware {Version}.

Example	WBM: User admin failed to activate firmware v2.0.
Explanation	Activation of a firmware version by a user has failed. In the example, the activation of the firmware version "v2.0" by the "admin" user failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: Firmware activation failed.

Example	WBM: Firmware activation failed.
Explanation	The firmware activation has failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

7.4 Keys and certificates

This section describes how to configure and manage keys and certificates.

7.4.1 Understanding keys and certificates

The use of keys and certificates allows you to encrypt the communication and to confirm the identity of communication partners:

- **Confidentiality**
Data is confidential and not readable for unauthorized eavesdroppers.
- **Integrity**
The message received by the recipient is the same, unchanged message as sent by the sender. The message was not changed during transport.
- **Endpoint authentication**
The communication partner as endpoint is exactly the one it claims to be and the one that is to be reached. The identity of the partner is verified.

SINEC OS uses the following components for this:

- An asymmetric encryption method with public and private keys
- Certificates
- Signatures

7.4.1.1 Key method

Symmetric key method

In the symmetric key method, both communication partners use the same key to encrypt and decrypt information.

The security of the method depends on the key not being known to anyone except the two communication partners. The key therefore needs to be exchanged via a secure, tap-proof and manipulation-proof channel.

Asymmetric key method

Asymmetric key methods work with a key pair consisting of a public key and a private key. They are unique and are related to one another by a mathematical algorithm.

- **Public key**
The public key is made available to the public, i.e. to every potential communication partner. Anyone who has the public key can encrypt messages to the owner. It must be possible to assign public keys uniquely to an owner. To ensure this, public keys have a digital certificate that contains information about the owner.
- **Private key**
Only the owner may know the private key. With the private key, owners can decrypt encrypted messages addressed to them. The private key is also used to sign certificates.

Because the public key is not secret, the communication channel does not need to be tap-proof in the asymmetric key method.

A disadvantage of the asymmetric key procedure is the relatively high effort for encryption and decryption, which has a negative effect on the computing speed.

Diffie-Hellman

The Diffie-Hellman method is an asymmetric key method which is used for key exchange and key agreement.

Diffie-Hellman key exchange enables two communication partners to agree on a shared secret key (session key) over a public line. The session key can then be used for a symmetric key method.

The Diffie-Hellman key agreement forms the basis for encryption protocol for secure data transmission (e.g. Transport Layer Security, TLS). During communication, the benefits of symmetric encryption (high computing speed) can be exploited while the key is protected from access by an attacker through the asymmetric encryption.

7.4.1.2 Default key pairs

SINEC OS devices are equipped with manufacturer-defined key pairs for HTTPS and SSH.

The SSH server requires a corresponding key pair so that the user can access the CLI user interface, for example, during initial commissioning of the device.

The following applies to default key pairs:

- The keys are unique for each device.
- When you reset the device to the default settings, the keys and certificates defined by the manufacturer are retained.
- When a default key pair is renewed, a corresponding entry is made in the system protocol. Renewal is necessary if the existing data is corrupted or stricter key requirements are introduced by a firmware update.

User-defined key pairs and certificates can be used for HTTPS.

7.4.1.3 Certificates

Digital certificates are used to confirm identities and thus prevent man-in-the-middle attacks. Identities can be people, computers or machines.

A certificate according to the X.509 standard has the following main components:

- A public key
- Information about the certificate owner (i.e. the key owner)
- Attributes such as
 - Serial number
 - Lease time
 - Attribute: keyEncipherment
A symmetric key that is encrypted with the key contained in the certificate is used for data encryption.
 - Attribute: digitalSignature
A digital signature (authentication) of the certificate authority that issued the certificate

Certificates are issued by official certificate authorities (CA) or the certificate owners themselves.

7.4.1.4 Certificates from an official certificate authority

The following steps are required to obtain a certificate from an official certificate authority:

1. Anyone wishing to obtain a certificate submits a certificate request via a registration body connected to the certificate authority.
2. The certificate authority evaluates the request and subject based on defined criteria.
3. If the identify of the subject can be clearly established, the certificate authority authenticates this identity by issuing a signed certificate. The subject has now become the certificate owner.

7.4.1.5 Self-signed certificates

Self-signed certificates are certificates whose signature originates from the certificate owner and not from an independent certificate authority.

Examples:

- You can create a certificate and sign it yourself to encrypt messages to a communication partner, for example.
Certificate owners could sign their own certificates with their private key. Using the public key, the communication partner can check that the signature and public key fit together. This is sufficient for simple plant-internal communication that is to be encrypted. However, self-signed certificates are not suitable for signing other certificates.
- A root certificate is, for example, a self-signed certificate by the certificate authority (issuer) which contains the public key of the certificate authority.

7.4.1.6 Certificate chain

A digital certificate connects an identity with the data of a certificate owner to the public key of the identity. In turn, the digital certificate itself is protected by a digital signature, whose authenticity can be checked with the public key of the certificate issuer. A digital certificate is then needed to check the identity of the issuer key. In this way, a chain of digital certificates is formed, which each confirm the authenticity of the public key with which the preceding certificate can be checked. This is called a certificate chain.

Certificates are organized hierarchically for this purpose:

- **Root certificates**
At the tip of the hierarchy are the root certificates. These are certificates that do not need to be authenticated by another instance. They are issued by a reliable Certificate Authority. Certificate owner and certificate issuer of root certificates are identical. Root certificates are fully trusted, they are the "anchor" of trust and must therefore be known by the recipient as trustworthy certificates. The communication partner must be able to rely on the authenticity of the certificate without an additional certificate.
- **Intermediate certificates**
Root certificates are used to sign certificates from lower-level certificate authorities, so-called intermediate certificates. This transfers the trust from the root certificate to the intermediate certificate. An intermediate certificate can sign a certificate just like a root certificate, therefore both are "CA certificates".
- **User certificates**
This hierarchy can continue over several intermediate certificates as far as the user certificate, also called the end entity certificate. The user certificate is the certificate of the identity to be identified.

The chain of intermediate certificates as far as the root certificate must exist in the correct order in each device that should validate the user certificate of a communication partner.

7.4.1.7 Signatures

Create

The issuer of a certificate generates a hash value (fingerprint) from the data of the certificate with a specific hash algorithm (e.g. SHA-2, Secure Hash Algorithm). It then generates a digital signature from the hash value and its private key. The RSA signature method is often used for this. The digital signature is saved in the certificate. The certificate is signed in this way.

Verify

The verifier of a certificate obtains the certificate of the issuer and with it the public key. The verifier then generates a hash value again from the data of the certificate using the same hash algorithm that was used for signing (e.g. SHA-2). This hash value is compared to the hash value that is determined using the public key of the certificate issuer and the signature algorithm for checking the signature.

If the signature check returns a positive result and the hash values match, the identity of the certificate owner and the integrity, i.e. the authenticity and genuineness of the certificate content, are proven. Anyone who has the public key, i.e. the certificate of the certificate authority, can check the signature and thus determine that the certificate was actually signed by the certificate authority.

7.4.1.8 Storage locations

SINEC OS defines the following storage locations for keys and certificates:

- **Keystore**

Key pairs are saved in the keystore that SINEC OS uses as follows:

- For providing a server service (e.g. HTTPS)
- For authentication as client (e.g. to establish a secure connection for data transmission)

Together with the key pair, one or more certificates can be saved to sign the public key.

- **Truststore**

In the truststore, certificates with which SINEC OS authenticates other devices are saved. An entry can contain multiple certificates. For example, all certificates from reliable certificate authorities can be stored in one entry.

The use of a reliable certificate authority can reduce the configuration workload. A truststore with only one certificate can authenticate multiple remote servers.

The keystore and the truststore are central storage locations in SINEC OS. Other functions can use key pairs or reliable public keys and certificates from the keystore and truststore.

7.4.1.9 Access rules

The following rules apply to accessing keys and certificates:

- Users can neither change nor delete manufacturer-defined key pairs and certificates.
- Users cannot add user-defined certificates for manufacturer-defined key pairs.
- Users cannot read private keys and key pairs, regardless of whether they are manufacturer- or user-defined.
- Users with administrator rights have full access rights to user-defined key pairs and certificates.
- When you save the configuration, manufacturer-defined key pairs are saved with a specific tag.
- When you load a configuration (as file or from a CLP), user-defined key pairs and certificates cannot be changed. The device restores its own manufacturer-defined key pairs and certificates.

7.4.1.10 Related events

The following events are triggered for keys and certificates and recorded directly in the Syslog.

Event	Severity	Syslog message
Generation of a new SSH host key due to invalid key in the EE-PROM.	Info	An invalid SSH server key has been detected. As such, a new key has been generated.

7.4.2 Managing the keystore

To configure the keystore, do the following:

- [Optional] Add key pairs in the keystore.
For more information, refer to "Importing a key pair from a local client PC (Page 149)" and "Importing a key pair from a remote server (Page 151)".
- [Optional] Add certificates in the keystore to sign the public key.
For more information, refer to the **SINEC OS CLI Configuration Manual**.

7.4.2.1 Importing a key pair from a local client PC

You can load a file from a file server and thus import a contained key pair into the keystore.

In addition to the private key, the file can contain a self-signed user certificate or a certificate chain to sign the public key. Private keys do not need to be encrypted. This also applies to private keys with the format PKCS#12.

SINEC OS supports the following formats:

- PEM-coded keys
 - Public-Key Cryptography Standards (PKCS#1, PKCS#8)
 - Elliptic Curve Cryptography (nach RFC 5915)
- PEM-coded X.509 certificates
- PKCS#12

Note

If the file contains more than one certificate, the order of certificates must correspond to the order of the certificate chain. The first certificate in the file has to be the user certificate and the last one has to be a root certificate. There can be intermediate certificates in between.

To import a certificate from a local client PC to the keystore, do the following:

1. Navigate to **System » Load & Save » Keys & Certificates**.
2. Under **Load Certificate to Keystore from Local PC**, enter a name for the key pair in **Key Name**.
Condition:
 - Must be between 1 and 32 characters long
3. Under **Certificate Name**, enter the name of the user certificate that is to be created or overwritten.
Condition:
 - Must be between 1 and 64 characters long
4. Under **Format**, select the format of the certificate.
Options include:

Option	Description
PEM	The file is available in PEM format.
PKCS12	The file is available in PKCS#12 format.

5. [Optional] If you have selected the option **PKCS12** under **Format** and the PKCS#12 file is encrypted, enter the password for the file under **Password (if applicable)**.
Condition:
 - Must be between 1 and 255 characters long
6. [Optional] If a CA certificate is contained in a PKCS#12 file and it is to be stored in the truststore, enter the name of the certificate folder under **Certificate Bag** and the name of the certificate under **Certificate Entry Name**.
Condition for the name of the certificate folder:
 - Must be between 1 and 32 characters long
 Condition for the name of the certificate:
 - Must be between 1 and 64 characters long
7. Under **Certificate File**, open a dialog window to select a file using the button.
8. Select the corresponding file via the dialog and click **Open**.
9. Click **Load** to load the certificate.
While the certificate is being loaded, a load symbol appears beside the button on the right.
 - When the load operation is complete, a green check mark appears.
 - If the load operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.
10. Commit the change.
11. To activate the certificate, restart the device.
For more information, refer to "Restarting the device (Page 80)".
When the restart is complete, the login page is displayed.
12. Log in.
For more information, refer to "Logging in to a configured device (Page 75)".

7.4.2.2 Importing a key pair from a remote server

You can load a file from a file server and thus import a contained key pair into the keystore.

Requirements

- You have configured a server accordingly.
- The certificate is on the server.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.

Loading a file into the device

In addition to the private key, the file can contain a self-signed user certificate or a certificate chain to sign the public key. Private keys do not need to be encrypted. This also applies to private keys with the format PKCS#12.

SINEC OS supports the following formats:

- PEM-coded keys
 - Public-Key Cryptography Standards (PKCS#1, PKCS#8)
 - Elliptic Curve Cryptography (nach RFC 5915)
- PEM-coded X.509 certificates
- PKCS#12

Note

If the file contains more than one certificate, the order of certificates must correspond to the order of the certificate chain. The first certificate in the file has to be the user certificate and the last one has to be a root certificate. There can be intermediate certificates in between.

To import a certificate from a remote server to the keystore, do the following:

1. Navigate to **System » Load & Save » Keys & Certificates**.
2. Under **Load Certificate to Keystore from Remote Server**, enter a name for the key pair in **Key Name**.
Condition:
 - Must be between 1 and 32 characters long
3. Under **Certificate Name**, enter the name of the user certificate that is to be created or overwritten.
Condition:
 - Must be between 1 and 64 characters long
4. Under **Format**, select the format of the certificate.
Options include:

Option	Description
PEM	The file is available in PEM format.
PKCS12	The file is available in PKCS#12 format.

5. [Optional] If you have selected the option **PKCS12** under **Format** and the PKCS#12 file is encrypted, enter the password for the file under **Password (if applicable)**.
Condition:
 - Must be between 1 and 255 characters long
6. [Optional] If a CA certificate is contained in a PKCS#12 file and it is to be stored in the truststore, enter the name of the certificate folder under **Certificate Bag** and the name of the certificate under **Certificate Entry Name**.
Condition for the name of the certificate folder:
 - Must be between 1 and 32 characters longCondition for the name of the certificate:
 - Must be between 1 and 64 characters long
7. Configure the settings for the remote server.
For more information on loading files via a remote server, see "Loading and saving files via a remote server (Page 54)".
8. Click **Load** to load the certificate.
While the certificate is being loaded, a load symbol appears beside the button on the right.
 - When the load operation is complete, a green check mark appears.
 - If the load operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.
9. Commit the change.
10. To activate the certificate, restart the device.
For more information, refer to "Restarting the device (Page 80)".
When the restart is complete, the login page is displayed.
11. Log in.
For more information, refer to "Logging in to a configured device (Page 75)".

7.4.3 Managing the truststore

To configure the truststore, do the following:

1. [Optional] Create a certificate folder in the truststore and add certificates. You can group certificates in a certificate folder. If you create a new certificate folder, you need to add at least one certificate to it directly.
For more information, refer to "Importing a certificate from a local client PC (Page 153)" and "Importing a certificate from a remote server (Page 154)".
2. [Optional] Create a key bag in the truststore and add known hosts. You can group known hosts in a key bag. When you create a new key bag, you need to add at least one known host.
For more information, refer to the **SINEC OS CLI Configuration Manual**.
There is a security prompt on the first connection establishment with an SFTP server. When you commit this prompt, the device automatically creates a key bag and saves the data of the known host.
For more information, refer to "Loading and saving files via a remote server (Page 54)".

7.4.3.1 Importing a certificate from a local client PC

You can load a certificate from a local client PC to the truststore.

SINEC OS supports the following formats:

- PEM-coded X.509 certificates
- PEM-coded certificate in PKCS#7 format

Note

If the file contains more than one certificate, the order of certificates must correspond to the order of the certificate chain. The first certificate in the file has to be the user certificate and the last one has to be a root certificate. There can be intermediate certificates in between.

To import a certificate from a local client PC to the truststore, do the following:

1. Navigate to **System » Load & Save » Keys & Certificates**.
2. Under **Load Certificate to Truststore from Local PC**, enter the name of the certificate folder to which you want to add the certificate in **Certificate Bag**.
If you want to create a new certificate folder, assign a name to the certificate folder.
Condition:
 - Must be between 1 and 32 characters long
3. Under **Certificate Name**, assign a name for the certificate or the certificate chain.
Condition:
 - Must be between 1 and 64 characters long
4. Under **Format**, select the format of the certificate.
Options include:

Option	Description
PEM	The file is available in PEM format.
PKCS7	The file is available in PKCS#7 format.
5. Under **Certificate File**, open a dialog window to select a file using the button.
6. Select the corresponding file via the dialog and click **Open**.
7. Click **Load** to load the certificate.
While the certificate is being loaded, a load symbol appears beside the button on the right.
 - When the load operation is complete, a green check mark appears.
 - If the load operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.
8. Commit the change.
9. To activate the certificate, restart the device.
For more information, refer to "Restarting the device (Page 80)".
When the restart is complete, the login page is displayed.
10. Log in.
For more information, refer to "Logging in to a configured device (Page 75)".

7.4.3.2 Importing a certificate from a remote server

You can load a certificate from a remote server to the truststore.

SINEC OS supports the following formats:

- PEM-coded X.509 certificates
- PEM-coded certificate in PKCS#7 format

Note

If the file contains more than one certificate, the order of certificates must correspond to the order of the certificate chain. The first certificate in the file has to be the user certificate and the last one has to be a root certificate. There can be intermediate certificates in between.

Requirements

- You have configured a server accordingly.
- The certificate is on the server.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.

Loading a certificate

To import a certificate from a remote server to the truststore, do the following:

1. Navigate to **System » Load & Save » Keys & Certificates**.
2. Under **Load Certificate to Truststore from Remote Server**, enter the name of the certificate folder to which you want to add the certificate in **Certificate Bag**.
If you want to create a new certificate folder, assign a name to the certificate folder.
Condition:
 - Must be between 1 and 32 characters long
3. Under **Certificate Name**, assign a name for the certificate or the certificate chain.
Condition:
 - Must be between 1 and 64 characters long
4. Under **Format**, select the format of the certificate.
Options include:

Option	Description
PEM	The file is available in PEM format.
PKCS7	The file is available in PKCS#7 format.

5. Configure the settings for the remote server.
For more information on loading files via a remote server, see "Loading and saving files via a remote server (Page 54)".

6. Click **Load** to load the certificate.
While the certificate is being loaded, a load symbol appears beside the button on the right.
 - When the load operation is complete, a green check mark appears.
 - If the load operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.
7. Commit the change.
8. To activate the certificate, restart the device.
For more information, refer to "Restarting the device (Page 80)".
When the restart is complete, the login page is displayed.
9. Log in.
For more information, refer to "Logging in to a configured device (Page 75)".

7.4.4 Monitoring certificates

This section describes how to monitor keys and certificates and view detailed information.

7.4.4.1 Displaying key pairs in the keystore

To display key pairs in the keystore, go to **System >> Security >> Keys & Certificates**.

The following information is displayed under **Keystore - Key Pairs**:

Parameter	Description
Key Name	Shows the name of the key pair.
Public Key Format	Shows the format of the public key. Options include: <ul style="list-style-type: none"> • ssh-public-key-format - Format for SSH keys • subject-public-key-info-format - Format for TLS keys
Public Key	Shows the public key.
Algorithm	Shows the hash algorithm with which the fingerprint was created. Possible values include: <ul style="list-style-type: none"> • md5 - Bit length 128 • sha1 - Bit length 160 • sha256 - Bit length 256
Fingerprint	Shows the fingerprint.

7.4.4.2 Displaying certificates in the keystore

To display certificates in the keystore, go to **System >> Security >> Keys & Certificates**.

The following information is displayed under **Keystore - Certificates**:

Parameter	Description
Key Name	Shows the name of the key pair.
Certificate Name	Shows the name of the certificate or the certificate chain.
Certificate	Shows the certificate.
Algorithm	Shows the hash algorithm with which the fingerprint was created. Possible values include: <ul style="list-style-type: none"> • md5 - Bit length 128 • sha1 - Bit length 160 • sha256 - Bit length 256
Fingerprint	Shows the fingerprint.

7.4.4.3 Displaying certificates in the truststore

To display certificates in the truststore, go to **System » Security » Keys & Certificates**.

The following information is displayed under **Truststore - Trusted Certificates**:

Parameter	Description
Certificate Bag	Shows the name of the certificate folder.
Certificate Entry Name	Shows the name of the certificate or the certificate chain.
Certificate	Shows the certificate.
Algorithm	Shows the hash algorithm with which the fingerprint was created. Possible values include: <ul style="list-style-type: none"> • md5 - Bit length 128 • sha1 - Bit length 160 • sha256 - Bit length 256
Fingerprint	Shows the fingerprint.

7.4.4.4 Displays known hosts

To display known hosts in the truststore, navigate to **System » Security » Keys & Certificates**.

The following information is displayed under **Truststore - Known Hosts**:

Parameter	Description
Public Key Bag	Shows the name of the key bag.
Public Key Name	Shows the name of the known host.
Public Key Format	Shows the format of the public key. Options include: <ul style="list-style-type: none"> • ssh-public-key-format - Format for SSH keys • subject-public-key-info-format - Format for TLS keys
Public Key	Shows the public key.

Parameter	Description
Algorithm	Shows the hash algorithm with which the fingerprint was created. Possible values include: <ul style="list-style-type: none"> • md5 - Bit length 128 • sha1 - Bit length 160 • sha256 - Bit length 256
Fingerprint	Shows the fingerprint.

7.5 User authentication

SINEC OS offers various options for authenticating users attempting to access the device.

7.5.1 Understanding User Authentication

Any user attempting to access the device, either through SSH, HTTPs, etc., must provide valid credentials or be denied access. Users can be authenticated against credentials stored locally on the device or by an external service.

7.5.1.1 Authentication mode

Authentication options can be combined to provide a fallback should one method fail (e.g. credentials are not found locally, external service is unreachable, etc.). The full list of authentication modes includes:

- **Local only**
Users are only authenticated locally.
- **RADIUS only**
Users are only authenticated by an external RADIUS server.
- **Local and then RADIUS**
Users are first authenticated locally. If the user is unknown, credentials are forwarded to an external RADIUS server.
- **RADIUS and then local**
Users are first authenticated by an external RADIUS server. If the server is unreachable, users are then authenticated locally.

For more information about setting the authentication mode, refer to "Selecting the user authentication mode (Page 161)".

7.5.1.2 RADIUS Authentication

The Remote Authentication Dial-In User Service (RADIUS) is a UDP-based protocol that provides Authentication, Authorization, and Accounting (AAA) management for users attempting to access the device. The device features a RADIUS client that forwards user credentials to a remote RADIUS server.

When a user attempts to access the device, either through SSH, HTTPS, etc., the RADIUS client forwards their credentials (i.e. username and password) to a remote RADIUS server. The server compares the user's credentials against a database (or other external source) and grants access if the user can be verified.

Note

For more information about the RADIUS protocol, refer to RFC 2865 (<https://tools.ietf.org/html/rfc2865>).

RADIUS servers

The RADIUS client communicates with an external RADIUS server using authentication requests. A basic request will include the following information:

- The user's username and password
- The destination's IPv4 address/domain name and port number of the server where the request will be sent
- A shared-secret key to authenticate the device to the server
- Vendor-specific information

For redundancy, primary and secondary RADIUS servers can be defined. If the primary server does not respond, the authentication request is forwarded to the secondary server. If both servers do not respond to the request, access is denied.

Destination port

The RADIUS client uses a specific destination UDP port. UDP port 1812 is used by default, but this can be changed by the user.

Related events

The following RADIUS-related events are recorded directly in the syslog.

Event	Severity	Syslog Message	Condition
EXT_AUTH_UNREACHABLE	Error	{ protocol };{ user } external authentication failed: Servers are unreachable	The external RADIUS server required to authenticate is unreachable.
EXT_AUTH_FAIL	Error	{ protocol };{ user } external authentication failed: Invalid username or password	The external RADIUS server required to authenticate is reachable, but either the username and/or password is incorrect.
EXT_AUTH_SUCCESS	Info	{ protocol };{ user } external authentication succeeded via { IP address } - logged in	The external RADIUS server required to authenticate is reachable, and the username and password have been accepted.

7.5.2 Configuring user authentication

To configure how users are authenticated, do the following:

1. If RADIUS authentication is required, configure the RADIUS client.
For more information, refer to "Configuring RADIUS Authentication (Page 159)".
2. Set the user authentication mode.
For more information, refer to "Selecting the user authentication mode (Page 161)".

7.5.3 Configuring RADIUS Authentication

To configure RADIUS authentication, do the following:

1. Configure a server profile for a RADIUS server.
The server profile defines the connection to the external server. You can configure a primary server and a secondary server as backup.
For more information, refer to "Configuring a RADIUS server profile (Page 159)".
2. Test the connection to the RADIUS server(s).
For more information, refer to "Testing a RADIUS server connection (Page 161)".

7.5.3.1 Configuring a RADIUS server profile

A RADIUS server profile defines the IP address and other credentials required to access an external RADIUS server.

At least one server profile is required. This is the primary RADIUS server. A secondary profile can also be defined as a fallback should the primary server be unreachable.

To configure a RADIUS server profile, do the following:

1. Navigate to **System » Security » RADIUS Client**.
2. Under **Remote Authentication Dial-In User Service (RADIUS) Client**, click **Add**. A new row is added to the table.

Note

Server Type is defined automatically.

3. Under **Name**, set the name of the server profile.
Condition:
 - Must be between 1 and 253 characters long
4. Under **Shared Secret**, set the authentication key required by the server.
Conditions:
 - Must be between 1 and 128 characters long
 - Allowed ASCII signs are 0x21 to 0x7EThe key is AES encrypted once committed.
5. Under **Shared Secret Confirm**, set the authentication key again.
Conditions:
 - Must be between 1 and 128 characters long
 - Allowed ASCII signs are 0x21 to 0x7EThe key is AES encrypted once committed.
6. Under **Server Address | FQDN**, specify whether the server is reached via IP address or domain name.
Condition:
 - Must be between 1 and 253 characters long
7. [Optional] Under **Primary**, specify if the server is the primary server.
If a server profile is not explicitly designated as primary, the first profile defined will be automatically designated as the primary.
The server cannot be set as primary if the other server profile is already set as primary.
8. [Optional] Under **UDP Port**, set the destination UDP port to use when communicating with the server.
Condition:
 - A number between 1 and 65535Default: 1812
9. [Optional] Under **Attempts**, set the number of times the RADIUS client will attempt to reach the server.
Condition:
 - A number between 1 and 5Default: 3

10. [Optional] Under **Timeout**, set the time in seconds (s) the RADIUS client will wait for a response after each attempt to reach the server.

Conditions:

- Formatted as nYnMnDnHnmns, where n is a user-defined number
- Minimum 1 second (1s)
- Maximum 255 seconds (255s)



Default: 5s (5 seconds)

11. Commit the changes.

7.5.3.2 Testing a RADIUS server connection

After configuring (or modifying) a RADIUS server profile, and before enabling RADIUS authentication, it is important to verify the connection with the targeted RADIUS server. A server's availability may also be tested at any other time as a troubleshooting step.

To test the availability of an external RADIUS server, do the following:

1. Navigate to **System » Security » RADIUS Client**.
2. For the desired RADIUS server profile, click **Test Credentials**.
 - If the RADIUS server responds,  appears temporarily next to the button.
 - If the RADIUS server does not respond,  appears temporarily next to the button.

7.5.4 Selecting the user authentication mode

The user authentication mode determines how users are authenticated: locally, by an external service (e.g. RADIUS), or a combination of both.

To select the authentication mode, do the following:

Note

Only enable RADIUS authentication after verifying a connection with an external RADIUS server.

7.6 Management Access Control List (ACL)

1. Navigate to **System » Security » User Management**.
2. Under **Login Authentication Type & Order**, set the authentication mode under **Type & Order**.
Options include:

Option	Description
Local	Default Users are authenticated locally.
RADIUS	Users are authenticated by an external RADIUS server.
Local and RADIUS	Users are first authenticated locally. If the user is unknown, credentials are forwarded to an external RADIUS server.
RADIUS and fallback local	Users are first authenticated by an external RADIUS server. If the server is unreachable, users are then authenticated locally.

3. Commit the change.

7.5.5 Monitoring User Authentication

This section describes how to monitor aspects of user authentication.

7.5.5.1 Displaying RADIUS statistics

To display statistics related to a RADIUS server, navigate to **System » Security » RADIUS Client**.

Note

All RADIUS statistics are cleared automatically when the device is reset.

The following information is displayed for each RADIUS server defined.

Statistic	Description
Name	The name assigned to the RADIUS server.
Accepted	The number of RADIUS authentication requests accepted by the server.
Rejected	The number of RADIUS authentication requests rejected by the server.
Lost	The number of RADIUS authentication requests lost because the server was unreachable.

7.6 Management Access Control List (ACL)

The management Access Control List (ACL) restricts access to your device to specific remote hosts, referred to as authorized managers. All other remote hosts are denied access.

Each entry (or rule) in the ACL defines the IP address of a specific remote host or a range of IP addresses that can access the device. The entry can also restrict authorized managers to send traffic on specific VLANs or use specific user interfaces.

7.6.1 Understanding management ACLs

Each entry in the management ACL defines a rule that determines which remote hosts are authorized managers and how they can access the device. At minimum, a rule must specify the IP address of a remote host or the IP range for a series of hosts. The rule can further specify a VLAN or VLANs the authorized manager should use when sending traffic. It can also restrict which user interfaces the authorized manager can access:

- Web UI
- NETCONF
- SNMP
- CLI

If a specific VLAN or user interface is not specified in a rule, the associated authorized manager can send traffic on any VLAN and access any user interface.

Access authorization

Only traffic sent by an authorized manager to a user interface is inspected for access authorization. All other traffic sent by the authorized manager is allowed to passthrough normally.

Multiple rules for the same authorized manager

When multiple rules apply to the same authorized manager, they are applied in the order in which they were entered. For instance, a rule applies to remote hosts within the range of 1.1.1.0/24 and restricts access to the CLI. A second rule applies specifically to a remote host within that range, 1.1.1.16/32, and restricts access to the Web UI. As a result, the remote host at 1.1.1.16/32 is granted access to both the CLI and Web UI.

Generic rule

If you want to create a single rule that only restricts access to a VLAN or user interface, consider creating a general rule for the IP address 0.0.0.0/0. This rule will grant access to all remote hosts, but give you options to control how they access the device.

7.6.2 Configuring the management ACL

To configure the management ACL, do the following:

1. Add one or more authorized managers to the ACL.
For more information, refer to "Adding a rule (Page 164)".
2. Enable the management ACL.
For more information, refer to "Enabling the management ACL (Page 166)".

Once the management ACL is enabled, you can perform the following optional steps to modify an existing rule:

- Restrict the authorized manager to sending traffic on a specific VLAN or VLANs
For more information, refer to "Restricting access based on VLAN interface (Page 165)".
- Restrict the authorized manager to accessing a specific user interface or interfaces
For more information, refer to "Restricting access based on user interface (Page 165)".

7.6.2.1 Adding a rule

To add a rule to the management ACL, do the following:

NOTICE
Configuration hazard - risk of connectivity loss
Make sure to first add a rule that matches your own workstation before adding others. Once the management ACL is enabled, only remote hosts designated as authorized managers will be able to access the device.

Note

SINEC OS limits the number of rules that can be defined. For more information, refer to "Configuration limits (Page 27)".

1. Navigate to **System » Security » Management ACL**.
2. Under **Management Access Control List (ACL)**, click **Add**. A new row is added to the table.
3. Under **Source IPv4 Address / Prefix**, enter the IP address and prefix length of a remote host. An authorized manager with an IP address of 0.0.0.0/0 applies to all remote hosts. A rule with this IP address allows you to restrict access to specific user interfaces or limit ingress traffic to specific VLANs.
To create a single authorized manager for a range of remote hosts, enter the shared octets. For example, an authorized manager with an IP address of 1.1.1.0/24 applies to all remote hosts at 1.1.1.0/32 to 1.1.1.255/32.
4. [Optional] In the **Interfaces** column, select either **All** or specific VLAN interfaces the authorized manager can use to access device.
By default, inbound traffic from an authorized manager is permitted on all VLAN interfaces. For more information about changing the interface used by an existing authorized manager, refer to "Restricting access based on VLAN interface (Page 165)".

5. [Optional] In the **Services** column, select one or more user interfaces the authorized manager can use when accessing the device.

By default, authorized managers can use any of the following user interfaces:

- Web UI
- NETCONF
- SNMP
- CLI

Only select the user interfaces you want the authorized manager to access. All others are inaccessible.

For example, the following restricts the authorized managers from accessing the Web UI: `NETCONF, SNMP, CLI`

Allowed user interfaces can also be redefined after the authorized manager is added.

For more information about redefining allowed user interfaces for an existing authorized manager, refer to "Restricting access based on user interface (Page 165)".

6. Commit the change.

7.6.2.2 Restricting access based on VLAN interface

By default, an authorized manager can send traffic to the device on all available VLAN (Layer 3) interfaces. However, it can be restricted to a singular VLAN interface, if needed.

You have the option to restrict an authorized manager to a specific VLAN interface when you add the rule initially. You can also add or change the interface later on, if needed.

To select or change the VLAN interface an authorized manager can use when accessing the device, do the following:

1. Navigate to **System** » **Security** » **Management ACL**.
2. Under **Management Access Control List (ACL)**, select either **All** or specific VLAN interfaces from the **Interfaces** list for the selected authorized manager.
3. Commit the change.

7.6.2.3 Restricting access based on user interface

By default, an authorized manager can use any of the following user interfaces when accessing the device:

- Web UI
- NETCONF
- SNMP
- CLI

7.6 Management Access Control List (ACL)

To restrict or allow an existing authorized manager to use a specific user interface or interfaces, do the following:

1. Navigate to **System » Security » Management ACL**.
2. Under **Management Access Control List (ACL)**, select one or more user interfaces from the **Services** list for the selected authorized manager.
Note that clearing all interfaces is equivalent to selecting all interfaces.
3. Commit the change.

7.6.2.4 Enabling the management ACL

To enable the management ACL, do the following:

NOTICE
Configuration hazard - risk of connectivity loss
Make sure your own workstation is designated as an authorized manager. You will be unable to access the device otherwise once the management ACL is enabled.
If this occurs, the device must be reset to factory defaults and then reconfigured, or reconfigured via a direct serial connection.

Note

At least one authorized manager must be defined for the management ACL to be enabled.

1. Navigate to **System » Security » Management ACL**.
2. Under **Management Access Control List (ACL)**, change **Management ACL** to **Enabled**.
3. Commit the change.

7.6.3 Configuration examples

The following configuration examples demonstrate different ways to configure authorized managers in the management ACL.

7.6.3.1 Creating an authorized manager for a range of remote hosts

A single authorized manager can be configured to apply to a range of remote hosts. Access to the device is granted to all hosts within the IP range and all hosts are governed by the defined rules. However, you can grant additional access to a specific remote host or a subset of hosts within that range.

Consider the following authorized managers defined for the management ACL:

Source IPv4 Address / Prefix	Interfaces	Services
1.1.1.0/24	All	NETCONF,SNMP,CLI
1.1.1.10/32	All	Web UI

Source IPv4 Address / Prefix	Interfaces	Services
2.2.2.20/32	All	CLI
2.2.2.0/24	All	NETCONF,SNMP

Description

The first authorized manager grants all hosts within the IP range of 1.1.1.0/24 access via NETCONF, SNMP, and the CLI.

The second authorized manager grants a specific host (1.1.1.10/32) within that IP range additional access to the Web UI.

The third authorized manager grants another host (2.2.2.20/32) access to the CLI.

The fourth authorized manager grants all hosts within the IP range of 2.2.2.0/24 access via NETCONF and SNMP. This includes the host at 2.2.2.20/32, which already has access to the CLI.

Interface management

This chapter describes how to configure and manage interfaces on the device.

8.1 Interfaces

Each physical port and VLAN is represented by an interface. Each interface features various options for controlling the ingress and egress of traffic.

This section describes the interface types and their configurable settings.

NOTICE
Security hazard - risk of unauthorized access and/or exploitation
All bridge ports are enabled by default. Additionally, when the device is reset to its default settings (factory reset), any bridge port that had been disabled previously is re-enabled.
Only bridge ports that are in use should be enabled. An unused bridge port not properly configured could potentially be used to gain access to the network behind the device.

8.1.1 Understanding interfaces

SINEC OS supports the following interface types:

Type	Description
Bridge ports	Fixed or Small-Factor Pluggable (SFP) Ethernet ports.
VLAN interfaces	Logical interfaces for VLANs. They can be assigned IP addresses and allow a VLAN to participate in Layer 3 activities.
Function Extender Interfaces (FEIs)	Ports that represent physical connectors on an external Local Processing Enging (LPE).

Each port has configurable options for port speed, duplexing, auto-negotiation, and more.

8.1.1.1 Interface naming conventions

Interfaces are named based on the following conventions:

Naming convention	Examples	Description
ethernet{ Slot }{ Port }	ethernet0/1, ethernet3/2	Bridge ports are named based on the slot where the physical port resides and the port number. If the device does not support module slots, as is the case with most small form-factor devices, the slot number is zero (0).
vlan{ ID }	vlan1, vlan2	Interfaces for VLANs are named based on the VLAN ID.
extender{ Slot }{ Port }	extender0/1, extender0/2	Function Extender Interface (FEI) ports are named extender , followed by the slot number and associated port number. If the device does not support module slots, as is the case with most small form-factor devices, the slot number is zero (0).

8.1.1.2 Auto-negotiation

SINEC OS supports auto-negotiation for 1000 Mbps (or higher) bridge ports, as defined by IEEE 802.3.

Auto-negotiation allows two bridge ports upon link detection to share their capabilities and negotiate common transmission settings (i.e. speed, flow control, and duplex mode) to the highest common denominator. This allows for zero touch provisioning (i.e. ports automatically configure themselves). It also provides flexible support for link partners that do not have the same hardware capabilities as your device.

8.1.1.3 Duplex communication

Duplex communication allows link partners to communicate with one another in both directions. SINEC OS supports the following communication channel types:

- **Full-duplex**

Full-duplex allows both link partners to send and receive signals in both directions at the same time. Voice Over Internet Protocol (VOIP) communications are an excellent application of this communication channel type. Speakers on both ends of the call can speak and be heard by one another because their ends of the channel can send and receive signals at the same time.



Figure 8-1 Full-duplex communication

- **Half-duplex**

Half-duplex allows both link partners to send and receive signals in both directions, but only one at a time. The walkie-talkie is a good example of a half-duplex communication channel. When you press the button to speak, you cannot hear the person on the other end, but they can hear you.



Figure 8-2 Half-duplex communication

NOTICE**Configuration hazard - risk of severe frame loss**

Switches at both ends of the link must be configured to be in the same duplex mode. If Switch A is in full-duplex mode and Switch B is in half-duplex mode, significant frame loss will occur during periods of heavy network traffic.

8.1.1.4 Controller protection through Link Fault Indication (LFI)

Modern industrial controllers often feature backup interfaces used in the event of a link failure. When these interfaces are supported by media that employ separate transmit and receive paths, the interface can be vulnerable to failures that occur in only one of the two paths.

Scenario

Consider for instance two switches, S1 and S2, connected to a controller. S1 is connected to the main port on the controller. S2 is connected to the backup port, which is administratively disabled by the controller while the link with S1 is active. S2 must forward frames to the controller through S1.

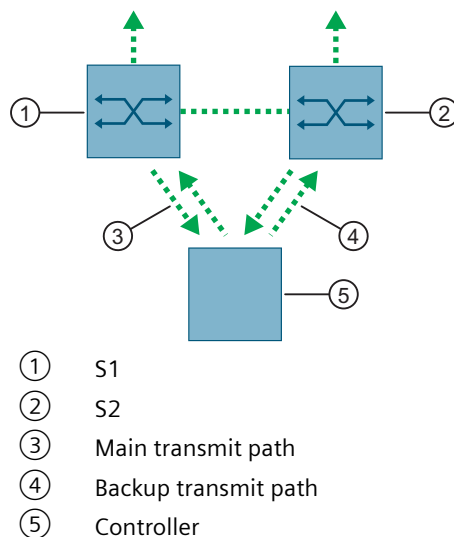


Figure 8-3 Scenario

If the transmit path from the controller to S1 fails, S1 still generates a link signal to the controller through the receive path. The controller still detects the link with S1 and does not fail-over to the backup port.

This situation illustrates the need for a notification method that tells a link partner when the link integrity signal has stopped. Such a method natively exists in some link media, but not all.

Native notification mechanisms

Media	Native link partner notification mechanism
100Base-TX 1000Base-T 1000Base-X	Includes a built-in auto-negotiation feature (i.e. a special flag called Remote Fault Indication is set in the transmitted auto-negotiation signal).
100Base-FX	<p>May include Far-End-Fault-Indication (FEFI), as defined by IEEE 802.3. This feature includes:</p> <ul style="list-style-type: none"> • Transmitting FEFI Transmits a modified link integrity signal in case a link failure is detected (i.e. no link signal is received from the link partner) • Detecting FEFI Indicates link loss in case an FEFI signal is received from the link partner <p>FEFI is an optional feature according to the IEEE 802.3 standard. Not all link partners will support this method.</p>
10Base-FL	Not supported.

Link Fault Indication (LFI)

Consider for instance two switches, S1 and S2, connected to a controller. S1 is connected to the main port on the controller. S2 is connected to the backup port, which is administratively disabled by the controller while the link with S1 is active. S2 must forward frames to the controller through S1.

Note

LFI can only be enabled for fiber ports.

In the scenario described previously, S1 will stop generating a link integrity signal if it fails to receive a link signal from the controller. The controller will detect the link failure and fail-over to the backup interface.

SINEC OS can also be configured to flush the MAC address for the controller port. Frames destined for the controller will be flooded to S2 where they will be forwarded to the controller (after the controller transmits its first frame).

NOTICE**Configuration hazard - risk of communication failure**

When LFI is supported by both link partners, LFI must only be enabled by one link partner. If LFI is enabled by both, a link cannot be established, as both ends will be waiting for the other to transmit a link integrity signal.

8.1.1.5 Flow control

Flow control is an optional feature that enables a Gigabit capable bridge port to listen for a PAUSE frame sent by its link partner. This frame is sent when the link partner has become flooded with more frames than it is able to process efficiently. It needs time to clear its queues before it can receive more frames.

The PAUSE frame includes a timer. If the sender does not receive another PAUSE frame before the timer expires, it can resume forwarding traffic.

While SINEC OS supports the PAUSE frame, other devices may not. As such, flow control must be negotiated.

8.1.1.6 Function Extender Interface (FEI) ports

Function Extender Interface (FEI) ports represent the physical connectors between the device and an external Local Processing Engine (LPE), such as a device in the SCALANCE LPE-9000 family. An LPE can be used for various applications, such as traffic mirroring or as an IoT device.

FEI ports are visible at all times in the UI for SINEC OS, even if an LPE is not attached. They are represented in the UI as extender0/N (e.g. extender0/1, extender0/2, extender0/3), and always appear at the end of the interface list.

Note

Restrictions

- Duplex mode, speed, auto-negotiation, and downshift settings are read-only
 - If an LPE is attached, you can configure LLDP and DCP for FEI ports
 - Cable tests cannot be performed on FEI ports
-

FEI port configuration

The following are the fixed settings for FEI ports:

FEI port	Auto-negotiation	Speed	Duplex mode	Downshift
extender0/1	Disabled	1 Gbps	Full Duplex	Disabled
extender0/2	Disabled	1 Gbps	Full Duplex	Enabled
extender0/3	Disabled	10 Gbps	Full Duplex	Enabled

8.1.1.7 SFP Transceiver Ports

Devices with SFP transceiver ports can be flexibly fitted with SFP (Small Form-factor Pluggable) transceivers.

SFPs are standardized, exchangeable modules for network connections and offer a large number of different properties (e.g. transmission speed, cable length, transmission medium).

SINEC OS supports a large number of SFP transceivers with which the range and functionality of a network can be extended.

Note

Use only approved SFP transceivers.

If you use SFP transceivers that are not approved by Siemens, there is no guarantee the device will function according to the specification.

If you use unapproved SFP transceivers, this can lead to the following problems:

- Damage to the device
- Loss of the approvals
- Violation of the EMC regulations

You can find a list of approved SFP transceivers in the manuals for the respective devices.

Hot swappable

All SFP transceivers can be replaced during operation. You can pull and plug SFP transceivers without interrupting device operation. When an SFP transceiver is pulled, only a previously established link on the SFP transceiver interface is affected.

Automatic detection

SINEC OS actively monitors every SFP transceiver port to determine whether a transceiver was pulled or plugged. Each event triggers an alarm, which is recorded in the Syslog.

Smart SFP

Smart SFP is enabled for every SFP transceiver interface by default.

With Smart SFP, SINEC OS can automatically configure the settings of an interface for speed, duplex mode and auto negotiation that are suitable for a plugged SFP transceiver. These settings are based on the properties of the SFP transceiver.

The settings of the interface are retained when an SFP transceiver is pulled or the device is restarted. This means that an SFP transceiver can be quickly and easily replaced by another SFP transceiver of the identical type, i.e. with the same article number. If the device detects a different SFP transceiver type with different properties, the configuration is automatically overwritten by the values of the current SFP transceiver.

If the properties of an SFP transceiver cannot be evaluated, you can disable the automatic configuration. In this way, you prevent SINEC OS from configuring potentially incorrect settings for an interface.

Note

SFP transceivers approved by Siemens support Smart SFP. SFP transceivers that do not support Smart SFP can be disabled on plugging and designated as **Unidentified**. In this case, disable Smart SFP and configure the interface manually.

For example, when Smart SFP is enabled and a 1000Base-X SFP transceiver that supports 100Base-X and 1000Base-X is inserted, the interface is automatically configured to 1000Base-X.

Related Events

The following events are triggered by SFP transceivers and recorded directly in the Syslog.

Event	Severity	Syslog message
Module-presence	Warning	Module { SFP transceiver name/type } [Inserted Removed]
Module-state	Warning	Unknown SFP module on interface { SFP transceiver interface } (vendor: { Vendor })
		Rejected SFP module on interface { SFP transceiver interface }
		Unsupported SFP module on interface { SFP transceiver interface }

8.1.2 Configuring bridge ports

By default, all bridge ports are administratively enabled and have auto-negotiation configured. Physically connecting the associated ports to a link partner is typically all that is required. However, some additional settings may need to be configured.

Note

The following bridge port features are only configurable via the CLI:

- Enabling Link Fault Indication (LFI)
- Disabling a bridge port automatically on a link down event

For information about these features, refer to the **SINEC OS CLI Configuration Manual**.

To configure a bridge port, do the following:

1. [Optional] Add or change the description for the bridge port.
For more information, refer to "Adding a description for a bridge port (Page 176)".
2. [Optional] Enable auto-negotiation.
This feature allows link partners to negotiate and automatically configure their settings based on their capabilities. By default, auto-negotiation is enabled for all bridge ports. For more information, refer to "Enabling auto-negotiation (Page 176)".
3. [Optional] Select the speed at which the bridge port sends frames.
The speed is typically auto-negotiated with the link partner, but may need to be set explicitly for non-Gigabit bridge ports. For more information, refer to "Selecting the bridge port speed (Page 177)".
4. [Optional] Select the duplex mode.
This feature controls how link partners communicate with one another. The duplex mode is typically auto-negotiated with the link partner, but may need to be set explicitly, especially for non-Gigabit bridge ports. For more information, refer to "Selecting the duplex mode (Page 178)".
5. [Optional] Enable downshift.
This feature allows two 1000Base-T bridge ports to negotiate a lower data rate to support a twisted-pair copper cable, which is intended only for 100Base-TX connections. For more information, refer to "Enabling downshift for gigabit interfaces (Page 179)".

8.1 Interfaces

6. [Optional] Enable alarms to be triggered on a link down/up event.
For more information, refer to "Enabling link up/down traps (Page 179)".
7. [Optional] Assign a static IPv4 address to the bridge port.
For more information, refer to "Configuring a static IPv4 address (Page 193)".
8. [Optional] Activate Smart SFP (for SFP ports only).
For more information, refer to "Enabling Smart SFP (for SFP ports only) (Page 179)".
9. Make sure the bridge port is enabled.
For more information, refer to "Enabling a bridge port (Page 180)".

8.1.2.1 Adding a description for a bridge port

Each bridge port can be given a description to better identify the interface. This may include, for example, the name of the manufacturer, product name, hardware/firmware version, and/or the unique identifier of the interface.

To add a description for a bridge port, do the following:

1. Navigate to **Interfaces** » **Ethernet Interfaces** » **Interfaces**.
2. Under **Ethernet Interfaces**, enter a description for the selected bridge port under **Description**.
Condition:
 - Must be between 0 and 64 characters long
3. Commit the change.

8.1.2.2 Enabling auto-negotiation

To enable auto-negotiation for a bridge port, do the following:

NOTICE
Restrictions <ul style="list-style-type: none">• Auto-negotiation is only available for 1 Gigabit Ethernet (or higher) bridge ports. For information on how to determine if a specific bridge port supports auto-negotiation, refer to the SINEC OS CLI Configuration Manual.• Auto-negotiation must be enabled for 1 Gigabit copper Ethernet ports when the speed is set to 1000 Mbps.• Auto-negotiation must be enabled for all 10 Gigabit copper Ethernet ports.• Auto-negotiation must be disabled for all 10 Gigabit fiber optic Ethernet ports.

Note

Auto-negotiation is disabled by default for all 100BASE-FX, 1000BASE-X, and 10GBASE-X ports.

Auto-negotiation is enabled by default for all other ports that support the feature.

Auto-negotiation can only be disabled for a bridge port if the speed and duplex mode are assigned fixed values (i.e. not `auto`).

1. Navigate to **Interfaces** » **Ethernet Interfaces** » **Interfaces**.
2. Under **Ethernet Interfaces**, change **Auto-Negotiation** to **Enabled** for the selected bridge port.
3. Commit the change.

8.1.2.3 Selecting the bridge port speed

The speed at which a bridge port transmits frames can be set to a fixed value. The speed can also be auto-negotiated between the port and its link partner, if auto-negotiation is enabled. For example, a Gigabit Ethernet port can be set to send frames at 100 Mb/s, allowing it to be connected to a Fast Ethernet port.

To select the speed at which a bridge port transmits frames, do the following:

NOTICE	
Restrictions	
<ul style="list-style-type: none"> • Auto-negotiation must be enabled for 1 Gigabit copper Ethernet ports when the speed is set to 1 Gb/s • The speed must be set to 1 Gb/s for all 1 Gigabit fiber optic Ethernet ports • The speed must be set to 10 Gb/s for all 10 Gigabit fiber optic Ethernet ports 	

1. Navigate to **Interfaces** » **Ethernet Interfaces** » **Interfaces**.
2. Under **Ethernet Interfaces**, select the speed for the selected bridge port under **Speed**. Options include:

Option	Description
Auto	Frames are sent at the speed determined through auto-negotiation
10 Mb/s	Frames are sent at 10 Mbps
100 Mb/s	Frames are sent at 100 Mbps
1 Gb/s	Frames are sent at 1 Gbps
2.5 Gb/s	Frames are sent at 2.5 Gbps
5 Gb/s	Frames are sent at 5 Gbps
10 Gb/s	Frames are sent at 10 Gbps

If auto-negotiation is enabled, the interface advertises the selected option as its speed capability to its link partner.

If auto-negotiation is disabled, the interface operates at the speed in which it is capable.

Default: **Auto**

3. Commit the change.

8.1.2.4 Selecting the duplex mode

Duplex communications allow a bridge port and its link partner to communicate with one another in both directions. Depending on the mode chosen, frames can be sent in both directions either simultaneously or in one direction at a time. The duplex mode can also be negotiated between both link partners to determine the best option based on the capabilities of both interfaces.

To select the duplex mode for a bridge port, do the following:

NOTICE
Configuration hazard - risk of severe frame loss
Switches at both ends of the link must be configured to be in the same duplex mode. If one switch is in full-duplex mode and the other is in half-duplex mode, significant frame loss will occur during periods of heaving network traffic.

NOTICE
Restriction
<ul style="list-style-type: none"> Duplex must be set to Full-duplex for all 1 Gigabit (or higher) copper and fiber Ethernet ports

- Navigate to **Interfaces » Ethernet Interfaces » Interfaces**.
- Under **Ethernet Interfaces**, elect the duplex mode for the selected interface under **Duplex Mode**.
Options include:

Option	Description
Auto	Default The duplex mode is determined through auto-negotiation.
Half-duplex	Communication between the interface and its link partner occurs in both directions, but only one at a time. This option cannot be selected if the speed is set to 1 Gb/s.
Full-duplex	Communication between the interface and its link partner can occur simultaneously in both directions (bi-directional).

- Commit the change.

8.1.2.5 Enabling downshift for gigabit interfaces

Downshift allows you to use a twisted-pair copper cable between two 1000Base-T Ethernet ports. When a twisted-pair copper cable is in use and downshift is enabled, the interfaces for each end of the link will automatically reduce the data rate to 10 or 100 Mbps.

Note

Downshift is enabled by default for all Gigabit-capable bridge ports.

If downshift is disabled, both ports will attempt to establish a connection at 1000 Mbps, which the cable does not support.

To enable downshift for a bridge port, do the following:

1. Navigate to **Interfaces** » **Ethernet Interfaces** » **Interfaces**.
2. Under **Ethernet Interfaces**, change **Downshift** to **Enabled** for the selected bridge port.
3. Commit the change.

8.1.2.6 Enabling link up/down traps

SNMP traps for link up and link down events can be enabled/disabled for specific bridge ports. When disabled, the alarms associated with these events are never triggered for those interfaces.

Note

By default, link up and link down traps are disabled on all bridge ports.

To enable link up and link down SNMP traps for a bridge port, do the following:

1. Navigate to **Interfaces** » **Ethernet Interfaces** » **Interfaces**.
2. Under **Ethernet Interfaces**, change **Link Up/Down Traps** to **Enabled** for the selected bridge port.
3. Commit the change.

8.1.2.7 Enabling Smart SFP (for SFP ports only)

As soon as an SFP transceiver is plugged, the corresponding SFP transceiver port is enabled administratively by default and has Smart SFP enabled. SINEC OS then configures the settings of the interface (speed, duplex mode and autonegotiation) in a suitable way for the plugged SFP transceiver.

A "-" is displayed for the function for all non-SFP ports.

To enable Smart SFP, do the following:

1. Navigate to **Interfaces** » **Ethernet Interfaces** » **Interfaces**.
2. Under **Ethernet Interfaces**, change the **SFP Auto Config** parameter for the selected SFP transceiver port to **Enabled**.
3. Commit the change.

8.1.2.8 Enabling a bridge port

To enable a bridge port, do the following:

NOTICE**Security hazard - risk of unauthorized access and/or exploitation**

All bridge ports are enabled by default. Additionally, when the device is reset to its default settings (factory reset), any bridge port that had been disabled previously is re-enabled.

Only bridge ports that are in use should be enabled. An unused interface not properly configured could potentially be used to gain access to the network behind the device.

1. Navigate to **Interfaces » Ethernet Interfaces » Interfaces**.
2. Under **Ethernet Interfaces**, change **Interface State** to **Enabled** for the selected bridge port.
3. Commit the change.

8.1.3 Configuring VLAN interfaces

At least one VLAN interface must be defined to access the device remotely via an IP protocol (e.g. HTTP, SNMP, NETCONF, SSH, etc.). Otherwise, the device can only be accessed through a direct serial connection.

To configure a VLAN interface, do the following:

1. Define a VLAN interface.
For more information, refer to "Adding a VLAN interface (Page 180)".
2. [Optional] Add a description for the interface.
For more information, refer to "Adding a description for a VLAN interface (Page 181)".
3. [Optional] Configure the MTU size.
For more information, refer to "Configuring the MTU size (Page 181)".
4. [Optional] Enable alarms to be triggered on a link down/up event.
For more information, refer to "Enabling link up/down traps (Page 181)".
5. [Optional] Assign a static IPv4 address to the interface or enable DHCP.
For more information, refer to "IP Address Assignment (Page 193)".
6. Enable the VLAN interface.
For more information, refer to "Enabling a VLAN interface (Page 182)".

8.1.3.1 Adding a VLAN interface

To add a VLAN interface, do the following:

1. Make sure a static VLAN exists to which the new interface can be associated with.
For more information about adding static VLANs, refer to "Adding or modifying a static VLAN (Page 296)".
2. Navigate to **Interfaces » IP Interfaces**.

3. Under **IP Interfaces**, click **Add**. A new row is added to the table.
4. Under **Interface**, select an existing VLAN.
5. Commit the change.

8.1.3.2 Adding a description for a VLAN interface

A description can be added to a VLAN interface to help identify it amongst others, such as "Interface to production network" or "Interface to management network".

To add a description for a VLAN interface, do the following:

1. Navigate to **Interfaces** » **IP Interfaces**.
2. Under **IP Interfaces**, enter a description for the selected interface under **Description**.
Condition:
 - Must be between 0 and 64 characters long
3. Commit the change.

8.1.3.3 Configuring the MTU size

The Maximum Transmission Unit (MTU) is the maximum size of a single frame the VLAN interface can forward. Frames that exceed this limit are broken into smaller fragments, which can slow the transmission process. It is important to select an MTU size that helps optimize network performance.

To set the MTU size for a VLAN interface, do the following:

1. Navigate to **Interfaces** » **IP Interfaces**.
2. Under **IP Interfaces**, set the MTU size for the selected interface under **MTU Size**.
Condition:
 - A number between 68 and 1500Default: 1500
3. Commit the change.

8.1.3.4 Enabling link up/down traps

SNMP traps for link up and link down events can be enabled/disabled for specific VLAN interfaces. When disabled, the alarms associated with these events are never triggered for those interfaces.

By default, link up and link down traps are disabled on all VLAN interfaces.

To enable link up and link down SNMP traps for a VLAN interface, do the following:

1. Navigate to **Interfaces** » **IP Interfaces**.
2. Under **IP Interfaces**, change **Link Up/Down Trap** to **Enable** for the selected interface.
3. Commit the change.

8.1.3.5 Enabling a VLAN interface

To enable a VLAN interface, do the following:

Note

All VLAN interfaces are enabled by default.

1. Navigate to **Interfaces** » **IP Interfaces**.
2. Under **IP Interfaces**, change **Interface State** to **Enable** for the selected interface.
3. Commit the change.

8.1.4 Resetting a bridge port

Bridge ports may need to be reset in the following scenarios:

- The port was disabled automatically by SINEC OS due to an error/malfunction. Resetting the port remotely in this case may resolve the problem.
- The port has been disabled temporarily by a feature, such as BPDU Guard, until it is reset.
- Diagnostics were run on the cable and communication needs to be restored with the neighboring port.

To reset a bridge port, do the following:

1. Navigate to **Interfaces** » **Ethernet Interfaces** » **Interfaces**.
2. Under **Ethernet interfaces**, click **Reset** in the **Interface Reset** column for the selected interface.

8.1.5 Monitoring interfaces

This section describes the various ways to look up information about the available interfaces.

8.1.5.1 Displaying bridge ports

To display the available bridge port configurations, navigate to **Interfaces** » **Ethernet Interfaces** » **Interfaces**.

The following information is displayed for each bridge port:

Parameter	Description
Interface	The name of the bridge port in the form of "{ Type } { Slot } / { Port }". For example: <ul style="list-style-type: none"> • ethernet0/1 • extender0/1
Description	An optional, user-defined description of the interface.

Parameter	Description
Link Up/Down Trap	When set to enabled , SNMP traps are triggered when link up or down events occur.
Interface State	The administrative (or configured) state of the interface. When set to enabled , the interface can receive and forward data.
Operational Status	The operational (or running) state of the interface. Possible values include: <ul style="list-style-type: none"> • dormant - The interface is waiting for external actions • down - The interface is down • lower-layer-down - The interface is down due to the state of the lower layer interface • not-present - A component is missing (e.g. hardware) • testing - The interface is currently being tested • unknown - The current state cannot be determined • up - The interface is up
Auto-Negotiation	The state of auto-negotiation for the bridge port.
Speed	The speed setting for bridge port.
Negotiated Speed	The maximum speed negotiated between the bridge port and its link partner.
Duplex Mode	The duplex mode set for the bridge port.
Negotiation Duplex Mode	The duplex mode negotiated between the bridge port and its link partner.
Downshift	The downshift state set for the bridge port.

8.1.5.2 Displaying VLAN interfaces

To display the available VLAN interfaces, navigate to **Interfaces » IP Interfaces**.

The following information is displayed for each interface:

Parameter	Description
Name	The name of the interface in the form of "vlan{ VLAN ID }". The value is read-only.
Description	An optional, user-defined description of the interface. The string can be up to 64 characters.
Link Up/Down Trap	When set to enable , SNMP traps are triggered when link up or down events occur.
MTU	The Maximum Transmission Unit (MTU) setting for the interface.
Interface State	The administrative (or configured) state of the interface. When set to enable , the interface can receive and forward data. The value is read-only.

8.1.5.3 Displaying receive/transmit statistics for all interfaces

To display statistics for all interfaces (e.g. bridge ports, VLAN interfaces, etc.), navigate to **Interfaces » Interface Statistics**.

The following tables are displayed:

- **Interface Statistics (In)**
- **Interface Statistics (Out)**

The following information is displayed for each interface:

Statistic	Description
Interface	The name of the interface.
In Octets	The total number of octets in all valid frames received by the interface.
In Unicast (pkts)	The number of unicast frames successfully received by the interface.
In Broadcast (pkts)	The number of broadcast frames successfully received by the interface.
In Multicast (pkts)	The number of multicast frames successfully received by the interface.
In Discards (pkts)	The number of frames received by the interface that were dropped due to congestion at the input queue.
In Errors (pkts)	The number of invalid frames received by the interface.
Out Octets	The total number of octets in all valid frames forwarded by the interface.
Out Octets (pkts)	The number of unicast frames successfully forward by the interface.
Out Broadcast (pkts)	The number of broadcast frames successfully forwarded by the interface.
Out Multicast (pkts)	The number of multicast frames successfully forwarded by the interface
Out Discards (pkts)	The number of frames the interface due to congestion at the output queue.
Out Errors (pkts)	The number of invalid frames forwarded by the interface.

8.1.5.4 Displaying receive/transmit statistics for only bridge ports

To display statistics collected for only bridge ports, navigate to **Interfaces » Ethernet Interfaces » Statistics**.

The following tables are displayed:

- **Interface Statistics (In)**
- **Interface Statistics (Out)**
- **Packet Size**

The following information is displayed for each interface:

Statistic	Description
In Broadcast Frames	The number of broadcast frames that have been successfully received by the bridge port.
In Error FCS Frames	The number of frames received by the bridge port that are of valid length, but do not pass the Frame Check Sequence (FCS) check.
In Error Oversize Frames	The number of frames received by the bridge port that are larger than the maximum permitted frame size (specified by max-frame-length).
In Error Undersize Frames	The number of frames received by the bridge port that are less than 64 bytes in length.
In Errors	The number of invalid frames received by the bridge port.
In Frames	The total number of frames successfully received by the bridge port.
In Multicast Frames	The number of multicast frames successfully received by the bridge port.
In Total Frames	The total number of frames (including bad frames) received by the bridge port.
In Total Octets	The total number of data octets (including those in bad frames) received by the bridge port.
In Unicast Frames	The number of unicast frames successfully received by the bridge port.
Out Broadcast Frames	The number of broadcast frames successfully sent by the bridge port.
Out Frames	The total number of frames successfully sent by the bridge port.
Out Multicast Frames	The number of multicast frames successfully sent by the bridge port.
Out Octets	The number of data octets successfully sent by the bridge port.
Out Unicast Frames	The number of unicast frames successfully sent by the bridge port.
64 Octets	The number of 64 octet packets received and transmitted, including dropped packets
65 to 127 Octets	The number packets between 65 and 127 octets received and transmitted, including dropped packets
128 to 255 Octets	The number packets between 128 and 255 octets received and transmitted, including dropped packets
256 to 511 Octets	The number packets between 256 and 511 octets received and transmitted, including dropped packets
512 to 1023 Octets	The number packets between 512 and 1023 octets received and transmitted, including dropped packets
1024 to 1536 Octets	The number packets between 1024 and 1536 octets received and transmitted, including dropped packets

8.1.5.5 Monitoring SFP Transceivers

To show the status of SFP transceivers, navigate to **Interfaces** » **Ethernet Interfaces** » **SFP Diagnostics**.

The following information is displayed:

Parameter	Description
Model	Shows the name/type of the SFP transceiver.
Description	Displays a description of the SFP transceiver.
Vendor (Name)	Shows the manufacturer of the SFP transceiver.
Article Number	Shows the article number of the SFP transceiver.
Part Revision	Shows the hardware version of the SFP transceiver.
Speed	Shows the transmission speed with which frames are transmitted at the SFP transceiver port. Possible values include: <ul style="list-style-type: none"> • Auto - Frames are sent with the speed determined by autonegotiation. • 10 Mb/s - Frames are sent with 10 Mbps. • 100 Mb/s - Frames are sent with 100 Mbps. • 1 Gb/s - Frames are sent with 1 Gbps. • 2,5 Gb/s - Frames are sent with 2.5 Gbps. • 5 Gb/s - Frames are sent with 5 Gbps. • 10 Gb/s - Frames are sent with 10 Gbps.
Serial Number	Shows the serial number of the SFP transceiver.
9um Max Link Length	Shows the maximum cable length with a fiber core diameter of 9 µm in meters (m).
50um Max Link Length	Shows the maximum cable length with a fiber core diameter of 50 µm in meters (m).
62um Max Link Length	Shows the maximum cable length with a fiber core diameter of 62.5 µm in meters (m).
Temperatur (°C)	Shows the current temperature of the SFP transceiver in degrees Celsius (°C).
Rx-Power (dBm)	Shows the current value of the receive power in decibel-milliwatts (dBm).
Min Rx-Power (dBm)	Shows the smallest possible value of the receive power of the SFP transceiver in decibel-milliwatts (dBm).
Max Rx-Power (dBm)	Shows the largest possible value of the receive power of the SFP transceiver in decibel-milliwatts (dBm).
Tx-Power (dBm)	Shows the current value of the sent power in decibel-milliwatts (dBm).
Min Tx-Power (dBm)	Shows the smallest possible value of the send power of the SFP transceiver in decibel-milliwatts (dBm).
Max Tx-Power (dBm)	Shows the largest possible value of the send power of the SFP transceiver in decibel-milliwatts (dBm).

8.2 MAC address table

SINEC OS maintains a MAC address table to efficiently map ingress frames to their intended destination.

8.2.1 Understanding the MAC address table

The Media Access Control (MAC) address table is an internal list of MAC addresses for devices on the network. It allows the device to efficiently direct ingress frames destined for a specific MAC address to the appropriate interface.

The table is comprised of statically-defined MAC addresses (defined by users) and dynamically-learned addresses (defined by the device itself).

8.2.1.1 Dynamic MAC entries

Dynamic MAC entries are those learned automatically by the device as it receives and forwards frames from host devices on the network.

Aging out

Dynamic MAC entries are subject to aging and will be removed automatically after a period of time if a frame is not received from the associated host before the time expires. This allows the table to remain current.

Learning new entries

Following a restart, the MAC address table is purged of all dynamic entries and the device waits to receive frames. As frames are received and forwarded, the table is populated with the MAC addresses of each link partner.

To illustrate, consider the following topology where two hosts (A and B) forward data to one another via the switch (SW).

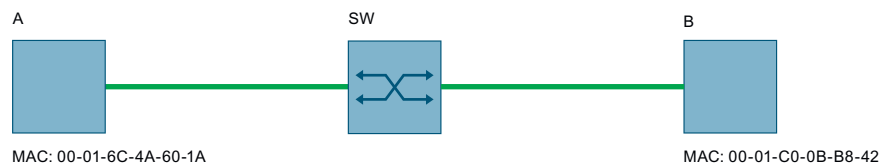


Figure 8-4 Learning MAC addresses from two hosts

The switch has recently been restarted, so its MAC address table is empty.

VIDS	MAC ADDRESS	TRAFFIC CLASS	ENTRY TYPE	FORWARDING PORT
%No entries found%				

When host A sends a frame to host B, the switch learns the MAC address of host A and adds it to the list.

VIDS	ADDRESS	TRAFFIC CLASS	ENTRY TYPE	FORWARDING PORT
1	00-01-6C-4A-60-1A	unprioritized	dynamic	ethernet0/1

When host B replies with its own frame, the switch learns the MAC address of that host as well. Soon, all devices communicating on the network are added to the switch's MAC address table.

VIDS	ADDRESS	TRAFFIC CLASS	ENTRY TYPE	PORT REF
1	00-01-6C-4A-60-1A	unprioritized	dynamic	ethernet0/1
1	00-01-C0-0B-B8-42	unprioritized	dynamic	ethernet0/1

8.2.1.2 Static MAC entries

Static MAC filtering entries in the MAC address table represent MAC addresses defined by users. These entries establish a fixed association between a MAC address and VLAN. Static entries do not age out and can only be removed individually by users.

8.2.2 Configuring the MAC address table

To configure how and when MAC addresses are removed from the MAC address table, do the following:

1. [Optional] Set the aging time.
The aging time is the maximum time each entry is held in the MAC address table before it is removed automatically. If a frame associated with the MAC address is received before the timer expires, the timer is reset.
For more information, refer to "Configuring the MAC address aging time (Page 188)".
2. [Optional] Enable the device to automatically remove (age out) entries when a link failure is detected.
For more information, refer to "Enabling MAC address aging on link failure (Page 189)".

8.2.2.1 Configuring the MAC address aging time

Dynamically learned MAC addresses are aged out after a configurable period of time. They are removed automatically from the MAC address table once the timer expires, unless a frame associated with the MAC address is received within the time limit.

To configure the aging time for MAC address entries, do the following:

1. Navigate to **Layer 2 » MAC Address Table » MAC Address Table**.
2. Under **Media Access Control (MAC) Address Table**, change **Aging Time** to the time that dynamically learned MAC addresses are kept in the MAC address table.
Conditions:
 - Formatted as nYnMnDnhnmns, where n is a user-defined number
 - Minimum of 15 seconds (15s)
 - Maximum of 13 minutes (13m) or 800 seconds (800s)
 Default: 5m (5 minutes)
3. Commit the change.

8.2.2.2 Enabling MAC address aging on link failure

Dynamically-learned MAC addresses can be removed (aged out) automatically upon a link failure event. This prevents the switch from forwarding traffic to a link partner that cannot receive them.

Note

MAC address aging is enabled by default, but may be disabled in some applications.

To enable SINEC OS to automatically remove dynamically-learned MAC address when a link failure is detected, do the following:

1. Navigate to **Layer 2 » MAC Address Table » MAC Address Table**.
2. Under **Media Access Control (MAC) Address Table**, change **Age Out Upon Link Loss** to **Enabled**.
3. Commit the change.

8.2.3 Configuring static MAC filtering entries

To configure a static MAC filtering entry, do the following:

1. Define a static MAC filtering entry.
For more information, refer to "Adding a static MAC filtering entry (Page 189)".
2. [Optional] Assign a traffic class queue to the entry.
This overrides any traffic class settings on the ingress interface, forcing any frames associated with the MAC address to be prioritized and forwarded to the specified queue.
For more information, refer to "Assigning a traffic class queue (Page 190)".

8.2.3.1 Adding a static MAC filtering entry

Configuring a static MAC filtering entry adds a MAC address to the MAC address table. MAC addresses added statically are not aged out. They can only be removed from the table explicitly by a user.

Add static MAC filtering entries for important MAC addresses you wish to keep in the MAC address table.

Note

A maximum of 256 static MAC filtering entries can be added to the MAC address table.

Note

The following MAC addresses are prohibited:

- zero MAC addresses
- broadcast MAC addresses
- reserved MAC addresses
- virtual router MAC addresses
- the device's own MAC address

To add a static MAC filtering entry, do the following:

1. Navigate to **Layer 2 » MAC Address Table » Static**.
2. Under **Media Access Control (MAC) Address Table (Static Entries)**, click **Add**. A new row is added to the table.
3. Under **VLAN ID**, select an existing VLAN to associated with the MAC address.
4. Under **MAC Address**, enter the MAC address.
5. Under **Forwarding Port**, select a bridge port. Frames matching this entry will be forwarded on this bridge port.
6. Commit the changes.

Example

The following adds an entry and selects **ethernet0/1** as the forwarding port.

VLAN ID	MAC Address	Traffic Class	Forwarding Port
10	3A:34:52:C4:69:B8 b8:e6:45:c6:87:9b	Unprioritized	ethernet0/1

8.2.3.2 Assigning a traffic class queue

When a static MAC filtering entry is assigned a traffic class queue, all traffic class settings defined for the forwarding interface are overridden. Any frame associated with the MAC address is automatically prioritized and forwarded to the specified traffic class queue.

To assign a traffic class queue to a static MAC filtering entry, do the following:

1. Navigate to **Layer 2 » MAC Address Table » Static**.
2. Under **Media Access Control (MAC) Address Table (Static Entries)**, select a traffic class queue under **Traffic Class** for the selected static MAC filtering entry.
Options include:
 - **0 - 7** - A traffic class queue
 - **Unprioritized** - No traffic class queue is assigned
 Default: **Unprioritized**
3. Commit the change.

Example

The following assigns queue 7 to a static entry.

VLAN ID	MAC Address	Traffic Class	Forwarding Port
10	b8:e6:45:c6:87:9b	7	ethernet0/4

8.2.4 Monitoring the MAC address table

This section describes the various ways to view and manage the MAC address table.

8.2.4.1 Displaying the MAC address table

To display the MAC address table, navigate to **Layer 2 » MAC Address Table » MAC Address Table**.

Example

VLAN ID	MAC Address	Traffic Class	Forwarding Port	Entry Type
1	00:01:6C:4A:60:1A	Unprioritized	ethernet0/1	Dynamic
10	3A:34:52:C4:69:B8	7	ethernet0/1	Static
2	00:01:C0:0B:B8:42	Unprioritized	ethernet0/1	Dynamic

Description

The following is displayed for each entry under **Media Access Control (MAC) Address Table**:

Parameter	Description
VLAN ID	The VID of the VLAN associated with the MAC address.
MAC Address	The MAC address.
Traffic Class	The traffic class queue assigned to the MAC address. Possible values include: <ul style="list-style-type: none"> • 0 - 7 - A traffic class queue • Unprioritized - No traffic class queue is assigned
Forwarding Port	The outbound forwarding port associated with the MAC address. Frames matching the MAC address entry are forwarded through this interface.
Entry Type	The entry type. Possible values include: <ul style="list-style-type: none"> • Static - The MAC address was created statically by a user • Dynamic - The MAC address was learned dynamically

8.2.4.2 Clearing dynamic MAC addresses

When needed, the MAC address table can be cleared of all dynamically-learned addresses. The table will be repopulated immediately once the device starts receiving frames.

To clear the MAC address table of all dynamically-learned MAC addresses, do the following:

1. Navigate to **Layer 2 » MAC Address Table » MAC Address Table**.
2. Under **Purge Dynamic Entries**, click **Purge**.

IP Address Assignment

This chapter describes features related to the assignment of IP addresses, such as DHCP and DNS.

9.1 Static IP address assignment

IP addresses can be assigned statically (manually) to an IP interface. This is suitable for IP interfaces that should always be accessible under the same IP address.

To configure a static IPv4 address, do the following:

1. Make sure that an IP interface is configured.
For more information, refer to "VLANs (Page 288)".
2. Configure a static IPv4 address.
For more information, refer to "Configuring a static IPv4 address (Page 193)".

9.1.1 Configuring a static IPv4 address

To configure a static IPv4 address, do the following:

1. Navigate to **Interfaces** » **IP Interfaces**.
2. Make sure the IP interface to which you want to assign a static IPv4 address is configured as follows:
 - Under **IP Interfaces**, set **DHCP** to **Disabled**.
3. Under **IPv4 Static Addresses**, click **Add**.
A new row is added to the table.
4. Under **Interface**, select an IP interface.
You can only edit the IP interface directly after adding the new row. As soon as the field is no longer active, the IP interface is write-protected. If you want to change the IP interface, you need to delete the entry and re-configure it.
5. Under **IP Address**, enter an IPv4 address.
You can only edit the IP address directly after adding the new row. As soon as the field is no longer active, the IP address is write-protected. If you want to change the IP address, you need to delete the entry and re-configure it.
6. Enter a prefix under **Prefix Length**.
7. Commit the changes.

9.1.2 Listing the IPv4 address configuration

To display the IPv4 address configuration, navigate to **Interfaces** » **IP Interfaces**.

The following information is displayed under **IPv4 Static Addresses**:

Parameter	Description
Interface	VLAN ID of the IP interface
IP Address	IP address of the IP interface
Prefix Length	Subnet displayed as prefix length

9.2 Static DNS

This section describes how to configure a device so that you can specify the host or domain name instead of the IP address (e.g. ping or traceroute) for selected configurations.

9.2.1 Understanding DNS

Domain Name System (DNS) is a distributed database system in which a domain name can be assigned to an IP address. The DNS service converts a domain name into an IP address and vice versa. With static DNS, an IP address is fixed to a domain name. If the IP address changes, no connection can be established via the domain name and the destination cannot be reached.

DNS uses UDP and TCP on port 53 for transmission.

9.2.1.1 Basic terms for DNS

The following table explains basic DNS terms.

Term	Explanation
Domain name	<p>A domain name has a hierarchical structure and consists of several levels. The individual levels stand for name parts and are connected by dots.</p> <p>A domain name is read from right to left. A full domain name is referred to as Fully Qualified Domain Name (FQDN). It describes an exact position in the DNA hierarchy by indicating all levels, but at least a second level domain and top level domain.</p> <p>Example: www.industry.siemens.com</p> <p>In this example, "com" corresponds to the top-level domain. "siemens" corresponds to the second-level domain. "industry" forms an optional sub-level domain and "www" is the hostname.</p>
Domain	<p>A domain is a contiguous area of the DNS. A domain includes all hosts that are grouped under a common domain name.</p> <p>A domain that is located in the hierarchy under another domain is called a subdomain. Subdomains are used for logical structuring and can be managed by different DNS servers.</p>
Zone	<p>A zone is a part of the DNS that is managed by a DNS server. A zone can consist of an entire domain with subdomains, but also individual subdomains.</p>

Term	Explanation
DNS server	A DNS server or name server has information that resolves a domain name into an IP address. A DNS server can provide the information of one or more DNS zones: <ul style="list-style-type: none"> • An authoritative DNS server provides data from one or more zones. • A recursive DNS server obtains its information from other DNS servers.
Root server	Root servers or root name servers form the highest level of the DNS and thus the starting point of the hierarchical structure. Root servers answer queries on DNS servers of the top-level domain (TLD).
DNS resolver	A DNS resolver is a program that acts as an interface between DNS clients and DNS servers. It resolves a client request by collecting the requested information from DNS servers and forwarding it to the client. For the DNS resolver to work, it needs the IP address of at least one DNS server.
Search domain	A search domain is used to avoid having to manually enter the entire address of frequently used domains. The search domains you configure are automatically appended to the names you enter. DNS resolvers use search domains to create an FQDN from relative domain names you enter.
DNS client	The DNS client is the DNS application interface. The DNS client sends its DNS queries to a DNS resolver. When you configure a DNS server for a DNS client, this refers to a DNS resolver.

9.2.1.2 DNS communication

A DNS client that wants to resolve a domain name to an IP address makes a request to a DNS resolver. The DNS resolver either forwards the query to another DNS resolver known to it or resolves the query by asking for the individual levels of the DNS hierarchy.

If, for example, the domain name `www.industry.siemens.com` is to be resolved, the DNS resolver asks a root server for the DNS server of the top-level domain `.com`. In turn, the DNS resolver asks the DNS server of the top-level domain for the DNS server of the next hierarchy level `siemens.com`. According to this principle, the DNS resolver asks for all levels of the domain name until the query has been resolved or an error occurs, for example because a sub-level domain cannot be resolved or the responsible DNS server does not respond.

If a domain name cannot be resolved, you cannot connect to that host.

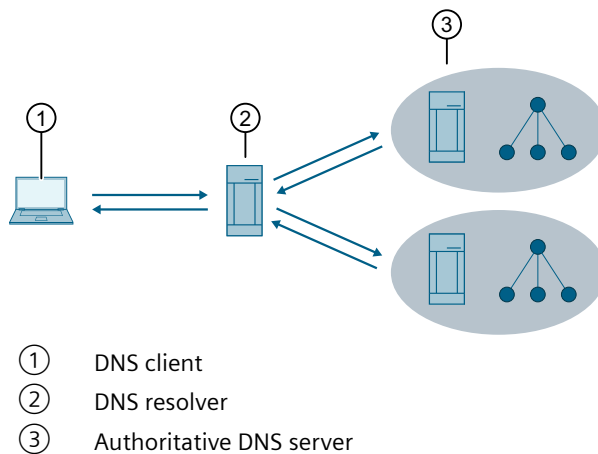


Figure 9-1 DNS communication

9.2.2 Configuring DNS

To configure DNS, do the following:

1. Configure at least one DNS server.
For more information, refer to "Configuring a DNS server (Page 196)".
2. [Optional] Configure a search domain.
For more information, refer to "Configuring a search domain (Page 197)".

9.2.2.1 Configuring a DNS server

Multiple DNS servers can be defined on the device. An index is assigned to the DNS servers in the order in which they are created. If there is more than one DNS server, an index specifies the order in which the servers are queried. The server with the lowest index is queried first. Manually configured DNS servers are given preference.

To configure a DNS server, do the following:

1. Navigate to **System** » **DNS Client**.
2. Under **DNS Servers (Static)**, click **Add**.
A new row is added to the table.
3. Enter the name of the DNS server under **Name**.
You can only edit the name directly after adding the new row. As soon as the field is no longer active, the name is write-protected. If you want to change the name, you need to delete the DNS server and re-configure it.
4. Enter the IP address of the DNS server under **Server Address**.
5. Commit the changes.

9.2.2.2 Configuring a search domain

Multiple search domain names can be stored on the device. These domains are searched when a domain name is resolved. An index is assigned to them in the order in which the search domains are created or learned. The index determines the order in which they are used when there are several search domains. The search domain with the lowest index is requested first.

If search domains are stored, you can enter the domain name for some IP address fields.

To define a search domain, do the following:

1. Navigate to **System » DNS Client**.
2. Under **Domain Search List (Static)**, click **Add**.
A new row is added to the table.
3. Enter the name of the search domain under **Domain Name**.
Condition:
 - Must be between 1 and 251 characters long
4. Commit the changes.

9.2.3 Displaying the DNS configuration

To display the DNS configuration, navigate to **System » DNS Client**.

The following information is displayed under **Domain Name System (DNS) Information**:

Parameter	Description
Origin	Indicates how the DNS server was added. Options include: <ul style="list-style-type: none"> • static - The DNS server was added manually. • dynamic - The DNS server was learned dynamically.

The following information is displayed under **DNS Servers**:

Parameter	Description
Server Address	Shows the IP addresses of the configured DNS servers.

The following information is displayed under **Domain Search List**:

Parameter	Description
Domain Name	Shows the configured search domains.

9.3 DHCP

This section describes how to configure a device to obtain its IP configuration from a DHCP server.

9.3.1 Configuring the device as a DHCP client

NOTICE**Configuration hazard - risk of communication failure**

The DHCP client is restarted every time you change a configuration parameter of the DHCP client. During the restart, IP communication with the management interface of the device is briefly interrupted because the device is retrieving its new IP address. This can result in brief communication failures in the network.

To configure the device as DHCP client, do the following:

1. Enable the DHCP client interface.
For more information, refer to "Enabling a DHCP client interface (Page 198)".
2. [Optional] Set a lease time.
For more information, refer to "Requesting a lease time (Page 198)".
3. [Optional] Change the client ID of a DHCP client interface.
For more information, refer to "Changing the client ID of an interface (Page 199)".
4. [Optional] Enable the use of the hostname.
For more information, refer to "Including the hostname in DHCP messages (Page 200)".
5. [Optional] Enable that the DHCP client request a configuration file from the DHCP server.
For more information, refer to "Requesting a Configuration File from the DHCP Server (Page 200)".

9.3.1.1 Enabling a DHCP client interface

By default, all DHCP client interfaces are disabled. Exception: For the VLAN 1, DHCP is activated in the factory state.

To enable a DHCP client interface, do the following:

1. Navigate to **Interfaces** » **IP Interfaces**.
2. Under **IP Interfaces**, change **DHCP** to **Enabled**.
3. Commit the change.

9.3.1.2 Requesting a lease time

The lease time specifies how long the IP address assigned by the DHCP server remains valid. The lease time requested by the client can be accepted or ignored by the server.

The DHCP client does not request a lease time by default.

To set a lease time, do the following:

1. Navigate to **Interfaces** » **IP Interfaces**.
2. Under **Dynamic Host Configuration Protocol (DHCPv4) Client** in the **Lease Time Requested [s]** column, define the lease time that a DHCP client interface requests from the DHCP server.
Conditions:
 - Formatted as nYnMnDnHnMns, where n is a user-defined number
 - Minimum 2 minutes (2m)
 - Maximum 136 years 2 months 9 days 10 hours 28 minutes 15 seconds (136Y2M10D6h28m15s)
3. Commit the change.

9.3.1.3 Changing the client ID of an interface

To change the client ID of a DHCP client interface, do the following:

1. Navigate to **Interfaces** » **IP Interfaces**.
2. Under **Dynamic Host Configuration Protocol (DHCPv4) Client** in the **Client ID** column, change the client ID of a DHCP client interface.
Options include:

Option	Description
MAC Address	Default The DHCP client identifies itself to the DHCP server with its MAC address.
Hostname	The DHCP client identifies itself to the DHCP server with its hostname. For more information, refer to "Changing the host name (Page 76)".
Name of Station	The DHCP client identifies itself to the DHCP server with its PROFINET device name.
Select or add new...	The DHCP client identifies itself with a freely selectable ID. Click Client ID and enter a user-defined ID. Conditions: <ul style="list-style-type: none"> • Must be between 1 and 152 characters long • All standard characters are allowed, plus the following special characters: _ - . : < = > @ ()

3. Commit the change.

9.3.1.4 Including the hostname in DHCP messages

If you enable this option, the hostname of the DHCP client is used in communication with the DHCP server. The DHCP server stores the hostname together with the assigned IP address and can use this information as follows:

- To identify the DHCP client
- To forward the assignment to a DNS server

The hostname is not specified in DHCP messages by default.

To use the hostname of the DHCP client in DHCP messages, do the following:

1. Navigate to **Interfaces** >> **IP Interfaces**.
2. Under **Dynamic Host Configuration Protocol (DHCPv4) Client**, change **Send Hostname** to **Enabled**.
3. Commit the change.

9.3.1.5 Requesting a Configuration File from the DHCP Server

When you enable this function, the DHCP client requests from the DHCP server the information of a TFTP server from which the client can load a configuration file, as well as the name of the relevant configuration file:

- DHCP option 66: IP address or FQDN of the TFTP server
- DHCP option 67: Name of the configuration file

When you enable or disable the function, the DHCP client is restarted in the device and a new DHCP request to a DHCP server is triggered.

As soon as the DHCP client receives the information, it downloads the configuration file and applies the configuration. The parameters of the running configuration contained in the configuration file are deleted and replaced by the contents of the configuration file. Parameters of the currently running configuration are only replaced if the corresponding parameters are contained in the configuration file. The loading and applying of the configuration file is recorded in the system log (Syslog).

NOTICE

Security hazard - risk of unauthorized access and/or misuse

The function can potentially be used to change the functionality of the device and thus cause the failure of data traffic. Users with malicious intent could cause the device to load a manipulated configuration file to change the configuration to their benefit.

To prevent unauthorized access and/or misuse, disable the function if you are not using it (**Off**).

In a device with default setting (**Setup**), no configuration file is loaded from the DHCP server even if the options 66 and 67 are still contained in the DHCP queries of the DHCP client after the first login with the default user profile **admin** and the assignment of a new password.

NOTICE**Configuration hazard - risk of communication failure**

When you load a configuration file from a DHCP server to a device, this can result in unintended behavior or a communication failure.

To prevent unintended behavior, reset the device to its default settings. After the reset, the device can only be reached via the serial interface. If you assign an IP address to the device via DHCP or DCP (e.g. SINEC PNI), you can access the CLI and Web UI of the device via a network connection with a preset user profile.

Requirements

- You have configured a server accordingly.
- The configuration file (.xml) is on the server.
- There is a connection between the device and the server.

Requesting a configuration file

To configure the function for a DHCP client interface, do the following:

1. Navigate to **Interfaces** » **IP Interfaces**.
2. Under **Dynamic Host Configuration Protocol (DHCPv4) Client** in the **Request Config File** column, configure whether the DHCP client requests a configuration file.
Options include:

Option	Description
Setup	<p>Default</p> <p>The function depends on the status of the device.</p> <p>In the delivery state and after reset to default settings, the function behaves as with the setting On. This means the function is enabled for all DHCP client interfaces.</p> <p>The following events trigger a status change of the device:</p> <ul style="list-style-type: none"> • The first login with the default user profile admin and the associated assignment of a new password • Loading a configuration file <p>Afterwards, the device is in the secure operating state. In the secure operating state, the function behaves as with the setting Off. This means the function is disabled for all DHCP client interfaces.</p> <p>The status change takes place automatically and once.</p>
On	The function is enabled. The DHCP client requests a configuration file with the next DHCP query.
Off	The function is disabled. The DHCP client does not request a configuration file.

3. Commit the change.

9.3.2 Showing the configuration data of DHCP client interfaces

To display the configuration data of DHCP client interfaces, navigate to **Interfaces » IP Interfaces**.

The following information is displayed under **IP Interfaces**:

Parameter	Description
Interface	VLAN ID of the DHCP client interface
DHCP	Indicates whether DHCP client is enabled for the specified interface

The following information is displayed for active DHCP client interfaces under **Dynamic Host Configuration Protocol (DHCP4) Client**:

Parameter	Description
Interface	VLAN ID of the DHCP client interface
IP Address Granted	IPv4 address of the interface
Prefix Length	Subnet displayed as prefix length
Lease Time Granted [s]	Validity period formatted as nYnMnDnHnmns assigned by the DHCP server
Lease Time Requested [s]	Validity period formatted as nYnMnDnHnmns the DHCP client requested from the DHCP server
Client ID	ID the DHCP client uses to log in to the DHCP server
Send Hostname	Indicates whether the host name of the DHCP client is used in communication with the DHCP server.
Request Config File	Shows whether the DHCP client requests a configuration file from the DHCP server
TFTP Server Name	IP address or FQDN of the TFTP server
Bootfile Name	Name of the configuration file

Network redundancy

This chapter describes the network redundancy features available. Network redundancy provides a failover mechanism to protect the network from crippling service disruptions that may be caused by a single point of failure.

10.1 Spanning Tree Protocol (STP)

SINEC OS supports the IEEE 802.1Q:2014 standard, which includes Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Both are network redundancy protocols for eliminating redundant paths to prevent loops in your network.

Improvements to the Rapid Spanning Tree Protocol are also provided by the Siemens proprietary enhanced Rapid Spanning Tree Protocol (eRSTP).

10.1.1 Understanding STP

The IEEE 802.1D Spanning Tree Protocol (STP) was developed to enable the construction of robust networks that incorporate redundancy, while at the same time pruning the active network topology to prevent loops.

10.1.1.1 Rapid Spanning Tree Protocol (RSTP)

The Rapid Spanning Tree Protocol (RSTP) is an evolution of STP.

While STP is effective, it requires the transfer of frames to halt for 30 seconds during a link outage until all bridges on the network are guaranteed to be aware of the new topology. RSTP replaces this setting period with an active handshake between bridges that guarantees the rapid propagation of topology information throughout the network.

RSTP states and roles

RSTP bridges are assigned the role of either root or designated bridge by other bridges on the network.

- The Root bridge is the logical center of the network
- Designated bridges are all other bridges on the network

Each port of a bridge is also assigned a state and a role.

- The state describes what is happening at the port in relation to address learning and frame forwarding
- The role indicates if the port is facing the center or the edges of the network, and if the port can be used

10.1 Spanning Tree Protocol (STP)

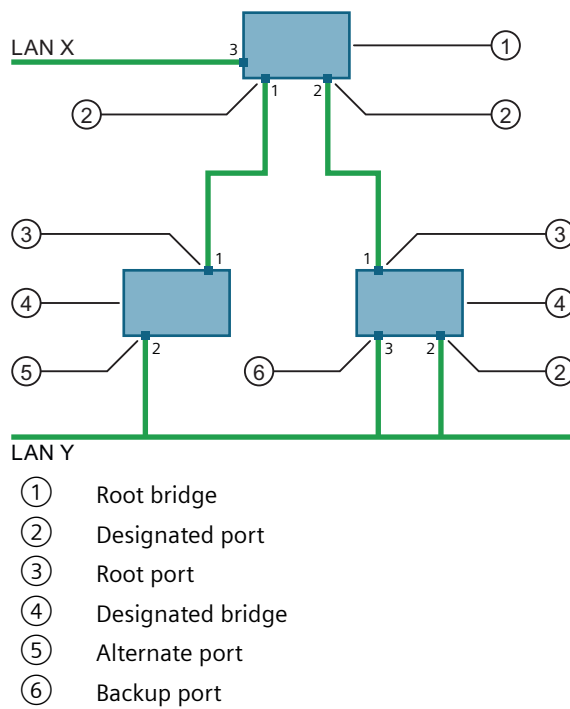


Figure 10-1 RSTP states and roles

Port roles

RSTP bridge ports can be assigned one of the following roles:

- **Root**
A port in the **root** role is the fastest route to the root bridge. Each designated bridge must have a single root port. Root ports are not permitted on a root bridge.
- **Alternate**
A port in the **alternate** role is the next fastest, alternative route to the root bridge. This port does not participate in the RSTP network. It waits to assume the role of root port if the current root port fails.
- **Designated**
A port in the **designated** role is the one that sends the best BPDU for a particular Local Area Network (LAN) segment. RSTP bridges on the same LAN segment listen for messages from one another and agree on which bridge among them sends the best BPDU. Ports of other bridges on the same segment must take one of the other available roles.

- **Backup**
A port in the **backup** role is a backup port for a designated port on the same RSTP bridge. Like alternate ports, this port does not participate in the RSTP network. It waits to assume the role of designated port if its companion port fails.
- **Edge**
Ports directly connected to an end station are assigned the **edge** role. Edge ports cannot create bridging loops in the network and can thus directly transition to the forwarding state, skipping the discarding and learning states.

Note

A port will lose its edge role and become a normal RSTP port if it receives an RSTP message from the root bridge. A loop created on an improperly connected edge port is thus quickly repaired.

Note

Since edge ports only service end stations, topology changes are not communicated to the root bridge when its link toggles.

Port states

RSTP bridge ports can be in one of the following states:

- **Discarding**
The **discarding** state is the initial state of each port when it is put into service. In this state, the port does not learn addresses and does not forward RSTP frames.
The port looks for RSTP traffic to determine its role in the network. When RSTP traffic is detected, the port state changes to **learning**.
- **Learning**
In the **learning** state, the port attempts to learn addresses of other RSTP bridges, but does not participate in the transfer of frames.
In a network of RSTP bridges, time spent in this state is short. RSTP bridges operating in STP compatibility mode will spend six to 40 seconds in this state.
Once the port has finished learning the addresses of all RSTP bridges, the port state changes to **forwarding**.
- **Forwarding**
In the **forwarding** state, the port participates in the transfer of frames and actively scans for addresses of new RSTP bridges.
- **Disabled**
The **disabled** state indicates that RSTP has been disabled for the port.
- **Link Down**
The **link down** state indicates that RSTP is enabled for the port, but the port is currently unable to forward frames.

Point-to-point and shared links

To prevent a disruption in services or the creation of a loop, RSTP uses a Proposal/Agreeing process on point-to-point links to quickly put the port into a forwarding state.

RSTP is a point-to-point protocol and as such, the Proposal/Agreeing process fails on multipoint links (i.e. when more than two bridges operate on a shared media link).

When RSTP detects this condition (based on the port's half-duplex state after link up), it will skip the Proposal/Agreeing process. The port must transition through the learning and forwarding states, spending one forward delay in each state.

There are circumstances in which RSTP will make an incorrect decision about the point-to-point state of a link simply by examining the half-duplex status, namely:

- The port attaches only to a single partner, but through a half-duplex link.
- The port attaches to a shared media hub through a full-duplex link. The shared media link attaches to more than one RSTP enabled bridge.

In such cases, the bridge can be configured to override the half-duplex determination mechanism and force the link to be treated normally.

Path and port costs

The STP path cost is the main metric by which root and designated ports are chosen. The path cost for a designated bridge is the sum of the individual port costs of the links between the root bridge and that designated bridge. The port with the lowest path cost is the best route to the root bridge and is chosen as the root port.

Bridge ID

In actuality, the primary determinant for root port selection is the root Bridge ID (RID), an 8 byte field comprised of the assigned 2 byte bridge priority and the bridge's 6 byte MAC address.

The RID is important mainly at network startup when the bridge with the lowest RID is elected as the root bridge.

After startup, when all bridges agree on the root bridge's RID, the path cost is used to select root ports. If the path costs of candidates for the root port are the same, the port that connects to the neighboring bridge with the lowest RID is selected.

Finally, if candidate root ports have the same path cost and peer bridge RID, the port RID of the peer bridge is used to select the root port. In all cases the lower RID, path cost, or port RID is selected as the best.

How port costs are generated

Port costs can be generated either as a result of link auto-negotiation or manual configuration. When the link auto-negotiation method is used, the port cost is derived from the speed of the link. This method is useful when a well-connected network has been established. It can be used when the designer is not concerned with the resultant topology as long as connectivity is assured.

Manual configuration is useful when the exact topology of the network must be predictable under all circumstances. The path cost can be used to establish the topology of the network exactly as the designer intends.

STP vs. RSTP costs

The STP specification limits port costs to values of 1 to 65536. Designed at a time when 9600 bps links were state of the art, this method breaks down in modern use, as the method cannot represent a link speed higher than 10 Gbit/s.

To remedy this problem in future applications, the RSTP specification limits port costs to values of 1 to 20000000, and a link speed up to 10 Tbit/s can be represented with a value of 2.

Bridge diameter

The bridge diameter is the maximum number of bridges between any two possible points of attachment of end stations to the network.

The bridge diameter reflects the realization that topology information requires time to propagate hop-by-hop through a network. If configuration messages take too long to propagate end-to-end through the network, the result will be an unstable network.

There is a relationship between the bridge diameter and the maximum age parameter.

Note

The RSTP algorithm is as follows:

- STP configuration messages contain age information.
 - Messages transmitted by the root bridge have an age of 0. As each subsequent designated bridge transmits the configuration message it must increase the age by at least 1 second.
 - When the age exceeds the value of the maximum age parameter the next bridge to receive the message immediately discards it.
-

To achieve extended ring sizes, Siemens' eRSTP™ uses an age increment of $\frac{1}{4}$ of a second. The value of the maximum bridge diameter is thus four times the configured maximum age parameter.

10.1.1.2 RSTP Applications

The following explores some of the many applications of RSTP:

- RSTP in structured wiring applications
- RSTP in ring backbone applications
- RSTP and port redundancy

RSTP In structured wiring applications

RSTP may be used to construct structured wiring systems where connectivity is maintained in the event of link failures. For example, a single link failure of any link between A and N in the figure "Example - RSTP Structured Wiring Configuration" would leave all the ports of bridges 555 through 888 connected to the network.

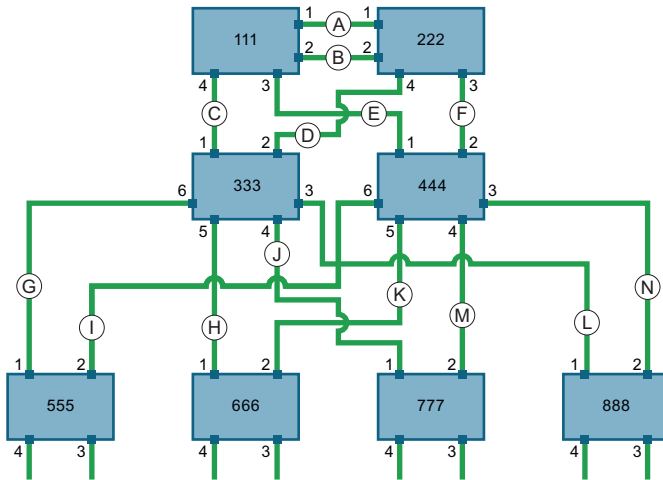


Figure 10-2 Example - RSTP structured wiring configuration

To design a structured wiring configuration, do the following:

1. Select the design parameters for the network.
 - What are the requirements for robustness and network failover/recovery times?
 - Are there any special requirements for diverse routing to a central host computer?
 - Are there any special port redundancy requirements?
2. Identify required legacy support.
 - Are STP bridges used in the network?
 - These bridges do not support rapid transitioning to forwarding. If these bridges are present, can they be re-deployed closer to the network edge?
3. Identify edge ports and ports with half-duplex/shared media restrictions.
 - Ports that connect to host computers, IEDs and controllers may be set to edge ports to guarantee rapid transitioning to forwarding as well as to reduce the number of topology change notifications in the network.
 - Ports with half-duplex/shared media restrictions require special attention to guarantee they do not cause extended failover/recovery times.
4. Choose the root bridge and backup root bridge carefully.
 - The root bridge should be selected to be at the concentration point of network traffic.
 - Locate the backup root bridge adjacent to the root bridge.
 - One strategy that may be used is to tune the bridge priority to establish the root bridge and then tune each bridge’s priority to correspond to its distance from the root bridge.

5. Identify the desired steady state topology.
 - Identify the desired steady state topology, taking into account link speeds, offered traffic, and traffic classes.
 - Examine the effects of breaking selected links, taking into account network loading and the quality of alternate links.
6. Decide upon a port cost calculation strategy.
 - Select whether fixed or auto-negotiated costs should be used.
It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style.
 - Select whether the STP or RSTP cost style should be used. Make sure to configure the same cost style on all devices on the network.
7. Enable the Fast Root Failover option.
 - It is recommended to enable the Fast Root Failover option in mesh network topologies to minimize the network downtime in the event of a root bridge failure.
 - Fast Root Failover is a Siemens' proprietary eRSTP feature.
 - Fast Root Failover must be supported by all switches in the network, including the root, to guarantee optimal performance.
8. Calculate and configure priorities and costs.
9. Implement the network and test under load.

RSTP In ring backbone configurations

RSTP may be used in ring backbone configurations where rapid recovery from link failure is required. In normal operation, RSTP will block traffic on one of the links.

For example, refer to link H in the figure "Example - RSTP Ring Backbone Configuration". In the event of a failure on link D, bridge 444 will unblock link H and bridge 333 will communicate with the network through link F.

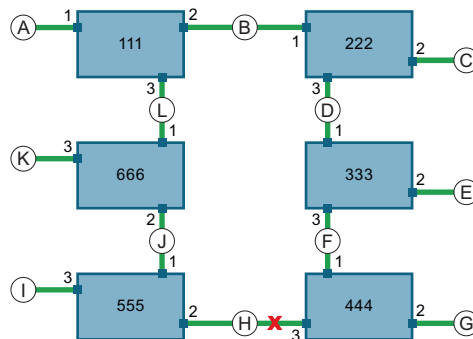


Figure 10-3 Example - RSTP ring backbone configuration

To design a ring backbone configuration with RSTP, do the following:

1. Select the design parameters for the network.
 - What are the requirements for robustness and network failover/recovery times?
 - Typically, ring backbones are chosen to provide cost effective but robust network designs.
2. Identify required legacy support and ports with half-duplex/shared media restrictions.
 - These bridges should not be used if network fail-over/recovery times are to be minimized.
3. Identify edge ports.
 - Ports that connect to host computers, LEDs and controllers may be set to edge ports to guarantee rapid transitioning to forwarding, as well as to reduce the number of topology change notifications in the network.
4. Choose the root bridge.
 - The root bridge can be selected to equalize either the number of bridges, number of stations, or amount of traffic on either of its legs. It is important to understand the ring will always be broken in one spot and that traffic always flows through the root.
5. Assign bridge priorities to the ring.
 - For more information, refer to the white paper "Performance of RSTP in Ring Network Topologies" (<https://assets.new.siemens.com/siemens/assets/api/uuid:d4af5d17-728c-493f-b00a-9c4db67b23ed/RSTP-whitepaper-EN-09-2020.pdf>).
6. Decide upon a port cost calculation strategy.
 - It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style.
 - Select whether the STP or RSTP cost style should be used.
 - Make sure to configure the same cost style on all bridges on the network.
7. Disable the Fast Root Failover option for eRSTP.
 - This option is enabled by default. It is recommended to disable this feature when operating in a single ring network topology.
8. Implement the network and test under load.

RSTP and port redundancy

In cases where port redundancy is essential, RSTP allows more than one bridge port to service a LAN. In the following example, if port 3 is designated to carry the network traffic of LAN A, port 4 will block traffic. Should an interface failure occur on port 3, port 4 will assume control of the LAN.

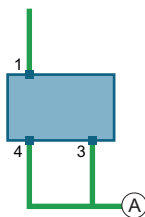


Figure 10-4 Example - Port redundancy

10.1.1.3 Enhanced Rapid Spanning Tree Protocol (eRSTP)

An evolution of STP and RSTP, Siemens' eRSTP (enhanced Rapid Spanning Tree Protocol) is designed to prevent broadcast storms.

Broadcast storms occur in ring network topologies when a switch receives a broadcast frame whose destination MAC address cannot be determined. The switch then floods the frame to all ports, causing the frame to circulate through the ring endlessly, consuming available bandwidth and rendering the network unusable.

STP was designed to solve the problem of traffic loops by identifying the loop and having a switch block the port that created it. However, STP's fault recovery time was too slow for most real-time control applications.

RSTP, like STP, is designed for mesh network topologies, not ring networks, and does not support ring sizes larger than 40 switches.

Siemens' eRSTP builds on the RSTP standard and enhances it in two ways:

- Optimizes the standard RSTP definition/implementation to achieve the best possible recovery time performance
- Improves the fault recovery time performance in the root bridge failure scenario
- Improves performance for large ring network topologies (up to 80 switches)

eRSTP is also compatible with standard RSTP for interoperability with commercial switches.

BPDU Guard Timeout

BPDU Guard Timeout is a component of eRSTP that addresses network security.

Standard RSTP must process every received BPDU and take appropriate action. This offers attackers an opportunity to influence the RSTP topology by injecting RSTP BPDUs into the network.

When enabled, BPDU Guard Timeout protects the network from BPDUs received by a port where RSTP capable devices are not expected to be attached. If a BPDU is received by a port configured to be an edge port or RSTP is disabled, the port will be shutdown for a configurable time period or until the port is reset.

Fast Root Failover

Fast Root Failover algorithm improves upon RSTP's handling of root bridge failures in mesh-connected networks.

In mesh network topologies, the standard RSTP algorithm does not guarantee deterministic network recovery time in the case of a root bridge failure. Such a recovery time is difficult to calculate and can be different (and relatively long) for any given mesh topology. However, the Fast Root Failover algorithm is able to detect the failure of the root bridge and apply extra RSTP processing steps to significantly reduce the network recovery time and make it deterministic.

When enabled, Fast Root Failover can operate in one of two modes:

- **Robust**
In robust mode, the algorithm ensures deterministic root failover time. However, all bridges on the network, including the root, must support Fast Root Failover to guarantee optimal performance.
- **Relaxed**
Relaxed mode is similar to robust mode, except the root bridge is not required to support Fast Root Failover.

Note

The minimum interval for root failures is one second. Multiple, near simultaneous root failures (within less than one second of each other) are not supported by Fast Root Failover.

Recommendations on the use of Fast Root Failover

- Do not enable Fast Root Failover in single ring network topologies
- It is strongly recommended to always connect the root bridge to each of its neighbor bridges using more than one link

Fast Root Failover and RSTP performance

- Running RSTP with Fast Root Failover disabled has no impact on RSTP performance.
- Fast Root Failover has no effect on RSTP performance in the case of failures that do not involve the root bridge or one of its links.
- The extra processing introduced by Fast Root Failover significantly decreases the worst-case failover time in mesh networks, with a modest increase in the best-case failover time. The effect on failover time in ring-connected networks, however, is to only increase it.

10.1.1.4 Multiple Spanning Tree Protocol (MSTP)

The Multiple Spanning Tree Protocol (MSTP) provides greater control and flexibility than RSTP and legacy STP. MSTP is an extension of RSTP, whereby multiple spanning trees may be maintained on the same bridged network. Data traffic is allocated to one or several spanning trees by mapping one or more VLANs to different Multiple Spanning Tree Instances (MSTIs).

The sophistication and utility of the MSTP implementation on a given bridged network is proportional to the amount of planning and design invested in configuring MSTP.

If MSTP is activated on some or all of the bridges in a network with no additional configuration, the result will be a fully and simply connected network. At best though, the result will be the same as a network using only RSTP. Taking full advantage of the features offered by MSTP requires a potentially large number of configuration variables to be derived from an analysis of data traffic on the bridged network, and from requirements for load sharing, redundancy, and

path optimization. Once these parameters have all been derived, it is critical they are consistently applied and managed across all bridges in a Multiple Spanning Tree (MST) region.

Note**Use RSTP for mission critical applications**

By design, MSTP processing time is proportional to the number of active STP instances, making it significantly slower than RSTP. Therefore, for mission critical applications, RSTP should be considered a better network redundancy solution than MSTP.

CIST

The CIST (Common and Internal Spanning Tree) is the union of the CST and the ISTs in all MST regions. The CIST therefore spans the entire bridged network, reaching into each MST region via the latter's IST to reach every bridge on the network.

IST

An MST region always defines an IST (Internal Spanning Tree). The IST spans the entire MST region and carries all traffic that is not specifically allocated (by VLAN) to a specific MSTI. The IST is always computed and is defined to be MSTI zero.

The IST is also the extension inside the MST region of the CIST.

MSTI

An MSTI (Multiple Spanning Tree Instance) is one of sixteen independent spanning tree instances that may be defined in an MST region (not including the IST). An MSTI is created by mapping a set of VLANs to a given MSTI ID. The same mapping must be configured on all bridges that are intended to be part of the MSTI. Moreover, all VLAN-to-MSTI mappings must be identical for all bridges in an MST region.

SINEC OS supports up to 16 MSTIs in addition to the IST.

Each MSTI has a topology that is independent of others. Data traffic originating from the same source and bound to the same destination, but on different VLANs on different MSTIs, may therefore travel a different path across the network.

CST

The CST (Common Spanning Tree) spans the entire bridged network, including MST regions and any connected STP or RSTP bridges. An MST region is seen by the CST as an individual bridge, with a single cost associated with its traversal.

MSTP regions and interoperability

In addition to supporting multiple spanning trees in a network of MSTP-capable bridges, MSTP is capable of inter-operating with bridges that support only RSTP or legacy STP, without requiring any special configuration.

An MST region may be defined as the set of interconnected bridges whose MST Region Identification is identical. The interface between MSTP bridges and non-MSTP bridges, or between MSTP bridges with different MST Region Identification information, becomes part of an MST Region boundary.

Bridges outside an MST region will see the entire region as though it were a single (R)STP bridge, with the internal detail of the MST region being hidden from the rest of the bridged network. In support of this, MSTP maintains separate hop counters for spanning tree information exchanged at the MST region boundary versus information propagated inside the region. For information received at the MST region boundary, the (R)STP Message Age is incremented only once. Inside the region, a separate Remaining Hop Count is maintained, one for each spanning tree instance. The external Message Age parameter is referred to the (R)STP Maximum Age Time, whereas the internal Remaining Hop Counts are compared to an MST region-wide Maximum Hops parameter.

MSTP bridge and port roles

MSTP supports the following bridge and port roles:

Bridge Roles

Role	Description
CIST Root	The CIST Root is the elected root bridge of the CIST (Common and Internal Spanning Tree), which spans all connected STP and RSTP bridges and MSTP regions.
CIST Regional Root	The root bridge of the IST within an MSTP region. The CIST Regional Root is the bridge within an MSTP region with the lowest cost path to the CIST Root. Note that the CIST Regional Root will be at the boundary of an MSTP region. Note also that it is possible for the CIST Regional Root to be the CIST Root.
MSTI Regional Root	The root bridge for an MSTI within an MSTP region. A root bridge is independently elected for each MSTI in an MSTP region.

Port Roles

Each port on an MSTP bridge may have more than one CIST role depending on the number and topology of spanning tree instances defined on the port.

Role	Description
CIST Port Roles	<ul style="list-style-type: none"> The Root Port provides the minimum cost path from the bridge to the CIST Root via the CIST Regional Root. If the bridge itself happens to be the CIST Regional Root, the Root Port is also the Master Port for all MSTIs, and provides the minimum cost path to a CIST Root located outside the region. A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the CIST Regional Root. Alternate and Backup Ports function the same as they do in RSTP, but relative to the CIST Regional Root.
MSTI Port Roles	<p>For each MSTI on a bridge:</p> <ul style="list-style-type: none"> The Root Port provides the minimum cost path from the bridge to the MSTI Regional Root, if the bridge itself is not the MSTI Regional Root. A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the MSTI Regional Root. Alternate and Backup Ports function the same as they do in RSTP, but relative to the MSTI Regional Root. <p>The Master Port, which is unique in an MSTP region, is the CIST Root Port of the CIST Regional Root, and provides the minimum cost path to the CIST Root for all MSTIs.</p>
Boundary Ports	<p>A Boundary Port is a port on a bridge in an MSTP region that connects to either: a bridge belonging to a different MSTP region, or a bridge supporting only RSTP or legacy STP. A Boundary Port blocks or forwards all VLANs from all MSTIs and the CIST alike.</p> <p>A Boundary Port may be:</p> <ul style="list-style-type: none"> The CIST Root Port of the CIST Regional Root (and therefore also the MSTI Master Port). A CIST Designated Port, CIST Alternate/Backup Port, or Disabled. <p>At the MSTP region boundary, the MSTI Port Role is the same as the CIST Port Role. A Boundary Port connected to an STP bridge will send only STP BPDUs. One connected to an RSTP bridge need not refrain from sending MSTP BPDUs. This is made possible by the fact that the MSTP carries the CIST Regional Root Identifier in the field that RSTP parses as the Designated Bridge Identifier.</p>

Benefits of MSTP

MSTP is configured by default to arrive automatically at a spanning tree solution for each configured MSTI. However, advantages may be gained from influencing the topology of MSTIs in an MST region by way of the Bridge Priority and the cost of each port.

Load balancing

MSTP can be used to balance the data traffic load among sets of VLANs, enabling more complete utilization of a bridged network that has multiple redundant interconnections between bridges.

A bridged network controlled by a single spanning tree will block redundant links by design to avoid harmful loops. However, when using MSTP, any given link may have a different blocking state for MSTI, as maintained by MSTP. Any given link, therefore, might be in blocking state for

some VLANs, and in forwarding state for other VLANs, depending on the mapping of VLANs to MSTIs.

It is possible to control the spanning tree solution for each MSTI, especially the set of active links for each tree, by manipulating per MSTI the bridge priority and the port costs of links in the network. If traffic is allocated judiciously to multiple VLANs, redundant interconnections in a bridged network, which would have gone unused when using a single spanning tree, can now be made to carry traffic.

Isolation of Spanning Tree reconfiguration

A link failure in an MSTP region that does not affect the roles of Boundary ports will not cause the CST to be reconfigured, nor will the change affect other MSTP regions. This is due to the fact that MSTP information does not propagate past a region boundary.

MSTP versus PVST

An advantage of MSTP over the Cisco Systems Inc. proprietary Per-VLAN Spanning Tree (PVST) protocol is the ability to map multiple VLANs onto a single MSTI. Since each spanning tree requires processing and memory, the expense of keeping track of an increasing number of VLANs increases much more rapidly for PVST than for MSTP.

Compatibility with STP and RSTP

No special configuration is required for the bridges of an MST region to connect fully and simply to non-MST bridges on the same bridged network. Careful planning and configuration is, however, recommended to arrive at an optimal network design.

Implementing MSTP on a bridged network

The following procedure is recommended for configuring MSTP on a network.

Note

Careful network analysis and planning should inform each step of creating an MSTP network.

Note

MSTP does not need to be enabled to map a VLAN to an MSTI. However, the mapping must be identical for each bridge that belongs to the MSTP region.

Beginning with a set of MSTP-capable Ethernet bridges, do the following for each bridge on the network:

1. Disable STP globally.
For more information, refer to "Enabling STP (Page 218)".
2. Configure one or more Multiple Spanning Tree Instances (MSTI), each with a unique bridge priority.
For more information, refer to "Configuring Multiple Spanning Tree Instances (MSTIs) (Page 231)".
3. Create static VLANs and map them to the MSTIs.
For more information, refer to "Mapping a VLAN to an MSTI (Page 233)".

4. Set the STP protocol version to MSTP.
For more information, refer to "Selecting the STP version (Page 218)".
5. Configure the region revision level.
For more information, refer to "Configuring the region revision level (Page 230)".
6. Enable STP.
For more information, refer to "Enabling STP (Page 218)".

10.1.1.5 Related events

The following events are triggered by the STP service and recorded in the syslog:

- Bpdu-guard-activated
- Received-looped-back-bpdu
- New-stp-root
- Stp-topology-change

Each event is configurable.

For more information about these events and configuration options, refer to "Available alarms (Page 350)".

10.1.2 Configuring STP Globally

To configure STP globally, do the following:

1. Enable the Spanning Tree service.
For more information, refer to "Enabling STP (Page 218)".
2. Select the STP version that will run on the device (i.e. RSTP or MSTP).
For more information, refer to "Selecting the STP version (Page 218)".
3. Select the bridge priority.
If you want the bridge to be the root bridge, assign it a low priority.
For more information, refer to "Selecting the bridge priority (Page 219)".
4. Configure the Hello time.
This determines the interval at which STP configuration messages are sent.
For more information, refer to "Configuring the Hello time (Page 219)".
5. If the device is the root bridge, configure the maximum age time.
This determines the interval at which all other bridges refresh their configuration messages.
For more information, refer to "Configuring the maximum aging time (Page 220)".
6. Configure STP for one or more bridge ports.
Bridge ports forward and receive BPDUs for the Spanning Tree network.
For more information, refer to "Configuring STP for Bridge Ports (Page 221)".

10.1 Spanning Tree Protocol (STP)

- 7. [Optional] Configure the transmit hold count.
This determines how many Bridge Protocol Data Units (BPDUs) can be sent by each STP-enabled port. By default, there is no limit.
For more information, refer to "Configuring the transmit hold count (Page 221)".
- 8. [Optional] Configure the forward delay.
This determines how long each STP-enabled port spends in the listening and learning states.
For more information, refer to "Configuring the forward delay (Page 221)".

Following this initial configuration, configure the version of STP selected.

- For RSTP, configure the enhanced features added by eRSTP.
While the default settings for eRSTP are sufficient for most applications, you want to review and/or adjust them.
For more information, refer to "Configuring eRSTP (Page 227)".
- For MSTP, configure the global MSTP settings and define MSTIs.
For more information, refer to "Configuring MSTP (Page 230)".

10.1.2.1 Enabling STP

To enable the Spanning Tree service, including RSTP and MSTP, globally for the bridge, do the following:

Note

The Spanning Tree service is enabled by default.

- 1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
- 2. Under **Spanning Tree General Configuration**, change **Spanning Tree** to **Enabled**.
- 3. Commit the change.

10.1.2.2 Selecting the STP version

To control which version of Spanning Tree the bridge uses, do the following:

- 1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
- 2. Under **Spanning Tree General Configuration**, configure **Spanning Tree Version**.
Options include:

Option	Description
RSTP	Default The bridge will operate using the Rapid Spanning Tree Protocol (RSTP).
MSTP	The bridge will operate using the Multiple Spanning Tree Protocol (MSTP).

- 3. Commit the change.

10.1.2.3 Selecting the bridge priority

The bridge priority determines if the bridge becomes the root bridge in the network topology. The bridge with the lowest bridge priority is designated as the root bridge. If that bridge fails, the bridge with the next lowest priority becomes the root bridge.

Designated bridges also use the bridge priority to determine which of them is active.

Careful selection of bridge priorities can establish the path of traffic flows in normal and abnormal conditions.

To select the bridge priority for the bridge, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
2. Under **Spanning Tree General Configuration**, select a bridge priority under **Bridge Priority**. Options include:
 - 0
 - 4096
 - 8192
 - 12288
 - 16384
 - 20480
 - 24576
 - 28672
 - 32768 (Default)
 - 36864
 - 40960
 - 45056
 - 49152
 - 53248
 - 57344
 - 61440
3. Commit the change.

10.1.2.4 Configuring the Hello time

The Hello time is the time delay between STP configuration messages sent by the bridge. Shorter Hello times result in faster detection of topology changes at the expense of moderate increases in STP traffic.

10.1 Spanning Tree Protocol (STP)

To configure the Hello time for the bridge, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
2. Under **Spanning Tree General Configuration**, configure **Hello Time**.
Condition:
 - A number between 1 and 10Default: 2
3. Commit the change.

10.1.2.5 Configuring the maximum aging time

When the bridge is the root bridge, it controls the maximum aging time for all other bridges. The maximum aging time is the interval at which each bridge refreshes the configuration message it issues. A configuration message is a special Bridge Protocol Data Unit (BPDU) used in the root bridge selection process.

NOTICE
Configuration hazard - risk of reduced network performance
The maximum aging time is set by the root bridge for all bridges. Care should be taken when configuring this setting when many tiers of bridges exist or slow speed links (e.g. WANs) are part of the network.

NOTICE
Configuration hazard - risk of network instability
Make sure the maximum age time is greater than or equal to the maximum number of bridges in the network.
If the increment is too low, BPDUs will exceed their maximum age time and be dropped by the next bridge that receives them. Other bridges beyond that bridge will then become isolated from the Spanning Tree network, causing each to claim it is the root bridge and cause network instability.

To configure the maximum aging time, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
2. Under **Spanning Tree General Configuration**, configure **Max Age Time**.
The value must be greater or equal to:
 $2 \times [\{ \text{delay} \} + 1 \text{ s}]$
where { delay } is either the Hello time or the forward delay time, whichever is higher.
For example, if the Hello time is 6 seconds and the forward delay is 5 seconds, the maximum aging time must be greater or less than 13 seconds.
Default: 20
3. Commit the change.

10.1.2.6 Configuring the transmit hold count

The transmit hold count controls the maximum number of BPDUs that can be sent per second on each interface. Larger values allow the network to recover from failed links/bridges more quickly.

To configure the transmit hold count, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
2. Under **Spanning Tree General Configuration**, configure **Transmit Hold Count**.
Options include:

Option	Description
{ number }	A number between 3 and 100.
unlimited	Default There is no limit to the number of BPDUs that can be sent.

3. Commit the change.

10.1.2.7 Configuring the forward delay

The forward delay timer determines the amount of time (in seconds) each port spends in the listening and learning states. Setting a low value for this setting will allow ports to reach the forwarding state quickly, but at the expense of flooding unlearned addresses to all ports.

To configure the forward delay timer for all ports, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
2. Under **Spanning Tree General Configuration**, configure **Forward Delay**.
Condition:

- A number between 4 and 30

Default: 15

3. Commit the change.

10.1.3 Configuring STP for Bridge Ports

To configure a bridge port, do the following:

1. Enable STP for the bridge port.
For more information, refer to "Enabling STP for a bridge port (Page 222)".
2. Configure the path cost for the bridge port.
When multiple bridge ports are configured, the path cost is used to determine which port will be put in the forwarding state. Only one bridge port at a time can be in the forwarding state. For more information, refer to "Configuring the bridge port cost (Page 222)".
3. Select the bridge port priority.
When multiple bridge ports are configured and some have the same path cost, the port with the higher priority is put into the forwarding state. For more information, refer to "Selecting the bridge port priority (Page 223)".

10.1 Spanning Tree Protocol (STP)

4. [Optional] Select the edge port state for the bridge port.
An edge port is automatically put into the forwarding state. It sends STP configuration messages, but it does not participate otherwise in the Spanning Tree.
For more information, refer to "Selecting the edge port state (Page 224)".
5. [Optional] Select the port link type for the bridge port.
The port link type determines if the link is a point-to-point or shared link.
For more information, refer to "Selecting the bridge port link type (Page 225)".
6. [Optional] Restrict the role of the bridge port.
If the bridge port is connected to bridges outside the core region of the network, it can be restricted from becoming the bridge port for the Common Internal Spanning Tree (CIST) or any MSTI. This protects the Spanning Tree topology from being influenced by bridges that are outside of administrator control.
For more information, refer to "Restricting the role of a bridge port (Page 225)".
7. [Optional] Prevent the bridge port from forwarding Topology Change Notices (TCNs).
Bridge ports connected to bridges outside the core region of the network may cause unwanted address flushing in their region. Preventing those ports from forwarding TCNs can prevent flushing, but at the cost of network performance.
For more information, refer to "Preventing a bridge port from forwarding TCNs (Page 226)".

10.1.3.1 Enabling STP for a bridge port

To enable STP for a bridge port, do the following:

Note

STP cannot be enabled for a bridge port if:

- The bridge port is configured to participate in loop detection
 - Another network redundancy protocol is enabled for the same bridge port
-

Note

STP is enabled for all bridge ports by default.

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree Ports**.
2. Under **Spanning Tree Ports**, change **Bridge Port STP Enable** to **Enabled** for the selected bridge port.
3. Commit the change.

10.1.3.2 Configuring the bridge port cost

Each bridge port must be assigned a cost. The cost is used to determine the path costs of each bridge port and which bridge ports will forward traffic.

To configure the port cost for a bridge port, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree Ports**.
2. Under **Spanning Tree Ports**, configure **Cost** for the selected bridge port.
Options include:

Option	Description
{ number }	<p>Default</p> <p>A specific cost.</p> <p>Condition:</p> <ul style="list-style-type: none"> • A number between 1 and 2147483647 <p>Default:</p> <ul style="list-style-type: none"> • 199999 (port channels) • 20000 (physical interfaces)
auto	The standard RSTP port cost is negotiated automatically (i.e. 20000 for 1 Gbps links, 200000 for 100 Mbps links, 2000000 for 10 Mbps links).

3. Commit the change.

10.1.3.3 Selecting the bridge port priority

The port priority of a bridge port is considered when ports with the same port cost attach to the same LAN. The bridge port with the lowest port priority number (highest priority) is moved into the forwarding state.

10.1 Spanning Tree Protocol (STP)

To select the port priority for a bridge port, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree Ports**.
2. Under **Spanning Tree Ports**, configure **Port Priority** for the selected bridge port.
Options include:
 - 0
 - 16
 - 32
 - 48
 - 64
 - 80
 - 96
 - 112
 - 128 (Default)
 - 144
 - 160
 - 176
 - 194
 - 208
 - 224
 - 240
3. Commit the change.

10.1.3.4 Selecting the edge port state

Bridge ports designated as edge ports send STP configuration messages, but do not participate in the Spanning Tree. Edge ports transition directly to the forwarding state without any listening or learning delays. Their MAC tables also do not need to be flushed when topology changes occur.

Note

Unlike a bridge port that has STP disabled, accidentally connecting an edge port to another port in the Spanning Tree will result in a detectable loop. The bridge port will be converted to a regular bridge port and the standard RSTP rules will be applied until the next link outage.

Note

Edge ports do not trigger Topology Change Notifications (TCNs), whether it is configured manually or automatically.

To select the edge port state of a bridge port, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree Ports**.
2. Under **Spanning Tree Ports**, configure **Edge Port** for the selected bridge port.
Options include:

Option	Description
Auto	Default The bridge port is designated as an edge port automatically.
Enabled	The bridge port is designated as an edge port.
Disabled	The edge port state is removed from the bridge port.

3. Commit the change.

10.1.3.5 Selecting the bridge port link type

RSTP uses a peer-to-peer protocol that provides rapid transitioning on point-to-point links. This protocol is automatically disabled in situations where multiple STP bridges communicate over a shared (non point-to-point) LAN.

To select the port link type for a bridge port, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree Ports**.
2. Under **Spanning Tree Ports**, configure **Link Type** for the selected bridge port.
Options include:

Option	Description
Auto	Default Automatically sets the port link type to Point to point if the bridge port is in full-duplex mode, or Shared if the port is in half-duplex mode.
Point to point	The bridge port operates in half-duplex mode, but is a point-to-point link.
Shared	The bridge port operates in full-duplex mode, but it is a shared link.

3. Commit the change.

10.1.3.6 Restricting the role of a bridge port

To prevent bridges external to the core region of the network from influencing the Spanning Tree topology, an administrator can prevent bridge ports connected to those bridges from becoming the bridge port for the Common Internal Spanning Tree (CIST) or any Multiple Spanning Tree Instance (MSTI). These ports are instead designated as alternate ports after the root port has been selected.

An administrator may choose to apply this restriction to bridge ports connected to devices that are not under the administrator's control.

Note

This option is disabled by default.

To prevent a bridge port from becoming the root port, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree Ports**.
2. Under **Spanning Tree Ports**, change **Restricted Role** to **Enabled** for the selected bridge port.
3. Commit the change.

10.1.3.7 Preventing a bridge port from forwarding TCNs

To prevent bridges external to the core region of the network from causing address flushing in that region, an administrator can prevent bridge ports connected to those bridges from forwarding Topology Change Notices (TCNs) to other ports.

An administrator may choose to apply this restriction to bridge ports if, for example:

- those ports are connected to devices that are not under the administrator's control
- the MAC operational status parameter for the attached LANs transitions frequently

NOTICE
Configuration hazard - risk of reduced network performance
Preventing bridge ports from forwarding TCNs and topology changes can cause temporary losses in connectivity after changes to the Spanning Tree topology occur. This is the result of persistent, incorrectly learned, station location information.

Note

This option is disabled by default.

To prevent a bridge port from sending Topology Change Notices (TCNs) to other ports, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree Ports**.
2. Under **Spanning Tree Ports**, change **Restricted TCN** to **Enabled** for the selected bridge port.
3. Commit the change.

10.1.4 Configuring eRSTP

To configure eRSTP, do the following:

Note

eRSTP settings are ignored when Spanning Tree is in MSTP mode.

1. Select the maximum network diameter.
This is the maximum number of switches BPDUs have to traverse. Once the maximum network diameter is exceeded, the BPDU is dropped.
For more information, refer to "Selecting the maximum network diameter (Page 227)".
2. Configure the BPDU Guard Timeout.
This feature automatically blocks a bridge port that receives a BPDU from an unexpected bridge. It is disabled by default.
For more information, refer to "Configuring the BPDU Guard Timeout (Page 228)".
3. Select the Fast Root Failover mechanism.
This feature makes network recovery time deterministic.
For more information, refer to "Selecting the Fast Root Failover mechanism (Page 229)".
4. Enable IEEE 802.1w interoperability.
This feature eliminates recovery time issues that may arise when other non-Siemens devices in the Spanning Tree are running a version of RSTP compatible only with the IEEE 802.1w standard.
For more information, refer to "Enabling IEEE 802.1w interoperability (Page 229)".

10.1.4.1 Selecting the maximum network diameter

The maximum network diameter represents the maximum number of switches BPDUs have to traverse. In standard RSTP, the maximum network diameter is equal to the maximum aging time. However, with eRSTP, the maximum network diameter can be increased up to four times.

Note

The maximum aging time is controlled by the **Max Age Time** parameter.

For information about setting the **Max Age Time** parameter, refer to "Configuring the maximum aging time (Page 220)".

10.1 Spanning Tree Protocol (STP)

To select the maximum network diameter, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
2. Under **eRSTP Configuration**, configure **Max Network Diameter**.
Options include:

Option	Description
4x Max Age Time	Default The maximum network diameter is four times (4x) larger than the maximum aging time.
Max Age Time	The maximum network diameter is equal to the maximum aging time.

3. Commit the change.

10.1.4.2 Configuring the BPDU Guard Timeout

BPDU Guard Timeout disables bridge ports that receive BPDUs from RSTP-capable devices that are not expected to be attached to the network.

Note

This feature is disabled by default.

With BPDU Guard Timeout disabled, an attacker can influence the RSTP topology by injecting RSTP BPDUs into the network without detection. However, when enabled, BPDU Guard Timeout detects an unexpected BPDU and automatically disables the port that received it for either a set time period or until the port is re-enabled.

To configure BPDU Guard Timeout, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
2. Under **eRSTP Configuration**, configure **BPDU Guard Timeout**.
Options include:

Option	Description
<code>do-not-shutdown</code>	Default Disables BPDU Guard Timeout.
<code>until-reset</code>	Disables ports until they are re-enabled if they receive a BPDU from an unexpected device.
<code>{ seconds }</code>	Disables ports for the specified number of seconds if they receive a BPDU from an unexpected device. Condition: <ul style="list-style-type: none"> • A number between 1 and 86400

3. Commit the change.

10.1.4.3 Selecting the Fast Root Failover mechanism

The Fast Root Failover mechanism makes network recovery time deterministic in the case of a root bridge failure.

NOTICE

Configuration hazard - risk of reduced network performance

Fast Root Failover is ideally suited for mesh networks. Do not enable Fast Root Failover on devices connected to a single ring network. The extra processing introduced by the Fast Root Failover mechanism will increase the worst-case failover time.

To select the Fast Root Failover mechanism, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
2. Under **eRSTP Configuration**, configure **Fast Root Failover**.
Options include:

Option	Description
On	Default Enables Fast Root Failover in robust mode.
Off	Disables Fast Root Failover.
Off with Standard Root	Enables Fast Root Failover in relaxed mode.

3. Commit the change.

10.1.4.4 Enabling IEEE 802.1w interoperability

SINEC OS supports IEEE 802.1D-2004 RSTP. When other devices on the network are running RSTP compatible with the IEEE 802.1w standard, longer recovery times from failures on the network can be expected.

Fortunately, eRSTP offers an IEEE 802.w interoperability mode. This mode introduces enhancements to RSTP that negate any interoperability issues with non-Siemens devices.

Note

IEEE 802.1w interoperability is enabled by default.

To enable IEEE 802.1w interoperability, do the following:

1. Navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.
2. Under **eRSTP Configuration**, change **IEEE802.1w Interoperability** to **Enabled**.
3. Commit the change.

10.1.5 Configuring MSTP

To configure MSTP, do the following:

1. Select the maximum number of hops BPDUs can be forwarded in the Multiple Spanning Tree (MST) region.
For more information, refer to "Selecting the maximum number of hops (Page 230)".
2. Add the name of the region.
For more information, refer to "Adding the region name (Page 230)".
3. Select the region revision level.
All bridges within the same MST region have the same revision level.
For more information, refer to "Configuring the region revision level (Page 230)".
4. Configure one or more Multiple Spanning Tree Instances (MSTIs).
For more information, refer to "Configuring Multiple Spanning Tree Instances (MSTIs) (Page 231)".

10.1.5.1 Selecting the maximum number of hops

To select the maximum number of hops BPDUs can be forwarded within the MST region, do the following:

1. Navigate to **Layer 2 » Spanning Tree » MSTP General**.
2. Under **MSTP General**, set **MSTP Max Hops** to the maximum number of hops.
Default: 20
3. Commit the change.

10.1.5.2 Adding the region name

The default name for each MSTP region is the MAC address of the device. However, any name can be assigned if needed.

To add the name for an MSTP region, do the following:

1. Navigate to **Layer 2 » Spanning Tree » MSTP General**.
2. Under **MSTP General**, set **Region Name** to the name of the MSTP region.
Default: 00-0A-DC-92-00-00
3. Commit the change.

10.1.5.3 Configuring the region revision level

Each bridge in an MST region must be assigned a revision level. Typically, all bridges belonging to the same MST region (as identified by the regional root ID) have the same revision level. However, bridges within the same MST region can have different revision levels, which creates sub-regions.

Assigning different revision levels may be a way of marking topology changes.

Note

It is recommended to assign the same revision level to all bridges within the same MST region.

To configure the revision level for the device, do the following:

1. Navigate to **Layer 2 » Spanning Tree » MSTP General**.
2. Under **MSTP General**, configure the revision level under **Region Revision Level**.
Condition:
 - A number between 0 and 65335Default: 0
3. Commit the change.

10.1.6 Configuring Multiple Spanning Tree Instances (MSTIs)

To configure a Multiple Spanning Tree Instance (MSTI), do the following:

Note

Only MST 0 is created implicitly and cannot be controlled by the user. All other MSTIs must be created explicitly.

Note

MSTIs are only activated when associated with a static VLAN.

1. Create the MSTI.
For more information, refer to "Creating an MSTI (Page 232)".
2. Select the bridge priority for the MSTI.
This is used by MSTP to determine the regional root bridge for the instance.
For more information, refer to "Selecting the bridge priority (Page 232)".
3. Map one or more VLANs to the MSTI.
Like a logical port, an MSTI can be mapped to multiple VLANs.
For more information, refer to "Mapping a VLAN to an MSTI (Page 233)".
4. Select the MSTI port priority for the bridge port.
This is required for each bridge port mapped to the MSTI to help resolve loops.
For more information, refer to "Configuring the bridge port priority for an MSTI (Page 233)".
5. Select the MSTI cost for the bridge port.
This is required for each bridge port mapped to the MSTI to determine the path costs and which bridge port will forward traffic.
For more information, refer to "Configuring the MSTI cost for a bridge port (Page 234)".

10.1.6.1 Creating an MSTI

To create an MSTI, do the following:

1. Navigate to **Layer 2 » Spanning Tree » MSTP General**.
2. Under **MSTP Instances**, click **Add**.
3. Under **Instance ID**, enter an ID for the instance.
Condition:
 - A number between 1 and 16
4. Commit the change.

10.1.6.2 Selecting the bridge priority

Each MSTI must be assigned a bridge priority. The bridge priority of all bridges in the same instance are compared to determine which is the regional root bridge. The lower the value, the higher the priority

The regional root bridge provides paths to other instances that share one or more of the same VLANs.

To select the bridge priority for an MSTI, do the following:

1. Navigate to **Layer 2 » Spanning Tree » MSTP General**.
2. Under **MSTP Instances**, configure **Priority** for the selected MSTI.
Options include:
 - 0
 - 4096
 - 8192
 - 12288
 - 16384
 - 20480
 - 24576
 - 28672
 - 32768
 - 36864
 - 40960
 - 45056
 - 49152
 - 53248
 - 57344
 - 61440Default: 32768
3. Commit the change.

10.1.6.3 Mapping a VLAN to an MSTI

To map a VLAN to an MSTI, do the following:

Note

With the exception of MST 0, the MSTI must be created before it can be mapped to a VLAN.

1. Navigate to **Layer 2 » Spanning Tree » MSTP General**.
2. Under **MSTP VLAN to MST Instance Mapping**, configure **Instance ID** for the selected VLAN.
3. Commit the change.

10.1.6.4 Configuring the bridge port priority for an MSTI

Bridge ports mapped to an MSTI must be assigned a port priority. When loops occur, the port with the lowest priority is put into the forwarding state. This only occurs if the loop cannot be resolved using bridge IDs or the path cost.

10.1 Spanning Tree Protocol (STP)

If all bridge ports have the same port priority, the port with the lowest bridge port number is put into the forwarding state.

To configure the port priority for an MSTI-enabled bridge port, do the following:

1. Navigate to **Layer 2 » Spanning Tree » MSTP Ports**.
2. Under **Interface Selection**, select an MSTI-enabled bridge port.
3. Under **MST Ports**, configure **Port Priority**.
Options include:
 - 0
 - 16
 - 32
 - 48
 - 64
 - 80
 - 96
 - 112
 - 128
 - 144
 - 160
 - 176
 - 194
 - 208
 - 224
 - 240Default: 128
4. Commit the change.

10.1.6.5 Configuring the MSTI cost for a bridge port

Each bridge port mapped to an MSTI must be assigned a cost. The cost is used to determine the path costs of each bridge port and which bridge ports will forward traffic.

To configure the MSTI cost for an MSTI-enabled bridge port, do the following:

1. Navigate to **Layer 2 » Spanning Tree » MSTP Ports**.
2. Under **Interface Selection**, select a bridge port.

3. Under **MST Ports**, configure **Cost**.
Options include:
 - { number } - A specific cost
 - **auto** - The standard RSTP port cost is negotiated automatically (i.e. 20000 for 1 Gbps links, 200000 for 100 Mbps links, 2000000 for 10 Mbps links)
 Default: **auto**
4. Commit the change.

10.1.7 Monitoring STP

This section describes the various methods for monitoring the Spanning Tree service.

10.1.7.1 Displaying the status of STP

To display the status of the Spanning Tree service, as well as related statistics, navigate to **Layer 2 » Spanning Tree » Spanning Tree General**.

The following information is displayed under **Spanning Tree General Status**:

Parameter	Description
Bridge Status	The Spanning Tree status of the bridge. Possible values: <ul style="list-style-type: none"> • unknown - The bridge status is undetermined • designated-bridge - The bridge is a designated bridge • not-designated-for-any-lan - No VLANs are assigned to the bridge • root-bridge - The bridge is the root bridge
Bridge ID	The bridge ID for the device. The ID is a combination of its bridge priority and its MAC address.
Root ID	The bridge ID for the root bridge. The ID is a combination of its bridge priority and its MAC address.
Root Port	The port that provides connectivity towards the root bridge.
Root Cost	The root path cost, which is the sum of the costs of each link on the path to the root bridge.
Learned Hello Time	The Hello time learned by the device from its root bridge. The root bridge sets the Hello time for all designated bridges.
Learned Forward Delay	The forward delay duration learned by the device from its root bridge. The root bridge sets the forward delay timer for all designated bridges.
Learned Max Age	The maximum age time learned by the device from its root bridge. The root bridge sets the maximum age time for all designated bridges.

Parameter	Description
Total Topology Changes	The number of topology changes detected by the device since the statistics were cleared. The device counts topology changes based on link failures it detects and information it receives from neighboring bridges.
Time Since the Last Topology Change	The time since the last topology change occurred. Time is displayed in days (D), hours (H), minutes (M), and seconds (S). For example, the following shows it has been 1 day, 10 hours, 33 minutes, and 40 seconds ago since the last topology change. "1D10h33m40s"

10.1.7.2 Displaying the status of STP per bridge port

To display the status of a bridge port for which Spanning Tree is enabled, navigate to **Layer 2 » Spanning Tree » Spanning Tree Ports**.

The following information is displayed for each bridge port under **Spanning Tree Ports**:

Parameter	Description
State	The state of the bridge port. Possible values: <ul style="list-style-type: none"> • disabled - STP is disabled for the bridge port • blocking - The bridge port is blocking STP traffic • learning - The bridge port is learning MAC addresses to prevent flooding when it begins forwarding traffic • forwarding - The bridge port is forwarding traffic • linkdown - STP is enabled on the bridge port, but the link is down • discarding - The link is not used in the Spanning Tree topology, but it is standing by
Role	The role of the bridge port. Possible values: <ul style="list-style-type: none"> • designated - The bridge port carries traffic towards for the LAN to which it is connected. • root - The bridge port provides connectivity towards the root bridge. • backup - The bridge port is attached to a LAN that is serviced by another port on the bridge. It is not used, but it is standing by. • alternate - The bridge port is attached to a bridge that provides connectivity to the root bridge. It is not used, but it is standing by. • master - This role is only applicable to MSTP. The bridge port is an MST region boundary port. It is the only port on the bridge that provides connectivity for the MSTI towards the CST root bridge.

Parameter	Description
Oper Cost	The operational cost of the bridge port. A bridge port that transitions to STP will have its operational cost limited to 65535.
rs-rst	The number of RSTP configuration messages received by the bridge port.
tx-rst	The number of RSTP configuration messages sent by the bridge port.
Designated Bridge ID	The designated bridge ID for the bridge port. The designated bridge ID is the ID of the bridge to which a bridge port is connected. The ID of the bridge is a combination of the bridge's designated bridge priority and its MAC address.
Oper Edge	The operational edge state of a bridge port. Possible values: <ul style="list-style-type: none"> true - the bridge port is an edge port false - the bridge port is not an edge port

10.1.7.3 Displaying MSTP region information

To display information about the MSTP region, navigate to **Layer 2 » Spanning Tree » MSTP General**.

The following information is provided under **MSTP General**:

Parameter	Description
Regional Root ID	The MSTP regional root ID. The ID is a combination of the priority and the device's MAC address.
Regional Root Cost	The CIST external root path cost, which is the total cost of each link between the IST root bridge (i.e. regional root), and the CST root bridge (i.e. network root).
Region Digest	A 16-octet signature that details characteristics of the region. The region (or configuration) digest is included in each BPDU forwarded by a bridge. For consistent VLAN to MST instance mapping within a region, it is necessary for each bridge to determine exactly the boundaries of its MST region. To this end, bridges compare their region digests to determine if they are allocating the same VLAN IDs to the spanning trees in their MST region as their neighbors.

10.1.7.4 Displaying the status of an MSTI

To display the status of an MSTI, navigate to **Layer 2 » Spanning Tree » MSTP General**.

The following information is provided under **MSTP Instances** for each MSTI:

Parameter	Description
Bridge Status	The bridge status of the MSTI. Possible values: <ul style="list-style-type: none"> • <code>unknown</code> - The bridge status cannot be determined • <code>root-bridge</code> - The MSTI is the root bridge • <code>designated-bridge</code> - The MSTI is the designated bridge • <code>not-designated-for-any-lan</code> - The MSTI is not designated for any LAN
Bridge ID	The MSTI's bridge ID. The ID is a combination of the bridge priority and the device's MAC address. Note that a bridge ID is only assigned to an MSTI once it is mapped to a VLAN.
Root ID	The MSTI's root ID. The ID is a combination of the bridge priority and the device's MAC address. Note that a root ID is only assigned to an MSTI once it is mapped to a VLAN.
Root Port	The bridge port that provides connectivity towards the root bridge of the MSTP network. A root port is only displayed when the MSTI is the designated bridge.
Root Cost	The root path cost, which is the total cost of each link on the path to the root bridge. For the Common and Internal Spanning Tree (CIST), the root path cost is an external root path cost, which is the cost of the path from the Internal Spanning Tree (IST) root bridge to the Common Spanning Tree (CST) root bridge.
Total Topology Changes	The total number of topology changes. An excessively high count or rapidly increasing counts indicate network issues.

10.1.7.5 Displaying the status of an MSTI per bridge port

To display the status of an MSTI-enabled bridge port, navigate to **Layer 2 » Spanning Tree » MSTP Ports**.

The following information is provided under **MSTP Ports** for each MSTI:

Parameter	Description
Instance ID	The ID of the MSTI.
State	<p>The state of the MSTI.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • disabled - STP is disabled on the port • blocking - The port is blocking traffic • learning - The port is learning MAC addresses to prevent flooding when it begins forwarding traffic • forwarding - The port is forwarding traffic • linkdown - STP is enabled on the port, but the link is down • discarding - The link is not used in the STP topology, but is standing by
Role	<p>The role of the MSTI in the MSTP network.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • designated - The port is designated for (i.e. carries traffic towards the root for) the LAN to which it is connected. • root - The single port on the bridge, which provides connectivity towards the root bridge. • backup - The port is attached to a LAN that is serviced by another port on the bridge. It is not used, but is standing by. • alternate - The port is attached to a bridge that provides connectivity to the root bridge. It is not used, but is standing by. • master - The port is an MST region boundary port and the single port on the bridge. The port provides connectivity for the MSTI towards the Common Spanning Tree (CST) root bridge. It is the root port for the Common Spanning Tree Instance (CSTI).
Bridge Port Cost	The operational cost of the MSTI.
Designated Bridge ID	<p>The MSTI designated bridge ID for the bridge port.</p> <p>The MSTI designated bridge ID is the ID of the bridge to which the bridge port is connected. The ID is a combination of the bridge's priority and MAC address.</p>

10.1.8 Configuration Examples

The following configuration examples demonstrate how to configure Spanning Tree.

10.1.8.1 A basic MSTP configuration

In this example, two devices (A and B) receive multicast traffic from separate sources and then forward both streams to devices on their shared LAN segment. MSTP is enabled to prevent traffic loops.

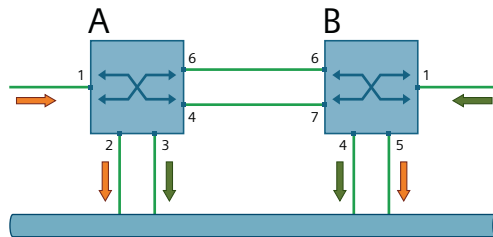


Figure 10-5 Example of a Basic MSTP Configuration

Configuration of Device A

To configure device A, do the following:

1. Create VLANs 10 and 20.
For more information, refer to "Adding or modifying a static VLAN (Page 296)".
2. Create VLAN interfaces for the new VLANs.
For more information, refer to "Adding a VLAN interface (Page 180)".
3. Map VLAN 10 to bridge ports ethernet0/1, ethernet0/2, and ethernet0/6.
For more information, refer to "Configuring the port VLAN ID (Page 298)".
4. Map VLAN 20 to bridge ports ethernet0/3 and ethernet0/4.
For more information, refer to "Configuring the port VLAN ID (Page 298)".
5. Assign the IP address `192.168.10.1` to the VLAN10 interface.
For more information, refer to "Configuring a static IPv4 address (Page 193)".
6. Assign the IP address `192.168.20.1` to the VLAN20 interface.
For more information, refer to "Configuring a static IPv4 address (Page 193)".
7. Set the port membership type to `trunk` for bridge ports ethernet0/4 and ethernet0/6.
For more information, refer to "Selecting the port membership type (Page 298)".
8. Set the Spanning Tree version to `mstp`.
For more information, refer to "Selecting the STP version (Page 218)".
9. Set the name of the MSTP region to `sinecos`.
For more information, refer to "Adding the region name (Page 230)".
10. Set the region revision level for the MSTP region to 1.
For more information, refer to "Configuring the region revision level (Page 230)".
11. Map VLAN 10 to MSTI 1 and VLAN 20 to MSTI 2.
For more information, refer to "Mapping a VLAN to an MSTI (Page 233)".

Configuration of Device B

To configure device B, do the following:

1. Create VLANs 10 and 20.
For more information, refer to "AUTOHOTSPOT".
2. Create VLAN interfaces for the new VLANs.
For more information, refer to "Adding a VLAN interface (Page 180)".
3. Map VLAN 10 to bridge ports ethernet0/5 and ethernet0/6.
For more information, refer to "Configuring the port VLAN ID (Page 298)".
4. Map VLAN 20 to bridge ports ethernet0/1, ethernet0/4, and ethernet0/7.
For more information, refer to "Configuring the port VLAN ID (Page 298)".
5. Assign the IP address 192.168.10.2 to the VLAN10 interface.
For more information, refer to "Configuring a static IPv4 address (Page 193)".
6. Assign the IP address 192.168.20.2 to the VLAN20 interface.
For more information, refer to "Configuring a static IPv4 address (Page 193)".
7. Set the port membership type to `trunk` for bridge ports ethernet0/6 and ethernet0/7.
For more information, refer to "Selecting the port membership type (Page 298)".
8. Set the Spanning Tree version to `mstp`.
For more information, refer to "Selecting the STP version (Page 218)".
9. Set the name of the MSTP region to `sinecos`.
For more information, refer to "Adding the region name (Page 230)".
10. Set the region revision level for the MSTP region to 1.
For more information, refer to "Configuring the region revision level (Page 230)".
11. Map VLAN 10 to MSTI 1 and VLAN 20 to MSTI 2.
For more information, refer to "Mapping a VLAN to an MSTI (Page 233)".

10.2 Loop Detection

This section describes how to use and configure Loop Detection for detecting and resolving network loops.

10.2.1 Understanding the detection of network loops

Loop Detection is a proprietary protocol. The main application of the function is the detection of network loops and to limit their effects.

Network loops are faults in the network design. They are formed when two bridge ports of the same device are connected to one another or if there are at least two active connections between two devices that are not managed by a protocol (e.g. Spanning Tree). One cause can be an improperly connected cable, for example, during the commissioning and servicing of a facility.

A network loop results in circulating frames that are duplicated continuously and thus flood the network. Loops can turn broadcast frames into a broadcast storm in seconds. The growing

number of frames results in an overload of the network and loss of packets. The high network load also severely limits diagnostics.

Bridge ports that were configured to detect loops cyclically send Protocol Data Units (PDUs) to a specified multicast address to detect network loops. A loop exists if the same device that sent the PDU also receives it.

You can configure how the Loop Detection reacts to a recognized network loop and how it signals such a loop. By default, the function disables the bridge port that sends the PDUs and signals the loop as follows:

- The event is recorded in the system log.
- The signaling contact is triggered.
- The alarm LED is lit.

When a network loop occurs, the network must be checked by a network administrator. Network loops can be eliminated, for example, by changing the topology, adjusting the cabling or disabling bridge ports.

10.2.1.1 Port modes

When Loop Detection is enabled, you can configure the following modes for the bridge ports:

- **sending mode**
The bridge port sends PDUs and forwards PDUs.
To detect a network loop, a device must send its own PDUs. Therefore, configure the **sending** parameter for at least one bridge port of the device.
Note the PDUs sent for the detection of network loops result in an additional network load. Be careful when selecting the bridge ports that are sending PDUs, such as those at the branches of a ring (P1 in the example below).
- **forwarding mode**
The bridge port only forwards PDUs.
Loops can only be detected between bridge ports that at least forward the PDUs. Therefore, configure the **forwarding** parameter for additional bridge ports (P2 in the example below).
- **blocking mode**
The bridge port sends no PDUs and does not forward PDUs.
When PDUs interfere with traffic, configure the **blocking** parameter for the respective bridge ports. For example:
 - For adjoining network segments in which Loop Detection is not enabled (P3 in the example below)
 - For connected terminal devices (P4 in the example below)

The following example shows a switch and the various port modes for Loop Detection:

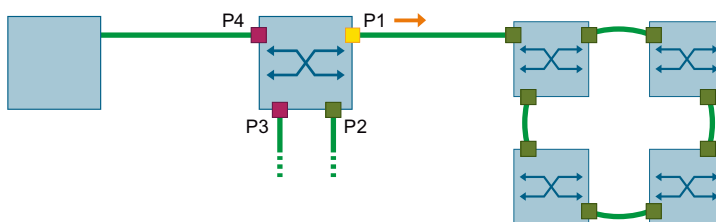


Figure 10-6 Port modes of Loop Detection

10.2.1.2 Types of network loops

Loop Detection distinguishes between the following types of loops:

- **Local network loop**

A local loop exists when a device receives a sent PDU at a different bridge port.

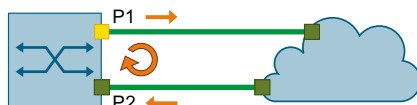


Figure 10-7 Local network loop

Loop Detection can interrupt a local loop by disabling the bridge port that sent the PDU.

- **Remote network loop**

A remote loop exists when a device receives a sent PDU at the same bridge port.

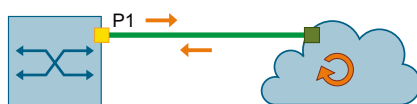


Figure 10-8 Remote network loop

Loop Detection cannot interrupt a remote loop but limit its negative effects. By disabling the bridge port of the device, the function prevents connected network segments from being flooded with circulating frames.

10.2.1.3 VLAN mode

By default, only the physical level is examined during the detection of network loops. In a network with VLAN configuration, Loop Detection may detect physical loops that do not impair data traffic. The affected bridge ports can be logically separated by a VLAN configuration.

When VLAN Mode is active, the function takes into account the VLAN configuration of the bridge ports when processing PDUs. For a device that receives a PDU that it has sent, the function can only detect a loop when the PDU is sent and received on the same VLAN.

10.2.1.4 Related events

The following events are triggered by Loop Detection and recorded directly in the Syslog.

Event	Severity	Syslog message
Local loop detected	Error	"Loop Detection" has detected a local loop.
Remote loop detected	Error	"Loop Detection" has detected a remote loop.

10.2.2 Configuring the detection of network loops

Note

Use the function specifically in network segments where Spanning Tree is not configured and the network stations do not forward Spanning Tree Bridge PDUs.

Note

The detection of network loops does not replace other functions such as Spanning Tree or redundancy protocols.

Note

The function is interface-based and can be configured for individual or bundled bridge ports.

To configure Loop Detection, do the following:

1. Configure how a bridge port processes PDUs for the detection of network loops.
For more information, refer to "Configuring bridge ports for the detection of network loops (Page 245)".
2. [Optional] Configure the interval at which a bridge port sends PDUs.
For more information, refer to "Configuring the send interval (Page 245)".
3. [Optional] Define the number of received PDUs after which the function detects a local network loop.
For more information, refer to "Defining the limit for the detection of a local network loop (Page 245)".
4. [Optional] Configure the effects on a bridge port when a local network loop is detected.
For more information, refer to "Configuring the reaction to local network loops (Page 246)".
5. [Optional] Configure the effects on a bridge port when a remote network loop is detected.
For more information, refer to "Configuring the reaction to remote network loops (Page 247)".
6. [Optional] Define in seconds the duration for which a bridge port is disabled when a loop is detected in the network.
For more information, refer to "Configuring the duration for disabling a bridge port (Page 247)".
7. Enable taking into account the VLAN configuration of a bridge port.
For more information, refer to "Enabling VLAN mode (Page 248)".
8. Enable Loop Detection.
For more information, refer to "Enabling Loop Detection (Page 248)".
9. [Optional] Reset a bridge port manually after a loop has been removed from the network.
For more information, refer to "Resetting a bridge port manually after detection of a network loop (Page 249)".

10.2.2.1 Configuring bridge ports for the detection of network loops

Note the layout of the network when configuring bridge ports. For more information, refer to "Port modes (Page 242)".

To configure how a bridge port processes PDUs for the detection of network loops, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
2. Under **Loop Detection**, configure the **Transmission State** for the selected bridge port. Options include:

Option	Description
Forwarding	Default The bridge port only forwards PDUs.
Sending	The bridge port sends PDUs and forwards PDUs.
Blocking	The bridge port sends no PDUs and does not forward PDUs.

3. Commit the change.

10.2.2.2 Configuring the send interval

The send interval defines the time that passes between the transmission of consecutive PDUs for the detection of network loops.

The interval is only applied when it is configured for a bridge port that it sends and forwards PDUs (Sending parameter). For more information, refer to "Configuring bridge ports for the detection of network loops (Page 245)".

To configure the send interval for PDUs, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
2. Under **Loop Detection**, configure **Transmission Interval** for the selected bridge port. Conditions:
 - Formatted as nYnMnDnhnmns, where n is a user-defined number
 - Minimum 0.5 seconds (0.5 s)
 - Maximum 5 seconds (5 s)
 Default: 1 s (1 second)
3. Commit the change.

10.2.2.3 Defining the limit for the detection of a local network loop

To detect a network loop, a bridge port must receive a defined number of consecutive PDUs that it has sent itself.

You can configure this limit for local network loops. A remote network loop is detected as soon as a bridge port receives the first PDU that it sent itself.

It is recommended to use different limits for each device in a network. In a tree topology, it makes sense to assign the devices a limit that is decreasing from top to bottom. With this

configuration, the local devices (③ in the figure) react first and disable a specific bridge port before higher-level devices (② or ①) separate an entire cell.

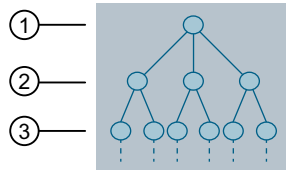


Figure 10-9 Tree topology

To define the limit for the detection of a local network loop, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
2. Under **Loop Detection**, configure **Threshold** for the selected bridge port.
Condition:
 - A number between 1 and 500
 Default: 2
3. Commit the change.

10.2.2.4 Configuring the reaction to local network loops

A local network loop is detected when the number of received PDUs at a bridge port exceeds the limit.

To configure the effects of a local network loop on a bridge port, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
2. Under **Loop Detection**, configure **Local Reaction** for the selected bridge port.
Options include:

Option	Description
Disable Interface	<p>Default</p> <p>As soon as the function detects a local network loop, it disables the bridge port. The network loop is interrupted.</p> <p>The following options are available to enable the bridge port again:</p> <ul style="list-style-type: none"> • You reset the bridge port manually. For more information, refer to "Resetting a bridge port manually after detection of a network loop (Page 249)". • When a link-down event occurs at a disabled bridge port, the function resets the bridge port to the state that it was in before the network loop. • The timer for disabling a bridge port has elapsed. For more information, refer to "Configuring the duration for disabling a bridge port (Page 247)".
No Reaction	A local network loop has no effects on the bridge port.

3. Commit the change.

10.2.2.5 Configuring the reaction to remote network loops

As soon as a bridge port receives the first PDU that it sent itself, a remote network loop is detected.

To configure the effects of a remote network loop on a bridge port, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
2. Under **Loop Detection**, configure **Remote Reaction** for the selected bridge port. Options include:

Option	Description
Disable Interface	<p>Default</p> <p>As soon as the function detects a remote network loop, it disables the bridge port. This does not interrupt the network loop but connected network segments are not flooded by circulating frames.</p> <p>The following options are available to enable the bridge port again:</p> <ul style="list-style-type: none"> • You reset the bridge port manually. For more information, refer to "Resetting a bridge port manually after detection of a network loop (Page 249)". • When a link-down event occurs at a disabled bridge port, the function resets the bridge port to the state that it was in before the network loop. • The timer for disabling a bridge port has elapsed. For more information, refer to "Configuring the duration for disabling a bridge port (Page 247)".
No Reaction	A remote network loop has no effects on the bridge port.

3. Commit the change.

10.2.2.6 Configuring the duration for disabling a bridge port

Temporary network loops can occur especially during the commissioning or maintenance of a plant. When the function disables a bridge port as soon as a loop was detected, you can use this parameter to specify how long the bridge port remains disabled. Loop Detection waits for the configured duration to expire and resets the bridge port to the state that it was in before it was disabled.

When the network loop still occurs, the network must be checked by a network administrator.

You can only configure the timeout when it has been configured for a bridge port that it is disabled by a local as well as a remote network loop.

To configure the duration for disabling a bridge port, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
2. Make sure the bridge port for which you want to configure the timeout is configured as follows:
 - Under **Loop Detection**, set **Local Reaction** to **Disable Interface**.
The bridge port is disabled in the event of a local network loop.
For more information, refer to "Configuring the reaction to local network loops (Page 246)".
 - Under **Loop Detection**, set **Remote Reaction** to **Disable Interface**.
The bridge port is disabled in the event of a remote network loop.
For more information, refer to "Configuring the reaction to remote network loops (Page 247)".
3. Under **Loop Detection** you configure the **Reaction Timeout** parameter for the corresponding bridge port.
The bridge port is enabled again after the timer has elapsed.
When the value **0s** is configured, the bridge port is not automatically enabled again. Check the network and reset the bridge port manually. For more information, refer to "Resetting a bridge port manually after detection of a network loop (Page 249)".
Conditions:
 - Formatted as nYnMnDnhnmns, where n is a user-defined number
 - Minimum 0 seconds (0s)
 - Maximum 86400 seconds (86400 s)Default: 0s (0 seconds)
4. Commit the change.

10.2.2.7 Enabling VLAN mode

Enable VLAN mode to take into account the VLAN configuration of the bridge port when processing PDUs. When VLAN mode is enabled, a loop is only detected when the device receives its own PDU that was sent and received on the same VLAN.

VLAN mode is disabled by default.

To enable VLAN mode for all Loop Detection bridge ports, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
2. Under **Loop Detection**, change **VLAN Loop Detection** to **Enabled**.
3. Commit the change.

10.2.2.8 Enabling Loop Detection

By default, Loop Detection is disabled for all bridge ports.

To enable Loop Detection for all bridge ports, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
2. Under **Loop Detection**, change **Loop Detection** to **Enabled**.
3. Commit the change.

10.2.2.9 Resetting a bridge port manually after detection of a network loop

When the device does not automatically reset a bridge port after detecting a network loop, you can reset the bridge port manually to the state that it was in before the network loop.

To reset a bridge port manually, do the following:

1. Navigate to **Layer 2 » Loop Detection**.
2. To reset the bridge port manually, click **Reset** in the last column.

10.2.3 Showing the status of Loop Detection

To display the status of the Loop Detection, navigate to **Layer 2 » Loop Detection**.

The following information is displayed under **Loop Detection**:

Parameter	Description
Operational State	Shows the operating status of Loop Detection. Options include: <ul style="list-style-type: none"> • disabled - This operating state means: <ul style="list-style-type: none"> – Loop Detection is disabled and the bridge port does not send any PDUs – Loop Detection is enabled, but the bridge port is in a link-down state • active - Loop Detection is enabled. PDUs are sent or forwarded at the bridge port. • detected-local-loop - Loop Detection has detected a local network loop. • detected-remote-loop - Loop Detection has detected a remote network loop.
Ingress Interface	Bridge port at which own PDU was received For a remote network loop, this parameter is not displayed. The device receives its PDU at the bridge port for which the status is displayed.
Ingress VLAN ID	VLAN ID of the bridge port at which own PDU was received This parameter is only displayed when VLAN mode is enabled.

10.3 Device Level Ring

Device Level Ring (DLR) is a Layer 2 redundancy method for EtherNet/IP. This makes it possible to establish ring topologies with EtherNet/IP. When the communication chain is interrupted, communication over a redundant path is maintained.

DLR provides the following benefits:

- Media redundancy
- A single fault in the communication change does not restrict the reachability of individual stations.
- Fast fault detection and reconfiguration after the occurrence of a single fault

Note

DLR is not fully described in this document. You will find more detailed information on DLR on the Open DeviceNet Vendor Association (ODVA) (<https://www.odva.org/>) website.

10.3.1 Understanding DLR

In a DLR network, every network node has one of the following roles:

- Ring Supervisor
- Ring Node

Each network node is integrated in the network via 2 Ethernet ports. This creates a ring topology in which each node is connected with 2 different neighbor nodes. To prevent network loops, a network node (the active ring supervisor) blocks one of its DLR ports.

10.3.1.1 Ring Supervisor

DLR distinguishes between active and backup ring supervisors:

- **Active ring supervisor**

An active ring supervisor has the following tasks:

- Manages the DLR network
- Regularly sends Beacon and Announce frames
A ring supervisor requires the ability to send and process Beacon frames with the default send interval of 400 μ s.
- Constantly monitors the status of the DLR network
- Detects faults in the DLR network
- Collects diagnostics information via the DLR network

- **Backup ring supervisor**

If the active ring supervisor fails, the backup ring supervisor takes over management of the DLR network.

As backup ring supervisor, the device acts like a Beacon-based ring node.

There must be one active ring supervisor in a DLR network. Backup ring supervisors are recommended, but not essential.

A precedence is configured for each ring supervisor. The ring supervisor with the highest precedence value acts as active ring supervisor. If 2 ring supervisors have the same precedence value, the ring supervisor with the numerically highest MAC address becomes the active ring supervisor. All other ring supervisors become the backup ring supervisor.

10.3.1.2 Ring Nodes

Network nodes without supervisor properties are classified as follows:

- **Beacon-based ring node**

A Beacon-based ring node has the following tasks:

- Processes Beacon frames to track the status of the DLR network
- Requires corresponding hardware support to not have to process the Beacon frames in the CPU
- Forwards Announce frames
- Learns the new network topology in the event of a fault
- Informs the ring supervisor about faults in the DLR

- **Announce-based ring node**

An Announce-based ring node has the following tasks:

- Forwards Beacon frames
- Processes Announce frames to track the status of the DLR network
- Learns the new network topology in the event of a fault
- Informs the ring supervisor about faults in the DLR

Note

SINEC OS devices can only be operated as Announce-based ring nodes.

10.3.1.3 DLR Frames

Beacon and Announce frames are both used to inform the ring nodes about the current status of the DLR network.

The two frame types differ in the following ways:

- **Beacon frames**
 - The ring supervisor sends Beacon frames with a send interval of 400 μ s by default.
 - The ring supervisor sends Beacon frames over both DLR ports.
 - Beacon frames contain the precedence value of the ring supervisor that sent the frame.
 - Through the loss of Beacon frames, the ring supervisor detects faults in the DLR network.
- **Announce frames**
 - The ring supervisor sends Announce frames with a send interval of 1 s by default, or immediately when a fault is detected.
 - The ring supervisor sends Announce frames only over one of its DLR ports.

Note

Due to the different send intervals, DLR networks with Announce-based ring nodes have longer recovery times than with Beacon-based ring nodes.

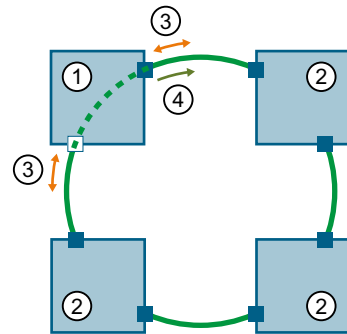
10.3.1.4 DLR Network

DLR distinguishes between the following states:

- **Normal state**

The DLR network is in the normal state when the active ring supervisor has blocked one of its DLR ports. In this state, the active ring supervisor sends Beacon and Announce frames (also over the blocked DLR port) to monitor the status of the DLR network. All other ring nodes process the frames according to their abilities.

As long as the active ring supervisor receives its sent Beacon frames again, all communication paths in the DLR network are intact.



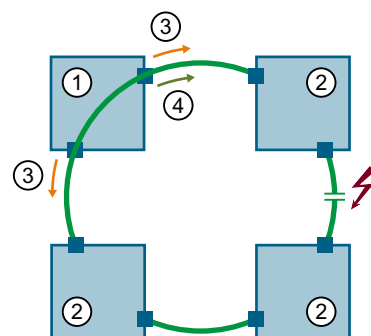
- ① Active ring supervisor
- ② Ring node
- ③ Beacon frames
- ④ Announce frames

Figure 10-10 DLR network in normal state

- **Error state**

If the communication chain is broken at one point, e.g. when a cable is disconnected or a station fails, the Beacon frames no longer arrive at the active ring supervisor. The ring supervisor enables its blocked DLR port and thus the alternative communication path. It informs the ring nodes about the fault. The ring nodes learn the new communication path. The DLR network is in the error state.

As soon as the reconfiguration is complete, communication between all network nodes is possible again.



- ① Active ring supervisor
- ② Ring node
- ③ Beacon frames
- ④ Announce frames

Figure 10-11 DLR network in error state

10.3.2 Configuring DLR

To configure DLR, do the following:

1. Enable EtherNet/IP.
For more information, refer to "Enabling EtherNet/IP (Page 275)".
2. Add a static VLAN for DLR.
For more information, refer to "Adding or modifying a static VLAN (Page 296)".
3. Configure the ports that you wish to use as DLR ports as trunk ports.
For more information, refer to "Selecting the port membership type (Page 298)".
4. [Optional] Make sure that the ports that you wish to use as DLR ports are tagged members in the DLR VLAN.
This configuration is only necessary if the DLR VLAN corresponds to the native VLAN of the DLR ring ports.
For more information, refer to "Enabling PVID tagging on egress traffic (Page 299)".
5. Disable STP for the ports that you wish to use as DLR ports.
For more information, refer to "AUTOHOTSPOT".
6. Select the DLR VLAN.
For more information, refer to "Selecting the DLR VLAN (Page 254)".
7. Select the DLR ports.
For more information, refer to "Selecting the DLR Ports (Page 255)".
8. Enable DLR.
For more information, refer to "Enabling DLR (Page 255)".

10.3.2.1 Selecting the DLR VLAN

To select the VLAN in which DLR frames are sent, do the following:

1. Make sure that the desired VLAN is configured for DLR.
For more information on adding a static VLAN, refer to "Adding or modifying a static VLAN (Page 296)".
2. Navigate to **System** » **EtherNet/IP & DLR**.
3. Under **EtherNet/IP**, select the VLAN for DLR under **DLR VLAN ID**.
4. Commit the change.

10.3.2.2 Selecting the DLR Ports

To select the DLR ports, do the following:

1. Make sure that both ports that you wish to use as DLR ports are configured as trunk ports. For more information on configuring the type of port membership, refer to "Selecting the port membership type (Page 298)".
2. [Optional] Make sure that the ports that you wish to use as DLR ports are tagged members in the DLR VLAN.
This configuration is only necessary if the DLR VLAN corresponds to the native VLAN of the DLR ring ports.
For more information on configuring the type of port membership, refer to "Enabling PVID tagging on egress traffic (Page 299)".
3. Make sure that STP is disabled for the ports that you wish to use as DLR ports.
For more information on configuring STP for a bridge port, refer to "AUTOHOTSPOT".
4. Navigate to **System » EtherNet/IP & DLR**.
5. Under **EtherNet/IP**, select the first DLR port under **DLR Port 1**.
6. Select the second DLR port under **DLR Port 2**.
7. Commit the changes.

10.3.2.3 Enabling DLR

DLR is disabled by default.

To enable DLR, do the following:

1. Navigate to **System » EtherNet/IP & DLR**.
2. Under **EtherNet/IP**, change the parameter **DLR** to **Enabled**.
3. Commit the change.

10.3.3 Monitoring DLR

To monitor the DLR network, navigate to **System » EtherNet/IP & DLR**.

The following information is displayed under **Device Level Ring** :

Parameter	Description
Supervisor IP Address	Shows the IP address of the active ring supervisor.
Supervisor MAC Address	Shows the MAC address of the active ring supervisor.

Parameter	Description
Ring Topology	Shows the current topology of the DLR network. Possible values include: <ul style="list-style-type: none"> • linear - The linear topology means that a ring node has no connection to the active ring supervisor and does not receive any supervisor frames. The device is in the status (Node State) idle still or again. • ring - The ring topology means that a ring node is in the status (Node State) normal or fault, i.e. receives supervisor frames. The device has at least one connection to the active ring supervisor.
Ring State	Shows whether the ring is open or closed. Possible values include: <ul style="list-style-type: none"> • normal - The active ring supervisor has blocked one of its DLR ports. Communication in the network works in a line topology. • fault - The active ring supervisor has enabled its blocked DLR port. Communication in the network is reconfigured to the alternative communication path.
Node State	Shows the internal status of an Announce-based ring node (SINEC OS device). Possible values include: <ul style="list-style-type: none"> • idle - The initial status of the device. The device changes to the idle status if it does not receive any Announce frames. • fault - The device has the status fault if a fault has been detected in the network. • normal - The device has the status normal if communication with all network nodes is possible.
Network Status	Shows the current status of the DLR network. Possible values include: <ul style="list-style-type: none"> • normal - Communication is possible between all network nodes. • ring fault - A fault was detected in the network.
Ring Port 1 Status	Shows the current status of the DLR port 1. Possible values include: <ul style="list-style-type: none"> • up - The interface is enabled. • down - The interface is disabled.
Ring Port 2 Status	Shows the current status of the DLR port 2. Possible values include: <ul style="list-style-type: none"> • up - The interface is enabled. • down - The interface is disabled.

10.3.4 Configuration examples

Below, you will find examples for the use of DLR.

10.3.4.1 Using DLR in VLAN 0

Because frames that are tagged with a VLAN ID of 0 are handled separately, it is possible to operate a ring across VLAN limits. The ring nodes can be members in different VLANs.

To configure a SINEC OS device in such a way that it can participate in a DLR in VLAN 0, follow these steps:

1. [Optional] Make sure that the ports that you wish to use as DLR ports are configured as access ports.
For more information, refer to "Selecting the port membership type (Page 298)".
2. Disable STP for the ports that you wish to use as DLR ports.
For more information, refer to "AUTOHOTSPOT".
3. Configure EtherNet/IP.
For more information, refer to "Configuring EtherNet/IP (Page 274)".
4. Select the DLR ports.
For more information, refer to "Selecting the DLR Ports (Page 255)".
5. Configure the same native VLAN for both DLR ports.
For more information, refer to "Configuring the port VLAN ID (Page 298)".
6. Enable VLAN 0 tunnel mode for the native VLAN of the DLR ports.
For more information, refer to "Enabling VLAN-0-Tunnel mode (Page 297)".
7. Enable DLR.
For more information, refer to "Enabling DLR (Page 255)".
8. Ensure that **no** DLR VLAN is configured.
For more information, refer to "Selecting the DLR VLAN (Page 254)".

Network discovery and management

This chapter describes the various network discovery and management features available. These features allow for the automatic discovery of devices on the network, as well as network monitoring and automated device management.

11.1 LLDP

You can determine the topology of local networks using the Link Layer Discovery Protocol (LLDP). The information on the topology with the physical connections between the network components is a prerequisite for the management of local networks.

11.1.1 Configuring the sending and receiving of LLDPDUs for a bridge port

To configure how a bridge port sends or receives LLDPDUs, do the following:

1. Navigate to **Layer 2 » Network Discovery » LLDP**.
2. Under **LLDP Interfaces**, configure **Local Settings** for the selected bridge port. Options include:

Option	Description
Receive and Transmit	Default LLDPDUs are sent and received on the bridge port.
Disabled	LLDPDUs are neither sent nor received on the bridge port.
Receive	LLDPDUs are received but not sent on the bridge port.
Transmit	LLDPDUs are sent but not received on the bridge port.

3. Commit the change.

11.1.2 Monitoring the LLDP information of neighbor devices

To display the LLDP information of neighbor devices, navigate to **Layer 2 » Network Discovery » LLDP**.

If neighboring devices that support LLDP are connected, the following information is displayed under **Link Layer Discovery Protocol (LLDP) Neighbors**:

Parameter	Description
Local Interface	Port at which the information about the connected device was received
Remote System Name	System name of the connected device

Parameter	Description
Remote Device ID	ID of the connected device The ID corresponds to the device name assigned via SINEC PNI (STEP 7). If no device name is assigned, the MAC address of the device is displayed.
Remote Hold Time	Time period formatted as nYnMnDnhnmns for which LLDP information of the connected device is stored before the device deletes it
Remote Capability	Properties activated on the connected device
Remote Port ID	Port of the connected device

11.2 DCP

SINEC OS supports the Discovery and basic Configuration Protocol (DCP) to recognize devices and for configuring basic network parameters.

11.2.1 Understanding DCP

DCP is used in the PROFINET environment to assign basic parameters to devices, such as the IP address or PROFINET device name. Typically, DCP is used by PROFINET controllers or engineering tools (e.g. SINEC PNI, STEP 7) to find and configure devices. DCP cannot be routed and is limited to the local Layer 2 network.

11.2.2 Configuring DCP

To configure DCP, do the following:

1. Configure the access rights of DCP.
For more information, refer to "Configuring the access rights of DCP (Page 261)".
2. Configure whether DCP frames can be sent from a bridge port.
For more information, refer to "Configuring the sending of DCP frames for a bridge port (Page 263)".

11.2.2.1 Configuring the access rights of DCP

NOTICE
Security hazard - risk of unauthorized access and/or misuse
<p>By definition, DCP is not secure. The access rights of DCP depend on the status of the device.</p> <ul style="list-style-type: none">• In the delivery state and after reset to default settings, DCP is enabled. Device parameters can be both read and modified. The access rights of DCP correspond to the Read-Write option. The Read-Write setting could potentially be used to change the functionality of the device and thus cause the failure of data traffic. Users with malicious intent who are in the same local network segment can change IP parameters and/or the PROFINET device name without authentication.• After the first login with the default user profile admin and the assignment of a new password, the device changes to the secure operating state. In the secure operating state, the access rights of DCP are automatically changed to read-only access. The device parameters can only be read and not modified. The access rights of DCP correspond to the Read-Only option from this time. <p>To prevent unauthorized access and/or misuse, configure write-protected access rights for DCP (Read-Only).</p>

NOTICE
Configuration hazard - risk of connection loss
<p>If you use the device in PROFINET operation with the DCP option <code>read-only</code>, there is a risk of connection losses.</p> <p>Because a PROFINET controller only sets the IP address temporarily by default, the device can lose its IP address on voltage loss (cold restart) or restart (warm restart). Without IP address, the device can only be reached via a serial connection.</p> <p>To set the IP address retentively so that it is retained after a cold or warm restart, you have the following options:</p> <ul style="list-style-type: none">• Assign the IP address manually.• Configure the prioritized startup mode for the device in a configuration tool (STEP 7 or TIA Portal).

To configure the access rights of DCP, do the following:

1. Navigate to **System » PROFINET » DCP**.
2. Under **Discovery and basic Configuration Protocol (DCP)**, configure the access rights of DCP in the **DCP Mode** field.

Options include:

Option	Description
Setup	<p>Default</p> <p>The access rights of DCP depend on the status of the device. In the delivery state and after reset to default settings, DCP is enabled. The device parameters can be both read and modified. The access rights of DCP correspond to the Read-Write option.</p> <p>The following events trigger a status change of the device:</p> <ul style="list-style-type: none"> • The first login with the default user profile admin and the associated assignment of a new password • Loading a configuration file <p>Afterwards, the device is in the secure operating state. The status change takes place automatically and once. In secure operating state, the device parameters can be read but cannot be modified. The access rights of DCP correspond to the Read-Only option from this time.</p>
Read-Write	<p>DCP is enabled. Device parameters can be both read and modified. IP parameters and/or the PROFINET device name can be changed or reset.</p>
Read-Only	<p>DCP is enabled. Device parameters can be read but cannot be modified. The device does not respond to write DCP commands. This means, for example, that no new parameters can be assigned using an engineering tool. The device itself is visible.</p> <p>If you have configured this option and wish to use the device as a PROFINET device, the following settings must match those in the controller:</p> <ul style="list-style-type: none"> • IP address • Subnet mask • Gateway IP address • PROFINET device name <p>If the settings match, DCP assignment is not necessary. The PROFINET communication can take place.</p>
Off	<p>DCP is disabled. Device parameters can neither be read nor modified. The device cannot be operated as a PROFINET device with this setting.</p>

3. Commit the change.

11.2.2.2 Configuring the sending of DCP frames for a bridge port

Receiving of DCP frames cannot be disabled. You can configure whether a bridge port sends DCP frames.

DCP frames are sent and received on all bridge ports by default.

To configure whether DCP frames are sent for a bridge port, do the following:

1. Navigate to **System » PROFINET » DCP**.
2. Under **DCP Forwarding** in the **Forwarding Mode** column, configure whether DCP frames are sent for a bridge port.
Options include:

Option	Description
Receive and Transmit	Default DCP frames are sent and received on the port.
Receive	DCP frames are received but not sent on the port.

3. Commit the change.

11.3 PROFINET

PROFINET (Process Field Network) is an open Ethernet standard for industrial automation. PROFINET uses existing IT standards and enables continuous communication from the field level to the control level, as well as plant-wide engineering.

PROFINET is implemented as follows:

- PROFINET IO enables communications between field devices.
- Installation technology and network components are available as SIMATIC NET products.
- Ethernet standard protocols and procedures are used for remote maintenance and network diagnostics (e.g. SNMP for network parameter assignment and diagnostics).

The IE switch of a PROFINET controller can be configured and exchange diagnostic data via PROFINET.

Note

PROFINET is not fully described in this document. You can find more information on PROFINET as follows:

- A compilation of the most important PROFINET application examples, FAQs and other contributions to Industry Online Support can be found in this FAQ (<https://support.industry.siemens.com/cs/ww/en/view/108165711>).
 - At the Internet address (<http://www.profibus.com>) of the PROFIBUS user organization "PROFIBUS & PROFINET International", which is also responsible for PROFINET.
 - You will find more detailed information on the Siemens website (<http://www.siemens.com/profinet>).
-

11.3.1 Understanding PROFINET

PROFINET as an Ethernet-based automation standard from PROFIBUS International that defines a manufacturer-independent communication, automation and engineering model.

PROFINET is primarily used in industrial automation systems and process control networks where asset management is important.

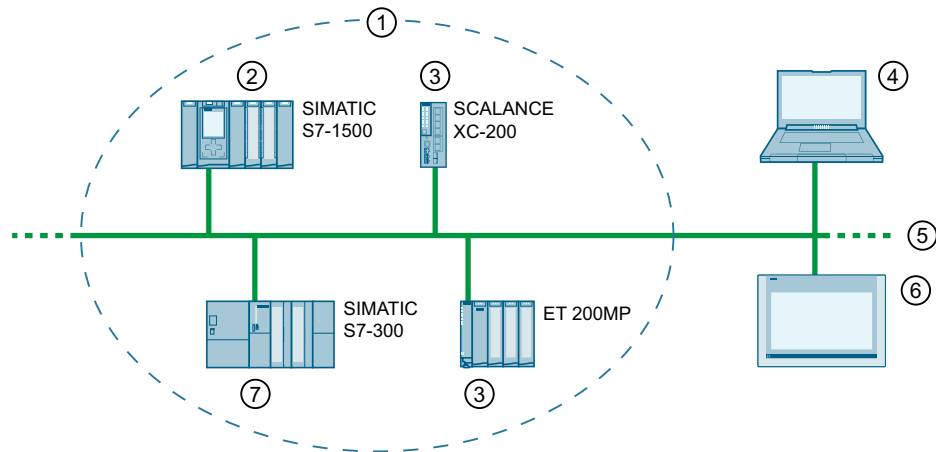
Properties of PROFINET

- Open Ethernet standard based on Industrial Ethernet (IEC 61918, also IEC 61158/61784)
- Compatibility of Industrial Ethernet and standard Ethernet components
- Continuous communication from the field level to the control level as well as plant-wide engineering
- Highly rugged due to Industrial Ethernet devices that are suitable for industrial environments (temperature, immunity to interference, etc.)
- Use of TCP/IP and IT standards
- Real-time capability
- Seamless integration of other fieldbus systems
- High safety, reliability and availability requirements

11.3.1.1 PROFINET components

A PROFINET device always has a PROFINET interface (electrical, optical, wireless).

The following graphic provides an overview of the most important PROFINET components:



PROFINET components	Description
① PROFINET IO system	-
② PROFINET controller	Device via which the connected PROFINET devices are addressed. This means the following: The PROFINET controller exchanges input and output signals with field devices. The PROFINET controller is the controller in which the automation program runs.
③ PROFINET device	A field device in a distributed configuration that is assigned to a PROFINET controller, e.g. distributed IO, valve terminals, frequency converters, switches with integrated PROFINET IO functionality.
④ PG/PC (PROFINET IO Supervisor)	PG/PC/HMI device for commissioning and diagnostics
⑤ PROFINET/Industrial Ethernet	Network infrastructure
⑥ HMI (Human Machine Interface)	Operating and monitoring apparatus
⑦ I-device	Intelligent IO device

Figure 11-1 PROFINET components

11.3.1.2 Device Addressing

Each PROFINET device can be uniquely identified in the network via its PROFINET interface. Every PROFINET interface has this:

- **A MAC address** (default setting)
 - Held by every Ethernet subscriber and is unique worldwide.
 - Used in PROFINET as the source/destination address for cyclic data exchange.
 - Offers little convenience for the device designation, because it cannot be changed.
- **An IP address**
 - Freely assigned by the project engineer and used for acyclic data exchange. This includes the project transfer to the CPU, device configuration by the CPU, reading out device information (e.g. firmware version) or reading out diagnostic information.
 - PROFINET uses the User Datagram Protocol (UDP) for these services. This works on layer 4 and therefore needs an IP address as a base.
 - Written to the devices by the CPU during system startup.
- **A PROFINET device name**
 - Required during system startup. The CPU searches for the devices using the PROFINET device name.
 - Offers a high level of convenience because it is easy to change.
 - Enables device replacement without reconfiguration of the hardware. In contrast, the MAC address would need to be adjusted in the hardware configuration.
 - Can be assigned manually or automatically (naming).

11.3.1.3 PROFINET communication

PROFINET communication takes place via Industrial Ethernet. When doing this, the following transmission modes are supported:

- Acyclic transmission of engineering and diagnostic data and alarms
- Cyclic transmission of user data

Industrial communication, especially in factory and process automation, requires real-time and deterministic data transmission. Real-time means that a system processes external events within a specific time. If the reaction is predictable (deterministic), this is known as a deterministic system.

For cyclic exchange of time-critical IO user data, PROFINET IO therefore does not use TCP/IP but real-time communication (RT) or isochronous real-time communication (IRT) for synchronized data exchange in reserved time intervals.

According to IEEE802.1Q, PROFINET IO frames are given priority over standard frames. This ensures the required deterministic. In this process, the data are transferred using prioritized Ethernet frames.

Real-Time (RT)

In RT communication the cyclic data are transferred between the PROFINET controller and PROFINET device, however, not synchronized.

PROFINET with RT is suitable for:

- Time-critical applications in factory automation
Time-critical data are transferred at guaranteed time intervals.
- Transfer of alarms and cyclic data
- The implementation of large quantities in process plants

Isochronous Real-Time (IRT)

IRT is a synchronized transmission mode. The communication over Ethernet is divided into individual cycles. Each cycle consists of two phases, an IRT channel reserved for extremely time-critical data, and an "open channel", within which RT and non-time critical frames can be sent. This allows time-critical and uncritical data to be sent on the same connection. The reserved IRT channel guarantees the IRT data can be transferred unaffected by other high network loads (e.g. TCP/IP communication or additional real-time communication) at reserved, synchronized intervals.

PROFINET with IRT is suitable for:

- High deterministic even with high network load through standard communication
- The cyclic exchange of IRT data between PROFINET devices
- Parallel transmission of production and TCP/IP data over one line even at high data load ensuring the forwarding of production data through the reservation of the transmission bandwidth.

Non Real-Time (NRT)

NRT communication is non-time -critical communication and corresponds to the communication of Industrial Ethernet with the protocol family TCP/IP. Everything that is transferred using Industrial Ethernet can also be transferred via PROFINET, for example, HTTP, TCP, UDP, SNMP, ARP.

11.3.1.4 PROFINET relations

An Application Relation (AR) is set up between a PROFINET controller and a PROFINET device. Communication relations (CR) with different properties are specified over this AR:

- **Record Data CR** for the acyclic parameter transfer
- **IO Data CR** for the cyclic parameter transfer
- **Alarm CR** for signaling of alarms in real-time

11.3.1.5 I&M data

Identification and maintenance (I&M) data is information stored in a device to assist you with the following tasks:

- Checking the plant configuration
- Locating hardware changes in a plant

I&M data is defined in the PROFINET standard.

11.3 PROFINET

Identification data (I data) is information about the device, such as article number and serial number, some of which is also printed on the device enclosure. I data is manufacturer information about the device and can only be read.

Maintenance data (M data) is plant-dependent information, such as location code and installation date. M data is created during configuration. You can configure M data, for example, with SINEC PNI. With SINEC OS, M data can also be read only.

I&M data can be used to uniquely identify devices online.

11.3.1.6 GSD file

A GSD file contains the specific properties of a device. GSD files are provided in the XML-based language GSDML (General Station Description Markup Language).

To configure a device with a configuration tool (e.g. STEP 7/TIA Portal), the device must be available in the hardware catalog. If the device you are using is not listed in the hardware catalog, you can install the GSD file of the device and thus make the device available in the hardware catalog.

11.3.2 Configuring PROFINET

To configure PROFINET, do the following:

1. [Optional] Configure the TIA interface.
For more information, refer to section "Configuring the TIA interface (Page 268)".
2. Enable PROFINET.
For more information, refer to section "Configuring PROFINET runtime mode (Page 269)".
3. [Optional] Save the GSD file.
For more information, refer to section "Saving the GSD File on a Local Client PC (Page 269)" or "Saving the GSD File on a Remote Server (Page 269)".

11.3.2.1 Configuring the TIA interface

All PROFINET functions of the device are available over the TIA Interface.

The following conditions apply to the TIA Interface:

- There must only ever be one configured TIA Interface.
- Only one IP interface can be configured as TIA Interface.
- The IP interface that is configured as TIA Interface cannot be deleted.

The TIA interface that you configure only becomes active after the next device restart.

The PROFINET runtime mode that you configure will become active after the next device restart.

To configure the TIA Interface, do the following:

1. Navigate to **System » PROFINET » PROFINET Mode**.
2. Select an IP interface under **PROFINET** in the **TIA Interface after Restart** field.
3. Commit the change.

4. To activate the new TIA interface, restart the device.
For more information, refer to "Restarting the device (Page 80)".
The device restarts. When the restart is complete, the login page is displayed.
5. Log in.
For more information, refer to "Logging in to a configured device (Page 75)".

11.3.2.2 Configuring PROFINET runtime mode

The PROFINET runtime mode that you configure will become active after the next device restart.

To configure the PROFINET runtime mode, do the following:

1. Navigate to **System » PROFINET » PROFINET Mode**.
2. Select the PROFINET Runtime Mode under **PROFINET** in the **Runtime Mode after Restart** field.

Options include:

Option	Description
On	Default PROFINET is enabled.
Off	Only DCP and LLDP are enabled.

3. Commit the change.
4. To enable the PROFINET runtime mode, restart the device.
For more information, refer to "Restarting the device (Page 80)".
The device restarts. When the restart is complete, the login page is displayed.
5. Log in.
For more information, refer to "Logging in to a configured device (Page 75)".

11.3.2.3 Saving the GSD File on a Local Client PC

The GSD file in ".xml" format is saved as a ZIP file together with product images in ".bmp" format.

To save the GSD file of the device on a local PC, do the following:

1. Navigate to **System » Load & Save » Data Models**.
2. Under **Save Data Model to Local PC**, select the **GSDML** option for the **File Type** parameter.
3. Click **Save**.

It depends on the browser settings whether the file is saved directly to a specified folder or if you will first see a prompt in which you can select the storage location.

As optical feedback, a load symbol appears beside the button on the right.

- When the save operation is complete, a green check mark appears.
- If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

11.3.2.4 Saving the GSD File on a Remote Server

The GSD file in ".xml" format is saved as a ZIP file together with product images in ".bmp" format.

You can save the GSD file on a remote server.

Requirements

- You have configured a server accordingly.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.

Saving the GSD file

To save the GSD file of the device on a remote server, do the following:

1. Navigate to **System » Load & Save » Data Models**.
2. Under **Save Data Model to Remote Server**, select the **GSDML** option for the **File Type** parameter.
3. Configure the settings for the remote server.
For more information on loading and saving files via a remote server, see "Loading and saving files via a remote server (Page 54)".
4. Click **Save**.
As optical feedback, a load symbol appears beside the button on the right.
 - When the save operation is complete, a green check mark appears.
 - If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

11.3.3 Monitoring PROFINET

This section describes the various ways in which you can monitor PROFINET.

11.3.3.1 Displaying the current PROFINET runtime mode

To display the PROFINET configuration, navigate to **System » PROFINET » PROFINET Mode**.

The following information is displayed under **PROFINET** :

Parameter	Description
Current Runtime Mode	Displays the PROFINET runtime mode. Options include: <ul style="list-style-type: none">• off - Only DCP and LLDP are enabled.• on - PROFINET is enabled.

11.3.3.2 Monitoring the connection to a PROFINET controller

To display the PROFINET configuration, navigate to **System » PROFINET » PROFINET Mode**.

The following information is displayed under **PROFINET** :

Parameter	Description
State of Controller Connection	Shows whether there is a connection to a PROFINET controller. Options include: <ul style="list-style-type: none"> • offline - There is no connection to a PROFINET controller. • online - There is a connection to a PROFINET controller.

11.3.3.3 Monitoring the TIA interface

Note that a change to the TIA interface only becomes active after a restart. A distinction is therefore made between the active and the configured TIA interface.

To monitor the TIA interface, navigate to **System » PROFINET » PROFINET Mode**.

The following information is displayed under **PROFINET** :

Parameter	Description
TIA Interface after Restart	Shows the configured TIA interface. This TIA interface is enabled after the next restart.
Current TIA Interface	Shows the current TIA interface.

11.3.3.4 Displaying the I&M data

Only the I&M data of the device is displayed. The I&M data of lower-level components with their own article numbers is not displayed (e.g. plug-in transceivers).

To show the I&M data of the device, navigate to **System » PROFINET » I & M**.

The following information is displayed under **Identification & Maintenance (I & M)** :

Parameter	Description
Manufacturer ID	Shows the vendor ID.
Order ID	Shows the order number of the device.
Serial Number	Shows the serial number of the device.
Hardware Revision	Shows the hardware version of the device.
Software Revision	Shows the software version currently running on the device.
Revision Counter	Counts the number of software updates performed. Regardless of a version change, this box always displays the value "0".
Revision Date	Shows the date and time of the last change to the plant or location identifier.
Function Tag	Shows the function tag (plant designation) of the device. The plant designation is a unique identification of the device within the plant. You can configure the plant designation, for example, with SINEC PNI.

Parameter	Description
Location Tag	Shows the location identifier of the device. The location identifier is a unique identifier of the device location. You can configure the location identifier, for example, with SINEC PNI.
Date	Shows the date of installation or initial commissioning of the device. You can configure the date, for example, with SINEC PNI.
Descriptor	Displays additional information about the device. You can configure the additional information, for example, with SINEC PNI.

11.3.3.5 Displaying the PROFINET device name

To display the PROFINET configuration, navigate to **System » PROFINET » PROFINET Mode**.

The following information is displayed under **PROFINET** :

Parameter	Description
Name of Station	Shows the PROFINET device name. You configure the PROFINET device name. for example, with SINEC PNI. If you configure the PROFINET device name with SINEC PNI and it does not comply with the rules of IEC 61158-6-10, it is converted accordingly. The converted name is displayed in this field.

Alternatively, navigate to the start page. The PROFINET device name is also displayed under **Information Dashboard » PROFINET Name of Station**.

11.4 EtherNet/IP

Ethernet Industrial Protocol (EtherNet/IP, EIP) is an open industrial standard for industrial real-time Ethernet, based on TCP/IP and UDP/IP.

Note

EtherNet/IP is not fully described in this document. You will find more information on EtherNet/IP on the Open DeviceNet Vendor Association (ODVA) (<https://www.odva.org/>) website.

11.4.1 Understanding EtherNet/IP Protocol

With EtherNet/IP, Ethernet is expanded by the Common Industrial Protocol (CIP) at the application layer. The lower layers of the OSI reference model are taken by EtherNet/IP from Ethernet with the transmission, switching, network and transport functions.

11.4.1.1 Common Industrial Protocol

Common Industrial Protocol (CIP) is an application protocol for automation, which supports the transition of the fieldbuses in industrial Ethernet and in IP networks.

EtherNet/IP uses CIP in the application layer as an interface between the deterministic fieldbus world and the automation application (controller, HMI, OPC, etc). CIP is located above the transport layer and expands the pure transport services with communications services for automation engineering. This includes services for the cyclic, time-critical and event-controlled data traffic.

11.4.1.2 Message Types

CIP distinguishes between the following message types:

- **Implicit messages**
This message type is used to exchange time-critical IO data.
- **Explicit messages**
This message type is used for parameter access (write, read).

In SINEC OS devices, an explicit message server is implemented for EtherNet/IP which responds to the request/answer-controlled communication of explicit network clients.

11.4.1.3 Producer-Consumer Relationship

With CIP, the transfer of messages is based on product-consumer relationships.

In contrast to the traditional addressing scheme, the messages do not contain a destination address, but a unique identifier.

A sender (Producer) sends a message that can be received by one or more receivers (Consumer). Based on the identifiers in the message, the receivers determine whether the data is relevant or not relevant for it. This means that the corresponding data does not need to be sent multiple times from one source to multiple destinations.

A product-consumer relationship is used if fast data exchange without management data is required. In producer-consumer relationships, the network traffic is lower and the transmission speed higher.

11.4.1.4 Object Model

CIP uses an object model to describe devices:

- Application objects define how device information is displayed and made accessible in a generally valid way.
- Network-specific objects define the configuration of parameters (e.g. the IP address).
- Communication objects and services enable the establishment of communication relationships and enable access to device information over the network.

Every CIP object has attributes (data), services (commands), connections and behaviors (relationships between attribute values and services). CIP comprises a comprehensive object library to support general network communication, network services, such as file transfer, and typical automation functions.

11.4.1.5 Supported Objects

The following CIP objects are supported:

Object class	Code	Description
Identity Object	01h	The Identity object enables the identification of EtherNet/IP devices and provides general information about the device. The Vendor ID of Siemens is 1251. The Device Type is 2Ch (Managed Ethernet Switch).
Message Router Object	02h	The Message Router object forwards explicit messages to the corresponding objects.
Ethernet Link Object	F6h	The Ethernet Link object saves link-specific counters and status information of IEEE 802.3 communication interface.
TCP/IP Interface Object	F5h	The TCP/IP Interface object offers a mechanism for configuring the TCP/IP network interface of an EtherNet/IP device. The configurable elements include the IP address, the network mask, the gateway address and the host name of the device.
Connection Manager Object	06h	The Connection Manager object manages the internal resources that are required for implicit and explicit messages.
Assembly Object	04h	The Assembly object enables the assignment of attributes of different EtherNet/IP objects to a data structure that can be transferred as read or write. Process data is typically assembled with the Assembly object.
Base Switch Object	51h	The Base Switch object represents the interface of the CIP application layer to basic status information of a device of the type Managed Ethernet Switch.

11.4.1.6 Electronic Data Sheet

An Electronic Data Sheet (EDS) is an electronic data sheet that serves as common configuration basis. The properties of an EtherNet/IP device are described in an EDS. It contains all information required for device integration in an EtherNet/IP system.

An EDS contains information such as:

- Product symbol
- Manufacturer and device names
- The available cyclic data

11.4.2 Configuring EtherNet/IP

To configure EtherNet/IP, do the following:

1. [Optional] Configure the management interface.
For more information, refer to section "Configuring the Management Interface (Page 275)".
2. Enable EtherNet/IP.
For more information, refer to section "Enabling EtherNet/IP (Page 275)".

3. [Optional] Save the EDS file.
For more information, refer to section "Saving the EDS File on a Local Client PC (Page 275)" or "Saving the EDS File on a Remote Server (Page 276)".
4. [Optional] Configure DLR.
For more information, refer to section "Device Level Ring (Page 250)".

11.4.2.1 Configuring the Management Interface

All EtherNet/IP functions of the device are available over the management interface.

The IP interface **vlan1** is configured by default.

The following conditions apply to the management interface:

- There must only ever be one configured management interface.
- Only one IP interface can be configured as management interface.
- The IP interface that is configured as management interface cannot be deleted.

To configure the management interface, do the following:

1. Navigate to **System** » **EtherNet/IP & DLR**.
2. Select an IP interface under **EtherNet/IP** in the **Management Interface** field.
3. Commit the change.

11.4.2.2 Enabling EtherNet/IP

EtherNet/IP is disabled by default.

To enable EtherNet/IP, do the following:

1. Navigate to **System** » **EtherNet/IP & DLR**.
2. Under **EtherNet/IP**, change the parameter **EtherNet/IP** to **Enabled**.
3. Commit the change.

11.4.2.3 Saving the EDS File on a Local Client PC

The EDS file in the format ".eds" is saved as ZIP file.

To save the EDS file of the device on a local PC, do the following:

1. Navigate to **System** » **Load & Save** » **Data Models**.
2. Under **Save Data Model to Local PC**, select the **EDS** option for the **File Type** parameter.
3. Click **Save**.

It depends on the browser settings whether the file is saved directly to a specified folder or if you will first see a prompt in which you can select the storage location.

As optical feedback, a load symbol appears beside the button on the right.

- When the save operation is complete, a green check mark appears.
- If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

11.4.2.4 Saving the EDS File on a Remote Server

The EDS file in the format ".eds" is saved as ZIP file.

You can save the EDS file on a remote server.

Requirements

- You have configured a server accordingly.
- There is a connection between the device and the server.
- Depending on your configuration, user name and password must be known.

Saving the EDS file

To save the EDS file of the device on a remote server, do the following:

1. Navigate to **System » Load & Save » Data Models**.
2. Under **Save Data Model to Remote Server**, select the **EDS** option for the **File Type** parameter.
3. Configure the settings for the remote server.
For more information on loading and saving files via a remote server, see "Loading and saving files via a remote server (Page 54)".
4. Click **Save**.
As optical feedback, a load symbol appears beside the button on the right.
 - When the save operation is complete, a green check mark appears.
 - If the save operation has failed, a red exclamation mark and an error message are displayed. Repeat the last steps.

11.5 ARP

SINEC OS supports Address Resolution Protocol (ARP) tables for individual bridge ports for IP address resolution.

11.5.1 Understanding ARP

An ARP table, or cache, maintains the internal mapping of IP addresses to physical MAC addresses. When the gateway attempts to route an incoming frame, ARP provides the physical address of any host machine listed in this table that has the matching IP address. If a host is not found, ARP broadcasts an ARP message to all hosts on the network in search of the host that has that IP address. If such a host exists, ARP dynamically adds it to the table for future reference and provides the physical address to the gateway.

A separate ARP table is maintained for each internal VLAN interface.

Each ARP table supports up to 1024 entries. When the table reaches 512 entries, the service will wait five seconds before automatically removing the oldest, non-permanent, and less frequently used entries to make room for new entries.

Note

Only IPv4 addresses are supported.

11.5.2 Displaying the ARP table summary

To display the ARP table summary for all VLAN interfaces, navigate to **System » ARP Table**.

The following is displayed for each VLAN interface under **Address Resolution Protocol (ARP) Table**:

Parameter	Description
Interface	The name of the VLAN interface.
IP Address	The IP address of the neighboring node.
MAC Address	The link-layer or Media Access Control (MAC) address of the neighboring node.
Origin	The method in which the entry was added. Possible values include: <ul style="list-style-type: none"> dynamic - The mapping was dynamically resolved by the ARP protocol
Age	The elapsed time since the neighbor entry was last updated. Time is expressed in the form of nYnMnDnhnmns. For more information about how time durations are expressed, refer to "Specifying a duration (Page 56)".

Parameter	Description
Type	The encapsulation method used for ARP message. Possible values include: <ul style="list-style-type: none"> • arpa - Stands for Advanced Research Projects Agency. This indicates the interface is connect to an IEEE 802.3 network.
State	The state of the neighbor entry. Possible values include: <ul style="list-style-type: none"> • reachable - The neighbor is considered reachable. The ARP protocol queries neighbors it has found at a random interval that can be between 15 and 45 seconds. Reachability may also be verified by a higher level protocol communicating with the neighbor. • stale - The neighbor is considered unreachable. Reachability will be reassessed the next time traffic is sent to the neighbor. • delay - ARP is preparing to probe the neighbor to determine if it is reachable. After 5 seconds, the state will change to probe. • probe - Unicast Neighbor Solicitation probes have been sent to the neighbor. Up to three unicast probes are sent. If no response is received, up to three multicast probes are sent. If the neighbor fails to respond to all probes, the ARP entry is deemed invalid and removed from the table. If a response is received, the state changes to reachable.

11.6 SNMP

The Simple Network Management Protocol (SNMP) allows central management of network components such as switches, controllers, communications modules, routers and PCs.

With SNMP, network components can be monitored and controlled from a remote management station.

The SINEC OS Web user interface offers restricted configuration options and an overview of SNMP. For information on the complete configuration of SNMP and on concepts and procedures, refer to the **SINEC OS CLI Configuration Manual**.

11.6.1 Configuring the SNMP agent

To configure the SNMP agent, do the following:

1. [Optional] Configure which SNMP version(s) the SNMP agent supports.
For more information, refer to "Configuring the SNMP versions the SNMP agent supports (Page 279)".
2. [Optional] Configure a server endpoint for SNMP.
For more information, refer to "Configuring a server endpoint for SNMP (Page 279)".

3. Enable a server endpoint for SNMP.
For more information, refer to "Enabling a server endpoint for SNMP (Page 280)".
4. Make sure the SNMP agent is enabled.
For more information, refer to "Enabling the SNMP agent (Page 280)".

11.6.1.1 Configuring the SNMP versions the SNMP agent supports

By default, the SNMP agent supports all SNMP versions.

To enable all SNMP versions for the SNMP agent, do the following:

1. Navigate to **System » Management Services » Overview**.
2. Under **SNMP**, change **SNMPv1** to **Enabled**.
3. Under **SNMP**, change **SNMPv2c** to **Enabled**.
4. Under **SNMP**, change **SNMPv3** parameter to **Enabled**.
5. Commit the changes.

11.6.1.2 Configuring a server endpoint for SNMP

Configure the local IP address and the port via which a server endpoint processes SNMP requests.

NOTICE
Configuration hazard - risk of connection loss
If the device is assigned its IP address dynamically via DHCP, not the following: If the IP address that the device receives via DHCP does not match the IP address that you configured for the NETCONF server endpoint, the device cannot be reached via the NETCONF server endpoint. You have the following options to prevent connection loss: <ul style="list-style-type: none"> • Allows client request on all local addresses (default IP address: 0.0.0.0). • Assign a static IP address for the device. • Make sure that the same IP address is always assigned via DHCP.

The following server endpoints are predefined by default:

Endpoint	Default
Name	default
Endpoint enabled	Yes
IP address	0.0.0.0
Port	161

Only users with the **Admin** user profile can configure a server endpoint.

11.6 SNMP

To configure a server endpoint, do the following:

1. Navigate to **System » Management Services » Overview**.
The available server endpoints for SNMP are displayed under **SNMP » Endpoint**.
2. Under **Endpoint**, select an endpoint. In the **UDP Port** column, change the port over which SNMP requests are being processed.
Conditions:
 - The number 161
 - A number between 1024 and 49151
 - A number between 49500 and 65535Default: 161
3. Under **Endpoint**, select an endpoint. In the **IP Address** column, change the IP address over which SNMP requests are being processed.
Default: 0.0.0.0
The default IP address allows client requests on all local addresses.
4. Commit the changes.

11.6.1.3 Enabling a server endpoint for SNMP

The server endpoint for SNMP is enabled by default.

Only users with the **Admin** user profile can enable a server endpoint.

To enable a server endpoint for SNMP, do the following:

1. Navigate to **System » Management Services » Overview**.
The available server endpoints for SNMP are displayed under **SNMP » Endpoint**.
2. Under **Endpoint**, select an endpoint and change **Status** to **Enabled**.
3. Commit the change.

11.6.1.4 Enabling the SNMP agent

The SNMP agent is disabled by default. SNMP is then disabled for the device and the SNMP port is closed. If you are not using SNMP and to prevent unauthorized access to the device, leave the SNMP agent in the disabled state.

Note

In STEP7 classic, there is a topology editor that you can use to compare the offline topology with the real connections of the device (online topology). When SNMP is disabled, this function is not available in STEP7 classic. Enable SNMP to use the function.

To enable the SNMP agent, do the following:

1. Navigate to **System » Management Services » Overview**.
2. Under **SNMP**, change **Status** to **Enabled**.
3. Commit the change.

11.6.2 Changing the name of an SNMP community

The community name corresponds to the community string that a user specifies in an SNMP request via SNMPv1 and v2c.

To change the name of an SNMP community, do the following:

1. Navigate to **System » Management Services » SNMP**.
The available SNMP communities are displayed under **SNMPv1/v2c Community Strings » Index**.
2. Under **SNMPv1/v2c Community Strings** change the name of an SNMP community.
Options include:

Option	Description
Text Name	The community name as string.
Binary Name	The community name in hexadecimal representation with colons as separator. Use this option when the community name contains characters that cannot be displayed. Example: The value "0x123456ABCD" is configured/displayed as follows: 12:34:56:AB:CD.

Condition:

- Must be between 1 and 256 characters long
3. Commit the change.

11.6.3 Changing the IP address of an SNMP target

To change the IP address of an SNMP target, do the following:

1. Navigate to **System » Management Services » SNMP**.
The available SNMP targets are displayed under **SNMPv1 Trap Receiver » Name**.
2. Under **SNMPv1 Trap Receiver**, change **IP Address** for an SNMP target.
3. Commit the change.

11.6.4 Changing the port of an SNMP target

To change the port of an SNMP target, do the following:

1. Navigate to **System » Management Services » SNMP**.
The available SNMP targets are displayed under **SNMPv1 Trap Receiver » Name**.
2. Under **SNMPv1 Trap Receiver**, change **UDP Port** for an SNMP target.

Condition:

- A number between 1 and 65535
- Default: 162
3. Commit the change.

11.6.5 Displaying the engine ID

To show the engine ID of the device, navigate to **System » Management Services » SNMP**.

The following information is displayed under **SNMP Engine ID**:

Parameter	Description
SNMP Engine ID	Shows the SNMP engine ID of the device.

Traffic control and classification

This chapter describes the traffic control and classification features available. Use these sub-systems to control the flow of data packets to connected network features. Tools for traffic analysis and characterization are also available.

12.1 Rate limiting

SINEC OS supports rate limiting on individual network interfaces. Rate limiting controls the rate at which an interface sends and/or receives traffic.

12.1.1 Understanding rate limiting

Rate limiting restricts the bandwidth for a specific interface. The restriction can be applied to ingress and/or egress traffic, and to a specific type of traffic (e.g. unicast, multicast, broadcast, etc.). In some applications, controlling bandwidth may be required to maintain quality of service.

Rate limiting also provides a layer of defense against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks exhaust network resources by flooding a device with requests.

Note

Limits are based on the capabilities of the port media behind each Ethernet interface. Before applying rate limiting to an interface, check the capabilities of the physical port through SINEC OS.

For more information, refer to "Determining interface capabilities (Page 284)"

Note

SINEC OS counts all Layer 1 bits in each ingress and egress frame, including the preamble and inter frame gap. For example, 80 bytes would be counted for a 64 byte Layer 2 frame (8 byte preamble + 12 byte inter frame gap + 64 byte Layer 2 frame).

12.1.2 Configuring rate limiting

To configure a bridge port to apply rate limiting on egress or ingress traffic, do the following for the selected bridge port and direction of traffic:

1. [Optional] Determine the rate limit capabilities of the selected bridge port for the chosen direction. Based on the media type, some bridge ports may not support all options. For more information, refer to "Determining interface capabilities (Page 284)".
2. Select the type of frames to limit. For more information, refer to "Selecting the type of frames to limit (Page 286)".
3. Select the rate of control. For more information, refer to "Selecting the rate limit (Page 287)".
4. Enable rate limiting. For more information, refer to "Enabling rate limiting (Page 287)".

12.1.2.1 Determining interface capabilities

The capabilities of bridge ports are limited based on their physical media. With respect to rate limiting, the following capabilities are important:

- The maximum configurable speed (in kbps)
- The minimum configurable speed (in kbps)
- The type of traffic permitted

These capabilities determine the rate limit setting for ingress and egress traffic traversing the bridge port.

Note

Capabilities are often different for ingress and egress traffic. For example, a bridge port may be able to control ingress frames based on their traffic type (e.g. broadcast, multicast, unicast, etc.), but not on egress.

To determine the different rate limit capabilities for ingress or egress traffic, navigate to **Interfaces » Ethernet Interfaces » Rate Control**.

Capabilities are listed under **Ethernet Rate Control Capabilities** for each individual bridge port.

Parameter	Description
Interface	The name of the interface.
Supported Ingress Traffic Types	The type of traffic supported by the bridge port on ingress. Possible values include: <ul style="list-style-type: none"> • all - All traffic types are supported • broadcast - Only broadcast traffic supported • multicast - Only multicast traffic supported • unknown-unicast - Only unknown unicast traffic is supported • mcast-and-unknown-ucast - Only multicast and unknown unicast traffic is supported • bcast-and-unknown-ucast - Only broadcast and unknown unicast traffic is supported • bcast-and-mcast - Only broadcast and multicast traffic is supported • bcast-and-mcast-and-unknown-ucast - Only broadcast, multicast, and unknown unicast traffic is supported
Supported Ingress Rate Types	The data transfer speed for ingress rate limits. Default: kbps
Ingress Rate Min	The minimum ingress rate in kilobits-per-second (kbps).
Ingress Rate Max	The maximum ingress rate in kilobits-per-second (kbps).
Supported Egress Traffic Types	The type of traffic supported by the bridge port on egress. Possible values include: <ul style="list-style-type: none"> • all - All traffic types are supported • broadcast - Only broadcast traffic supported • multicast - Only multicast traffic supported • unknown-unicast - Only unknown unicast traffic is supported • mcast-and-unknown-ucast - Only multicast and unknown unicast traffic is supported • bcast-and-unknown-ucast - Only broadcast and unknown unicast traffic is supported • bcast-and-mcast - Only broadcast and multicast traffic is supported • bcast-and-mcast-and-unknown-ucast - Only broadcast, multicast, and unknown unicast traffic is supported
Supported Egress Rate Types	The data transfer speed for egress rate limits. Default: kbps
Egress Rate Min	The minimum egress rate in kilobits-per-second (kbps).
Egress Rate Max	The maximum egress rate in kilobits-per-second (kbps).

12.1.2.2 Selecting the type of frames to limit

To configure a bridge port to limit only a specific type of traffic on ingress or egress, do the following:

1. [Optional] Check the capabilities of the selected interface to determine if it can limit the frame type you want to control in the chosen direction (i.e. ingress or egress). For example, if the traffic type capability for an interface is **all** for egress traffic, the rate cannot be limited on egress based on the traffic type. For more information, refer to "Determining interface capabilities (Page 284)".
2. Navigate to **Interfaces » Ethernet Interfaces » Rate Control**.
3. Under **Ethernet Rate Control**, configure **Ingress Traffic Type** and/or **Egress Traffic Type** for the selected bridge port. Options include:

Option	Description
all	Default Rate limiting is applied to all traffic.
broadcast	Rate limiting is applied to only broadcast traffic.
unknown-unicast	Rate limiting is applied to only unknown unicast traffic.

Note the following options are available as well, but are not supported in this release:

Option	Description
bcast-and-mcast	Rate limiting is applied to both broadcast and multicast traffic.
bcast-and-mcast-and-unknown-ucast	Rate limiting is applied to broadcast, multicast, and unknown unicast traffic.
bcast-and-unknown-ucast	Rate limiting is applied to both broadcast and unknown unicast traffic.
mcast-and-unknown-ucast	Rate limiting is applied to both multicast and unknown unicast traffic.
multicast	Rate limiting is applied to only multicast and unknown multicast traffic.
unicast	Rate limiting is applied to only unicast and unknown unicast traffic.
unknown-multicast	Rate limiting is applied to only unknown multicast traffic.

4. Commit the change.

12.1.2.3 Selecting the rate limit

To select the rate of control applied by a bridge port on egress or ingress traffic, do the following:

1. [Optional] Check the capabilities of the selected bridge port to determine if it can limit the frame type you want to control in the chosen direction (i.e. ingress or egress).
For example, if the traffic type capability for a bridge port is **all** for egress traffic, the rate cannot be limited on egress based on the traffic type.
For more information, refer to "Determining interface capabilities (Page 284)".
2. Navigate to **Interfaces » Ethernet Interfaces » Rate Control**.
3. Under **Ethernet Rate Control**, select a bridge port and then enter a value under **Ingress Rate** and/or **Egress Rate**. The rate is defined in kilobits-per-second (kbps).
Default: 0
4. Commit the change.

12.1.2.4 Enabling rate limiting

By default, rate limiting is disabled in both traffic directions for all bridge ports.

To enable rate limiting for a specific bridge port, do the following:

Note

Rate limiting is enabled separately for ingress and egress traffic.

1. Navigate to **Interfaces » Ethernet Interfaces » Rate Control**.
2. Under **Ethernet Rate Control**, select a bridge port and then change **Ingress Rate Control State** and/or **Egress Rate Control State** to **Enabled**.
3. Commit the change.

12.1.3 Configuration examples

The following are examples of how to apply rate limiting.

12.1.3.1 Limiting the rate of traffic

In this example, the device forwards traffic on interface ethernet0/1 (a 1000Base-FX port) to a server that only accepts data at 100 kbps. If this limit is exceeded, frames are dropped.



Figure 12-1 Limiting the flow of traffic to a server

12.2 VLANs

To limit the rate of traffic to the server, do the following:

1. Set the rate limit for egress traffic for ethernet0/1 to 100 kbps.
For more information, refer to "Selecting the rate limit (Page 287)".
2. Enable rate limiting for the egress traffic on ethernet0/1.
For more information, refer to "Enabling rate limiting (Page 287)".

12.2 VLANs

This section describes the configuration and successful deployment of VLANs on Layer 2 networks to virtually bridge different LAN segments together.

Note

The Web user interface only displays and allows configuration of statically configured VLANs. VLANs dynamically learned through the GARP VLAN Registration Protocol (GVRP) are only displayed through the CLI.

12.2.1 Understanding VLANs

Virtual Local Area Networks (VLANs) are a Layer 2 function defined by the IEEE 802.1Q standard. They are used to logically group traffic by function or organization, or to contain broadcast-, unknown-, and multicast-traffic (BUM).

In a non-VLAN implementation, BUM-traffic is forwarded to all nodes on the LAN, enabling any-to-any unicast traffic. However, with VLANs, all traffic remains within the VLAN, thus easing the load on the LAN.

VLANs are typically associated with IP subnetworks, where each end station in a specific IP subnet is a member of the same VLAN. Therefore inter-VLAN traffic, in case of IP, will typically be enabled through the use of IP routers.

Since VLANs define logical connections rather than physical connections, they greatly reduce the design complexity, labor, and resource requirements of a traditional LAN. At the same time, they improve security and traffic management.

Traffic is grouped by applying tags to frames that emanate from nodes within the same broadcast domain.

Each device can define one or more VLANs (broadcast domains), up to a total of 4094.

Note

Since VLANs on the same physical link share bandwidth, it is recommended to configure traffic classes to improve routing efficiency. For more information about traffic classes, refer to "Traffic classes (Page 301)".

The following illustrates how traffic emanating from different LAN segments can be logically grouped into VLANs.

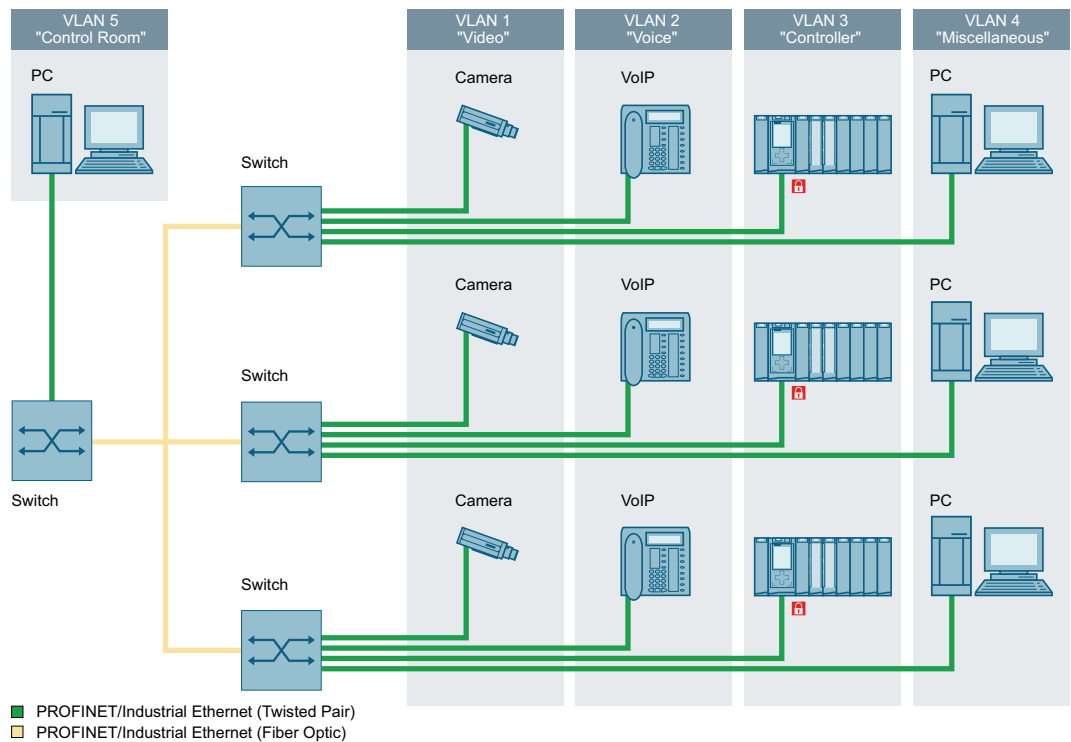


Figure 12-2 Separation of traffic using multiple VLANs

12.2.1.1 How VLANs are created

VLANs are created either statically or dynamically:

- **Statically**
Static VLANs can be defined directly in SINEC OS.
- **Dynamically**
VLANs can be learned through the GARP VLAN Registration Protocol.

12.2.1.2 VLAN-aware and VLAN-unaware modes

Devices that comply with the IEEE 802.1Q standard are considered **VLAN-aware** and operate at all times in VLAN-aware mode. These devices recognize VLAN tags on inbound (ingress) frames and use the tag along with the destination MAC or IP address to transmit the frame on the correct virtual LAN segment.

In contrast, devices that do not comply with IEEE 802.1Q are considered **VLAN-unaware**. These devices ignore VLAN tags and forward frames unaltered to their destination MAC or IP address. VLAN tags are not stripped from the frame's header.

12.2 VLANs

SINEC OS is VLAN-aware and therefore complies with the following rules set by the IEEE 802.1Q standard:

- Valid VLAN IDs (VIDs) must be within the range of 1 to 4094. VID's equal to 0 or 4095 are reserved.
- Each inbound (ingress) frame must be associated with a valid VID.
- Each outbound (egress) frame must be either tagged with a valid VID or sent untagged. Frames tagged with an invalid VID will never be forwarded by a VLAN-aware device.

SINEC OS also accepts frames tagged with a VLAN ID of 0. However, a special **VLAN-0-Tunnel** mode must be enabled for such frames to be forwarded properly. For more information on VLAN-0-Tunnel mode, refer to "VLAN-0-Tunnel mode (Page 294)".

12.2.1.3 Tagged vs. untagged frames

VLAN (or IEEE 802.1Q) tags in a frame's Ethernet header identify frames as part of a VLAN network. When a network switch receives a frame with a VLAN tag, the VLAN identifier (VID) is extracted from the header and the frame is forwarded to its destination on the same VLAN.

When a frame does not contain a VLAN tag, or contains an IEEE 802.1p (prioritization) tag that only has prioritization information and a VID of 0, it is considered an untagged frame.

Preamble (7 bytes)	Start Frame Delimiter (1 byte)	Destination MAC Address (6 bytes)	Source MAC Address (6 bytes)	Length/ Type (2 bytes)	Payload (46 to 1500 bytes)	Frame Check Sequence (4 bytes)
-----------------------	---	--	---------------------------------------	------------------------------	----------------------------------	---

Figure 12-3 Header for an untagged frame

Preamble (7 bytes)	Start Frame Delimiter (1 byte)	Destination MAC Address (6 bytes)	Source MAC Address (6 bytes)	Tag Protocol Identifier (2 bytes)	Tag Control Information (2 bytes)	Length/ Type (2 bytes)	Payload (42 to 1500 bytes)	Frame Check Sequence (4 bytes)
-----------------------	---	--	---------------------------------------	---	--	------------------------------	----------------------------------	---

Figure 12-4 Header for a tagged frame

Tag Protocol Identifier (TPI)

The Tag Protocol Identifier (TPI) field identifies the frame as a tagged frame. It consists of a 16-bit field set to 0x8100.

Tag Control Information (TCI)

The Tag Control Information (TCI) field defines:

- **Priority Code Point (PCP)**

A 3-bit sub-field that identifies the IEEE 802.1p Class of Service (CoS) assigned to the frame. The value of this field maps to a specific priority level as follows:

PCP	Priority	Type	Description
111	7	Network Control	Traffic that supports the configuration and maintenance of the network structure.
110	6	Internetwork Control	Traffic supporting the network infrastructure that needs to be distinguished by administrative domain.
101	5	Voice	Traffic with a delay of less than 10 milliseconds and maximum jitter.
100	4	Video	Traffic with a delay of 100 milliseconds or other applications with low latency, such as interactive video communications.
011	3	Critical Applications	Traffic that requires a guaranteed minimum bandwidth, but is subject to a form of admission control to prevent one application from consuming bandwidth at the expense of others.
010	2	Excellent Effort	Traffic an information services organization may prioritize for select customers. This is a best-effort type of service.
001	1	Background	Traffic that supports non-critical background operations (e.g. bulk transfers) that do not impact the use of the network for other users and applications.
000	0	Best Effort	Traffic for non-prioritized applications. Fairness is based on the dynamic windowing and retransmission strategy defined by the service's Transmission Control Protocol (TCP). This is a best effort type of service assigned to traditional LAN traffic.

- **Drop Eligible Indicator (DEI)**

A 1-bit sub-field that indicates if the frame can be dropped during periods of traffic congestion. It can be used separately or along with the PCP value.

Value	Description
0	The format of the MAC address is canonical. In the canonical representation, the least significant bit in the address is transferred first.
1	The format of the MAC address is non-canonical.

- **VLAN ID (VID)**

A 12-bit sub-field that specifies the VLAN to which the frame belongs.

Value	Description
0	No VLAN ID. The frame only contains priority information (priority tagged frame).
1 - 4094	VLAN IDs within this range are valid.
4095	This VLAN ID is reserved.

12.2.1.4 Access and trunk ports

Each bridge port can be made an **access** or **trunk** port.

- **Access ports**

An access port forwards traffic on its native VLAN typically to a single end device (e.g. a PC or Intelligent Electronic Device).

- **Trunk ports**

A trunk port can forward traffic on one or more VLANs simultaneously across the same link. This is intended for switch-to-switch applications.

To make sure traffic belonging to different VLANs remains separate in the trunk, each frame is encapsulated with an IEEE 802.1Q tag that identifies the VLAN to which the frame belongs. Frames associated with a trunk port's native VLAN can egress as untagged frames.

By default, each trunk port is a member of each available VLAN, including those learned dynamically by GVRP. Membership can be restricted by defining a forbidden VLANs list per port.

Note

Both ends of a trunk interface connection must be configured with the same native VLAN ID.

By default, each access and trunk port is given a PVID of 1. In the case of trunk ports, this represents the port's native VLAN. The PVID can be changed to any statically defined VLAN between 1 and 4094.

For information about configuring a bridge port to be an access or trunk port, refer to "Selecting the port membership type (Page 298)".

12.2.1.5 Native VLAN vs. default VLAN

The **default VLAN** is designated as VLAN 1. All bridge ports are assigned to this VLAN by default until they are explicitly assigned to another VLAN.

The **native VLAN** is most commonly used for access ports. It is the VLAN assigned to the port by its Port VLAN ID (PVID). Any untagged or priority-tagged frame received by the port is forwarded on the native VLAN. The default ID for the native VLAN (or PVID) is 1, but it can be set to any statically defined VLAN between 1 and 4094.

For information about how to set the native VLAN for a bridge port, refer to "Configuring the port VLAN ID (Page 298)".

12.2.1.6 Ingress filtering

Ingress filtering is a feature that can be enabled on a per-port basis. It evaluates each inbound (ingress) frame before it is granted entry to the network to make sure it originated from the source from which it was expected.

When ingress filtering is enabled, the device verifies any tagged frames arriving at the bridge port. If the bridge port is not a member of the VLAN to which the frame is associated, the frame is dropped.

When ingress filtering is disabled, frames from all VLANs configured on the device are accepted.

Note

Enable ingress filtering when using forbidden VLAN lists. Forbidden VLAN lists only prevent an interface from joining specific VLANs. They do not prevent a frame associated with a VLAN on the forbidden VLAN list from being forwarded to another interface that is a member of that VLAN.

For more information about enabling ingress filtering, refer to "Enabling ingress filtering (Page 300)".

12.2.1.7 Ingress and egress rules

The following rules are applied when processing incoming (ingress) and outgoing (egress) frames.

Ingress traffic rules

- A bridge port that does not apply ingress filtering or accepts only a specific frame type forwards all frames within the VLAN associated with each frame.
- When ingress filtering is enabled for a bridge port:
 - The port accepts only frames with a VID that matches the VLAN to which the interface is assigned
 - Frames are dropped if their VID does not match the VLAN assigned to the port that receives them
- If a bridge port is configured to accept only one type of frame:
 - If the port only accepts untagged and priority tagged frames, tagged frames are dropped
 - If the port only accepts tagged frames, untagged and priority tagged frames are dropped
- Untagged frames or frames that have a priority tag are associated with the ingress interface's PVID.

Egress traffic rules

- Frames egressing on an access interface are dropped if they are associated with a VLAN other than the egress interface's native VLAN
- Frames egressing on a trunk interface are tagged with their VID (not the egress interface's native VLAN) if they are associated with a VLAN to which the egress interface is a member
- If PVID tagging is enabled, outgoing frames are tagged if they are associated with the egress interface's native VLAN, regardless of the egress interface's membership type (access or trunk)
- If a forbidden VLANs list is defined for an egress interface, frames are dropped if they are associated with a VLAN on the list

12.2.1.8 GARP VLAN Registration Protocol (GVRP)

GARP VLAN Registration Protocol (GVRP) is a standard protocol built on Generic Attribute Registration Protocol (GARP) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured by neighbors are learned through GVRP. A GVRP-aware end station (i.e. PC or Intelligent Electronic Device) configured for a specific VID can be connected to a trunk interface on a GVRP-aware switch and automatically become a member of the selected VLAN.

Note

GVRP is only configurable via the CLI. For more information, refer to the **SINEC OS CLI Configuration Manual**.

12.2.1.9 Forbidden VLANs

By default, each trunk port is automatically a member of each defined VLAN. However, it may be necessary to restrict specific VLAN traffic on some bridge ports. This can be done by defining a forbidden VLANs list. This list is defined for individual bridge ports and controls which VLANs the port can become a member of. If ingress filtering is enabled, traffic belonging to any VLAN on the forbidden VLANs list is automatically dropped on ingress.

A forbidden VLANs list further prevents bridge ports from being added automatically to VLANs learned dynamically by GVRP. VLANs on a bridge port's forbidden VLANs list will also not be advertised by GVRP for that port.

Note

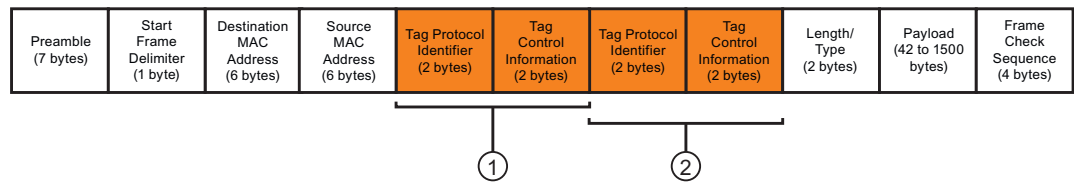
Enable ingress filtering when using forbidden VLAN lists. Forbidden VLAN lists only prevent bridge port's from joining specific VLANs. They do not prevent a frame associated with a VLAN on the list from being forwarded to another port that is a member of that VLAN.

12.2.1.10 VLAN-0-Tunnel mode

Some features, such as PROFINET, forward prioritized frames tagged with a VLAN ID of 0. These frames are intended to be forwarded with their given priority unmodified. However, in accordance with IEEE 802.1Q, by default, any priority tagged frame forwarded by a bridge port is assigned the port's PVID in place of its original VLAN ID.

To override this behavior, VLAN-0-Tunnel mode can be enabled for a VLAN. Bridge ports that are members of VLANs that have VLAN-0-Tunnel mode enabled will treat prioritized frames tagged with a VLAN ID of 0 as special.

- On ingress, such frames are queued based on their priority tag, rather than the bridge port's priority.
- On egress, if the bridge port is a **tagged** member of the VLAN, the frame will be double tagged with the egress port's VID on the outside ① and the frame's preserved priority tag on the inside ②. However, if the bridge port is an **untagged** member of the VLAN, the frame will only be forwarded with its priority tag unchanged.



- ① Outer tags (PVID)
- ② Inner tags (Priority Tag)

Figure 12-5 Double tagged frame

Note

VLAN 0 tagged frames are treated as regular frames when received by a bridge port whose native VLAN is a VLAN that **does not** have VLAN-0-Tunnel mode enabled.

Note

VLAN-0-Tunnel mode does not affect the handling of other untagged or tagged frames.

VLAN-0-Tunnel mode can be enabled for each active VLAN and applies to all bridge ports belonging to those VLANs.

12.2.1.11 Advantages and disadvantages of using VLANs

The following highlights some of the important advantages and disadvantages associated with VLANs.

Advantages

- **Traffic domain isolation**
VLANs are most often used for their ability to restrict traffic flows between groups of devices. Unnecessary broadcast traffic can be restricted to the VLAN that requires it. Broadcast storms in one VLAN need not affect users in other VLANs.
Hosts on one VLAN can be prevented from accidentally or deliberately assuming the IP address of a host on another VLAN.
The use of creative bridge filtering and multiple VLANs can carve seemingly unified IP subnets into multiple regions policed by different security/access policies.
Multi-VLAN hosts can assign different traffic types to different VLANs.
- **Administrative convenience**
VLANs simplify the sometimes necessary task of relocating equipment. When a switch is physically relocated, its connection point is often changed as well. But with VLANs, restoring the switch's VLAN membership is as simple as copying the membership to the new port.
- **Reduced hardware**
Without VLANs, traffic domain isolation requires the use of separate bridges for separate networks. VLANs eliminate the need for separate bridges.
The number of network hosts may often be reduced. Often, a server is assigned to provide services for independent networks. These hosts may be replaced by a single, multi-horned host supporting each network on its own VLAN. This hosts can perform routing between VLANs.
Multi-VLAN hosts can assign different traffic types to different VLANs.

Disadvantages

- **Limited number of VLANs**
Each network is limited to 4094 VLANs, with VIDs 0 and 4095 reserved. While 4094 may be more than enough for most networks, this could become a limitation in the future.
- **Security**
If the network spans more than one geographical region, VLAN traffic may be exposed to potential sniffing or Man in the Middle attacks. These can be difficult to address if Layer 3 security features (e.g. firewall, IPsec, etc.) are not also implemented.
- **Overhead**
Implementations that use primarily static VLANs (i.e. port-based, MAC-based) can be difficult to maintain if the network evolves over time. Monitoring and updating VLAN memberships can be a time-consuming task.

12.2.2 Configuring VLANs

To configure and assign VLANs, do the following:

1. Add static VLANs and/or enable GVRP.
GVRP can only be enabled/disabled via the CLI. For more information, refer to the **SINEC OS CLI Configuration Manual**.
For more information about adding static VLANs, refer to "Adding or modifying a static VLAN (Page 296)".

Note

An interface is created automatically for each new static VLAN.

2. [Optional] Configure the VLAN interface created for the static VLAN.
For more information, refer to "Configuring VLAN interfaces (Page 180)".
3. [Optional] Enable VLAN-0-Tunnel mode.
For more information, refer to "Enabling VLAN-0-Tunnel mode (Page 297)".
4. Configure the VLAN settings for one or more bridge ports.
For more information, refer to "Configuring VLAN settings for bridge ports (Page 297)".

12.2.2.1 Adding or modifying a static VLAN

To add or modify an existing static VLAN, do the following:

Note

Assign an IP address to the associated VLAN interface to make it a management interface. You can then use SSH to access the CLI through the management port.

For more information about assigning an IP address to a VLAN interface, refer to "Static IP address assignment (Page 193)".

1. Navigate to **Layer 2 » VLANs**.
2. Under **Static Virtual Local Area Networks (VLANs)**, either select an existing VLAN or click **Add** to add a new VLAN.
3. Under **VLAN ID**, enter the VLAN ID for the VLAN.
Condition:
 - A number between 1 and 4094
4. [Optional] Under **VLAN Name**, enter a name for the VLAN.
Condition:
 - Must be between 0 and 32 characters long

If no name is defined, a name is assigned to the VLAN in the VLAN database. The name is in the form of VLAN{ Number }, where { Number } is a four-digit number that includes the VID with leading zeros.
For example: VLAN0010 is the default VLAN name for VLAN 10.
5. Commit the change.

12.2.2.2 Enabling VLAN-0-Tunnel mode

VLAN-0-Tunnel mode enables all bridge ports belonging to a specific VLAN to forward prioritized frames tagged with a VLAN ID of 0 unmodified. This may be required by some features, such as PROFINET, to make sure a frame's priority tag is retained as it is forwarded to its destination. If VLAN-0-Tunnel mode is not enabled, in accordance with IEEE 802.1Q, any priority tagged frame forwarded by a bridge port is assigned the port's PVID in place of its original VLAN ID.

For more information, refer to "VLAN-0-Tunnel mode (Page 294)".

Note

VLAN-0-Tunnel mode can be enabled on all active VLANs. It is disabled by default.

To enable VLAN-0-Tunnel mode for a VLAN, do the following:

1. Navigate to **Layer 2 » VLANs**.
2. Under **Static Virtual Local Area Networks (VLANs)**, change **VLAN-0-Tunnel** to **Enabled** for the selected VLAN.
3. Commit the change.

12.2.3 Configuring VLAN settings for bridge ports

To configure the VLAN settings for a bridge port, do the following:

1. Define the bridge port as an access or trunk interface.
For more information, refer to "Selecting the port membership type (Page 298)".
2. [Optional] Change the bridge port's port VLAN ID. By default, the port VLAN ID is set to 1.
For more information, refer to "Configuring the port VLAN ID (Page 298)".

12.2 VLANs

3. [Optional] If GVRP is enabled, set the GVRP mode for the bridge port.
The GVRP mode can only be set via the CLI. For more information, refer to the **SINEC OS CLI Configuration Manual**.
4. [Optional] Enable PVID tagging for traffic egressing the bridge port.
For more information, refer to "Enabling PVID tagging on egress traffic (Page 299)".
5. [Optional] Control which frames are accepted by the bridge port.
 - To filter frames based on their type (i.e. tagged, untagged, or both), set the acceptable frame type.
For more information, refer to "Selecting the frame types accepted (Page 299)".
 - To filter frames based on their VID, enable ingress filtering.
For more information, refer to "Enabling ingress filtering (Page 300)".
6. [Optional] For trunk-type bridge ports only, define the forbidden VLANs list.
For more information, refer to "Restricting VLAN membership (Page 300)".

12.2.3.1 Selecting the port membership type

To select the port membership type for a bridge port, do the following:

1. If changing the port membership type from trunk to access, make sure GVRP mode is disabled for the selected bridge port and the forbidden VLANs list is cleared. These features are not supported by access ports.
The GVRP mode is only configurable via the CLI. For more information, refer to the **SINEC OS CLI Configuration Manual**.
For information about the forbidden VLANs list, refer to "Restricting VLAN membership (Page 300)".
2. Navigate to **Layer 2 » VLANs**.
3. Under **Port Based VLANs**, select a bridge port and then configure **Type**.
Options include:

Option	Description
Access	Default The bridge port only carries traffic on the native VLAN.
Trunk	The bridge port carries traffic for all VLANs.

4. Commit the change.

12.2.3.2 Configuring the port VLAN ID

The native VLAN for a bridge port is set by defining the Port VLAN ID (PVID). When set, any untagged or IEEE 802.1p priority tagged frame received by the bridge port is associated with this VLAN. However, frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID specified in the frame's header.

Note

Both ends of a trunk interface connection are typically configured with the same native VLAN ID.

To configure the port VLAN ID for a bridge port, do the following:

1. Navigate to **Layer 2 » VLANs**.
2. Under **Port Based VLANs**, select a port VLAN ID for the selected bridge port under **Native VLAN ID**.
Condition:
 - A number between 1 and 4094
3. Commit the change.

12.2.3.3 Selecting the frame types accepted

VLANs assigned to a bridge port accept tagged and untagged frames by default. However, when needed, they can be configured on a per-port basis to accept only tagged or untagged frames.

To select which frame types are accepted by a bridge port, do the following:

1. Navigate to **Layer 2 » VLANs**.
2. Under **Port Based VLANs**, configure **Acceptable Frame Type** for the selected bridge port.
Options include:

Option	Description
All	Default Both tagged and untagged ingress frames are accepted.
Tagged Frames Only	Only VLAN ingress tagged frames are accepted.
Untagged and Priority Tagged Only	Only untagged ingress frames or frames that have a priority tag are accepted.

3. Commit the change.

12.2.3.4 Enabling PVID tagging on egress traffic

PVID tagging makes sure all frames are tagged if they are egressing on a bridge port's native VLAN. By default, this option is disabled and frames are forwarded untagged.

Note

Enabling PVID tagging will result in increased bandwidth consumption, as additional VLAN tags are added to the header of each frame. Consumption will become more significant the smaller the frame size.

To enable PVID tagging for a bridge port, do the following:

1. Navigate to **Layer 2 » VLANs**.
2. Under **Port Based VLANs**, change **Egress Tag** to **Enabled** for the selected bridge port.
3. Commit the change.

12.2.3.5 Enabling ingress filtering

By default, ingress filtering is disabled for each bridge port.

To enable ingress filtering for a bridge port, do the following:

Note

Enable ingress filtering when using forbidden VLAN lists. Forbidden VLAN lists only prevent a bridge port from joining specific VLANs. They do not prevent a frame associated with a VLAN on the forbidden VLAN list from being forwarded to another bridge port that is a member of that VLAN.

1. Navigate to **Layer 2 » VLANs**.
2. Under **Port Based VLANs**, change **Ingress Filter** to **Enabled** for the selected bridge port.
3. Commit the change.

12.2.3.6 Restricting VLAN membership

To define the forbidden VLANs list for a bridge port, do the following:

NOTICE
Configuration hazard - risk of data loss
The forbidden VLANs list must be configured the same on both ends of the link. Excess frames may be discarded, otherwise.

Note

The selected bridge port must be defined as a trunk.

Note

Enable ingress filtering when using forbidden VLAN lists. Forbidden VLAN lists only prevent a bridge port from joining specific VLANs. They do not prevent a frame associated with a VLAN on the list from being forwarded to another bridge port that is a member of that VLAN.

For more information about enabling ingress filtering, refer to "Enabling ingress filtering (Page 300)".

1. Navigate to **Layer 2 » VLANs**.
2. Under **Port Based VLANs**, select a bridge port and then select one or more VLANs from the **Forbidden VLANs** list.
3. Commit the change.

12.3 Traffic classes

Traffic classification is the categorization and controlled transmission of frames. It is used to improve network performance and provide differing levels of service to select traffic types.

This section describes how to perform traffic classification using traffic classes.

12.3.1 Understanding traffic classes

Traffic classes are a form of traffic classification that place incoming frames in queues based on priority. An algorithm is then applied to each queue to determine which can forward frames first based on a weighting mechanism unique to each algorithm. This allows the device to prioritize the delivery of often loss- and time-sensitive data over less critical information.

Traffic classification is an automatic feature that can be customized on a per-port basis. Each bridge port can be configured to:

- Map frames to traffic class queues
- Change a frame's priority on egress.

When a frame is received on a bridge port, the ingress interface assigns the frame to a traffic class in the following phases:

1. Inspection and prioritization

Each frame is inspected on ingress and assigned a priority. Based on the individual settings of the bridge port, prioritization can be based on the following:

- the frame's Priority Code Point (PCP) tag
- the frame's Differentiated Services Code Point (DSCP) tag
- the bridge ports default priority

2. Mapping

The frame is mapped to a traffic class queue based on the priority determined in the previous phase. This mapping can be customized for PCP and or DSCP tags.

For information about default priority-to-queue mapping, refer to "Default mapping (Page 303)".

3. Forwarding

Once assigned to a traffic class queue, the frame waits to be forwarded. Forwarding is done in an order determined by a weighting algorithm. When frames in one queue have been forwarded, frames in the next queue are forwarded.

At this time, if needed, a different priority can be assigned to each Layer 2 802.1Q tagged frame on egress from a specific bridge port or the current priority can be maintained.

12.3.1.1 Traffic class queues

Traffic can be allocated into up to eight traffic class queues, labeled 0 to 7. Based on the IEEE 802.1Q standard, queues should be assigned the following priority and be used for the following traffic types:

Priority	Type	Description
7	Network Control	Traffic that supports the configuration and maintenance of the network structure.
6	Internetwork Control	Traffic supporting the network infrastructure that needs to be distinguished by administrative domain.
5	Voice	Traffic with a delay of less than 10 ms and maximum jitter.
4	Video	Traffic with a delay of 100 ms or other applications with low latency, such as interactive video communications.
3	Critical Applications	Traffic that requires a guaranteed minimum bandwidth, but is subject to a form of admission control to prevent one application from consuming bandwidth at the expense of others.
2	Excellent Effort	Traffic an information services organization may prioritize for select customers. This is a best-effort type of service.
0 (Default)	Best Effort	Traffic for non-prioritized applications. Fairness is based on the dynamic windowing and retransmission strategy defined by the service's Transmission Control Protocol (TCP). This is a best effort type of service assigned to traditional LAN traffic.
1	Background	Traffic that supports non-critical background operations (e.g. bulk transfers) that do not impact the use of the network for other users and applications.

12.3.1.2 Weighting algorithms

Weighting (or load-balancing) algorithms control the order in which traffic class queues are permitted to forward frames. Each applies its own rules/policies to provide a unique level of service.

At this time, SINEC OS applies the **strict** weighting algorithm only. This algorithm only allows frames to be transmitted from a traffic class queue once the frames from all higher priority queues have been transmitted. For example, traffic class queue 5 cannot be cleared until traffic class queue 6 has been cleared.

12.3.1.3 Default mapping

Incoming frames are mapped by default to traffic class queues as follows based on their PCP or DSCP markings:

DSCP	PCP	Queue
0 - 7	1	0
8 - 15	0	1
16 - 23	2	2
24 - 31	3	3
32 - 39	4	4
40 - 47	5	5
48 - 55	6	6
56 - 63	7	7

This mapping can be customized for PCP and/or DSCP tags. For more information, refer to "Mapping a PCP value to a traffic class (Page 306)" and/or "Mapping a DSCP tag to a traffic class (Page 307)".

12.3.1.4 Prioritization of ingress frames

The following details how ingress frames are prioritized and forwarded:

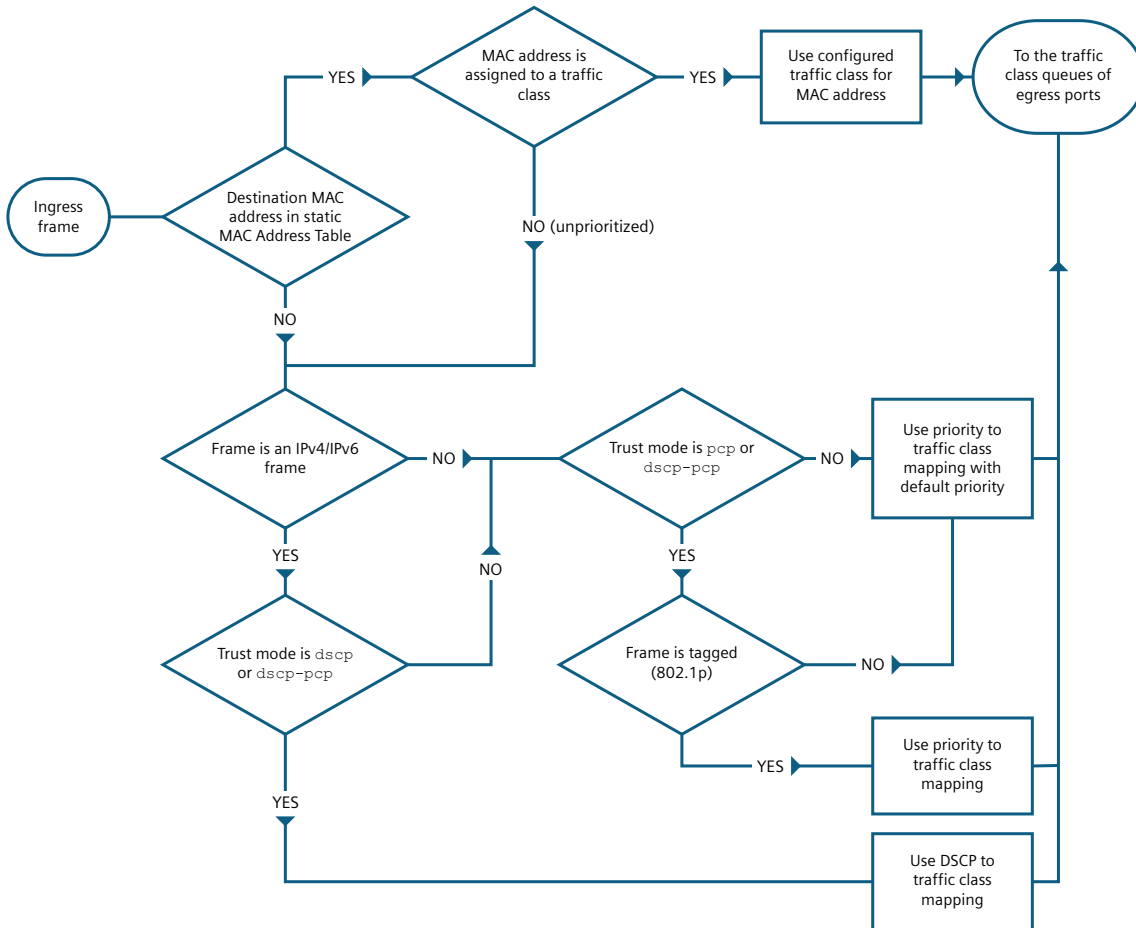


Figure 12-6 Ingress frame prioritization

12.3.1.5 Priority regeneration

The following details how the priority assigned to an ingress frame is regenerated on egress:

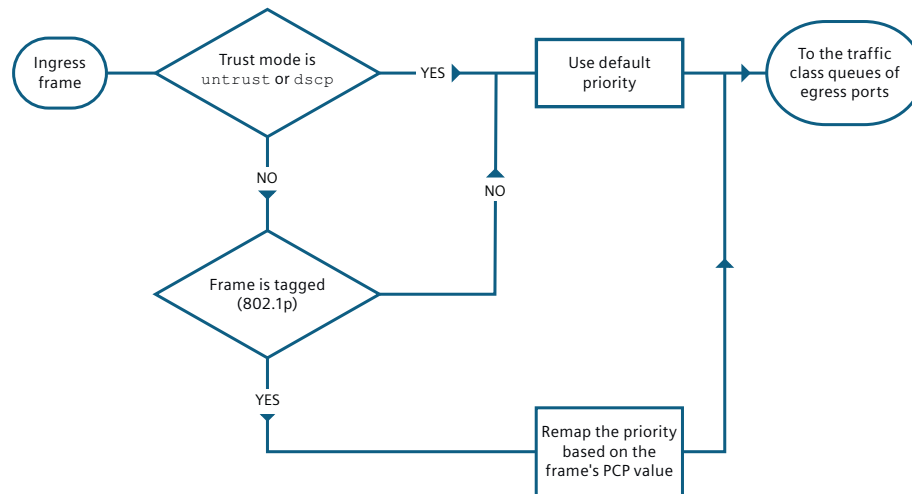


Figure 12-7 Priority regeneration

12.3.2 Configuring traffic classes

To configure traffic classes, configure one or more bridge ports to apply traffic classes to received frames.

Traffic classes are configured for bridge ports based on the type of traffic to be received on the associated port.

- Layer 2 802.1Q tagged frames feature a PCP tag in their header that is used to assign the frame to the proper traffic class queue
- Layer 3 frames feature a 6-bit DSCP tag in their header that is used to assign the frame to a traffic class queue

A bridge port may receive one or both types of frames. It may also receive frames that do not have either tag in their header.

To configure traffic classes for bridge ports, do the following:

1. [Optional] Configure the bridge port's default priority. This priority is assigned automatically to any frames that do not have a priority of their own.
For more information, refer to "Configuring the default priority (Page 306)".
2. Define how the bridge port maps frames to the appropriate traffic class queue.
 - For Layer 2 802.1Q tagged frames, refer to "Mapping a PCP value to a traffic class (Page 306)"
 - For Layer 3 frames, refer to "Mapping a DSCP tag to a traffic class (Page 307)"

12.3 Traffic classes

3. If the bridge port is an ingress interface, set the trust mode.
For more information, refer to "Configuring trust mode (Page 307)".
4. [Optional] For Layer 2 802.1Q tagged frames only, use priority regeneration to change the value of the PCP tag when the frame is transmitted.
For more information, refer to "Assigning different priorities to traffic on egress (Page 308)".

12.3.2.1 Configuring the default priority

Each bridge port must be assigned a default priority. This priority is assigned to any frame that has not been prioritized based on its contents. Specifically, the header is missing the Layer 2/3 fields required for automatic prioritization. A default priority is assigned automatically to such frames on ingress. The frames are then mapped to the appropriate traffic class queue based on the assigned priority.

The default priority may also be used if trust-mode is set to **untrust**, despite the presence of a PCP or DSCP value.

To configure the default priority for a bridge port, do the following:

1. Navigate to **Layer 2 » Traffic Classes » Queuing Policy & Trust Modes**.
2. Under **Default Priorities and Trust Modes**, configure **Default Priority** for the selected bridge port.
Condition:
 - A number between 0 and 7Default: 0
3. Commit the change.

12.3.2.2 Mapping a PCP value to a traffic class

Some Layer 2 802.1Q tagged frames include a Priority Code Point (PCP) value in their 802.1Q tag header. SINEC OS maps each value to a specific traffic class queue, which can be customized per bridge port.

For information about the default mapping of PCP values to traffic class queues, refer to "Default mapping (Page 303)".

Note

Up to eight mappings are permitted per bridge port.

To configure a bridge port to map a specific PCP value to a specific traffic class queue, do the following:

1. Navigate to **Layer 2 » Traffic Classes » Priority Mappings**.
2. Under **Interface Selection**, select a bridge port or select **All** to apply your changes to all bridge ports.

3. Under **PCP to Interface Queue Mappings**, select a traffic class queue under **Queue** for every code in the **PCP Code** column.
Layer 2 802.1Q tagged frames with one of the PCP values will be mapped to the associated traffic class queue.
4. Commit the change.

12.3.2.3 Mapping a DSCP tag to a traffic class

Some Layer 3 frames include a Differentiated Services Code Point (DSCP) value in their IPv4/IPv6 header. SINEC OS maps each value to a specific traffic class queue, which can be customized per bridge port.

For information about the default mapping of DSCP values to traffic class queues, refer to "Default mapping (Page 303)".

Note

Up to 64 mappings are permitted per bridge port.

To configure a bridge port to map a specific DSCP value to a specific traffic class queue, do the following:

1. Navigate to **Layer 2 » Traffic Classes » Priority Mappings**.
2. Under **Interface Selection**, select a bridge port or select **All** to apply your changes to all bridge ports.
3. Under **DSCP to Interface Queue Mappings**, select a traffic class queue under **Queue** for every code in the **DSCP Code** column.
Layer 3 frames with one of the DSCP values will be mapped to the associated traffic class queue.
4. Commit the change.

12.3.2.4 Configuring trust mode

Trust mode determines if a bridge port uses the Priority Code Point (PCP) and/or Differentiated Services Code Point (DSCP) value to prioritize ingress frames, or if it should apply its own default priority.

Trust mode can be configured in multiple ways:

- **Trust PCP values only (PCP)**
Frames are prioritized based on their PCP values only. DSCP values are ignored. If the PCP tag is missing, the default priority is applied.
- **Trust DSCP values only (DSCP)**
Frames are prioritized based on their DSCP values only. PCP values are ignored. If the DSCP tag is missing, the default priority is applied.

12.3 Traffic classes

- **Trust DSCP and PCP values (DSCP-PCP)**
Frames are prioritized based first on their DSCP tag and then by their PCP tag. If both tags are missing, the default priority is applied.
- **Do not trust DSCP or PCP values (Untrust)**
Neither DSCP or PCP values are trusted. The default priority is applied only to all ingress frames

To configure the trust mode for an ingress bridge port, do the following:

1. Navigate to **Layer 2 » Traffic Classes » Queuing Policy & Trust Modes**.
2. Under **Default Priorities and Trust Modes**, configure **Trust Mode** for the selected bridge port.
Options include:

Option	Description
PCP	Default Ingress frames are prioritized based on their PCP tag. The DSCP tag (if present) is ignored. If the PCP tag is missing, the frame is prioritized based on the interface's default priority.
Untrust	Ingress frames are prioritized based on the interface's default priority. PCP and DSCP values (if present) are ignored.
DSCP	Ingress frames are prioritized based on their DSCP tag. The PCP tag (if present) is ignored. If the DSCP tag is missing, the frame is prioritized based on the interface's default priority.
DSCP-PCP	Ingress frames are prioritized based on their DSCP tag first. If the DSCP tag is missing, the frame is prioritized based on its PCP tag (if present). If a frame has neither of these tags, the interface's default priority is applied.

3. Commit the change.

12.3.2.5 Assigning different priorities to traffic on egress

By default, the PCP tag for each Layer 2 802.1Q tagged frame is untouched as the frame ingresses and egresses the device. However, it may be desirable in some cases to assign a different priority to a frame as it is forwarded. For instance, when transmitting frames from one domain to another, it may be necessary to change the priority tag for specific frames to match with the priority-to-traffic-class mapping at the destination site.

Priority regeneration targets frames that have a specific priority tag at ingress and maps the priority tag to a new value at egress. Affected frames are still assigned to the appropriate traffic class queue based on the initial value of the priority tag, but they are transmitted with a different priority tag.

To configure a bridge port to apply priority regeneration to select frames, do the following:

1. Navigate to **Layer 2 » Traffic Classes » Priority Mappings**.
2. Under **Interface Selection**, select a bridge port or select **All** to apply your changes to all bridge ports.

3. Under **Priority Regeneration**, select a priority on egress under **Egress Priority** for the selected ingress priorities under **Ingress Priority**.
4. Commit the change.

12.3.3 Configuration examples

The following configuration examples demonstrate various methods for preventing the loss of high priority frames. Each is based on a single scenario where a series of sensors on a production line send messages to a SIMATIC S7 CPU via a switch running SINEC OS.

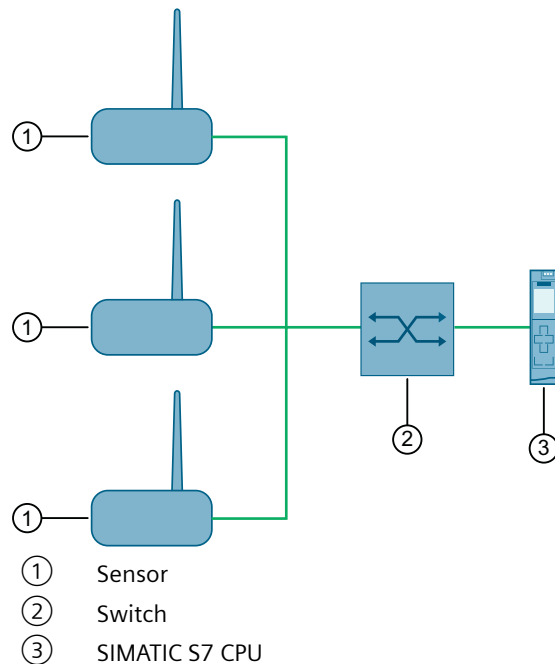


Figure 12-8 A Basic Traffic Class Topology

12.3.3.1 Prioritizing all frames

In this version of the scenario, all frames received by the switch are considered important, regardless of the priority assigned to each.

Method 1: Assign a high default priority to each frame

In SINEC OS, ignore each frame's priority tag and assign it the default priority of the receiving bridge port.

1. For each bridge port connected to the sensors, set the default priority to a high priority, such as 7 (the highest priority).
For more information, refer to "Configuring the default priority (Page 306)".
2. For each bridge port connected to the sensors, set the trust mode to **Untrust**.
For more information, refer to "Configuring trust mode (Page 307)".
3. [Optional] Send traffic from the sensors and observe the traffic queues to verify important frames are granted higher priority over other frames.

Method 2: Prioritize frames with a specific priority tag

In SINEC OS, only prioritize frames with PCP or DSCP values, or both.

1. For each bridge port connected to the sensors, set the trust mode to one of the following values:

Option	Description
PCP	All frames are placed in the queue mapped to their PCP value.
DSCP	All frames are placed in the queue mapped to their DSCP value.
DSCP-PCP	All frames are placed in the queue mapped to their DSCP or PCP value. Frames with a DSCP value are prioritized first.

2. [Optional] Send traffic from the sensors and observe the traffic queues to verify important frames are granted higher priority over other frames.

12.3.3.2 Prioritizing select frames

In this version of the scenario, priority is granted to specific frames carrying critical messages, such as those indicating a halt in production. These messages must be received by the SIMATIC S7 CPU before all other frames.

Method 1: Configure sensors to assign a high pPriority to each frame on egress

If sensors can control the priority assigned to frames on egress, configure each sensor to assign a high priority to frames carrying important information. The device will automatically place these frames in a high priority queue.

1. For each sensor, map a high priority to important frames on egress.
2. In the switch configuration, set the trust mode to either **PCP** (Layer 2 traffic only), **DSCP** (Layer 3 traffic only), or **DSCP-PCP** (Layer 3 traffic, followed by Layer 2 traffic).
For more information, refer to "Configuring trust mode (Page 307)".
3. [Optional] Send traffic from the sensors and verify using a packet capture utility at the end the priority of frames.

Method 2: Apply the bridge port's default priority to incoming frames

In SINEC OS, assign the bridge port that receives the frames a high default priority. Any frame not assigned a priority based on its contents will be automatically forwarded to the associated queue on ingress.

1. For each bridge port connected to the sensors, set the default priority to a high number, such as 7 (the highest priority).
For more information, refer to "Configuring the default priority (Page 306)".
2. Set the trust mode to either **PCP** (Layer 2 traffic only) or **DSCP-PCP** (Layer 3 traffic, followed by Layer 2 traffic).
For more information, refer to "Configuring trust mode (Page 307)".
3. [Optional] Send traffic from the sensors and verify using a packet capture utility at the end the priority of frames.

Method 3: Remap priorities on egress

In SINEC OS, remap the priority assigned to important frames to a higher priority.

1. For each bridge port connected to the sensors, map the priority assigned to important frames to a higher priority, such as 7 (the highest priority).
For more information, refer to "Mapping a PCP value to a traffic class (Page 306)" and/or "Mapping a DSCP tag to a traffic class (Page 307)".
2. Set the trust mode to either **PCP** (Layer 2 traffic only) or **DSCP-PCP** (Layer 3 traffic, followed by Layer 2 traffic).
For more information, refer to "Configuring trust mode (Page 307)".
3. [Optional] Send traffic from the sensors and verify using a packet capture utility at the end the priority of frames.

Time settings

This chapter describes how to configure the time services available for time-keeping and time synchronization. This includes setting the system time and date automatically using a service, such as NTP, or manually.

Configuring the correct time and making sure that time is synchronized across all devices is important for managing and troubleshooting a network. It is required for time-stamping system log entries, which aids in tracking events, such as network usage, security breaches, and device configuration changes.

Note

Only one time service can be enabled at a time. When the time is determined automatically by a service, such as NTP, or SIMATIC Time, the system time cannot be changed manually. Any attempt to change the time manually will be rejected.

13.1 Showing the date and the system time

To display information on the current system time, navigate to **System » System Time**.

The following information is displayed under **System Time**:

Parameter	Description
System Clock	Shows the set date and the system time.
Time Zone	Shows which time zone is set.

13.2 Configuring the date and the system time

To configure the date and the system time manually, do the following:

1. Navigate to **System » System Time**.
2. Under **System Time**, change **System Clock [YYYY-MM-DD HH:MM:SS]**.
Conditions:
 - **YYYY** stands for the year
 - **MM** stands for the month (01 - 12)
 - **DD** stands for the day (01 - 31)
 - **HH** stands for the hours (00 - 23)
 - **MM** stands for the minutes (00 - 59)
 - **SS** stands for the seconds (00 - 59)
3. Click **Apply**.

13.3 Using the date and the system time of the client PC

To use the date and system time of the connected client PC, do the following:

1. Navigate to **System** » **System Time**.
2. Under **System Time**, click **Use PC-Time**.
The device takes the data and the system time of the connected client PC. The date and system time are entered in the **System Clock** field.

13.4 Configuring the time zone

Note

Not all time zones include rules for switching to daylight saving time. Clarify in advance whether or not the desired time zone includes rules for the switch to daylight saving time.

To configure the time zone, do the following:

1. Navigate to **System** » **System Time**.
2. Under **System Time**, change **Time Zone**.
Default: UTC
3. Commit the change.

13.5 NTP

This section describes the configuration of the Network Time Protocol (NTP).

13.5.1 Understanding NTP

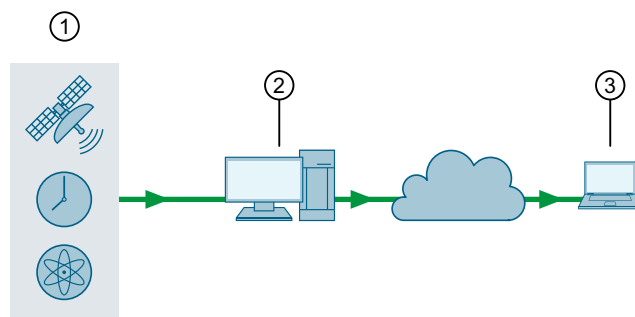
NTP is a protocol for hierarchical time synchronization between NTP servers and NTP clients in a network.

NTP implementations send and receive time information via the User Datagram Protocol (UDP) at port 123. You can configure NTP in such a way that NTP clients listen to broadcast or multicast frames with time updates.

NTP supports time stamps which you can use to compare diagnostic messages, events etc. of different network components.

NTP always sends the coordinated universal time UTC (Universal Time Coordinated). This corresponds to the time in the GMT (Greenwich Mean Time) time zone.

The advantage of NTP is that it allows for the time to be synchronized across subnets.



- ① Authoritative time source (e.g. atomic/radio clock, GPS receiver or modem time service)
- ② NTP Server
- ③ NTP Client

Figure 13-1 NTP

13.5.1.1 Stratum Number

An NTP network obtains its time information from an authoritative time source, such as atomic/radio clocks, GPS receivers or modem time services. This time information is then forwarded from servers to clients via NTP. The number of hops between a client and the authoritative time source is indicated by the stratum number.

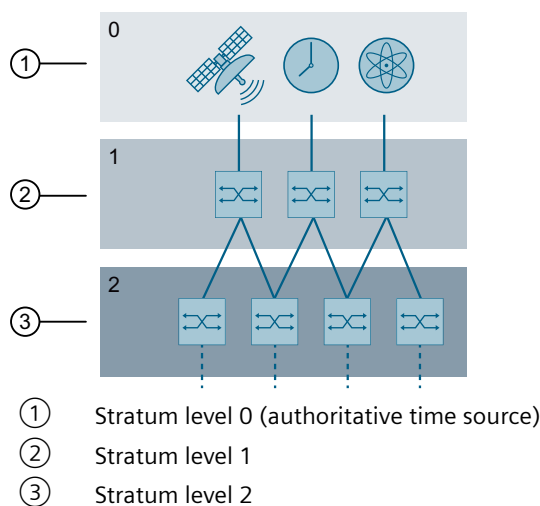


Figure 13-2 NTP stratum levels

A device can be an NTP client of the stratum above as well as a server of the stratum below if one exists:

- As NTP client, the device fetches the reference time from one or multiple NTP servers.
- As NTP server, the device compares its system time with other NTP servers. The NTP servers agree on a time that becomes binding for all.

NTP servers at stratum 1 synchronize themselves to a decisive time source at stratum 0. The NTP servers make their time available to NTP clients in the network that are referred to as stratum 2. A maximum of 16 stratum levels is possible.

NTP clients use the stratum number to make a decision for the most reliable time source. The stratum number is assigned automatically for NTP clients based on the number of hops to the authoritative time source.

13.5.1.2 NTP Server

An NTP server makes its time available to connected NTP clients. The NTP server listens for time requests at its NTP interfaces and responds with its reference time.

The stratum number of an NTP server corresponds to the stratum number of the upstream time server + 1.

The server itself can obtain its time information from different sources:

- NTP server
- NTP broadcast server
- NTP multicast server
- Local software clock

13.5.1.3 NTP Client

An NTP client sends time requests at regular intervals to actively synchronize its system time. The NTP client thereby compensates for delays caused by the transmission time with conversions.

The client can obtain its time information from different sources:

- NTP server
- NTP broadcast server
- NTP multicast server

If you configure multiple servers, the client queries all servers and evaluates their response frames. The client selects the server that is most accurate. This ensures that the client synchronizes its system time with an exact time. The accuracy depends on the quality of the server used.

13.5.2 Configuring NTP

Note

Do not connect the device to NTP servers on the Internet.

Only connect the device with trusted NTP servers in your own network.

To configure the device as NTP client, do the following:

1. Configure an NTP server.
For more information, refer to "Configuring an NTP server (Page 317)".
2. [Optional] Enable an NTP server.
For more information, refer to "Enabling an NTP server (Page 317)".

3. [Optional] If a version other than NTP V4 is required, define the NTP version.
For more information, refer to "Configuring the NTP version (Page 317)".
4. [Optional] Configure the values of the polling interval.
For more information, refer to "Configuring the polling interval (Page 318)".
5. [Optional] To accelerate synchronization during the first connection establishment, enable iBurst.
For more information, refer to "Enabling iBurst (Page 318)".
6. [Optional] To improve the quality of the time-of-day synchronization, enable Burst.
For more information, refer to "Enabling Burst (Page 319)".
7. Enable NTP.
For more information, refer to "Enabling NTP (Page 319)".

13.5.2.1 Configuring an NTP server

By default, no NTP server is configured.

To define an NTP server, do the following:

1. Navigate to **System » Time Synchronisation » NTP Client**.
2. Under **NTP Unicast Server**, click **Add**.
A new row is added to the table.
3. Enter the IP address of the NTP server under **Server Address**.
You can only edit the IP address of the NTP server directly after adding the new row. As soon as the field is no longer active, the IP address is write-protected. If you want to change the IP address, you need to delete the NTP server and re-configure it.
By default, a newly configured NTP server is automatically enabled.
4. Commit the changes.

13.5.2.2 Enabling an NTP server

By default, an NTP server is enabled.

To enable an NTP server, do the following:

1. Navigate to **System » Time Synchronisation » NTP Client**.
2. Under **NTP Unicast Server**, change **Status** to **Enabled**.
3. Commit the change.

13.5.2.3 Configuring the NTP version

Only change the NTP version if a version other than version 4 is required.

To configure the NTP version used, do the following:

1. Navigate to **System » Time Synchronisation » NTP Client**.
2. Under **NTP Unicast Server** in the **NTP version** column, change the NTP version.
Condition:
 - A number between 1 and 4Default: 4
3. Commit the change.

13.5.2.4 Configuring the polling interval

To configure the polling interval for an NTP server, do the following:

1. Navigate to **System » Time Synchronisation » NTP Client**.
2. Under **NTP Unicast Server** in the **Minpoll [s]** column, define the minimum value of the polling interval in seconds as power of 2.
Condition:
 - A number between 4 and 17Default: 6
The value 6 corresponds to 2^6 (64 seconds).
3. Under **Maxpoll [s]**, define the maximum value of the polling interval in seconds as power of 2.
Condition:
 - A number between 4 and 17Default: 10
The value 10 corresponds to 2^{10} (1024 seconds).
4. Commit the changes.

13.5.2.5 Enabling iBurst

iBurst (initial Burst) increases the number of frames from one frame to six frames per polling interval when the NTP server cannot be reached. This accelerates synchronization during the first connection establishment.

By default, iBurst is disabled. You can activate iBurst for each configured server.

To enable iBurst for an NTP server, do the following:

1. Navigate to **System » Time Synchronisation » NTP Client**.
2. Under **NTP Unicast Server**, change **iBurst** to **Enabled**.
3. Commit the change.

13.5.2.6 Enabling Burst

Burst increases the number of frames per polling interval when the NTP server can be reached. iBurst, in contrast to Burst, increases the number of frames per polling interval when the NTP server cannot be reached.

With Burst, deviations from the time source are reduced and the quality of time-of-day synchronization is improved.

The number of frames per Burst is calculated from the difference between the current and the smallest value of the polling interval as power of 2. A frame is sent at the preset lowest value of polling interval 6 (64 seconds). The maximum number of eight frames is sent as of a polling interval of 9 (512 seconds). This ensures the average polling interval does not exceed the smallest polling interval.

By default, Burst is disabled. You can activate Burst for each configured server.

To enable Burst for an NTP server, do the following:

1. Navigate to **System » Time Synchronisation » NTP Client**.
2. Under **NTP Unicast Server**, change **Burst** to **Enabled**.
3. Commit the change.

13.5.2.7 Enabling NTP

By default, NTP is disabled.

To enable NTP, do the following:

1. Navigate to **System » Time Synchronisation » NTP Client**.
2. Under **Network Time Protocol (NTP) Client**, change **NTP Client** to **Enabled**.
3. Commit the change.

13.5.3 Displaying the NTP configuration

To show the NTP configuration of the device, navigate to **System » Time Synchronisation » NTP Client**.

The following information is displayed under **Network Time Protocol (NTP) Client**:

Parameter	Description
NTP Client	Shows whether NTP is enabled.

The following information is displayed under **NTP Unicast Server**:

Parameter	Description
Server Address	Shows the IP address of the NTP server.
Status	Shows whether the NTP server is enabled.
NTP Version	Shows the NTP version used.
Minpoll [s]	Shows the minimum value of the polling interval.
Maxpoll [s]	Shows the maximum value of the polling interval.

Parameter	Description
iBurst	Shows whether iBurst is enabled.
Burst	Shows whether Burst is enabled.

13.6 PTP

The Precision Time Protocol (PTP) is a standard method of synchronizing network clocks over Ethernet. SINEC OS supports version 2 of the PTP standard defined in the IEEE 1588-2008 standard, also referred to as PTPv2. It is intended for applications that require higher synchronization accuracy than what can be achieved using the Network Time Protocol (NTP).

Note

PTP uses the hardware clock and can therefore operate independently of other time services, such as NTP and SIMATIC Time, that rely on the system clock.

13.6.1 Understanding PTP

PTP is a distributed protocol that allows multiple clocks in an IEEE 1588 network to synchronize their time with other clocks in the same domain. A PTP domain consists of ordinary and transparent clocks organized in a master-slave synchronization hierarchy. The hierarchy is determined through an election process where the clock deemed to be the most accurate time source is labeled the **grandmaster**. All other clocks are considered **masters** or **slaves**:

- Slave clocks synchronize their time with a master clock
- Master clocks serve their time to slave clocks, but also synchronize with their own master clock or the grandmaster clock
- Transparent clocks maintain clock accuracy between master and slave clocks

13.6.1.1 Supported clock types

The device operates at all times as a one-step peer-to-peer (P2P) transparent clock.

For more information, refer to "Transparent clocks (Page 323)".

13.6.1.2 PTP messages

Synchronization is achieved through the successful exchange of PTP timing messages between masters and slaves. PTP messages are used to either determine the clock hierarchy or to communicate time-related information.

Messages are categorized as either **general** or **event** class messages. Event messages are time-critical and have a direct impact on time synchronization. General messages contain important information, but their transmission is not time-sensitive.

The following types of messages are sent/received by PTP:

Message type	Class	Description
Sync	Event	Used by boundary and ordinary clocks to communicate time-related information between Masters and Slaves. Slaves use the information to determine the propagation delay and calculate the clock offset.
Follow_Up	General	
Delay_Req	Event	
Delay_Resp	General	
Pdelay_Req	Event	Used by transparent clocks to measure delays between the device and its directly connected neighbors.
Pdelay_Resp	Event	
Pdelay_Resp_Follow_Up	General	
Announce	General	Used by the Best Master Clock Algorithm (BMCA) to determine the grandmaster clock. Each message defines the properties of the device that sent it.
Management	General	Used by network management systems to remotely monitor and manage the PTP system.
Signaling	General	Used to communicate non-time-critical information between clocks.

All messages are sent using either User Datagram Protocol over Internet Protocol (UDP/IP) or Layer 2 Ethernet frames.

13.6.1.3 PTP domains

Each PTP clock must be assigned to a logical domain, which allows multiple PTP systems to operate independently on the same devices.

Based on the IEEE 1588-2008 standard, domain numbers represent the following:

Domain Number	Description
0	Default
1	Alternate domain 1
2	Alternate domain 2
3	Alternate domain 3
4 to 127	User-defined
128 to 253	Reserved
254	User-defined

13.6.1.4 PTP profiles

PTP profiles define a set of allowed PTP features, restrictions, and default values for a specific application. Profiles allow PTP to adapt itself to the requirements of specific scenarios.

PTP Default Profile (default-p2p-profile)

Features of default-p2p-profile include:

Characteristic		Default
Synchronization model		As defined by IEEE 1588-2008
Clock selection		As defined by IEEE 1588-2008
Port state decision		As defined by IEEE 1588-2008
Packet rates	Sync/follow-up packets	1 per second (s)
	Delay-request/delay-respond	1 per second (s)
	Announce messages	0.5 per second (s)
Announce Time Out Interval		3 seconds (s)
Transport mechanism		Layer 2 Multicast
Path delay mechanism		Peer-to-Peer (P2P)
Domain number		0

13.6.1.5 Best Master Clock Algorithm (BMCA)

The Best Master Clock Algorithm (BMCA) is a key part of the IEEE 1588 standard. It helps ordinary clocks determine the best master clock in their PTP domain, and if a master clock cannot be found, enable the clock to become the grandmaster for all clocks in its domain.

When the clock first starts, the BMCA listens for Announce messages from the available grandmaster clocks in the domain. An Announce message carries information about the grandmaster clock that sent it, which is used to determine which of the grandmaster clocks is the best.

In order of importance, an Announce message contains the following information:

- **Priority 1 Field**
An 8-bit user-defined value. Typically, a value of 128 is used for master-capable devices and 255 for slave-only devices, but any number is acceptable. The clock with the lowest value wins.
- **Clock Class**
Each clock belongs to a class based on its current state. Each class is assigned a different priority over others. For instance, a clock that is locked to UTC time has higher priority over one that uses its own local time.
- **Clock Accuracy**
The range of precision in nanoseconds (ns) between the clock and UTC. For example, 25-100 ns.
- **Clock Variance**
A log scaled statistic based on jitter, wander of the clock's oscillator, and other factors.
- **Priority 2 Field**
Another 8-bit user-defined value same as the Priority 1 field. Its purpose is to help identify primary and backup clocks among identical, redundant masters.
- **Source Port ID**
A unique ID, typically set to the device's MAC address. It is used as a tiebreaker when all other values are equal.

If the device does not find a clock better than itself before the Announce message interval expires, it becomes the grandmaster.

13.6.1.6 Transparent clocks

Packets traversing a PTP network are subject to queuing and buffering delays that need to be accounted for in path delay measurements. The extent of the delays can vary based on the network load and the architecture of the receiving/forwarding device.

The purpose of a transparent clock is to forward traffic and adjust the path delay for each PTP packet. They are placed in distributed networks between master and slave clocks to limit the impact of variable path delays on time synchronization.

SINEC OS accounts for path delays by measuring the **peer mean path delay** for each PTP packet it forwards. This is a measurement (in nanoseconds) done at each PTP-enabled bridge port that determines the packet propagation between peer devices. This time is added to the correction field in the synchronization message, along with the residence time of the packet.

A one-step transparent clock determines the peer mean path delay by exchanging the following event messages with a neighboring clock:

- Pdelay_Req
- Pdelay_Resp

These messages are exchanged in the following sequence:

Step	Message	Description
①	Pdelay_Req	The transparent clock sends a Pdelay_Req message to the neighboring clock with a timestamp (t1). The neighboring clock receives the message and generates a new timestamp (t2) to mark the time of receipt.
②	Pdelay_Resp	The neighboring clock returns a Pdelay_Resp message with a new timestamp (t3). The transparent clock receives the message and generates a new timestamp (t4) to mark the time of receipt.

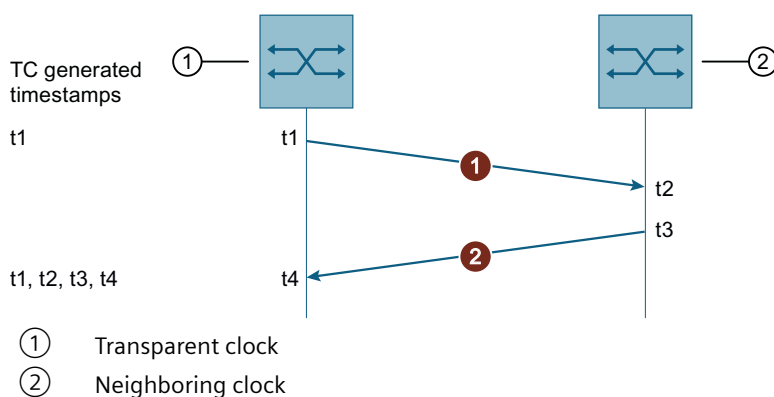


Figure 13-3 Transparent clock message exchange (one-step)

Once all required timestamps are collected, the transparent clock calculates the peer mean path delay using the following formula:

$$\text{Delay} = [(t4 - t1) - (t3 - t2)] / 2$$

For information about determining the peer mean path delay for an individual bridge port, refer to "AUTOHOTSPOT".

13.6.2 Configuring PTP

To configure PTP, do the following:

1. Set the PTP domain the clock will participate in.
For more information, refer to "Defining the PTP domain (Page 324)".
2. Make sure PTP is enabled for the selected bridge port or ports.
If PTP is disabled for a bridge port, the port does not participate in PTP protocol exchanges.
For more information, refer to "Enabling PTP for a bridge port (Page 324)".
3. Make sure the PTP service is enabled globally.
For more information, refer to "Enabling PTP globally (Page 324)".

13.6.2.1 Defining the PTP domain

Each PTP domain is a logical grouping of PTP clocks that synchronize time with one another. PTP clocks synchronize only with clocks in their domain. Synchronization requests from other domains are ignored.

To define the PTP domain in which your device will participate, do the following:

1. Navigate to **System** » **Time Synchronization** » **PTP Transparent Clock**.
2. Under **Precision Time Protocol (PTP) Transparent Clock**, configure **Domain Number**.
Condition:
 - A number between 0 and 127, or 254Default: 0
3. Commit the change.

13.6.2.2 Enabling PTP for a bridge port

PTP is enabled by default for all bridge ports. However, it may be necessary to disable PTP for a specific interface.

To enable a bridge port to participate in the exchange of PTP protocol exchanges, do the following:

1. Navigate to **System** » **Time Synchronization** » **PTP Transparent Clock**.
2. Under **PTP Interfaces**, change **PTP** to **Enabled** for the selected interface.
3. Commit the change.

13.6.2.3 Enabling PTP globally

The PTP service is enabled by default, but can be disabled when not required.

To enable PTP globally, do the following:

Note

PTP can be disabled for specific bridge ports. These interfaces do not participate in the PTP process.

1. Navigate to **System » Time Synchronization » PTP Transparent Clock**.
2. Under **Precision Time Protocol (PTP) Transparent Clock**, change **Status** to **Enabled**.
3. Commit the change.

13.6.3 Monitoring PTP

This section describes the various ways to look up information about the PTP service.

13.6.3.1 Displaying the peer mean path delay

The **peer mean path delay** is a measurement in nanoseconds (ns) of the packet propagation between peer devices. It is determined by each bridge port for which PTP is enabled and then added to the correction field in synchronization messages, along with the residence time of the packet.

For information about how the peer mean path delay is calculated, refer to "Transparent clocks (Page 323)".

To display the peer mean path delay determined for each PTP-enabled bridge port, navigate to **System » Time Synchronization » PTP Transparent Clock**. The peer mean path delay is displayed under **PTP Interfaces** in the **Pear Mean Path Delay** column.

Multicast filtering

This chapter describes features related to multicast filtering. Use multicast filtering to control the flow of multicast traffic through multicast group memberships.

14.1 Static multicast groups

This section describes how to define static entries for known multicast groups.

14.1.1 Configuring static multicast groups

To configure static multicast groups, do the following:

1. Add one or more static multicast groups.
For more information, refer to "Adding a static multicast group (Page 327)".
2. Set the traffic class for each static multicast group.
For more information, refer to "Selecting the traffic class for a static multicast group (Page 328)".
3. Assign a forwarding port to each static multicast group.
For more information, refer to "Assigning a forwarding port to a static multicast group (Page 328)".

Note

All static multicast groups are added to the multicast filtering database upon creation.
For more information, refer to "Multicast filtering database (Page 339)".

14.1.1.1 Adding a static multicast group

To add a static multicast group, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » Static**.
2. Under **Static Multicast Filtering**, click **Add**. A new row is added to the table.
3. In the **VLAN ID** column, select an existing static VLAN.
4. In the **MAC Address** column, enter a valid MAC address.
5. Commit the changes.

14.1.1.2 Selecting the traffic class for a static multicast group

To select the traffic class for a static multicast group, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » Static**.
2. Under **Static Multicast Filtering**, select a traffic class queue under **Traffic Class** for the selected static multicast group.
Options include:

- **0 - 7** - A traffic class queue
- **Unprioritized** - No traffic class queue is assigned

Default: **Unprioritized**

3. Commit the change.

14.1.1.3 Assigning a forwarding port to a static multicast group

Each static multicast group must be assigned a forwarding port through which multicast streams and IGMP messages can egress.

To assign a forwarding port to a static multicast group, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » Static**.
2. Under **Static Multicast Filtering** in the **Forwarding Ports** column, select an interface for the selected static multicast group.
3. Commit the change.

14.2 GMRP

GARP Multicast Registration Protocol (GMRP) is a form of multicast filtering intended for pruning Layer 2 mutlicast traffic.

14.2.1 Understanding GMRP

GMRP is an application of the Generic Attribute Registration Protocol (GARP). It provides a mechanism for managing multicast group memberships in a bridged Layer 2 network. It allows Ethernet switches and end stations to dynamically register multicast group membership with MAC bridges to the same LAN segment. That same information can be distributed across all bridges in the LAN segment that support Extended Filtering Services.

14.2.1.1 Joining/leaving multicast groups with GMRP

The following describes how GMRP manages memberships with multicast groups.

- **Joining a multicast group**

When end stations wish to join a multicast group, they send a GMRP **Join** message. The client switch that receives the **Join** message adds the port through which the message was received to the multicast group specified in the message. It then propagates the **Join** message to all other hosts in the VLAN, one of which is expected to be the multicast source. When a client switch transmits GMRP updates (from GMRP-enabled ports), all of the multicast groups known to the switch (whether added manually or learned dynamically through GMRP) are advertised to the rest of the network.

As long as one host on the Layer 2 network has registered for a given multicast group, traffic from the corresponding multicast source will be carried on the network. Multicast traffic forwarded by the source is only forwarded by other switches to the ports from which they have received **Join** messages for the multicast group.

- **Leaving a multicast group**

Client switches will occasionally send GMRP queries in the form of a **Leave All** message. If a host (either a switch or end station) wishes to remain in the multicast group, it reasserts its group membership by responding with an appropriate **Join** message. Otherwise, the host will respond with a **Leave** message or simply not respond.

If the client switch receives a **Leave** message or no response from the host within a given time period, the host is removed from the multicast group.

14.2.1.2 GARP attribute types

Since GMRP is an application of GARP, transactions take place using GARP.

GMRP defines the following two attribute types:

- **Group**

Identifies the group MAC addresses

- **Service requirement**

Identifies the service requirements for the group

Service Requirement attributes are used to change the receiving port's multicast filtering behavior to either:

- Forward all multicast group traffic in the VLAN
- Forward all unknown traffic (multicast groups) for which there are no members registered on the device in a VLAN

If GMRP is disabled, GMRP frames received will be forwarded like any other traffic. Otherwise, GMRP frames are processed and not forwarded.

14.2.2 Configuring GMRP

To configure GMRP, do the following:

- Enable GMRP globally.
For more information, refer to "Enabling GMRP (Page 330)".
- Select the GMRP mode for select bridge ports.
The GMRP mode determines how individual bridge ports process GMRP messages.
For more information, refer to "Selecting the GMRP mode per bridge port (Page 330)".
- [Optional] Select a time period for GMRP to wait before removing a registered multicast group after attempting to leave the group.
For more information, refer to "Configuring a delay before leaving a multicast group (Page 331)".
- [Optional] Enable topology change flooding.
For more information, refer to "Enabling topology change flooding (Page 331)".

14.2.2.1 Enabling GMRP

To enable GMRP for all bridge port interfaces, do the following:

Note

GMRP is disabled by default.

1. Navigate to **Layer 2 » Multicast Filtering » GMRP**.
2. Under **GARP Multicast Registration Protocol (GMRP)**, change **GMRP** to **Enabled**.
3. Commit the change.

14.2.2.2 Selecting the GMRP mode per bridge port

Bridge ports can be configured individually to ignore or process GMRP **join** and **leave** messages.

To configure how a bridge port interface to process GMRP messages, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » GMRP**.
2. Under **GARP Multicast Registration Protocol (GMRP)**, configure **GMRP Mode** for the selected bridge port.
Options include:

Option	Description
Disabled	Default GMRP is disabled on the interface.
Declare and Register	All multicast groups are declared and new groups are registered dynamically.
Declare Only	All multicast groups (configured or learned) are declared, but new groups are not registered.

3. Commit the change.

14.2.2.3 Configuring a delay before leaving a multicast group

When SINEC OS receives a **Leave** or **Leave All** message for a host belonging to a multicast group, it will proceed to remove that host from the specified multicast group(s). The time between receiving the message and removing the host can be delayed. This allows the host an opportunity to send a **Join** message and remain in the multicast group(s).

To set a delay before removing a host from a multicast group, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » GMRP**.
2. Under **GARP Multicast Registration Protocol (GMRP)**, configure **Leave Timer**.
Conditions:
 - Formatted as nYnMnDnhnmns, where n is a user-defined number
 - Minimum of 0.6 seconds (0.6s)
 - Maximum of 5 minutes (5m) or 300 seconds (300s)Default: 4s (4 seconds)
3. Commit the change.

14.2.2.4 Enabling topology change flooding

When STP topology changes occur or link changes occur without triggering a TCN, SINEC OS temporarily floods all interfaces controlled by GMRP. If topology change flooding is enabled, all RSTP non-edge interfaces are also flooded.

To enable topology change flooding, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » GMRP**.
2. Under **GARP Multicast Registration Protocol (GMRP)**, change **Topology Change Flooding** to **Enabled**.
3. Commit the change.

14.2.3 Configuration examples

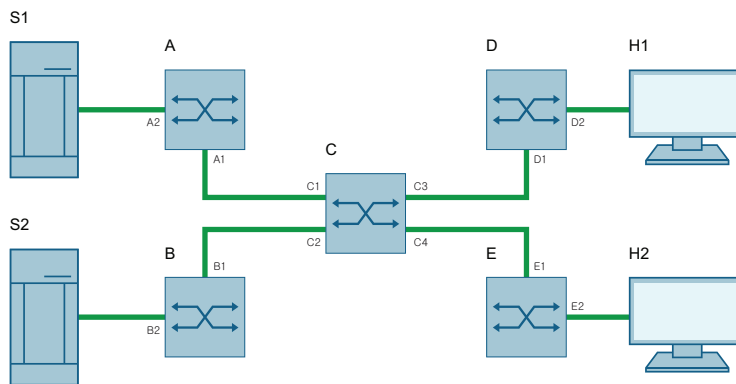
The following are examples of how to deploy GMRP.

14.2.3.1 Establishing membership with multicast groups using GMRP

This configuration example demonstrates how a network of hosts and switches can dynamically join two multicast groups using GMRP.

Overview

In this scenario, the SINEC OS device acts as intermediary between two multicast traffic sources and two hosts that wish to receive multicast streams from one of the sources.



■ PROFINET/Industrial Ethernet (Twisted Pair)

Figure 14-1 Topology

The multicast traffic sources, S1 and S2, are multicasting to multicast groups 1 and 2, respectively.

Host H1 is GMRP-unaware, but needs to receive multicast traffic from multicast group 1.

Host H2 is GMRP-aware and needs to receive multicast traffic from multicast group 2.

A network of switches with the SINEC OS device at their core connect the hosts to the multicast sources.

Configuration

1. Connect the devices as shown in the topology.
2. Enable GMRP globally on all switches (i.e. switch A, B, C, D, and E).
3. Configure interfaces for each switch to process GMRP messages (i.e. interface A1, A2, B1, B2, etc.).
4. On Switch D, add a static multicast group for VLAN 1, with interface D2 as the forwarding port.
This allows H1 to receive multicast traffic for multicast group 1.

Result

When all devices are connected and configured, hosts H1 and H2 can establish membership with the multicast group as follows:

1. On behalf of H1, Switch D advertises its membership to multicast group 1 to the network through interface D1. As a result, interface C3 on Switch C becomes a member of multicast group 1.
2. Switch C then propagates the **Join** message, causing interfaces A1, B1, C3 and E1 to become members of the multicast group on their respective switch.
3. Since H2 is GMRP-aware, it sends a Join message to Switch E to advertise its membership to multicast group 2. As a result, interface E2 becomes a member of multicast group 2.
4. Switch E propagates the **Join** message from H2, causing interfaces A1, B1, C4 and D1 to become members of multicast group 2.

GMRP-based registration has now propagated through the network, allowing multicast traffic from S1 and S2 to reach its destination as follows:

1. S1 forwards multicast traffic to interface A2 on Switch A.
2. Switch A forwards the traffic to interface A1, which is a member of multicast group 1.
3. From A1, the multicast traffic is forwarded to interface C3 and then to host H1.
4. S2 forwards multicast traffic to interface B2 on Switch B.
5. Switch B forwards the traffic to interface B1, which is a member of multicast group 2.
6. From B1, the multicast traffic is forwarded to interface C4 and then to host H2.

14.3 IGMP snooping

Internet Group Management Protocol (IGMP) snooping is a Layer 2 feature that enables Ethernet switches to listen in on IGMP communications between IP hosts and multicast routers. Ethernet switches can then intelligently direct multicast streams to only hosts that subscribe to the multicast group.

14.3.1 Understanding IGMP snooping

Some switches will forward by default multicast streams unsolicited to all interfaces in a VLAN, forcing some hosts in that broadcast domain to process mutlicast traffic they did not request. As a result, these hosts unnecessarily consume much needed resources and may be exposed to a denial-of-service attack.

IGMP snooping makes sure multicast streams are only forwarded to hosts that request it. By intercepting and analyzing (snooping) IGMP membership report messages from a multicast router and its clients, IGMP snooping determines which interfaces are connected to IGMP-enabled hosts. It then forwards the multicast traffic to those hosts only, rather than flooding the entire VLAN.

Note

SINEC OS supports IGMP snooping versions 2 and 3.

14.3.1.1 IGMP modes

IGMP snooping provides a means for switches to snoop the operation of multicast routers. As it detects IGMP general queries from the router, it can send **join/leave** requests on behalf of clients and hosts. IGMP snooping may also prune multicast streams accordingly.

IGMP snooping can be configured to operate in one of the following modes:

- **Passive mode**
In **passive** mode, IGMP snooping listens for IGMP general queries and sends **join/leave** requests on behalf of consumer ports. It cannot send queries.
Passive mode should be enabled if a remote multicast router is present.
- **Active mode**
In **active** mode, IGMP snooping is able to send IGMP general queries it would normally receive from a multicast router.
Active mode should be enabled if a remote multicast router is not present.

14.3.1.2 Filtering/pruning multicast traffic

IGMP Snooping filters (or prunes) IP multicast traffic to hosts using each frame's destination multicast MAC address, which is determined from the multicast group's IP multicast address.

For example, an IP multicast address of W.X.Y.Z corresponds to MAC address 01-00-5E-XX-YY-ZZ, where XX is the lower 7 bits of X, and YY and ZZ are Y and Z (respectively) coded in hexadecimal.

Note

Note that IP multicast addresses such as 224.1.1.1 and 225.1.1.1 will both map to the same MAC address (i.e. 01-00-5E-01-01-01). This is a known issue for which the IETF Network Working Group currently has offered no solution. Users are advised to be aware of and avoid this problem if possible.

14.3.1.3 IGMP snooping querier

In IGMP, the multicast router with the lowest IP address is elected the master router, or querier. The querier is responsible for soliciting IGMP report messages from hosts at regular intervals to determine which hosts wish to receive IP multicast traffic. IGMP snooping uses these reports to map hosts to specific multicast streams.

If, however, a multicast router is not available on the VLAN, IGMP snooping must be set to **active** mode on at least one switch on same local network. Switches with IGMP snooping set to **active** mode participate in the election process the same as multicast routers.

14.3.1.4 IGMP snooping rules

IGMP snooping adheres to the following rules:

- If IGMP snooping is in **passive** mode, at least one IGMP-enabled switch on the network must be in **active** mode to send IGMP general queries.
- By default, multicast traffic received from an unknown source is forwarded to all ports. However, if the multicast traffic comes from a known multicast group (i.e. at least one port is a member of the same group), the traffic is only forwarded to the port(s) that are members of that multicast group, or connected to the elected/configured IGMP querier (multicast router).

- Non-IGMP frames with a destination IP multicast address in the range of 224.0.0.0 to 224.0.0.255 are always forwarded to all ports. This behavior is based on the fact that many systems do not send membership reports for IP multicast addresses in this range while still listening to such frames.
- IGMP only forwards membership reports through ports connected to multicast routers. Sending reports to hosts is not supported, as this could prevent a host from joining a specific multicast group.
- Multicast routers use IGMP to elect a master router known as the querier. The querier is the route with the lowest IP address. All other routers become non-queriers, participating only in forwarding multicast traffic. IGMP-enabled devices running in **active** mode participate in the querier election process the same as multicast routers.
- When the querier election process completes, IGMP will relay queries received from the designated querier.
- When IGMP frames are forwarded, the querier sends IGMP general queries and assigns a source IP address of 0.0.0.0.

14.3.2 Configuring IGMP snooping

To configure IGMP snooping, do the following:

1. Enable IGMP snooping globally.
For more information, refer to "Enabling IGMP snooping (Page 335)".
2. Select the IGMP version. This determines the types of IGMP messages the device can send/receive.
For more information, refer to "Selecting the IGMP version (Page 336)".
3. Select the IGMP mode.
For more information, refer to "Selecting the IGMP mode (Page 336)".
4. Configure the IGMP query interval.
For more information, refer to "Configuring the IGMP query interval (Page 337)".
5. [Optional] Enable topology change flooding.
For more information, refer to "Enabling topology change flooding (Page 337)".
6. [Optional] Configure multicast router forwarding.
For more information, refer to "Configuring multicast router forwarding (Page 338)".
7. Enable IGMP snooping for one or more static VLANs.
For more information, refer to "Enabling IGMP snooping per VLAN (Page 337)".

14.3.2.1 Enabling IGMP snooping

To enable IGMP snooping, do the following:

Note

IGMP snooping is enabled by default.

1. Navigate to **Layer 2 » Multicast Filtering » IGMP Snooping**.
2. Under **Internet Group Management Protocol (IGMP)**, change **IGMP Snooping** to **Enabled**.
3. Commit the change.

14.3.2.2 Selecting the IGMP version

The IGMP version determined what type of IGMP messages can be sent and received by the bridge.

- When IGMPv2 is enabled, IGMPv3 messages are can only be sent, not received
- When IGMPv3 is enabled, all IGMP messages can be sent and received

To select the version of IGMP, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » IGMP Snooping**.
2. Under **Internet Group Management Protocol (IGMP)**, configure **Version**.
Options include:

Option	Description
2	Default Changes the IGMP version to IGMPv2.
3	Changes the IGMP version to IGMPv3.

3. Commit the change.

14.3.2.3 Selecting the IGMP mode

IGMP Snooping can be configured to operate in **active** or **passive** mode by enabling or disabling the IGMP querier.

- When enabled, IGMP snooping is in **active** mode
- When disabled, IGMP Snooping is in **passive** mode

Note

The IGMP querier is disabled (passive mode) by default.

Note

When IGMP snooping is in **passive** mode, at least one IGMP-enabled switch on the network must be in **active** mode to send IGMP general queries.

For more information about **active** and **passive** modes, refer to "IGMP modes (Page 333)".

To select the IGMP mode, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » IGMP Snooping**.
2. Under **Internet Group Management Protocol (IGMP)**, change **IGMP Querier** to either **Enabled** (active mode) or **Disabled** (passive mode).
3. Commit the change.

14.3.2.4 Configuring the IGMP query interval

The IGMP query interval determines how often IGMP queries are transmitted. The interval is measured in seconds between each successive transmission.

The query interval also determines when dynamically learned multicast groups age out. The age out period is $2 \times \{ \text{interval} \} + 10$ seconds.

To configure the IGMP query interval, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » IGMP Snooping**.
2. Under **Internet Group Management Protocol (IGMP)**, configure **Query Interval**.
Conditions:
 - Formatted as nYnMnDnhnmns, where n is a user-defined number
 - Minimum of 10 seconds (10s)
 - Maximum of 60 minutes (60m) or 3600 seconds (3600s)Default: 2m5s (2 minutes, 5 seconds)
3. Commit the change.

14.3.2.5 Enabling topology change flooding

When STP topology changes occur, SINEC OS temporarily floods all interfaces associated with IGMP snooping enabled VLANs. If topology change flooding is enabled, all RSTP non-edge interfaces are also flooded.

To enable topology change flooding, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » IGMP Snooping**.
2. Under **Internet Group Management Protocol (IGMP)**, change **Topology Change Flooding** to **Enabled**.
3. Commit the change.

14.3.2.6 Enabling IGMP snooping per VLAN

To enable IGMP Snooping on a static VLAN, do the following:

Note

IGMP snooping is disabled by default for each static VLAN.

1. Navigate to **Layer 2 » Multicast Filtering » IGMP Snooping**.
2. Under **IGMP Snooping VLANs**, change **IGMP Snooping** to **Enabled** for the selected static VLAN.
3. Commit the change.

14.3.3 Configuring multicast router forwarding

To configure multicast router forwarding, do the following:

1. Enable multicast router forwarding.
For more information, refer to "Enabling multicast router forwarding (Page 338)".
2. Configure one or more multicast router interfaces.
For more information, refer to "Configuring a multicast router interface (Page 338)".

14.3.3.1 Enabling multicast router forwarding

To enable multicast router forwarding, do the following:

Note

Multicast router forwarding is enabled by default.

1. Navigate to **Layer 2 » Multicast Filtering » IGMP Snooping**.
2. Under **Internet Group Management Protocol (IGMP)**, change **Router Forwarding** to **Enabled**.
3. Commit the change.

14.3.3.2 Configuring a multicast router interface

Multicast router interfaces establish a static connection to a multicast router.

To configuring a multicast router interface, do the following:

1. Navigate to **Layer 2 » Multicast Filtering » IGMP Snooping**.
2. Under **Internet Group Management Protocol (IGMP)**, select one or more interfaces from the **Multicast Router** list.
3. Commit the change.

14.3.4 Monitoring IGMP snooping

This section describes the various methods for monitoring the status of multicast groups learned through IGMP snooping.

14.3.4.1 Displaying the status of learned multicast groups

To display the status of multicast groups dynamically learned by IGMP Snooping, navigate to **Layer 2 » Multicast Filtering » IGMP Snooping**.

The following information is displayed under **IGMP Snooping Status**:

Parameter	Description
Interface	The bridge port on which the multicast group was learned.
VLAN ID	The VLAN ID of the VLAN on which the multicast group operates.
Address	The IPv4 address of the multicast group.
Last Reporter	The IPv4 address of the last host to send a report to join the multicast group.
MAC Address	The destination MAC address for traffic forwarded by the multicast group.
Up Time	The time in seconds (s) elapsed since the multicast group was learned.
Joined Ports	A list of bridge ports that received the IGMP Join messages from the multicast group.
Multicast Router	A list of bridge ports that will forward multicast traffic to multicast routers.

14.4 Multicast filtering database

The multicast filtering database records all current multicast groups that have been statically configured or dynamically learned through multicast filtering.

To display the multicast filtering database, navigate to **Layer 2 » Multicast Filtering » Filtering Database**.

The following is displayed for each entry under **Multicast Filtering Database**:

Parameter	Description
VLAN ID	The VID of the VLAN associated with the multicast group.
MAC Address	The destination MAC address for the multicast group.
Traffic Class	The traffic class queue assigned to the MAC address. Possible values include: <ul style="list-style-type: none"> • 0 - 7 - A traffic class queue • Unprioritized - No traffic class queue is assigned
Forwarding Ports and States	The outbound forwarding port(s) associated with the MAC address, as well as its state. Possible values for state include: <ul style="list-style-type: none"> • Static - The MAC address was added statically by a user • Dynamic - The MAC address was learned dynamically by a bridge protocol • Static-Dynamic - The MAC address was learned dynamically and then added statically by a user

Diagnostics

15.1 Diagnostics

This chapter describes the diagnostic tools available.

15.2 System status

This section describes how to monitor the system state, including uptime, last reboot, etc.

15.2.1 Displaying the system boot time

To display the date and time when the device was last rebooted, navigate to **System » Information & State**. The time is displayed in the **System State** area under **Boot Date/Time**.

Example

2021-01-01 00:08:00

15.2.2 Displaying the system up time

To display the total time the system has been running since the device was last rebooted, navigate to **System » Information & State**. The total time is displayed in the **System State** area under **Uptime**. The total time is displayed in number of days, hours, minutes, and seconds.

Example

2D4h37m37s

15.3 System logging

SINEC OS records all alarms and select events in a system log, or syslog. The system log is used by network administrators to identify events related to performance and security.

The system log is stored locally, but all or portions of the log can also be forwarded to a remote syslog server for retention and centralized monitoring.

Specific events, typically those that require immediate resolution, can also be highlighted to network administrators as they occur by e-mail and/or SNMP traps.

15.3.1 Understanding system logging

The syslog stores all event messages generated by the various system facilities running under SINEC OS.

The syslog is viewed through a logbook. The logbook displays the latest entries in the syslog, up to a maximum of 1000. As new events occur, the oldest entries are removed. The logbook shows all event messages by default, but can be filtered as needed.

Users are permitted to change the timestamp format for log entries.

15.3.1.1 Structure of a syslog entry

Each entry in the syslog represents a single event.

Example

```
2021-01-03T02:49:15-00:00 localhost 2m55s dmfd
info coldStart
```

This info-level entry indicates the device was restarted (either power was cycled manually or the device was restarted via SINEC OS) at 2021-01-03T02:49:15-00:00, or 2:49 AM on March 1st, 2021, GMT-0.

Description

Each entry in the syslog consists of the following elements:

{ timestamp }	{ hostname }	{ uptime }	{ program }	{ severity }	{ message }
The time stamp assigned to the event.	The host name assigned to the device.	The time between when the device was last rebooted and when the event occurred. Format: nYnMnDnhnm ns	The program that generated the message.	The severity of the message.	The event description.

15.3.1.2 Severity levels

Each event message in the system log is assigned one of the following standard severity levels:

Event Severity	Value	Description
Emergency	0	Indicates a critical error that prevents further operation of the device.
Alert	1	Indicates an error that requires immediate attention.
Critical	2	Indicates a primary system failure, such as device errors or system/application malfunctions. These alarms are typically non-recoverable.
Error	3	Indicates an error condition.
Warning	4	Indicates an error may occur if the associated condition is not resolved.

Event Severity	Value	Description
Notice	5	Indicates an event that is unusual, but is not an error conditions.
Info	6	Indicates a normal information message that does not require any action.

15.3.1.3 Syslog facilities

Syslog facilities represent the internal processes that generate events. Separating event messages by facility allows them to be filtered differently when forwarding messages to remote syslog servers.

The following are the available syslog facilities:

Facility	Description
kern	Kernel-related messages
user	User-level messages
mail	Mail-related messages
daemon	System daemon-related messages
auth	Authentication- and authorization-related messages
syslog	Systemd-related messages
authpriv	Non-system authorization-related messages

15.3.1.4 Remote logging

Entries from the syslog can be forwarded to up to five remote syslog servers for retention and centralized analysis. Which entries are forwarded can be controlled using filters.

Multiple filters, each applying to a specific facility, can be defined for each syslog server.

15.3.1.5 Event filtering

The system logging service includes a filtering mechanism.

Logbook filtering

For logbook, event messages can be filtered out by defining a filtering rule. This rule specifies a severity and tells the system whether to show only messages with this severity, or show messages with this severity and higher. For example, if a rule says include all messages with a severity of critical or higher, only messages matching that criteria will be displayed.

Remote syslog filtering

For remote syslog servers, one or more filtering rules can be defined per syslog facility and severity. Each rule is applied in the order in which they are defined. Only the messages captured by the rules are forwarded.

15.3.2 Configuring remote system logging

15.3.2.1 Configuring remote system logging

To forward events from the syslog to a remote syslog server, do the following:

1. Add a remote syslog server profile. Up to five servers can be defined.
For more information, refer to "Adding a remote syslog server profile (Page 344)".
2. Add at least one filtering rule for each remote syslog server to control which event messages are forwarded.
For more information, refer to "Defining a filtering rule for a remote syslog server (Page 345)".

15.3.2.2 Adding a remote syslog server profile

Up to five remote syslog server profiles can be configured. Each profile defines:

- The server's host name or IP address
- The server's designated port
- Which logs are forwarded to the server
- TLS certificates and keys (for TLS connections only)

Adding a remote syslog server profile for UDP connections

To add a remote syslog server profile, do the following:

1. Navigate to **System » Logging » Remote Syslog**.
2. Under **Remote Syslog UDP**, click **Add**. A new row is added to the table.
3. Under **Name**, assign a name to the server connection.
4. Under **Server Address/FQDN**, enter the remote syslog server's IPv4 address or host name.
5. Under **UDP Port**, enter the server's designated port.
Default: 514
6. Commit the changes.

Adding a remote syslog server profile for TLS connections

Note

For TLS server connections, a key-pair and certificate must be available in the keystore.

For information, refer to "AUTOHOTSPOT".

1. Navigate to **System » Logging » Remote Syslog**.
2. Under **Remote Syslog**, click **Add**. A new row is added to the table.
3. Under **Name**, assign a name to the server connection.
4. Under **Server Address/FQDN**, enter the remote syslog server's IPv4 address or host name.
5. Under **TLS Port**, enter the server's designated port.
Default: 6514

6. Under **Keystore Asymmetric Key**, select an asymmetric key to use for authentication with the remote syslog server.
7. Under **Keystore Identity Certificate**, select a certificate.
8. Under **Truststore Certificate Bag**, select a CA certificate.
9. Commit the changes.

15.3.2.3 Defining a filtering rule for a remote syslog server

Up to 10 filtering rules can be defined for each remote syslog server profile to individually control which event messages are forwarded. Multiple filtering rules allow for complex filtering.

Each rule applies to a specific syslog facility and severity. The severity can be singular or a range.

Rules are applied in the order in which they are read. A rule that excludes a set of event messages is overwritten if the next rule adds the same event messages. Similarly, a rule that adds a set of event messages is ignored if the next event messages produces the same list of event messages.

Note

At least one filtering rule is required per remote syslog server.

A filtering rule cannot be removed if it is the only rule defined for the remote syslog server. In this case, set the action to **block** to disable the rule.

To define a filtering rule to control which event messages are forwarded to a specific remote syslog server, do the following:

1. Navigate to **System » Logging » Remote Syslog**.
2. Make sure a remote syslog server profile has been configured.
For more information, refer to "Adding a remote syslog server profile (Page 344)".
3. Under **Name**, select a remote syslog server profile
4. Under **Remote Syslog Filter**, click **Add**. A new row is added to the table.
5. Under **Facility**, select a facility.
Options include:
 - **all** - All facilities
 - **auth** - Authentication- and authorization-related messages
 - **authpriv** - Non-system authroization-related messages
 - **daemon** - System daemon-related messages
 - **kern** - Kernel-related messages
 - **mail** - Mail related messages
 - **syslog**- Systemd-related messages
 - **user** - User-related messages

6. Under **Severity**, select a severity.
Options include:
 - **all** - Selects all events
 - **alert** - Selects alert-level events
 - **critical** - Selects critical-level events
 - **emergency** - Selects emergency-level events
 - **error** - Selects error-level events
 - **info** - Selects info-level events
 - **none** - No events are displayed
 - **notice** - Selects notice-level events
 - **warning** - Selects warning-level events
7. Under **Compare**, choose whether only the selected event is forwarded, or if the selected event and events with a higher severity level are forwarded.
Options include:
 - **equals** - Only event messages associated with the selected severity are forwarded
 - **equals-or-higher** - Event messages associated to the selected severity and higher are forwarded
8. [Optional] Under Action, choose whether or not the filtering rule is applied.
Options include:
 - **log** - The rule is applied.
 - **block** - The rule is ignored. Use this option for troubleshooting purposes.Default: log
9. Commit the changes.

15.3.3 Monitoring the system log

This section describes how to access the logbook and monitor the remoter server connections.

15.3.3.1 Displaying the logbook

To display the logbook, navigate to **System » Logging » Logbook**.

The following is displayed for each log entry under **Logbook**:

Parameter	Description
Time	The time stamp assigned to the event.
Uptime	The time between when the device was last rebooted and when the event occurred. Format: nYnMnDnhnmns.

Parameter	Description
Severity	The severity of the message.
Message	The message description.

15.3.3.2 Displaying remote logging servers

Entries from the system log can be forwarded to one or more remote syslog servers for retention and centralized analysis.

To display information about the remote logging servers that have been defined, navigate to **System » Logging » Remote Syslog**.

The following information is displayed for each server under **Remote Syslog**:

Parameter	Description
Name	The name assigned to the remote syslog server.
Server Address / FQDN	The remote syslog server's host name or IP address.
UDP Port	The designated port on the remote syslog server.

15.3.3.3 Clearing the logbook

To clear entries from the logbook, do the following:

Note

Clearing the logbook does not clear the system log.

1. Navigate to **System » Logging » Logbook**.
2. Under **Clear Logbook**, click **Clear**.

15.4 Event management

The event management system actively monitors the device and identifies specific events that occur during operation. All events are recorded in the system log (or syslog). An event can also trigger an SNMP trap, be e-mailed to administrators, and/or raise an alarm.

The configuration of individual alarms is supported under the event management system.

15.4.1 Understanding event management

The following describes the event management system and how it monitors, records, and notifies users of specific events that occur during operation.

15.4.1.1 Severity levels

Each event and alarm is assigned one of the following severity levels:

Event/alarm severity	Value	Description
Emergency	0	Indicates a critical error that prevents further operation of the device.
Alert	1	Indicates an error that requires immediate attention.
Critical	2	Indicates a primary system failure, such as device errors or system/application malfunctions. These alarms are typically non-recoverable.
Error	3	Indicates an error condition.
Warning	4	Indicates an error may occur if the associated condition is not resolved.
Notice	5	Indicates an event that is unusual, but is not an error conditions.
Info	6	Indicates a normal information message that does not require any action.

15.4.1.2 Resources and events

The following events are monitored by the device during operation. Each event is categorized by resource (subsystem) and assigned a severity level. Most events generate an alarm, which can be enabled/disabled, as needed.

Note

Some features trigger their own unique events outside of the event mangement system. These feature-specific events are recorded directly in the syslog. These are described in the sections related to these features.

For more information about severity levels, refer to "Severity levels (Page 348)".

PROFINET events

The following events are related to PROFINET activities.

Resource	Event ID	Default severity
PROFINET	Configuration*	Alert
PROFINET	IP-Configuration*	Alert
PROFINET	Connection	Notice
PROFINET	Fault	Alert

* No alarm associated.

Chassis management events

The following events are related to the hardware configuration of the device.

Resource	Event ID	Default severity
chassis-mgmt	Bad-power-supply	Alert
chassis-mgmt	Module-presence*	Warning
chassis-mgmt	Module-state*	Warning

* No alarm associated.

Device management events

The following events are related to user authentication, detected ambient temperature, etc.

Resource	Event ID	Default severity
device-mgmt	Authentication-failure	Warning
device-mgmt	Brute-force-prevention	Warning
device-mgmt	System-cold-start*	Info
device-mgmt	System-warm-start*	Info
device-mgmt	User-session-timeout*	Warning
device-mgmt	Vlan-linkDown/linkUp	Info

* No alarm associated.

Switch management events

The following events are related to switching activities, such as link up/down, looping, topology changes, etc.

Resource	Event ID	Default severity
switch-mgmt	Bouncing-link	Alert
switch-mgmt	Bpdu-guard-activated	Alert
switch-mgmt	Bundle-port-inconsistent-speed	Error
switch-mgmt	Ertm-target-ip-address-unresolved	Alert
switch-mgmt	Fast-link-detection-disabled	Warning
switch-mgmt	Gmrp-cannot-learn-more-addresses	Alert
switch-mgmt	Gvrp-cannot-learn-more-vlans	Alert
switch-mgmt	Igmp-group-membership-table-full	Alert
switch-mgmt	Igmp-mcast-forwarding-table-full	Alert
switch-mgmt	Intermittent-link	Alert
switch-mgmt	Linkdown/linkup	Info
switch-mgmt	Loop-detection	Alert
switch-mgmt	Mac-address-not-learned	Alert
switch-mgmt	Mcast-cpu-filtering-table-full	Alert
switch-mgmt	New-stp-root	Notice
switch-mgmt	Received-looped-back-bpdu	Alert
switch-mgmt	Stp-topology-change	Notice
switch-mgmt	Unresolved-speed	Error

Logging events

The following events are related to device credentials.

Resource	Event ID	Default severity
logging	Expired-certificate	Error
logging	Invalid-certificate	Error

15.4.1.3 Alarms

Some events can generate an alarm to alert users when the event occurs. Alarms are displayed in an alarms list and/or the system log.

Alarm types

There are two types of alarms:

- Conditional**
 Conditional alarms are generated when specific conditions are detected and can only be cleared when the conditions are resolved.
 An example of a conditional alarm is the **bad power supply** (Bad-power-supply) alarm. When the condition is resolved (i.e. input power is corrected), the alarm is ready to automatically clear once the event is acknowledged by a user.
 The alarm can also be acknowledged even if the condition has not yet been resolved. The alarm will clear automatically once the condition is resolved.
- Non-conditional**
 Non-conditional alarms are generated when an event occurs and remain active until cleared by a user.
 An example of a non-conditional alarm is the **authentication failure** (Authentication-failure) alarm. A user can acknowledge or clear this alarm at any time. If the alarm is set to auto-clear, acknowledgement will also clear the alarm.

Static vs. dynamic alarm messages

Some events have a static alarm message and a dynamic alarm message:

- Static alarm messages are fixed messages that appear in the alarm list. These messages also appear in any e-mails that are sent.
- Dynamic messages are more context-specific and provide more detail about the event (i.e. protocol, user, IP address, etc.). These appear in the logbook if the event is enabled. They may also appear in the alarm list if a static message is not defined for the event.

Available alarms

The following alarms are issued when specific events occur, if those events are configured to trigger an alarm. Alarms are displayed in the alarms list.

For more information about viewing active alarms, refer to "Listing active alarms (Page 358)".

PROFINET alarms

Related event	Conditional	Severity	Alarm message	Description	Suggested resolution
Configuration	Yes	Alert	<p>Static message "PROFINET configuration invalid, conflict detected."</p> <p>Dynamic messages "PROFINET configuration invalid, conflict detected: { message }." "PROFINET configuration on port { port number } invalid, conflict detected: { message }."</p>	An MRP configuration error has been detected.	Review the configuration and system logs for details.
IP-Configuration	Yes	Alert	<p>Static message "IP address collision detected."</p> <p>Dynamic message "IP address collision detected. The IP address { IP address } is already used."</p>	The specified IP address has already been used.	Review all IP addresses used in the network and determine a free IP address.
Connection	Yes	Notice	<p>Static message <i>None</i></p> <p>Dynamic messages "PROFINET connection established."</p>	A connection, or Application Relation (AR), has been established.	A notification. Nothing to be done.
Fault	Yes	Alert	<p>Static message <i>None</i></p> <p>Dynamic messages "PROFINET fault - please use STEP 7 for diagnostics."</p>	No connection, or Application Relation (AR), has been established in evident mode.	Establish a connection in evident mode. For more information, refer to the STEP 7 user documentation.

Chassis management alarms

Related event	Conditional	Severity	Alarm message	Description	Suggested resolution
Bad-power-supply	Yes	Alert	Static message None Dynamic message "Power line #{ number } lost."	Input power to the specified power supply is outside the normal operating range or the power cable is disconnected.	Make sure the input power is connected and the operating range meets the device requirements.
Module-presence	Yes	Warning	Static message None Dynamic messages "Module ({ slot }) Removed" "Module ({ slot }) Inserted" "LPE Module Connected" "LPE Module Removed"	A module has either been removed from or installed in the specified slot. For LPE modules specifically, indicates the module has been connected or disconnected.	Install or remove the module. Note that LPE modules are not hot-swappable. Restart the device after installing or removing the module.
Module-state	Yes	Warning	Static message None Dynamic messages "Unknown SFP module on interface { interface } (vendor: { vendor })" "Rejected SFP module on interface { interface }" "Unsupported SFP module on interface { interface }" "LPE Module Enabled" "LPE Module Disabled"	Indicates the state of SFP transceivers and LPE modules. For SFP transceivers, indicates the module is either not recognized, rejected, or not supported. For an LPE module, indicates the module state.	Use only Siemens approved SFP transceivers that are compatible with your device.

Device management alarms

Related event	Conditional	Severity	Alarm message	Description	Suggested resolution
Authentication-failure	No	Warning	<p>Static message "A user failed to login due to incorrect authentication credentials."</p> <p>Dynamic message(s) "{ Protocol } : Service account failed to log in." "{ Protocol } : User { User } failed to log in." "{ Protocol } : Service account failed to login from { IP Address }." "{ Protocol } : User { User } failed to login from { IP Address }."</p>	A user or service used the wrong authentication credentials to log in to the device.	<p>Inform the user or update the service to use the correct credentials.</p> <p>If the associated account or IP address is blocked by the brute force prevention mechanism, instruct the user/service to wait the allotted time period before trying again.</p>
Brute-force-prevention	No	Warning	<p>Static message "A user account or an IP address is temporarily blocked, after exceeding maximum count of unsuccessful login attempts."</p> <p>Dynamic message(s) "All: User { User } account is locked for { Minutes } minutes after { Counter } unsuccessful login attempts." "IP:{ IP Address } is temporarily blocked for { Seconds } seconds after { Counter } unsuccessful login attempts."</p>	The account or IP address used by a user or service has been blocked by the brute force prevention mechanism. This occurs after a series of unsuccessful login attempts.	Instruct the user or service to wait 10 minutes before attempting to log in again with the same account or IP address. They may also use a different account or IP address.
Vlan-linkDown/linkUp	No	Info	<p>Static message "VLAN interface up/down."</p> <p>Dynamic message(s) "vlan{ VID }[Up / Down]"</p>	The specified VLAN is up or down.	A notification. Nothing to be done.

Switch management alarms

Related event	Conditional	Severity	Alarm message	Description	Suggested resolution
Bouncing-link	No	Alert	<p>Static message "Bouncing link detected or disappeared on a port."</p> <p>Dynamic message "Bouncing link [is was] detected [on port { port number }]."</p>	Link detection on the specified port was interrupted too frequently.	Check cable connection on both ends. If the problem persists, contact Siemens Customer Support.
Bpdu-guard-activated	No	Alert	<p>Static message "BPDU Guard activated on a port."</p> <p>Dynamic message "Port { port number } BPDU Guard activated."</p>	BPDU guard has been activated and the specified bridge port has been disabled.	Re-enable the bridge port and determine why it received a BPDU.
Bundle-port-inconsistent-speed	No	Error	<p>Static message "Inconsistent speed detected or disappeared on a port."</p> <p>Dynamic message "Inconsistent speed [is was] detected on port { port number }."</p>	An inconsistent speed is detected on a bundle port.	Speed settings must be the same for all bundle ports.
Ertm-target-ip-address-unresolved	Yes	Alert	<p>Static message "Monitoring device with configured IP can't be reached."</p> <p>Dynamic message "[Local Remote] monitoring device with IP: { IP address } can't be reached, verify if the [monitoring device monitoring device and gateway] is up and running."</p>	The packet analyzer/sniffer (monitoring device to which mirrored traffic is sent) is unreachable.	<p>If the packet analyzer/sniffer is on the same subnet (local), make sure the device is operational.</p> <p>If the packet analyzer/sniffer is on a different subnet (remote), verify the gateway configuration and/or make sure the device is operational.</p>
Fast-link-detection-disabled	No	Warning	<p>Static message "FLD disabled or enabled on a port."</p> <p>Dynamic message "Bouncing link [was] detected [on port { port number }] [, disabling FLD]."</p>	Interrupt driven link detection is disabled on the specified port.	Contact Siemens Customer Support.

Related event	Conditional	Severity	Alarm message	Description	Suggested resolution
Intermittent-link	No	Alert	<p>Static message "Intermittent link detected or disappeared on a port."</p> <p>Dynamic message "Link [is was] intermittent on port { port number }."</p>	The link on the specified port goes up and down too frequently.	Check cable connection on both ends. If the problem persists, contact Siemens Customer Support.
Linkdown/linkup	No	Info	<p>Static message "Link status changed on a port."</p> <p>Dynamic message "Port { port number } [is was] down."</p>	The specified port is down.	This alarm clears when the port is up. If the port is not meant to be down, check the cable connection at both ends. If the cable is connected, make sure the port is enabled.
Loop-detection	Yes	Alert	<p>Static message "Loop Detected on a switch port."</p> <p>Dynamic messages "[remote local] loop detected, Interface: { port number } disabled [for { seconds } s]." "[remote local] loop detected, no further actions required for { port number }."</p>	Either a local or remote loop has been detected. The specified port may have been blocked.	Check your network for potential network loops and reset the loop detection state for the specified port.
Mac-address-not-learned	No	Alert	<p>Static message "MAC address failed to be learned on a VLAN."</p> <p>Dynamic message "VLAN { VID }: { MAC address } not learned { error }."</p>	The MAC address indicated was not learned on the VLAN. The maximum capacity for learned MAC addresses may have been reached or a MAC address hash collision may have occurred.	Either remove static entries or wait for entries no longer required by hosts to be removed dynamically.

Related event	Conditional	Severity	Alarm message	Description	Suggested resolution
Received-looped-back-bpdu	No	Alert	<p>Static message "Looped back BPDU received on a port."</p> <p>Dynamic message "Port { port number } received looped back BPDU."</p>	<p>A looped back BPDU is detected on the specified bridge port.</p> <p>This can happen when:</p> <ul style="list-style-type: none"> • A loopback cable/plug is plugged into the bridge port. • The bridge port was previously the root bridge port before the bridge priority was lowered. In this case, the bridge port may receive its own out-dated information before it has been aged-out. • A faulty cable or hardware. 	<p>Based on the possible reasons given, do the following:</p> <ul style="list-style-type: none"> • Remove the loopback stub • Wait for the out-dated information to age-out • Replace the faulty cable or hardware
Unresolved-speed	No	Error	<p>Static message "Unresolved speed detected or disappeared on a port."</p> <p>Dynamic message "[Was] [Unable unable] to obtain speed information from port { port number }."</p>	<p>Unable to determine the speed capabilities of the specified port.</p>	<p>Contact Siemens Customer Support.</p>
Gmrp-cannot-learn-more-addresses	Yes	Alert	<p>Static message <i>None</i></p> <p>Dynamic message "GMRP cannot learn more addresses."</p>	<p>The maximum number of learned multi-cast groups has been reached.</p>	<p>Wait until learned groups no longer required by hosts are removed dynamically.</p>
Gvrp-cannot-learn-more-vlans	Yes	Alert	<p>Static message <i>None</i></p> <p>Dynamic message "GVRP cannot learn more VLANs."</p>	<p>The device has reached the maximum number of supported VLANs.</p>	<p>Either remove static VLANs or wait for VLANs to be removed dynamically.</p>

Related event	Conditional	Severity	Alarm message	Description	Suggested resolution
Igmp-group-membership-table-full	Yes	Alert	Static message <i>None</i> Dynamic message "IGMP Group Membership table full."	The Layer 3 IGMP multicast group membership table is full. This internal table keeps track of unique MAC address/VLAN/port combinations.	Wait until learned groups no longer required by hosts are removed dynamically.
Igmp-mcast-forwarding-table-full	Yes	Alert	Static message <i>None</i> Dynamic message "IGMP Mcast Forwarding table full."	The Layer 2 IGMP multicast group forwarding table is full. This internal table keeps track of unique MAC address/VLAN combinations.	Wait until learned groups no longer required by hosts are removed dynamically.
Mcast-cpu-filtering-table-full	Yes	Alert	Static message <i>None</i> Dynamic message "Can't filter more mcast streams from CPU."	Maximum number of system-installed multicast stream entries has been reached.	An internal error. Nothing to be done.
New-stp-root	No	Notice	Static message <i>None</i> Dynamic message "New STP Root."	A new STP root has been elected.	Verify the change is expected due to changes in the network topology (i.e. network configuration or any unplanned/planned outages).
Stp-topology-change	No	Notice	Static message <i>None</i> Dynamic message "STP topology change."	A bridge port has transitioned from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state.	Verify the transition is expected due to changes in the network topology (i.e. network configuration or any unplanned/planned outages).

Logging aAlarms

Related event	Conditional	Severity	Alarm message	Description	Suggested resolution
Expired-certificate	No	Error	<p>Static message "The TLS certificate is expired."</p> <p>Dynamic message "Certificate validation failed; subject={ subject }, issuer={ issuer }, error='certificate has expired', depth={ depth }"</p>	The certificate for a TLS session has expired.	Replace the certificate used for the specified TLS session.
Invalid-certificate	No	Error	<p>Static message "The TLS certificate is invalid."</p> <p>Dynamic message "Certificate validation failed; subject={ subject }, issuer={ issuer }, error='{ error details }', depth='{ depth }"</p>	The certificate for a TLS session is invalid.	Replace the certificate used for the specified TLS session.

15.4.2 Configuring events

Event configuration is only available in the CLI.

For more information, refer to the SINEC OS Configuration Manual for the CLI.

15.4.3 Monitoring alarms

This section describes the various methods for monitoring alarms.

15.4.3.1 Listing active alarms

To list all alarms that are currently active, navigate to **System » Events » Active Alarms**.

All active alarms are listed in a table format.

The following will be displayed for each active alarm:

Parameter	Description
Date Time	The date and time at which the event occurred.
Resource	The resource (or subsystem) associated with the event.
Event ID	The name of the event.

Parameter	Description
Message	The error message.
Event Number	The number of active instances of the alarm raised by the same event. For example, a value of 2 indicates the same event has occurred twice. As each alarm is cleared, the event number decreases. The alarm is removed from the list once the event number is 0.
Severity	The severity level assigned to the event.
User Action	The required user action. Possible values include: <ul style="list-style-type: none"> • clear-or-ack - The alarm must be cleared or acknowledged • resolve-or-ack - Wait for the condition to resolve on its own or acknowledge the alarm
Actuators/Status	The status of actuators, such as the signaling contact or Alarm LED. Possible values include: <ul style="list-style-type: none"> • none - No effect on actuators • led - Only the Alarm LED is actuated • relay - Only the signaling contact is actuated • led-relay - The Alarm LED and signaling contact are actuated • acked - The event has been acknowledged by a user and the actuator(s) has been reset

15.4.3.2 Clearing and acknowledging alarms

Active alarms can be acknowledged or cleared individually or as a whole.

Acknowledging all active alarms

To acknowledge all active alarms, do the following:

1. Navigate to **System » Events » Active Alarms**.
2. Under **Active Alarms**, click **Acknowledge**.

Acknowledging select alarms

To acknowledge a specific conditional alarm, do the following:

1. Navigate to **System » Events » Active Alarms**.
2. Under **Active Alarms**, click **Acknowledge** in the table for the selected alarm.

Clearing all active alarms

To clear all active alarms, do the following:

1. Navigate to **System » Events » Active Alarms**.
2. Under **Active Alarms**, click **Clear**.

Clearing select alarms

To clear a specific non-conditional alarm, do the following:

1. Navigate to **System » Events » Active Alarms**.
2. Under **Active Alarms**, click **Clear** in the table for the selected alarm.

15.5 SMTP

Events can be configured to send an e-mail to a defined list of recipients when the event occurs. This allows, for example, a set of administrators to be notified when a problem has occurred on one of their devices.

E-mails are sent using the Simple Mail Transfer Protocol (SMTP).

Note

The SMTP service must be enabled globally and also for each event that will send a notification via e-mail.

For more information about configuring events, refer to the **SINEC OS CLI Configuration Manual**.

15.5.1 Understanding SMTP

The SMTP client communicates with a remote SMTP server to send e-mail notifications to a defined list of recipients. Some SMTP servers may require a user account and authentication before processing e-mail requests from the client.

15.5.1.1 SMTP client and server exchanges

When an event occurs and the associated alarm is configured to send an e-mail notification, the SMTP client on the device initiates a TCP connection with a remote SMTP server. The following exchange between the SMTP client and server then occurs:

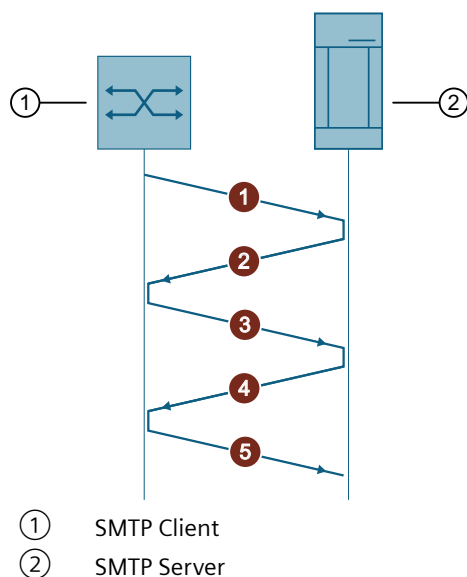


Figure 15-1 SMTP Communication Sequence

Step	Description
①	The SMTP client sends a HELO message to the SMTP server. The TCP connection is established.
②	The SMTP server responds to the HELO message.
③	The SMTP client sends: <ul style="list-style-type: none"> The e-mail address from which the message should be sent The list of recipients
④	The SMTP server accepts the e-mail address and list of recipients.
⑤	The SMTP client sends the e-mail message to the SMTP server.

15.5.1.2 E-mail message format

All e-mails sent by the SMTP service include the following information:

From:	{ SMTP e-mail address }
To:	{ List of recipients }
Subject:	Received event from device { Hostname } with resource({ Resource }) and ID ({ Event ID })

Date:	{ Date }
A new event is raised on device { Device name } (located at { Location }) with the following details:	
Resource: { Resource }	
Event ID: { Event ID }	
Severity: { Severity }	
Time: { Date and time }	
Serial number: { Serial number }	
Message: { Alarm message }	

Example

From:	alerts@company.com
To:	emmanuel.goldstein@company.com; winston.smith@company.com
Subject:	Received event from device XCM332 with resource (switch-mgmt) and ID(Linkdown/linkup)
Date:	Fri, 11 Jun 2021 16:24:38 +0000 (2021-06-11 12:24:38 PM)
A new event is raised on device XCM332 (located at facility 7B) with the following details:	
Resource:switch-mgmt	
Event ID:Linkdown/linkup	
Severity:info	
Fri Jun 11 16:24:38 2021	
Serial Number:VPM5001692	
Message:Port ethernet0/4 is down	

15.5.2 Configuring SMTP

To configure SMTP, do the following:

1. Add users that will receive e-mails from the SMTP service.
For more information, refer to "Adding e-mail recipients (Page 362)".
2. Configure the SMTP user account.
For more information, refer to "Configuring the SMTP account (Page 363)".
3. Configure the SMTP server settings.
For more information, refer to "Configuring the SMTP server (Page 364)".
4. Test the server connection.
For more information, refer to "Testing the SMTP server connection (Page 363)".
5. Enable SMTP.
For more information, refer to "Enabling SMTP (Page 363)".

15.5.2.1 Adding e-mail recipients

E-mails from the SMTP service can be sent simultaneously to up to 20 e-mail addresses.

To add an e-mail address to the recipients list, do the following:

1. Navigate to **System » SMTP Client**.
2. Under **SMTP Recipients**, click **Add**. A new row is added to the table.
3. Under **Email Address**, enter the e-mail address of the new recipient.
4. Commit the change.

15.5.2.2 Testing the SMTP server connection

To test the SMTP server connection, do the following:

1. Navigate to **System » SMTP Client**.
2. Under **Simple Mail Transfer Protocol (SMTP) Client**, click **Test SMTP**.

15.5.2.3 Enabling SMTP

To enable the SMTP service, do the following:

Note

The SMTP service is disabled by default.

Note

The SMTP account must be defined before the SMTP service can be enabled.

For information about defining the SMTP account, refer to "Configuring the SMTP account (Page 363)".

1. Navigate to **System » SMTP Client**.
2. Under **Simple Mail Transfer Protocol (SMTP) Client**, change **Status** to **Enabled**.
3. Commit the change.

15.5.3 Configuring the SMTP account

The SMTP service requires an e-mail account from which to send all event messages.

To configure the account, do the following:

1. Set the e-mail address from which all event messages will be sent.
For more information, refer to "Configuring the account e-mail address (Page 364)".
2. [Optional] Add a description for the address.
For more information, refer to "Adding a description for the account (Page 364)".

15.5.3.1 Configuring the account e-mail address

To set the e-mail account from which SMTP sends all event messages, do the following:

1. Navigate to **System » SMTP Client**.
2. Under **SMTP Account**, enter the e-mail address for the SMTP account under **Email Address**.
3. Commit the change.

15.5.3.2 Adding a description for the account

To give a description to the SMTP account, do the following:

1. Navigate to **System » SMTP Client**.
2. Under **SMTP Account**, enter a brief description under **Description**.
Condition:
 - Must be between 1 and 128 characters long
3. Commit the change.

15.5.4 Configuring the SMTP server

To configure the SMTP server settings, do the following:

Note

Only a single SMTP server can be defined.

1. Configure the SMTP server profile for the server that will be used to distribute e-mail notifications.
For more information, refer to "Configuring the SMTP server profile (Page 364)".
2. Set the maximum time in which SINEC OS will wait for a reply from the SMTP server.
For more information, refer to "Configuring the delay for SMTP responses (Page 365)".
3. [Optional] Configure the SMTP client to authenticate itself with the SMTP server.
For more information, refer to "Configuring SMTP authentication (Page 365)".

15.5.4.1 Configuring the SMTP server profile

To configure the profile for the SMTP server used to distribute e-mail notifications, do the following:

1. Navigate to **System » SMTP Client**.
2. Under **SMTP Server**, in the **Server Address/FQDN** column, enter the hostname or IP address.
Condition:
 - Must be between 0 and 253 characters long
3. Under **Port**, enter the port on which the SMTP server receives messages.
Default: 25

4. [Optional] Under **Description**, enter a description for the SMTP server.
Condition:
 - Must be between 1 and 128 characters long
5. Commit the changes.

15.5.4.2 Configuring the delay for SMTP responses

When the SMTP client initiates the TCP connection with the SMTP server, it sends a HELLO message. The SMTP server has a limited amount of time to reply before the client considers the server unreachable.

To configure how long the SMTP client will wait for a response from the SMTP server, do the following:

1. Navigate to **System » SMTP Client**.
2. Under **SMTP Server**, in the **Timeout** column, enter the time under **Timeout**.
Conditions:
 - Formatted as nYnMnDnhnmns, where n is a user-defined number
 - Minimum of 1 second (1s)
 - Maximum of 255 seconds (255s)Default: 30s (30 seconds)
3. Commit the change.

15.5.5 Configuring SMTP authentication

All communications between the SMTP client and server can be authenticated. This requires a user account on the SMTP server.

Note

The password is sent to the SMTP server as plain text. Make sure the SMTP server is configured to accept plain text passwords.

To configure the SMTP client to authenticate itself, do the following:

1. Setup an account on the SMTP server. Note the username and password credentials associated with the account.
2. Configure the SMTP client to submit the credentials when connecting with the SMTP server. For more information, refer to "Configuring the SMTP user (Page 366)".
3. Enable SMTP authentication. For more information, refer to "Enabling SMTP authentication (Page 366)".

15.5.5.1 Configuring the SMTP user

To configure the SMTP user, do the following:

1. Navigate to **System » SMTP client**.
2. Under **SMTP Account**, change **Username** to the username associated with the account on the SMTP server.
Conditions:
 - Must be between 1 and 128 characters long
 - Must start with either an underscore (_) or an alphanumeric character
 - The username may contain any alphanumeric, numeric, or ASCII (0x20 to 0x7E) characters, including underscores (_), hyphens (-), dots (.), and the at sign (@)
3. Under **Password**, enter the password associated with the username.
Conditions:
 - Must be between 1 and 128 characters long
 - Must start with either an underscore (_) or an alphanumeric character
 - The username may contain any alphanumeric, numeric, or ASCII (0x20 to 0x7E) characters, including underscores (_), hyphens (-), dots (.), and the at sign (@)
4. Enter the password again under **Password Confirm**.
5. Commit the changes.

15.5.5.2 Enabling SMTP authentication

To enable SMTP user authentication, do the following:

Note

SMTP user authentication is disabled by default.

1. Navigate to **System » SMTP client**.
2. Under **SMTP Account**, change **Authentication** to **Enabled**.
3. Commit the change.

15.5.6 Configuration examples

The following are examples of how to deploy SMTP.

15.5.6.1 Configuring SMTP to send event notifications

This example demonstrates how to configure the device to send e-mail notifications to a group of administrators.

The following topology shows an SMTP client sending e-mail notifications to a remote SMTP server, ATNSer6, on port 25.

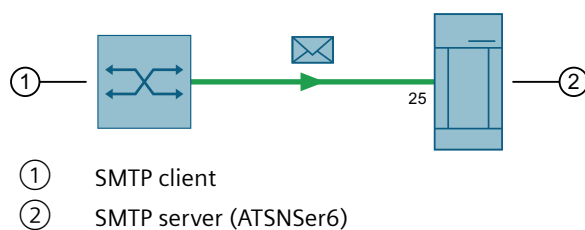


Figure 15-2 Sending e-mail notifications to ATNSer6

The client uses SMTP authentication to make sure communications are secure. It is also configured to wait up to 60 seconds for a response from the server.

To achieve this configuration, do the following:

1. Set the e-mail account that all e-mail notifications will be sent from.
For more information, refer to "Configuring the account e-mail address (Page 364)".
2. Set the SMTP server (ATNSer6) and port number (25).
For more information, refer to "Configuring the SMTP server profile (Page 364)".
3. Set the time delay for responses from the server to 60 seconds.
For more information, refer to "Configuring the delay for SMTP responses (Page 365)".
4. Set the SMTP username known to the SMTP server.
For more information, refer to "Configuring the SMTP user (Page 366)".
5. Enable SMTP authentication.
For more information, refer to "Enabling SMTP authentication (Page 366)".
6. Set the e-mail recipients.
For more information, refer to "Adding e-mail recipients (Page 362)".
7. Enable the SMTP service.
For more information, refer to "Enabling SMTP (Page 363)".
8. Configure one or more alarms to send an e-mail notification via SMTP.
For more information, refer to "Configuring events (Page 358)".
9. [Optional] Generate an alarm and monitor the SMTP server to verify the e-mail notification was forwarded.

15.6 Traffic mirroring

Traffic mirroring is a Layer 2 feature that allows the duplication of one or more traffic streams for the purpose of traffic monitoring and analysis. Mirrored traffic is forwarded to an external packet analyzer/sniffer. Network administrators and engineers analyze the traffic to detect intrusions, analyze data, troubleshoot/debug errors, and monitor the overall performance of the network.

15.6.1 Understanding traffic mirroring

Traffic received and/or transmitted on any bridge port or VLAN can be mirrored (copied and forwarded) to a packet analyzer/sniffer. The analyzer can be connected locally to the same device where mirrored traffic is generated, or it can be connected to a remote device accessible over the network.

15.6.1.1 Traffic mirroring sessions

A traffic mirroring session defines multiple traffic sources (i.e. bridge ports or VLANs) and a single destination to which the mirrored traffic will be forwarded. The destination must be unique between all sessions.

At this time, SINEC OS only supports one session (session 1), which is pre-configured with a destination port (ethernet0/1). This is a default configuration that can be changed as needed.

NOTICE

Configuration hazard - risk of connectivity loss

Bridge ports used to manage the device should not be selected as a destination for mirrored traffic. When a bridge port is designated as a traffic mirroring destination, it is automatically removed from all VLANs and put into switchport mode. Any active sessions on that port will be closed and future access to the device through that port will not be possible.
--

15.6.1.2 Traffic mirroring sources and destinations

Traffic mirroring requires one or more traffic sources and a single mirroring destination.

Traffic sources

A traffic source can be either a bridge port and/or a VLAN.

When a bridge port is the source, mirroring can be isolated to traffic travelling in a specific direction (ingress or egress), or all traffic traversing the port.

When a VLAN is the source, all traffic traversing the device that belongs to the VLAN is mirrored.

Mirroring destinations

A mirroring destination is either a dedicated bridge port or an IP address to which mirrored traffic is forwarded.

Use a dedicated bridge port if the packet analyzer/sniffer is connected directly to the device or to another device on the same network.

Alternatively, if the packet analyzer/sniffer is accessible by IP address, mirrored traffic can be forwarded using Encapsulated Remote Traffic Mirroring (ERTM). ERTM forwards mirrored traffic on a Layer 3 network over a GRE tunnel by encapsulating the traffic with MAC, IP, and GRE headers. The encapsulated traffic is routed to the analyzer like regular Layer 3 traffic, where it is decapsulated before being analyzed.

15.6.1.3 Deploying traffic mirroring

Before deploying traffic mirroring, note the following requirements and limitations:

- If the full-duplex rate of frames on the source bridge port exceeds the transmission speed of the destination port, frames will be dropped. Since both received and transmitted traffic on the source bridge port is mirrored to the destination port, frames will be discarded if the total traffic exceeds the destination port's transmission speed. This problem is amplified when traffic on a 100 Mbps full-duplex source port is mirrored to a 10 Mbps half-duplex destination port.
- Switch management frames generated by the device (e.g. Telnet, HTTP, SNMP, etc.) may not be mirrored.
- Invalid frames received on the monitor port will not be mirrored. These include CRC errors, oversized or undersized packets, fragments, jabbers, collisions, late collisions, and dropped events.

15.6.2 Configuring traffic mirroring

To configure traffic mirroring, do the following:

1. Define one or more traffic sources to monitor.
A traffic source can be a bridge port with a specific traffic direction (i.e. ingress, egress, or both) or a VLAN. Each traffic source must be defined separately.
For more information, refer to "Selecting a traffic source (Page 369)".
2. Select the destination for the mirrored traffic.
The destination can be either a bridge port or an IP address.
For more information, refer to "Configuring the mirroring destination (Page 371)".
3. Enable traffic mirroring.
For more information, refer to "Enabling traffic mirroring (Page 371)".

15.6.2.1 Selecting a traffic source

A single traffic mirroring session can define multiple traffic sources. Sources can be traffic received and/or forwarded by an interface, or traffic belonging to a specific VLAN.

To select a traffic source, do the following:

1. Navigate to **Layer 2 » Traffic Mirroring**.
2. Under **Traffic Mirroring Sources**, select either an interface or a VLAN source for the desired session.

For an interface, configure the following:

- **Ingress Traffic of Ports**
Select one or more interfaces. Traffic received by the interfaces will be mirrored.
- **Egress Traffic of Ports**
Select one or more interface. Traffic forwarded by the interfaces will be mirrored.

For a VLAN, configure the following:

- **Traffic of VLANs**
Select or enter a VLAN ID. Any traffic belonging to the specified VLAN will be mirrored.

3. Commit the changes.

Example

The following configures session 1 to only mirror the traffic forwarded on ethernet0/5.

Session	Traffic of VLANs	Ingress Traffic of Ports	Egress Traffic of Ports
1	-	0 items selected.	ethernet0/5

Example

The following configures session 1 to additionally mirror traffic received by ethernet0/2, ethernet0/3, and ethernet0/4.

Session	Traffic of VLANs	Ingress Traffic of Ports	Egress Traffic of Ports
1	-	ethernet0/2, ethernet0/3, ethernet0/4	ethernet0/5

Example

The following configures session 1 to additionally mirror traffic tagged for VLAN 10.

Session	Traffic of VLANs	Ingress Traffic of Ports	Egress Traffic of Ports
1	10	ethernet0/2, ethernet0/3, ethernet0/4	ethernet0/5

15.6.2.2 Configuring the mirroring destination

Mirrored traffic can be forwarded to an interface or an IP address.

NOTICE
Configuration hazard - risk of connectivity loss
Bridge ports used to manage the device should not be selected as a destination for mirrored traffic. When a bridge port is designated as a traffic mirroring destination, it is automatically removed from all VLANs and put into switchport mode. Any active sessions on that port will be closed and future access to the device through that port will not be possible.

To configure the destination for mirrored traffic, do the following:

1. Navigate to **Layer 2 » Traffic Mirroring**.
2. Under **Traffic Mirroring Sessions**, select a bridge port under **Destination Port** on which to forward mirrored traffic.
3. Under **Destination Remote IP**, enter an IP address to which mirrored traffic will be sent.
4. Commit the changes.

Example

The following configures session 1 to mirror traffic on ethernet0/2.

Session	State	Destination Port	Destination Remote IP
1	Disabled	ethernet0/2	

Example

The following configures session 1 to send mirrored traffic to IP address 172.30.141.141.

Session	State	Destination Port	Destination Remote IP
1	Disabled	-	172.30.141.141

15.6.2.3 Enabling traffic mirroring

Traffic mirroring is disabled by default.

NOTICE
Configuration hazard - risk of connectivity loss
Once traffic mirroring is enabled, the selected destination port will be automatically removed from all VLANs and converted to switchport mode. Any active sessions on that port will be closed and future access to the device through that port will not be possible.

To enable traffic mirroring, do the following:

1. Navigate to **Layer 2 » Traffic Mirroring**.
2. Under **Traffic Mirroring Sessions**, change **State** to **Enabled** for the select session.
3. Commit the change.

Example

The following enables traffic mirroring for session 1.

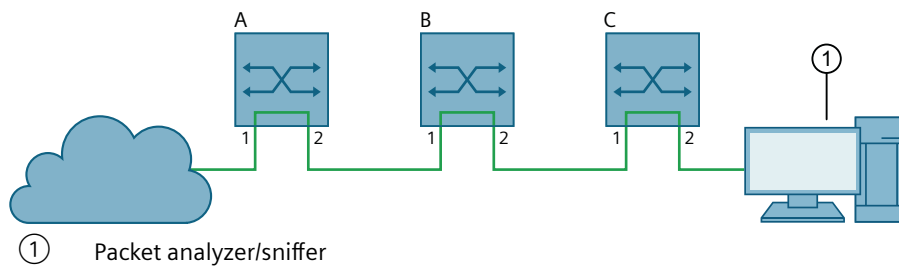
Session	State	Destination Port	Destination Remote IP
1	Enabled	ethernet0/1	

15.6.3 Configuration examples

The following are examples of how to deploy port mirroring.

15.6.3.1 Configuring traffic mirroring across a Layer 2 network

In this example, traffic received by bridge port ethernet0/1 on Switch A is mirrored and forwarded to Switch C, which is connected to a packet analyzer/sniffer. Mirrored traffic must be routed through Switch B.



① Packet analyzer/sniffer

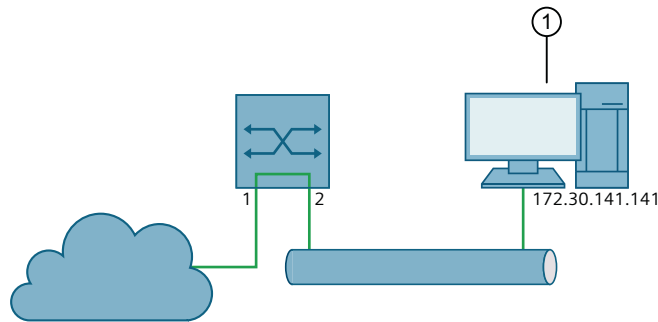
Figure 15-3 Traffic mirroring across a Layer 2 network

To configure each switch, do the following:

1. Set the source to bridge port ethernet0/1.
For more information, refer to "Selecting a traffic source (Page 369)".
2. Set the destination to bridge port ethernet0/2.
For more information, refer to "Configuring the mirroring destination (Page 371)".
3. Enable traffic monitoring.
For more information, refer to "Enabling traffic mirroring (Page 371)".

15.6.3.2 Configuring remote traffic mirroring

In this example, traffic received by ethernet0/1 is mirrored, encapsulated, and forwarded along a GRE tunnel to a computer running packet analyzer/sniffer software. The computer is available at 172.30.141.141.



① Packet analyzer/sniffer

Figure 15-4 Encapsulated remote traffic mirroring

To configure the device, do the following:

1. Set the source to be ingress traffic on bridge port ethernet0/1.
For more information, refer to "Selecting a traffic source (Page 369)".
2. Set the destination to IP address 172.30.141.141.
For more information, refer to "Configuring the mirroring destination (Page 371)".
3. Enable traffic monitoring.
For more information, refer to "Enabling traffic mirroring (Page 371)".

15.7 Cable diagnostics

Connectivity issues can sometimes be attributed to problems with Ethernet cables. To help detect cable faults, short circuits, open cables, or cables that are too long, SINEC OS includes a built-in cable diagnostics utility.

15.7.1 Running a cable diagnostic test

To run a cable diagnostic test on an Ethernet cable, do the following:

Note

The average duration of a cable diagnostic test on a single bridge port is one to two seconds.

Note

Cable diagnostic tests can be run simultaneously on different ports.

Note

Cable diagnostic tests can only be performed on copper Ethernet wires.

1. Determine the bridge port to which the target Ethernet cable is connected.
2. Make sure the other end of the cable is connected to a bridge port with the same network capabilities.
For example, connect a 100Base-T port to a 100Base-T port, or a 1000Base-T port to a 1000Base-T port.
3. Navigate to **Interfaces » Ethernet interfaces » Cable Diagnostics**.
4. Click **Start** for the selected bridge port to begin the cable diagnostic test.
Test results are displayed immediately once the test is complete.
For more information about the test results, refer to "Displaying cable diagnostics results (Page 374)".
5. [Optional] Reset the bridge port.
For more information, refer to "Resetting a bridge port (Page 182)".

15.7.2 Displaying cable diagnostics results

Test results are available under **Interfaces » Ethernet interfaces » Cable Diagnostics** and are displayed immediately after running a diagnostics test.

The following information is displayed for each bridge port that has been tested:

Parameter	Description
Diagnostic State	The current state of the cable diagnostics test. Possible values include: <ul style="list-style-type: none"> • <code>stopped</code> - The test is complete • <code>started</code> - The test is in progress
Result	The result of the last cable diagnostics test. Possible values include: <ul style="list-style-type: none"> • <code>passed</code> - The bridge port passed the last test • <code>failed</code> - The bridge port failed the last test

Parameter	Description
Result Pair [N]	<p>The cable test result for the wire pair, where <i>N</i> is either:</p> <ul style="list-style-type: none"> • 12 (pair 1/2) • 36 (pair 3/6) • 45 (pair 4/5) • 78 (pair 7/8) <p>Possible values include:</p> <ul style="list-style-type: none"> • <code>good</code> - No faults, shorts, or impedance mismatch were detected • <code>open</code> - An open circuit is detected in the cable (i.e. no pin contact) • <code>short</code> - A short circuit is detected in the cable • <code>impedance</code> - An impedance mismatch is detected <p>For FastEthernet bridge ports, a <code>good</code> result is required for <code>result-pair12</code> and <code>result-pair36</code>.</p> <p>For Gigabit Ethernet bridge ports, a <code>good</code> result is required for all wire pairs.</p>
Distance Pair [N]	<p>The Distance-to-Fault (DTF) measurement for the wire pair, where <i>N</i> is either:</p> <ul style="list-style-type: none"> • 12 (pair 1/2) • 36 (pair 3/6) • 45 (pair 4/5) • 78 (pair 7/8) <p>The measurement is the distance in meters (m) from the device to the fault in the wire.</p>

This section describes errors that can occur when working with SINEC OS or when developing a network, as well as corresponding solutions.

Note

If you need more support, please contact Siemens customer support.

16.1 The device is in a restart loop

The device is performing restarts continuously and you can no longer access the device.

Solution

If the device is in a restart loop, you have the following options:

- Contact Siemens customer service.
A Siemens service technician can load debug information from the device and investigate the error.
For more information, refer to "Customer support (Page 19)".
- Reset the device to default settings with the button.
The debug information saved by the device is lost and the error cannot be investigated.
For more information, refer to "Button functions (Page 103)".

16.1 The device is in a restart loop