

SIEMENS

SIMATIC NET

Industrial Ethernet Switches Command Line Interface (CLI) SINEC OS V2.4

Configuration Manual

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

10/2023


C79000-G8976-C498-07


| | |
|------------------------------------|----|
| 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 | 21 |
| 1.1 | Conventions | 21 |
| 1.1.1 | Alerts..... | 21 |
| 1.1.2 | CLI command syntax..... | 21 |
| 1.2 | System requirements/recommendations..... | 22 |
| 1.3 | Cybersecurity information..... | 22 |
| 1.4 | Firmware/software support..... | 23 |
| 1.5 | Open source | 23 |
| 1.6 | Trademarks..... | 23 |
| 1.7 | Related documents | 24 |
| 1.8 | Training..... | 26 |
| 1.9 | Customer support..... | 26 |
| 2 | Introduction..... | 27 |
| 2.1 | Features and benefits..... | 27 |
| 2.2 | Security recommendations..... | 30 |
| 2.3 | Configuration limits | 34 |
| 2.4 | Available services..... | 36 |
| 2.5 | Access rights..... | 37 |
| 2.6 | Device configuration | 39 |
| 2.7 | CLI modes..... | 41 |
| 3 | User interface | 43 |
| 3.1 | Basic commands | 43 |
| 3.1.1 | General commands..... | 43 |
| 3.1.2 | General commands in operational mode..... | 46 |
| 3.1.3 | General commands in configuration mode | 46 |
| 3.2 | Configuration transactions | 51 |
| 3.2.1 | Select a configuration mode..... | 52 |
| 3.2.2 | Displaying the current configuration..... | 52 |
| 3.2.3 | Using the no command..... | 53 |
| 3.2.4 | Committing configuration changes (Commit) | 55 |
| 3.2.5 | Restoring a configuration (Rollback) | 57 |
| 3.3 | Basic operation | 61 |
| 3.3.1 | Operating the CLI with the keyboard | 61 |
| 3.3.2 | Permitted characters | 63 |
| 3.3.3 | Using regular expressions..... | 63 |
| 3.3.4 | Configuring parameters in different ways..... | 64 |

| | | |
|----------|---|------------|
| 3.3.5 | Processing a series of commands | 65 |
| 3.3.6 | Executing commands as script..... | 65 |
| 3.3.7 | Specifying a URL | 67 |
| 3.3.8 | Specifying a duration | 69 |
| 3.3.9 | Showing operative data | 70 |
| 3.3.10 | Using wildcards to specify interfaces in show commands..... | 71 |
| 3.3.11 | Multiple selection of interfaces | 71 |
| 3.3.12 | Customizing the output of a command..... | 73 |
| 3.3.13 | Adapting the output of lists..... | 84 |
| 3.4 | Help commands..... | 86 |
| 3.4.1 | Displaying all available options for a command..... | 86 |
| 3.4.2 | Showing the infotext for a command..... | 87 |
| 3.4.3 | Completing a command | 87 |
| 3.5 | Configuration of the user interfaces | 88 |
| 3.5.1 | Configuring the NETCONF user interface..... | 90 |
| 3.5.1.1 | Enabling the NETCONF user interface | 90 |
| 3.5.1.2 | Changing the inactivity timeout for NETCONF sessions | 91 |
| 3.5.1.3 | Configuring a server endpoint for NETCONF..... | 92 |
| 3.5.1.4 | Changing the SSH key exchange method for a NETCONF server endpoint..... | 93 |
| 3.5.1.5 | Enabling a server endpoint for NETCONF | 95 |
| 3.5.2 | Configuring the CLI user interface | 96 |
| 3.5.2.1 | Changing the inactivity timeout for CLI sessions | 96 |
| 3.5.2.2 | Configuring a server endpoint for the CLI..... | 98 |
| 3.5.2.3 | Changing the SSH key exchange method for a CLI server endpoint..... | 99 |
| 3.5.2.4 | Enabling a server endpoint for the CLI | 101 |
| 3.5.2.5 | Configuring the local CLI environment..... | 102 |
| 3.5.3 | Configuring the Web user interface | 103 |
| 3.5.3.1 | Enabling the Web user interface..... | 103 |
| 3.5.3.2 | Changing the inactivity timeout for Web UI sessions | 104 |
| 3.5.3.3 | Configuring an HTTP server endpoint for the Web UI..... | 105 |
| 3.5.3.4 | Enabling an HTTP server endpoint for the Web UI | 106 |
| 3.5.3.5 | Configuring an HTTPS server endpoint for the Web UI..... | 107 |
| 3.5.3.6 | Enabling an HTTPS server endpoint for the Web UI | 108 |
| 3.5.3.7 | Using a user-defined HTTPS certificate | 109 |
| 4 | Getting started | 111 |
| 4.1 | Calling the CLI..... | 111 |
| 4.1.1 | Accessing the CLI through the USB console interface | 111 |
| 4.1.2 | Accessing the CLI via a network connection | 112 |
| 4.2 | Logging in | 112 |
| 4.2.1 | Default user profiles and passwords..... | 113 |
| 4.2.2 | Logging in to a device with default settings | 113 |
| 4.2.3 | Logging in to a configured device | 115 |
| 4.3 | Logging out | 115 |
| 4.4 | Basic settings | 115 |
| 4.4.1 | Configuring basic settings | 115 |
| 4.4.1.1 | Changing the host name..... | 116 |
| 4.4.1.2 | Specifying the device location | 117 |
| 4.4.1.3 | Specifying the contact person for the device..... | 117 |
| 4.4.1.4 | Defining the default gateway manually..... | 118 |

| | | |
|----------|--|------------|
| 4.4.2 | Displaying the basic settings | 119 |
| 5 | Device management..... | 121 |
| 5.1 | Restarting and shutting down the device..... | 121 |
| 5.1.1 | Understanding restarting and shutting down the device | 121 |
| 5.1.1.1 | Canceling a command..... | 121 |
| 5.1.1.2 | Exiting sessions..... | 121 |
| 5.1.1.3 | Taking configuration changes into account | 122 |
| 5.1.2 | Restarting the device | 122 |
| 5.1.3 | Shutting down the device | 122 |
| 5.2 | Resetting the device to default settings | 123 |
| 5.3 | Decommissioning the device..... | 124 |
| 5.4 | Firmware | 125 |
| 5.4.1 | Understanding firmware management | 125 |
| 5.4.2 | Displaying the current firmware version..... | 125 |
| 5.4.3 | Obtaining a firmware package..... | 126 |
| 5.4.4 | Upgrading the firmware | 127 |
| 5.4.5 | Downgrading the firmware | 129 |
| 5.4.6 | Rejecting a loaded firmware file..... | 131 |
| 5.4.7 | Activating the backup firmware | 131 |
| 5.5 | Device hardware | 132 |
| 5.5.1 | Listing Hardware Components | 133 |
| 5.5.2 | Displaying the Last Time the Hardware Information Was Changed..... | 134 |
| 5.6 | Configuration file | 134 |
| 5.6.1 | Saving the current configuration as a file on a remote server..... | 135 |
| 5.6.2 | Loading a configuration file from a remote server | 137 |
| 5.6.3 | Displaying the header information of a configuration file | 144 |
| 5.7 | Open Source Software information | 145 |
| 5.7.1 | Saving OSS information on a remote server | 146 |
| 5.8 | Signaling contact..... | 146 |
| 5.8.1 | Setting the signaling contact mode | 147 |
| 5.8.2 | Displaying the current signaling contact state..... | 147 |
| 5.9 | Button function | 148 |
| 5.9.1 | Understanding the button functions..... | 148 |
| 5.9.2 | Enabling the 'Reset to default settings' button function..... | 148 |
| 5.10 | Configuration and License PLUG | 149 |
| 5.10.1 | Understanding the CLP..... | 150 |
| 5.10.1.1 | Device replacement | 150 |
| 5.10.1.2 | Modes | 151 |
| 5.10.1.3 | Firmware on CLP..... | 151 |
| 5.10.1.4 | Encryption methods..... | 152 |
| 5.10.1.5 | Memory areas..... | 153 |
| 5.10.1.6 | Related events | 153 |
| 5.10.2 | Saving firmware on the CLP..... | 153 |
| 5.10.3 | Saving the device configuration on the CLP..... | 154 |
| 5.10.4 | Deleting data on the CLP..... | 154 |
| 5.10.5 | Resetting the CLP | 155 |
| 5.10.6 | Showing the status of the CLP | 155 |

| | | |
|----------|--|------------|
| 6 | System administration..... | 157 |
| 6.1 | Configuring a banner for login..... | 157 |
| 6.2 | Password policy | 158 |
| 6.2.1 | Configuring the password policy..... | 159 |
| 6.2.1.1 | Configuring the minimum number of characters..... | 159 |
| 6.2.1.2 | Configuring the maximum number of characters | 160 |
| 6.2.1.3 | Configuring the condition for numbers | 161 |
| 6.2.1.4 | Configuring the condition for lowercase letters | 161 |
| 6.2.1.5 | Configuring the condition for uppercase letters | 162 |
| 6.2.1.6 | Configuring the condition for special characters..... | 163 |
| 6.2.1.7 | Enabling the password policy | 163 |
| 6.2.2 | Displaying the password policy..... | 164 |
| 6.3 | User administration | 165 |
| 6.3.1 | Understanding user management | 165 |
| 6.3.1.1 | User profiles..... | 165 |
| 6.3.1.2 | Case sensitivity in user names | 166 |
| 6.3.1.3 | Deleting a user..... | 166 |
| 6.3.2 | Configuring users..... | 167 |
| 6.3.2.1 | Configuring a new user | 167 |
| 6.3.2.2 | Enabling the assignment of a new password | 169 |
| 6.3.2.3 | Changing the password of a user..... | 171 |
| 6.3.2.4 | Changing the user profile of a user | 173 |
| 6.3.3 | Monitoring users..... | 174 |
| 6.3.3.1 | Displaying active users | 174 |
| 6.3.3.2 | Displaying user details..... | 174 |
| 6.3.3.3 | Logging off a user | 175 |
| 6.3.3.4 | Sending messages to users | 176 |
| 6.4 | Preparing the device for troubleshooting | 176 |
| 6.4.1 | Saving debug information on a remote server | 176 |
| 6.4.2 | Enabling the Debug user account..... | 177 |
| 7 | Security..... | 179 |
| 7.1 | Brute-Force Attack (BFA) prevention | 179 |
| 7.1.1 | Understanding BFA prevention..... | 179 |
| 7.1.1.1 | How the prevention mechanism works..... | 179 |
| 7.1.1.2 | Related events | 180 |
| 7.1.2 | Configuring BFA prevention..... | 180 |
| 7.1.2.1 | Changing the auto-reset timer..... | 180 |
| 7.1.2.2 | Changing the maximum number of failed login attempts | 181 |
| 7.1.2.3 | Changing the time between failed login attempts..... | 183 |
| 7.1.2.4 | Enabling BFA prevention | 184 |
| 7.1.3 | Unblocking a user or IP address | 184 |
| 7.1.4 | Monitoring BFA prevention..... | 185 |
| 7.2 | Security-relevant events | 186 |
| 7.2.1 | Understanding security-relevant events..... | 186 |
| 7.2.1.1 | SIEM system | 186 |
| 7.2.1.2 | Structure of an event message | 188 |
| 7.2.1.3 | Variables in event messages..... | 189 |
| 7.2.2 | Monitoring security-relevant events | 190 |

| | | |
|----------|---|-----|
| 7.2.2.1 | Identification and authentication of human users | 191 |
| 7.2.2.2 | Identification and authentication of devices..... | 194 |
| 7.2.2.3 | User account management | 195 |
| 7.2.2.4 | Unsuccessful login attempts..... | 197 |
| 7.2.2.5 | Session lock..... | 197 |
| 7.2.2.6 | Limiting the number of simultaneous sessions | 198 |
| 7.2.2.7 | Configuration changes | 198 |
| 7.2.2.8 | Communication integrity | 199 |
| 7.2.2.9 | Software and information integrity..... | 199 |
| 7.2.2.10 | Session integrity | 200 |
| 7.2.2.11 | Protection from denial-of-service (DoS) attacks | 200 |
| 7.2.2.12 | Protection of check information | 201 |
| 7.2.2.13 | Restoring the automation system | 201 |
| 7.3 | Keys and certificates..... | 201 |
| 7.3.1 | Understanding keys and certificates..... | 202 |
| 7.3.1.1 | Key method | 202 |
| 7.3.1.2 | Default key pairs | 203 |
| 7.3.1.3 | Certificates..... | 203 |
| 7.3.1.4 | Certificates from an official certificate authority | 204 |
| 7.3.1.5 | Self-signed certificates | 204 |
| 7.3.1.6 | Certificate chain | 204 |
| 7.3.1.7 | Signatures | 205 |
| 7.3.1.8 | Storage locations | 206 |
| 7.3.1.9 | Access rules | 206 |
| 7.3.1.10 | Related events | 206 |
| 7.3.2 | Managing the keystore..... | 207 |
| 7.3.2.1 | Manually configuring a key pair | 207 |
| 7.3.2.2 | Importing a key pair | 209 |
| 7.3.2.3 | Manually configuring a certificate..... | 213 |
| 7.3.2.4 | Importing a certificate | 214 |
| 7.3.3 | Managing the truststore..... | 217 |
| 7.3.3.1 | Manually configuring a certificate..... | 217 |
| 7.3.3.2 | Importing a certificate | 218 |
| 7.3.3.3 | Manually configuring a known host..... | 221 |
| 7.3.4 | Monitoring certificates | 223 |
| 7.3.4.1 | Showing fingerprints..... | 223 |
| 7.4 | User authentication | 224 |
| 7.4.1 | Understanding user authentication | 224 |
| 7.4.1.1 | Authentication mode | 224 |
| 7.4.1.2 | RADIUS authentication..... | 225 |
| 7.4.2 | Configuring user authentication | 229 |
| 7.4.3 | Configuring RADIUS authentication | 229 |
| 7.4.3.1 | Configuring a RADIUS server profile | 229 |
| 7.4.3.2 | Configuring a RADIUS server..... | 232 |
| 7.4.3.3 | Testing a RADIUS server connection | 235 |
| 7.4.4 | Selecting the user authentication mode | 235 |
| 7.4.5 | Monitoring user authentication..... | 237 |
| 7.4.5.1 | Displaying RADIUS statistics | 237 |
| 7.5 | Management Access Control List (ACL)..... | 239 |
| 7.5.1 | Understanding management ACLs | 239 |
| 7.5.2 | Configuring the management ACL..... | 240 |

| | | |
|----------|---|------------|
| 7.5.2.1 | Adding a rule | 240 |
| 7.5.2.2 | Restricting access based on VLAN interface | 242 |
| 7.5.2.3 | Restricting access based on user interface | 243 |
| 7.5.2.4 | Enabling the management ACL | 245 |
| 7.5.3 | Monitoring the management ACL..... | 245 |
| 7.5.3.1 | Displaying the operational state of the management ACL | 246 |
| 7.5.4 | Configuration examples | 246 |
| 7.5.4.1 | Creating an authorized manager for a range of remote hosts | 246 |
| 7.6 | Port security | 248 |
| 7.6.1 | Understanding port security..... | 248 |
| 7.6.1.1 | Static MAC address-based authentication | 249 |
| 7.6.1.2 | IEEE 802.1X authentication..... | 249 |
| 7.6.1.3 | IEEE 802.1X authentication with MAB | 250 |
| 7.6.1.4 | Restricted VLANs..... | 251 |
| 7.6.1.5 | Assigning VLANs with tunnel attributes | 252 |
| 7.6.1.6 | Static VLAN requirement | 253 |
| 7.6.2 | Configuring port security..... | 253 |
| 7.6.2.1 | Enabling port security | 254 |
| 7.6.2.2 | Setting the security mode | 255 |
| 7.6.2.3 | Setting the Quarantine VLAN ID | 256 |
| 7.6.2.4 | Setting the Guest VLAN ID..... | 257 |
| 7.6.2.5 | Enabling sticky mode | 258 |
| 7.6.2.6 | Setting the maximum number of dynamically learned MAC addresses | 259 |
| 7.6.2.7 | Enabling administrative shutdown mode..... | 260 |
| 7.6.2.8 | Setting the administrative shutdown timer | 261 |
| 7.6.3 | Configuring IEEE 802.1X | 262 |
| 7.6.3.1 | Setting the held period | 263 |
| 7.6.3.2 | Setting the quiet period | 264 |
| 7.6.3.3 | Enabling the periodic reauthentication of supplicants..... | 265 |
| 7.6.3.4 | Setting the supplicant reauthentication timeout period | 266 |
| 7.6.3.5 | Setting the maximum number of reauthentication attempts | 267 |
| 7.6.3.6 | Setting the supplicant timeout period..... | 268 |
| 7.6.3.7 | Setting the authenticator timeout period..... | 269 |
| 7.6.4 | Monitoring port security | 270 |
| 7.6.4.1 | Displaying the security status of a bridge port..... | 270 |
| 8 | Interface management..... | 273 |
| 8.1 | Interfaces | 273 |
| 8.1.1 | Understanding interfaces..... | 273 |
| 8.1.1.1 | Interface naming conventions..... | 274 |
| 8.1.1.2 | Auto-negotiation | 274 |
| 8.1.1.3 | Duplex communication | 274 |
| 8.1.1.4 | Controller protection through Link Fault Indication (LFI) | 275 |
| 8.1.1.5 | Function Extender Interface (FEI) ports..... | 276 |
| 8.1.1.6 | Hot swapping/hot plugging..... | 277 |
| 8.1.1.7 | SFP transceiver ports..... | 277 |
| 8.1.2 | Configuring bridge ports | 279 |
| 8.1.2.1 | Adding a description for a bridge port | 279 |
| 8.1.2.2 | Enabling auto-negotiation..... | 280 |
| 8.1.2.3 | Selecting the bridge port speed..... | 281 |
| 8.1.2.4 | Selecting the duplex mode..... | 283 |
| 8.1.2.5 | Enabling downshift for gigabit interfaces | 285 |

| | | |
|----------|---|------------|
| 8.1.2.6 | Enabling Link Fault Indication (LFI) | 286 |
| 8.1.2.7 | Configuring the action for link down events..... | 286 |
| 8.1.2.8 | Enabling link up/down traps | 287 |
| 8.1.2.9 | Enabling Smart SFP (for SFP ports only) | 288 |
| 8.1.2.10 | Enabling a bridge port..... | 289 |
| 8.1.3 | Configuring VLAN interfaces | 289 |
| 8.1.3.1 | Adding a VLAN interface | 290 |
| 8.1.3.2 | Adding a description for a VLAN interface..... | 291 |
| 8.1.3.3 | Configuring the MTU size | 291 |
| 8.1.3.4 | Enabling link up/down traps..... | 292 |
| 8.1.3.5 | Enabling a VLAN interface..... | 293 |
| 8.1.4 | Resetting a bridge port..... | 294 |
| 8.1.5 | Monitoring interfaces..... | 294 |
| 8.1.5.1 | Displaying interface characteristics..... | 294 |
| 8.1.5.2 | Displaying receive/transmit statistics for all interfaces | 295 |
| 8.1.5.3 | Displaying receive/transmit statistics for only bridge ports | 297 |
| 8.1.5.4 | Displaying negotiated settings for each bridge port | 299 |
| 8.1.5.5 | Displaying the MAC address for each interface..... | 300 |
| 8.1.5.6 | Displaying the auto-negotiation capability of each bridge port..... | 300 |
| 8.1.5.7 | Displaying the administrative state of each interface | 301 |
| 8.1.5.8 | Displaying the link state of each interface..... | 302 |
| 8.1.5.9 | Monitoring SFP transceivers | 304 |
| 8.2 | MAC address table | 305 |
| 8.2.1 | Understanding the MAC address table | 305 |
| 8.2.1.1 | Dynamic MAC entries..... | 306 |
| 8.2.1.2 | Static MAC entries..... | 307 |
| 8.2.2 | Configuring the MAC address table..... | 307 |
| 8.2.2.1 | Configuring the MAC address aging time | 307 |
| 8.2.2.2 | Enabling MAC address aging on link failure..... | 308 |
| 8.2.3 | Configuring static MAC filtering entries | 309 |
| 8.2.3.1 | Adding a static MAC filtering entry | 309 |
| 8.2.3.2 | Assigning a traffic class queue | 310 |
| 8.2.4 | Monitoring the MAC address table..... | 311 |
| 8.2.4.1 | Displaying the MAC address table | 311 |
| 8.2.4.2 | Clearing dynamic MAC addresses | 312 |
| 9 | IP Address Assignment | 315 |
| 9.1 | Static IP address assignment..... | 315 |
| 9.1.1 | Configuring a static IPv4 address | 315 |
| 9.1.2 | Listing the IPv4 address configuration..... | 316 |
| 9.2 | Static DNS..... | 317 |
| 9.2.1 | Understanding DNS | 317 |
| 9.2.1.1 | Basic terms for DNS..... | 317 |
| 9.2.1.2 | DNS communication | 318 |
| 9.2.2 | Configuring DNS | 319 |
| 9.2.2.1 | Configuring a DNS server | 319 |
| 9.2.2.2 | Configuring the number of request attempts to a DNS server | 320 |
| 9.2.2.3 | Configuring the waiting time for a DNS server to respond | 321 |
| 9.2.2.4 | Configuring a search domain..... | 321 |
| 9.2.3 | Displaying the DNS configuration | 322 |
| 9.3 | DHCP..... | 323 |

| | | |
|-----------|---|------------|
| 9.3.1 | Understanding DHCP | 323 |
| 9.3.1.1 | DHCP communication | 323 |
| 9.3.1.2 | DHCP server..... | 325 |
| 9.3.2 | Configuring the device as a DHCP client..... | 325 |
| 9.3.2.1 | Enabling a DHCP client interface | 325 |
| 9.3.2.2 | Requesting a lease time | 326 |
| 9.3.2.3 | Changing the client ID of an interface | 327 |
| 9.3.2.4 | Including the hostname in DHCP messages | 328 |
| 9.3.2.5 | Requesting a configuration file from the DHCP server (option 66, 67)..... | 329 |
| 9.3.3 | Monitoring DHCP client interfaces..... | 331 |
| 9.3.3.1 | Listing configuration data of DHCP client interfaces | 331 |
| 9.3.3.2 | Monitoring DHCP messages..... | 333 |
| 9.3.3.3 | Clearing the statistics of DHCP messages | 334 |
| 10 | Network redundancy | 335 |
| 10.1 | Spanning Tree Protocol (STP)..... | 335 |
| 10.1.1 | Understanding STP..... | 335 |
| 10.1.1.1 | Rapid Spanning Tree Protocol (RSTP)..... | 335 |
| 10.1.1.2 | RSTP Applications..... | 340 |
| 10.1.1.3 | Enhanced Rapid Spanning Tree Protocol (eRSTP)..... | 344 |
| 10.1.1.4 | Multiple Spanning Tree Protocol (MSTP) | 345 |
| 10.1.1.5 | Related events | 350 |
| 10.1.2 | Configuring STP globally..... | 350 |
| 10.1.2.1 | Enabling STP..... | 351 |
| 10.1.2.2 | Selecting the STP version | 352 |
| 10.1.2.3 | Selecting the bridge priority | 353 |
| 10.1.2.4 | Configuring the Hello time | 354 |
| 10.1.2.5 | Configuring the maximum aging time | 355 |
| 10.1.2.6 | Configuring the transmit hold count..... | 356 |
| 10.1.2.7 | Configuring the forward delay..... | 357 |
| 10.1.3 | Configuring STP for bridge ports..... | 358 |
| 10.1.3.1 | Enabling STP for a bridge port | 358 |
| 10.1.3.2 | Configuring the bridge port cost..... | 359 |
| 10.1.3.3 | Selecting the bridge port priority..... | 360 |
| 10.1.3.4 | Selecting the edge port state..... | 361 |
| 10.1.3.5 | Selecting the bridge port link type..... | 362 |
| 10.1.3.6 | Restricting the role of a bridge port | 363 |
| 10.1.3.7 | Preventing a bridge port from forwarding TCNs | 364 |
| 10.1.3.8 | Enabling Enhanced Passive Listening Compatibility (EPLC) | 365 |
| 10.1.4 | Configuring eRSTP..... | 366 |
| 10.1.4.1 | Selecting the maximum network diameter | 367 |
| 10.1.4.2 | Configuring the BPDU Guard Timeout..... | 368 |
| 10.1.4.3 | Selecting the Fast Root Failover mechanism..... | 369 |
| 10.1.4.4 | Enabling IEEE 802.1w interoperability | 370 |
| 10.1.5 | Configuring MSTP | 371 |
| 10.1.5.1 | Selecting the maximum number of hops | 371 |
| 10.1.5.2 | Adding the region name | 372 |
| 10.1.5.3 | Configuring the region revision level | 373 |
| 10.1.6 | Configuring Multiple Spanning Tree Instances (MSTIs) | 373 |
| 10.1.6.1 | Creating an MSTI | 374 |
| 10.1.6.2 | Selecting the bridge priority | 375 |
| 10.1.6.3 | Mapping a VLAN to an MSTI..... | 375 |

| | | |
|-----------|---|-----|
| 10.1.6.4 | Configuring the bridge port priority for an MSTI..... | 376 |
| 10.1.6.5 | Configuring the MSTI cost for a bridge port..... | 377 |
| 10.1.7 | Monitoring STP | 378 |
| 10.1.7.1 | Displaying the status of STP..... | 378 |
| 10.1.7.2 | Displaying the status of STP per bridge port..... | 380 |
| 10.1.7.3 | Displaying MSTP region information | 383 |
| 10.1.7.4 | Displaying the status of an MSTI..... | 383 |
| 10.1.7.5 | Displaying the status of an MSTI per bridge port | 385 |
| 10.1.7.6 | Clearing STP statistics..... | 387 |
| 10.1.8 | Configuration examples | 387 |
| 10.1.8.1 | A basic MSTP configuration | 387 |
| 10.2 | Loop Detection | 389 |
| 10.2.1 | Understanding the detection of network loops | 389 |
| 10.2.1.1 | Port modes | 390 |
| 10.2.1.2 | Types of network loops | 391 |
| 10.2.1.3 | VLAN mode | 391 |
| 10.2.1.4 | Related events | 391 |
| 10.2.2 | Configuring Loop Detection..... | 392 |
| 10.2.2.1 | Requirements for sending PDUs..... | 393 |
| 10.2.2.2 | Configuring bridge ports for the detection of network loops..... | 394 |
| 10.2.2.3 | Configuring the send interval | 395 |
| 10.2.2.4 | Defining the limit for the detection of a local network loop | 396 |
| 10.2.2.5 | Configuring the reaction to local network loops | 397 |
| 10.2.2.6 | Configuring the reaction to remote network loops | 398 |
| 10.2.2.7 | Configuring the duration for disabling a bridge port..... | 399 |
| 10.2.2.8 | Enabling VLAN mode | 401 |
| 10.2.2.9 | Enabling Loop Detection | 401 |
| 10.2.2.10 | Resetting a bridge port manually after detection of a network loop..... | 402 |
| 10.2.3 | Monitoring the Loop Detection..... | 402 |
| 10.2.3.1 | Showing the status of Loop Detection | 402 |
| 10.3 | Device Level Ring | 403 |
| 10.3.1 | Understanding DLR | 404 |
| 10.3.1.1 | Ring supervisor | 404 |
| 10.3.1.2 | Ring nodes..... | 405 |
| 10.3.1.3 | DLR frames | 405 |
| 10.3.1.4 | DLR network | 407 |
| 10.3.2 | Configuring DLR..... | 408 |
| 10.3.2.1 | Selecting the DLR VLAN..... | 409 |
| 10.3.2.2 | Checking requirements for DLR ports..... | 409 |
| 10.3.2.3 | Selecting the DLR ports | 411 |
| 10.3.2.4 | Enabling DLR | 412 |
| 10.3.3 | Monitoring DLR..... | 413 |
| 10.3.4 | Configuration examples | 414 |
| 10.3.4.1 | Using DLR in VLAN 0 | 414 |
| 10.4 | Media Redundancy Protocol | 415 |
| 10.4.1 | Useful Information on MRP | 416 |
| 10.4.1.1 | MRP roles..... | 416 |
| 10.4.1.2 | MRP network | 417 |
| 10.4.1.3 | Media Redundancy Automanager..... | 419 |
| 10.4.1.4 | Ring ports..... | 420 |
| 10.4.1.5 | Redundancy domain | 420 |

| | | |
|-----------|--|------------|
| 10.4.1.6 | Reconfiguration time..... | 421 |
| 10.4.1.7 | Installation guide | 421 |
| 10.4.1.8 | MRP configuration via a PROFINET controller | 422 |
| 10.4.2 | Configuring MRP | 423 |
| 10.4.2.1 | Checking MRP requirements..... | 423 |
| 10.4.2.2 | Configuring an MRP instance..... | 426 |
| 10.4.2.3 | Enabling MRP globally..... | 428 |
| 10.4.2.4 | Changing the redundancy domain | 428 |
| 10.4.2.5 | Changing the MRP role..... | 430 |
| 10.4.2.6 | Changing ring ports | 431 |
| 10.4.3 | Monitoring MRP | 433 |
| 10.4.3.1 | Showing the operative MRP role..... | 433 |
| 10.4.3.2 | Showing the operative ring ports | 434 |
| 10.4.3.3 | Showing the status of the ring ports..... | 434 |
| 10.4.3.4 | Showing the delay of test frames | 435 |
| 10.4.3.5 | Showing the status of the MRM..... | 435 |
| 10.4.3.6 | Showing the number of status changes..... | 436 |
| 10.5 | Passive Listening | 436 |
| 10.5.1 | Understanding Passive Listening | 436 |
| 10.5.1.1 | Simple coupling without Passive Listening | 437 |
| 10.5.1.2 | Redundant coupling with Passive Listening..... | 437 |
| 10.5.1.3 | Topology changes | 440 |
| 10.5.2 | Configuring passive listening..... | 440 |
| 10.5.2.1 | Activating passive listening | 440 |
| 10.5.2.2 | Activating VLAN-specific forwarding of BPDUs | 441 |
| 10.5.2.3 | Blocking forwarding of (R)STP-BPDUs | 442 |
| 11 | Network discovery and management | 443 |
| 11.1 | LLDP..... | 443 |
| 11.1.1 | Understanding LLDP..... | 443 |
| 11.1.1.1 | TLV Format | 443 |
| 11.1.1.2 | LLDPDUs..... | 444 |
| 11.1.1.3 | Send and receive module | 445 |
| 11.1.2 | Configuring LLDP | 445 |
| 11.1.2.1 | Configuring the sending and receiving of LLDPDUs for a bridge port..... | 446 |
| 11.1.2.2 | Defining the TTL in outgoing LLDPDUs..... | 446 |
| 11.1.2.3 | Defining the send interval for LLDPDUs..... | 447 |
| 11.1.2.4 | Defining the delay of LLDPDUs during initialization of LLDP on a bridge port..... | 448 |
| 11.1.2.5 | Defining the transmission delay of the LLDPDU after a configuration change | 449 |
| 11.1.3 | Monitoring LLDP | 449 |
| 11.1.3.1 | Displaying the LLDP information of the device that is transmitted to neighbor devices..... | 450 |
| 11.1.3.2 | Monitoring the LLDP information of neighbor devices..... | 450 |
| 11.2 | DCP | 452 |
| 11.2.1 | Understanding DCP..... | 452 |
| 11.2.2 | Configuring DCP..... | 452 |
| 11.2.2.1 | Configuring the access rights of DCP..... | 452 |
| 11.2.2.2 | Configuring the forwarding of DCP frames for a bridge port..... | 456 |
| 11.3 | PROFINET..... | 457 |
| 11.3.1 | Understanding PROFINET | 457 |
| 11.3.1.1 | PROFINET components..... | 458 |
| 11.3.1.2 | Device addressing | 459 |

| | | |
|-----------|--|-----|
| 11.3.1.3 | PROFINET communication | 459 |
| 11.3.1.4 | PROFINET relations | 460 |
| 11.3.1.5 | I&M data..... | 460 |
| 11.3.1.6 | GSD file..... | 461 |
| 11.3.2 | Configuring PROFINET | 461 |
| 11.3.2.1 | Configuring the TIA interface..... | 461 |
| 11.3.2.2 | Configuring the behavior in case of a PROFINET error..... | 463 |
| 11.3.2.3 | Configuring PROFINET runtime mode | 463 |
| 11.3.2.4 | Saving the GSD file on a remote server | 464 |
| 11.3.3 | Monitoring PROFINET..... | 465 |
| 11.3.3.1 | Displaying the current PROFINET runtime mode..... | 465 |
| 11.3.3.2 | Monitoring the connection to a PROFINET controller..... | 466 |
| 11.3.3.3 | Monitoring the TIA interface | 466 |
| 11.3.3.4 | Displaying the I&M data | 467 |
| 11.3.3.5 | Displaying the PROFINET device name | 468 |
| 11.4 | EtherNet/IP | 468 |
| 11.4.1 | Understanding EtherNet/IP..... | 469 |
| 11.4.1.1 | Common Industrial Protocol | 469 |
| 11.4.1.2 | Message types | 469 |
| 11.4.1.3 | Producer-consumer relationship | 469 |
| 11.4.1.4 | Object model | 470 |
| 11.4.1.5 | Supported objects..... | 470 |
| 11.4.1.6 | Electronic Data Sheet | 470 |
| 11.4.2 | Configuring EtherNet/IP..... | 471 |
| 11.4.2.1 | Configuring the management interface | 471 |
| 11.4.2.2 | Enabling EtherNet/IP | 472 |
| 11.4.2.3 | Saving the EDS file on a remote server | 472 |
| 11.5 | ARP..... | 473 |
| 11.5.1 | Understanding ARP | 473 |
| 11.5.2 | Displaying the ARP table summary | 474 |
| 11.6 | SNMP | 475 |
| 11.6.1 | Understanding SNMP | 475 |
| 11.6.1.1 | SNMP versions | 476 |
| 11.6.1.2 | SNMP components..... | 476 |
| 11.6.1.3 | Engine ID..... | 477 |
| 11.6.1.4 | Management information base | 477 |
| 11.6.1.5 | Requests and notifications..... | 478 |
| 11.6.1.6 | SNMP communication..... | 478 |
| 11.6.1.7 | SNMP ports..... | 479 |
| 11.6.1.8 | Object identifier | 479 |
| 11.6.1.9 | sysName MIB object..... | 480 |
| 11.6.1.10 | Authentication and access rights..... | 480 |
| 11.6.1.11 | SNMP communities with SNMPv1 and SNMPv2c..... | 480 |
| 11.6.1.12 | User-based Security Model (USM) with SNMPv3 | 481 |
| 11.6.1.13 | Passwords and localized keys..... | 481 |
| 11.6.1.14 | View-based Access Control Model (VACM) for assigning access rights | 482 |
| 11.6.1.15 | Processing of an SNMP request..... | 483 |
| 11.6.2 | Configuring SNMP | 484 |
| 11.6.3 | Configuring the SNMP agent | 485 |
| 11.6.3.1 | Configuring the SNMP versions the SNMP agent supports | 485 |
| 11.6.3.2 | Configuring a server endpoint for SNMP | 487 |

| | | |
|-----------|--|------------|
| 11.6.3.3 | Enabling a server endpoint for SNMP..... | 488 |
| 11.6.3.4 | Enabling the SNMP agent..... | 489 |
| 11.6.4 | Configuring an SNMP community..... | 490 |
| 11.6.4.1 | Defining an SNMP community..... | 490 |
| 11.6.4.2 | Defining the context in which an SNMP community can access MIB data..... | 492 |
| 11.6.4.3 | Linking an SNMP community with an SNMP target..... | 493 |
| 11.6.5 | Configuring an SNMP user..... | 494 |
| 11.6.5.1 | Creating an SNMP user..... | 494 |
| 11.6.5.2 | Defining an authentication password for an SNMP user..... | 495 |
| 11.6.5.3 | Specifying a localized key for the authentication..... | 496 |
| 11.6.5.4 | Defining an encryption password for an SNMP user..... | 497 |
| 11.6.5.5 | Specifying a localized key for the encryption..... | 499 |
| 11.6.6 | Configuring SNMP access rights..... | 500 |
| 11.6.6.1 | Defining an SNMP view..... | 500 |
| 11.6.6.2 | Defining an SNMP group with access rights to MIB areas (views)..... | 502 |
| 11.6.6.3 | Assigning a security name with an SNMP group..... | 504 |
| 11.6.7 | Configuring an SNMP target..... | 506 |
| 11.6.7.1 | Configuring parameters for SNMPv1/v2c targets..... | 506 |
| 11.6.7.2 | Configuring parameters for SNMPv3 targets..... | 508 |
| 11.6.7.3 | Defining an SNMP target..... | 509 |
| 11.6.7.4 | Changing the port for receiving SNMP notifications..... | 511 |
| 11.6.8 | Configuring an SNMP notification..... | 512 |
| 11.6.8.1 | Configuring an SNMP notification..... | 512 |
| 11.6.9 | Monitoring SNMP..... | 513 |
| 11.6.9.1 | Displaying the engine ID..... | 513 |
| 12 | Traffic control and classification..... | 515 |
| 12.1 | Rate limiting..... | 515 |
| 12.1.1 | Understanding rate limiting..... | 515 |
| 12.1.2 | Configuring rate limiting..... | 516 |
| 12.1.2.1 | Determining interface capabilities..... | 516 |
| 12.1.2.2 | Selecting the type of frames to limit..... | 518 |
| 12.1.2.3 | Selecting the rate limit..... | 519 |
| 12.1.2.4 | Enabling rate limiting..... | 520 |
| 12.1.3 | Configuration examples..... | 521 |
| 12.1.3.1 | Limiting the rate of traffic..... | 521 |
| 12.2 | VLANs..... | 521 |
| 12.2.1 | Understanding VLANs..... | 522 |
| 12.2.1.1 | How VLANs are created..... | 523 |
| 12.2.1.2 | VLAN-aware and VLAN-unaware modes..... | 523 |
| 12.2.1.3 | Tagged vs. untagged frames..... | 524 |
| 12.2.1.4 | Access and trunk ports..... | 526 |
| 12.2.1.5 | Native VLAN vs. default VLAN..... | 526 |
| 12.2.1.6 | Ingress filtering..... | 526 |
| 12.2.1.7 | Ingress and egress rules..... | 527 |
| 12.2.1.8 | GARP VLAN Registration Protocol (GVRP)..... | 528 |
| 12.2.1.9 | Forbidden VLANs..... | 529 |
| 12.2.1.10 | VLAN-0-Tunnel mode..... | 529 |
| 12.2.1.11 | Advantages and disadvantages of using VLANs..... | 530 |
| 12.2.2 | Configuring VLANs..... | 531 |
| 12.2.2.1 | Adding or modifying a static VLAN..... | 531 |
| 12.2.2.2 | Enabling GVRP..... | 532 |

| | | |
|-----------|--|------------|
| 12.2.2.3 | Enabling VLAN-0-Tunnel mode | 533 |
| 12.2.3 | Configuring VLAN settings for bridge ports | 534 |
| 12.2.3.1 | Selecting the port membership type | 534 |
| 12.2.3.2 | Configuring the port VLAN ID | 535 |
| 12.2.3.3 | Selecting the frame types accepted | 535 |
| 12.2.3.4 | Selecting the GVRP mode | 536 |
| 12.2.3.5 | Enabling PVID tagging on egress traffic | 537 |
| 12.2.3.6 | Enabling ingress filtering | 538 |
| 12.2.3.7 | Restricting VLAN membership | 539 |
| 12.2.4 | Monitoring VLANs | 540 |
| 12.2.4.1 | Displaying dynamically-learned VLANs | 540 |
| 12.2.4.2 | Displaying untagged ports for static VLANs | 541 |
| 12.2.4.3 | Displaying egress ports for static VLANs | 541 |
| 12.3 | Traffic classes | 542 |
| 12.3.1 | Understanding traffic classes | 542 |
| 12.3.1.1 | Traffic class queues | 543 |
| 12.3.1.2 | Weighting algorithms | 543 |
| 12.3.1.3 | Default mapping | 544 |
| 12.3.1.4 | Prioritization of ingress frames | 545 |
| 12.3.1.5 | Priority regeneration | 546 |
| 12.3.2 | Configuring traffic classes | 546 |
| 12.3.2.1 | Configuring the default priority | 547 |
| 12.3.2.2 | Mapping a PCP value to a traffic class | 548 |
| 12.3.2.3 | Mapping a DSCP tag to a traffic class | 549 |
| 12.3.2.4 | Configuring trust mode | 550 |
| 12.3.2.5 | Assigning different priorities to traffic on egress | 552 |
| 12.3.3 | Configuration examples | 554 |
| 12.3.3.1 | Prioritizing all frames | 554 |
| 12.3.3.2 | Prioritizing select frames | 555 |
| 13 | Time settings | 557 |
| 13.1 | Manual time setting | 557 |
| 13.1.1 | Configuring the date and the system time manually | 557 |
| 13.1.2 | Showing the date and system time | 558 |
| 13.2 | Time change and daylight saving | 559 |
| 13.2.1 | Configuring the time zone | 559 |
| 13.2.2 | Configuring the time offset | 560 |
| 13.2.3 | Configuring a date for switching to daylight saving time | 561 |
| 13.2.4 | Configuring a rule for switching to daylight saving time | 562 |
| 13.2.5 | Configuring the time offset during daylight saving time | 563 |
| 13.3 | NTP | 564 |
| 13.3.1 | Understanding NTP | 564 |
| 13.3.1.1 | Stratum Number | 565 |
| 13.3.1.2 | NTP server | 565 |
| 13.3.1.3 | NTP client | 566 |
| 13.3.1.4 | NTP authentication | 566 |
| 13.3.2 | Configuring an NTP client | 566 |
| 13.3.2.1 | Enabling the NTP service | 567 |
| 13.3.2.2 | Configuring an NTP server | 568 |
| 13.3.2.3 | Enabling an NTP server | 569 |
| 13.3.2.4 | Changing the NTP version | 569 |

| | | |
|-----------|--|------------|
| 13.3.2.5 | Configuring the NTP polling interval | 570 |
| 13.3.2.6 | Enabling iBurst..... | 572 |
| 13.3.2.7 | Enabling Burst | 572 |
| 13.3.3 | Configuring NTP authentication..... | 574 |
| 13.3.3.1 | Configuring an authentication key..... | 574 |
| 13.3.3.2 | Applying an authentication key | 575 |
| 13.3.4 | Monitoring NTP..... | 576 |
| 13.3.4.1 | Displaying the NTP configuration..... | 576 |
| 13.3.4.2 | Showing the status of the NTP system time | 578 |
| 13.3.4.3 | Monitoring NTP connections | 579 |
| 13.4 | SIMATIC time | 581 |
| 13.4.1 | Understanding SIMATIC Time | 581 |
| 13.4.2 | Enabling the SIMATIC time client..... | 581 |
| 13.5 | PTP | 582 |
| 13.5.1 | Understanding PTP..... | 582 |
| 13.5.1.1 | Supported clock types | 582 |
| 13.5.1.2 | PTP messages | 582 |
| 13.5.1.3 | PTP domains | 583 |
| 13.5.1.4 | PTP profiles | 583 |
| 13.5.1.5 | Best Master Clock Algorithm (BMCA) | 584 |
| 13.5.1.6 | Transparent clocks | 585 |
| 13.5.2 | Configuring PTP | 586 |
| 13.5.2.1 | Defining the PTP domain | 586 |
| 13.5.2.2 | Enabling PTP for a bridge port | 587 |
| 13.5.2.3 | Enabling PTP globally | 588 |
| 13.5.3 | Monitoring PTP | 588 |
| 13.5.3.1 | Displaying the peer mean path delay..... | 588 |
| 14 | Multicast filtering | 591 |
| 14.1 | Static multicast groups..... | 591 |
| 14.1.1 | Configuring static multicast groups | 591 |
| 14.1.1.1 | Adding a static multicast group | 591 |
| 14.1.1.2 | Selecting the traffic class for a static multicast group | 592 |
| 14.1.1.3 | Assigning a forwarding port to a static multicast group..... | 593 |
| 14.2 | GMRP | 594 |
| 14.2.1 | Understanding GMRP | 594 |
| 14.2.1.1 | Joining/leaving multicast groups with GMRP | 595 |
| 14.2.1.2 | GARP attribute types | 595 |
| 14.2.2 | Configuring GMRP..... | 596 |
| 14.2.2.1 | Enabling GMRP | 596 |
| 14.2.2.2 | Selecting the GMRP mode per bridge port | 597 |
| 14.2.2.3 | Configuring a delay before leaving a multicast group | 597 |
| 14.2.2.4 | Enabling topology change flooding | 598 |
| 14.2.3 | Configuration examples | 599 |
| 14.2.3.1 | Establishing membership with multicast groups using GMRP | 599 |
| 14.3 | IGMP snooping | 601 |
| 14.3.1 | Understanding IGMP snooping..... | 601 |
| 14.3.1.1 | IGMP modes | 601 |
| 14.3.1.2 | Filtering/pruning multicast traffic | 602 |
| 14.3.1.3 | IGMP snooping querier..... | 602 |

| | | |
|-----------|--|------------|
| 14.3.1.4 | IGMP snooping rules | 602 |
| 14.3.2 | Configuring IGMP snooping | 603 |
| 14.3.2.1 | Enabling IGMP snooping | 603 |
| 14.3.2.2 | Selecting the IGMP version | 604 |
| 14.3.2.3 | Selecting the IGMP mode | 605 |
| 14.3.2.4 | Configuring the IGMP query interval | 606 |
| 14.3.2.5 | Enabling topology change flooding | 607 |
| 14.3.2.6 | Enabling IGMP snooping per VLAN | 608 |
| 14.3.3 | Configuring multicast router forwarding | 609 |
| 14.3.3.1 | Enabling multicast router forwarding | 609 |
| 14.3.3.2 | Configuring a multicast router interface | 610 |
| 14.3.4 | Monitoring IGMP snooping | 611 |
| 14.3.4.1 | Displaying the number of learned multicast groups | 611 |
| 14.3.4.2 | Displaying the status of learned multicast groups | 611 |
| 14.3.4.3 | Displaying the destination MAC address of a learned multicast group | 612 |
| 14.3.4.4 | Displaying the last host to send a report to a learned multicast group | 613 |
| 14.3.4.5 | Displaying the interfaces that receive IGMP join messages for a learned multicast group ... | 614 |
| 14.3.4.6 | Displaying the interfaces that forward multicast traffic to multicast routers for a learned multicast group | 615 |
| 14.3.4.7 | Displaying the uptime of a learned multicast group | 616 |
| 14.4 | Multicast filtering database | 617 |
| 14.4.1 | Displaying multicast filtering database | 617 |
| 14.4.2 | Displaying the traffic class assigned to a multicast group entry | 619 |
| 14.4.3 | Displaying the forwarding port assigned to a multicast group entry | 619 |
| 14.4.4 | Displaying the state of a forwarding port assigned to a multicast group entry | 620 |
| 15 | Diagnostics | 621 |
| 15.1 | System status | 621 |
| 15.1.1 | Displaying the system boot time | 621 |
| 15.1.2 | Displaying the system up time | 621 |
| 15.2 | Network utilities | 621 |
| 15.2.1 | Ping | 621 |
| 15.2.1.1 | Understanding Ping | 622 |
| 15.2.1.2 | Pinging an IP address or a host | 622 |
| 15.2.2 | Traceroute | 624 |
| 15.2.2.1 | Understanding the trace route | 624 |
| 15.2.2.2 | Determining the data path to a host (Traceroute) | 625 |
| 15.3 | System logging | 625 |
| 15.3.1 | Understanding system logging | 626 |
| 15.3.1.1 | Structure of a syslog entry | 626 |
| 15.3.1.2 | Severity levels | 627 |
| 15.3.1.3 | Syslog facilities | 627 |
| 15.3.1.4 | Remote logging | 627 |
| 15.3.1.5 | Event filtering | 627 |
| 15.3.1.6 | Repudiation | 628 |
| 15.3.2 | Configuring system logging | 628 |
| 15.3.2.1 | Setting the timestamp format | 629 |
| 15.3.2.2 | Filtering the logbook | 629 |
| 15.3.3 | Configuring remote system logging | 631 |
| 15.3.3.1 | Adding a remote syslog server profile | 631 |
| 15.3.3.2 | Defining a filtering rule for a remote syslog server | 634 |

| | | |
|----------|---|-----|
| 15.3.4 | Monitoring the system log | 637 |
| 15.3.4.1 | Displaying the logbook..... | 637 |
| 15.3.4.2 | Clearing the logbook..... | 637 |
| 15.3.4.3 | Clearing local system log files | 638 |
| 15.3.4.4 | Exporting the system log..... | 638 |
| 15.3.5 | Configuration examples | 639 |
| 15.3.5.1 | Filtering the logbook..... | 639 |
| 15.3.5.2 | Filtering messages forwarded to remote syslog servers | 639 |
| 15.4 | Event management..... | 640 |
| 15.4.1 | Understanding event management | 641 |
| 15.4.1.1 | Severity levels | 641 |
| 15.4.1.2 | Resources and events..... | 641 |
| 15.4.1.3 | Alarms..... | 643 |
| 15.4.2 | Configuring events..... | 651 |
| 15.4.2.1 | Enabling an event to generate an alarm | 652 |
| 15.4.2.2 | Defining the severity for an event | 653 |
| 15.4.2.3 | Enabling an event to issue an e-mail notification..... | 654 |
| 15.4.2.4 | Enabling an event to trigger an SNMP trap..... | 655 |
| 15.4.2.5 | Enabling an event to activate the signaling contact..... | 656 |
| 15.4.2.6 | Enabling an event to activate the alarm LED | 657 |
| 15.4.2.7 | Enabling alarms to clear automatically | 658 |
| 15.4.2.8 | Enabling an event | 659 |
| 15.4.3 | Monitoring alarms | 660 |
| 15.4.3.1 | Listing active alarms..... | 660 |
| 15.4.3.2 | Clearing and acknowledging alarms | 662 |
| 15.5 | SMTP | 663 |
| 15.5.1 | Understanding SMTP..... | 663 |
| 15.5.1.1 | SMTP client and server exchanges | 664 |
| 15.5.1.2 | E-mail message format..... | 664 |
| 15.5.2 | Configuring SMTP | 665 |
| 15.5.2.1 | Adding e-mail recipients..... | 665 |
| 15.5.2.2 | Testing the SMTP server connection | 666 |
| 15.5.2.3 | Enabling SMTP..... | 666 |
| 15.5.3 | Configuring the SMTP account | 667 |
| 15.5.3.1 | Configuring the account e-mail address | 667 |
| 15.5.3.2 | Adding a description for the account | 668 |
| 15.5.4 | Configuring the SMTP server | 669 |
| 15.5.4.1 | Configuring the SMTP server profile | 669 |
| 15.5.4.2 | Configuring the delay for SMTP responses | 670 |
| 15.5.5 | Configuring SMTP authentication | 671 |
| 15.5.5.1 | Configuring the SMTP user | 672 |
| 15.5.5.2 | Enabling SMTP authentication..... | 673 |
| 15.5.6 | Displaying the status of SMTP..... | 674 |
| 15.5.7 | Configuration examples | 674 |
| 15.5.7.1 | Configuring SMTP to send event notifications | 674 |
| 15.6 | Traffic mirroring | 675 |
| 15.6.1 | Understanding traffic mirroring | 676 |
| 15.6.1.1 | Traffic mirroring sessions..... | 676 |
| 15.6.1.2 | Traffic mirroring sources and destinations..... | 676 |
| 15.6.1.3 | Deploying traffic mirroring | 677 |
| 15.6.1.4 | Traffic mirroring and ARP..... | 677 |

| | | |
|-----------|--|------------|
| 15.6.2 | Configuring traffic mirroring | 677 |
| 15.6.2.1 | Selecting a traffic source | 677 |
| 15.6.2.2 | Configuring a mirroring destination | 679 |
| 15.6.2.3 | Enabling traffic mirroring | 681 |
| 15.6.3 | Configuration examples | 681 |
| 15.6.3.1 | Configuring traffic mirroring across a Layer 2 network..... | 682 |
| 15.6.3.2 | Configuring remote traffic mirroring | 682 |
| 15.7 | Cable diagnostics | 683 |
| 15.7.1 | Running a cable diagnostic test | 683 |
| 15.7.2 | Displaying cable diagnostics results | 684 |
| 16 | Troubleshooting..... | 687 |
| 16.1 | The device is in a restart loop | 687 |
| 16.2 | The device switches off during system startup | 687 |
| 16.3 | The device changes the mode of a bridge port (use of DLR in connection with loop detection)..... | 688 |
| 16.4 | The device cannot be reached via CLI and Web UI (loading a firmware file via TFTP) | 689 |
| 16.5 | The device interrupts the transmission of a firmware file from a remote server..... | 690 |
| 16.6 | Data traffic floods occur on conversion from MRP to Spanning Tree | 690 |

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 Conventions

This section describes the conventions used by this document to present information clearly and effectively.

1.1.1 Alerts

Throughout this document, alert messages, such as Danger, Warning, Caution, Notice, and Note, are inserted to highlight important information to the reader. Whenever possible, alerts are placed in context before the topic, sentence, table, or figure to which they are related. For example, a Danger or Warning alert will appear directly before a step that instructs users to do anything that is potentially harmful to themselves or others.

1.1.2 CLI command syntax

This document details CLI commands. A CLI command consists of a key command, parameters, options and/or user variables.

Elements of a CLI command

In the following command, `interface` is the key command, `{ name }` is a user-variable, `vlan` and `type` are parameters, and `[access | trunk]` are fixed options.

```
interface { name } vlan type [ access | trunk ]
```

Command formatting

CLI commands are displayed in this document according to the following syntax rules:

| Convention | Description | Example |
|---------------------|---|---|
| Font | All commands, parameters, and options are displayed in a monospace font. | <code>command parameter value</code> |
| User-Defined Values | Some parameters require a user-defined value. Values that need to be defined by you are wrapped in braces (curly brackets). The value can be a string, such as a name or description. The value may be a system component, such as an ID or interface. In all cases, the key word between the braces indicates the type of value to enter. | <code>command parameter { value }</code> |
| Number Ranges | When the value of a parameter is a number within a specific range, the range is enclosed in braces (curly brackets). | <code>command parameter { 0 - 10 }</code> |
| Options | When multiple choices are available for the value of a parameter, all choices are wrapped in square brackets. Choices are often comprised of fixed values, but may also include user-defined values and/or number ranges. | <code>command parameter [option1 option2 { value } { 1 - 10 }]</code> |

1.2 System requirements/recommendations

Every client PC used for connection with the SINEC OS user interface needs to meet the following system requirements:

- A functional Ethernet interface must be available.
- It must be possible to configure an IP address and netmask on the Ethernet interface of the client PC.
- A suitable Ethernet cable must be available.
- Terminal software must be installed on the client PC.
- To assign an IP address for the switch, SINEC PNI should be installed on the client PC. For more information about the system requirements and operation of SINEC PNI, see "Related documents (Page 24)".

1.3 Cybersecurity information

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

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

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

For additional information on industrial cybersecurity measures that may be implemented, please visit

<https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html> (<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 available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under

<https://new.siemens.com/global/en/products/services/cert.html> (<https://www.siemens.com/cert>).

1.4 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.

1.5 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 145)".

1.6 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.

1.7 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 Web UI Configuration Manual | Go to one of the following links: <ul style="list-style-type: none"> • SCALANCE XCH-300 (https://support.industry.siemens.com/cs/ww/en/ps/29449/man) • SCALANCE XCM-300 (https://support.industry.siemens.com/cs/ww/en/ps/29448/man) • SCALANCE XRH-300 (https://support.industry.siemens.com/cs/ww/en/ps/29451/man) • SCALANCE XRM-300 (https://support.industry.siemens.com/cs/ww/en/ps/29450/man) |
| "NETCONF for SINEC OS" Reference Manual | Go to one of the following links: <ul style="list-style-type: none"> • SCALANCE XCH-300 (https://support.industry.siemens.com/cs/ww/en/ps/29449/man) • SCALANCE XCM-300 (https://support.industry.siemens.com/cs/ww/en/ps/29448/man) • SCALANCE XRH-300 (https://support.industry.siemens.com/cs/ww/en/ps/29451/man) • SCALANCE XRM-300 (https://support.industry.siemens.com/cs/ww/en/ps/29450/man) |
| SCALANCE XCH-/XCM-300 Product Manual | Visit (https://support.industry.siemens.com/cs/ww/en/view/109808861) |
| SCALANCE XRH-/XRM-300 Product Manual | Visit (https://support.industry.siemens.com/cs/ww/en/view/109815005) |
| "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) |

1.8 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.

1.9 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://w3.siemens.com/aspa_app).



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 CLI Configuration Manual. This document details how to configure your device via the SINEC OS Command Line Interface (CLI).

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 (<https://support.industry.siemens.com/cs/ww/en/view/109814712>)". For information about how to configure NETCONF sessions in SINEC OS, refer to "Configuring the NETCONF user interface (Page 90)".
- **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.
- **Media Redundancy Protocol (MRP)**

The Media Redundancy Protocol (MRP) is a vendor-neutral redundancy protocol standardized according to IEC 62439-2 which ensures loop-free communication and the reconfiguration of a network in the event of interference. MRP makes it possible to establish ring topologies with PROFINET. When the communication chain is interrupted, communication over a redundant path is maintained.

- **Passive Listening**
Passive Listening allows a redundant coupling between (R)STP networks and MRP ring topologies.
- **Enhanced Passive Listening Compatibility (EPLC)**
Enhanced Passive Listening Compatibility (EPLC) is an extension of passive listening. Like Passive Listening, EPLC is required for a redundant coupling between (R)STP networks and MRP ring topologies to prevent network loops and reduce changeover times.
- **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 retrieves the current time from an NTP server and automatically synchronizes the internal clocks 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.
- **Hot swapping/hot plugging**
SINEC OS supports the hot swapping and hot plugging of SFP transceivers while the device is operational.
Following a hot swap or plug, the new transceiver is automatically configured to operate in the same operational state as the previous component.

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 (<https://www.siemens.com/industrialsecurity>).
- 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 631)".

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

- Use a trusted Certificate Authority (CA) that supports key revocation and certificate signing.
- SINEC OS includes default vendor certificates and keys for the purpose of initial onboarding. Do not deploy the device before installing certificates and keys signed by a trusted Certificate Authority (CA).
- 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 (BFA) prevention (Page 179)".
- 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 124)".

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.
- Whenever possible, use the SSH File Transfer Protocol (SFTP) to transfer files. While other protocols are available (e.g. FTP, TFTP, HTTP), SFTP is the only protocol that transfers files encrypted. The other protocols are not protected against interception and manipulation.
- 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 "DCP (Page 452)".

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 36)".
- 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/industrialsecurity>) website or the ProductCERT Security Advisories (<https://www.siemens.com/cert/en/cert-security-advisories.htm>) 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 a file on a remote server (Page 135)".
- When using SNMP (Simple Network Management Protocol):
 - Configure SNMP to raise a trap upon authentication failures.
For more information, refer to "SNMP (Page 475)".
 - 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:

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 |

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 |

Interface management

| Feature | | Limit |
|-------------------|--|-------|
| MAC addresses | Number of static unicast MAC filtering entries | 256 |
| MAC address table | Number of Dynamically Learned MAC Addresses | 32768 |
| VLAN interfaces | Number of Layer 3 interfaces | 17 |

IP address assignment

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

Network redundancy

| Function | | Limit value |
|----------|-------------------------|-------------|
| MRP | Number of MRP rings | 1 |
| | Number of MRP instances | 1 |

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 secured NTP servers | 4 |
| | Number of unsecured NTP servers | 2 |
| | Number of authentication keys | 4 |

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.
- **Default local port number**
The default port number assigned to the service.
- **Default remote port number**
The default port number assigned to the remote server.
- **Default server status**
The default state of the server.
- **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.

Clients

| Service | Protocol | Default local port number | Default remote port number | Configurable service | Configurable port number | Authentication | Encryption |
|---------------|----------|---------------------------|----------------------------|----------------------|--------------------------|----------------|------------|
| DHCP | UDP | 68 | 67 | ✓ | - | - | - |
| DNS | UDP/TCP | - | 53 | ✓ | - | - | - |
| FTP | TCP | - | 20/21 | ✓ | - | ✓ | - |
| HTTP | TCP | - | 80 | ✓ | ✓ | - | - |
| NTP | UDP | 123 | 123 | ✓ | - | Configurable | - |
| RADIUS | UDP | - | 1812 | ✓ | ✓ | - | - |
| Secure Syslog | TCP | - | 6514 | ✓ | ✓ | ✓ | ✓ |
| SFTP | TCP | - | 22 | ✓ | ✓ | ✓ | ✓ |
| SNMP trap | TCP | - | 162 | ✓ | - | - | - |
| Syslog | UDP | - | 514 | ✓ | ✓ | - | - |
| TFTP | UDP | - | 69 | ✓ | - | - | - |

Servers

| Service | Protocol | Default local port number | Default server status | Configurable service | Configurable port number | Authenticat-ion | Encryption |
|-------------|----------|--|-----------------------|----------------------|--------------------------|-----------------|--------------|
| EtherNet/IP | UDP | 2222 and four ports in the range of 49152 to 65535 | Disabled | ✓ | - | - | - |
| | TCP | 44818 | Disabled | ✓ | - | - | - |
| HTTP | TCP | 80 | Disabled | ✓ | ✓ | - | - |
| HTTPS | TCP | 443 | Enabled | ✓ | ✓ | ✓ | ✓ |
| PROFINET | UDP | 34964 and two ports in the range of 49152 to 65535 | Enabled | ✓ | - | - | - |
| SNMPv1/v2c | UDP | 161 | Disabled | ✓ | ✓ | Configurable | - |
| SNMPv3 | UDP | 161 | Disabled | ✓ | ✓ | Configurable | Configurable |
| SSH | TCP | 22 | Enabled | ✓ | ✓ | ✓ | ✓ |
| SSH/NETCONF | TCP | 830 | Enabled | ✓ | ✓ | ✓ | ✓ |

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 |

The following table shows the access rights to general CLI commands.

| Command | Access rights per user profile | |
|-------------------------|--------------------------------|-------|
| | Admin | Guest |
| exit | E | E |
| help | E | E |
| who | E | E |
| send | E | E |
| pwd | E | E |
| admin | E | No |
| terminal | E | E |
| history | E | E |
| config | E | E |
| config exclusive | E | No |
| commit | E | E |
| resolved | E | E |
| rollback | E | No |
| show configuration | E | E |
| show full-configuration | E | E |
| show history | E | E |
| top | E | E |
| validate | E | E |

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 52)".

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 "General commands in configuration mode (Page 46)".

Configuration limits

The configuration limits described apply to the configuration in the running data memory. For more information, refer to "Configuration limits (Page 34)".

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 55)".

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 "General commands in configuration mode (Page 46)".

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 57)".

2.7 CLI modes

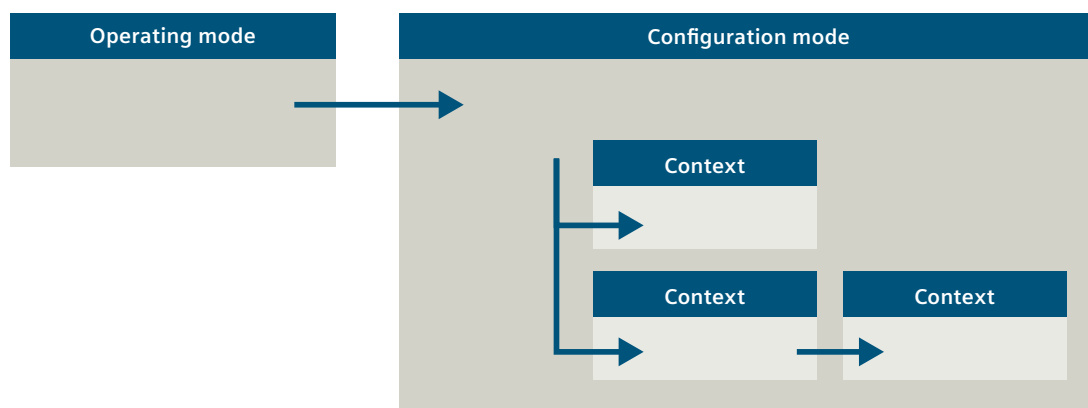
CLI modes

The CLI is divided up into multiple modes. Some commands can be executed in all modes. Other commands are assigned to a specific mode/context. This distinction allows different levels of access rights to the individual groups of commands. You can identify the current mode by the mode/context.

| Mode | Description | Command prompt |
|--|---|-----------------------------|
| Operating mode | The operating mode is active after you have logged in to the device. For more information, refer to "Logging in (Page 112)". This mode is used to display system status, monitor and diagnose network connectivity, configure the CLI environment, and start configuration mode. It is not possible to modify the configuration parameters in this mode. | localhost# |
| Configuration mode | Start the configuration mode from the operating mode with the command "config". For more information, refer to "General commands in operational mode (Page 46)". In this mode, you can change the actual configuration of the device. All changes to the configuration are made to a copy of the active configuration and saved temporarily. You must first commit the changes before they can take effect. For the configuration you can switch between a shared or an exclusive configuration mode. For more information, refer to "Select a configuration mode (Page 52)". | localhost(config)# |
| Context (Special configuration modes) | Within the configuration mode, you reach further configuration modes for special functions, e.g. LLDP. These are referred to as context. You can move from one context to another context without having to switch to the top level of the configuration mode in an intermediate step. For more information, refer to "Configuring parameters in different ways (Page 64)". | localhost(config- lldp)# |

Hierarchy of the CLI modes

The following graphic provides an overview of the hierarchy of the CLI modes.



User interface

This chapter describes how to use the SINEC OS Command Line Interface (CLI).

3.1 Basic commands

This section contains a description of the basic commands for configuration with the CLI. The commands are assigned to the CLI modes.

3.1.1 General commands

Use the following commands to perform basic CLI functions.

| Command | Description |
|-------------------------------|--|
| ? | Displays a list of available command options. For more information, refer to "Displaying all available options for a command (Page 86)". |
| ! | All characters in the command line that follow a "!" are ignored up to the next line break. This behavior allows comments to be included in a file with CLI commands, and the contents of the file can still be inserted and executed in a command line interface. In printouts, it is used as a separator for clarity. |
| <cr> | The entry stands for <code>carriage return</code> . If you log on with ? to view a list of available command options and <cr> is in the list, you can execute the previously entered command with Enter . If you execute a command and receive the feedback <code>incomplete path</code> , the command was not complete. View the list of available command options with ?. |
| <code>clear history</code> | Deletes the CLI history. |
| <code>exit</code> | Ends the current session or CLI session. |
| <code>help { command }</code> | Displays the help text for a specific command. For more information, refer to "Showing the infotext for a command (Page 87)". |

3.1 Basic commands

| Command | Description |
|--|---|
| pwd | <p>Displays the current mode/context.</p> <p>The backward slash \ reflects the structure of the CLI modes/context. The CLI is in the mode/context specified after the last forward slash. When you run the <code>exit</code> command, the CLI changes to the mode/context specified after the last forward slash.</p> <p>Example: <code>localhost# pwd</code> At top level</p> <p>Example: <code>localhost(config)# pwd</code> At top level</p> <p>Example: <code>localhost(config-vlan1)# pwd</code> Current submode path: <code>dhcp \ client \ ipv4 vlan1</code></p> <p>Example: <code>localhost(config)# system authentication user admin</code> <code>localhost(config-user-admin)# pwd</code> Current submode path: <code>system \ authentication \ user admin</code> <code>localhost(config-user-admin)# exit</code> <code>localhost(config-system-authentication)# pwd</code> Current submode path: <code>system \ authentication</code></p> |
| <p>show history</p> <p>show history { Number }</p> | <p>By default, displays the complete CLI command history.</p> <ul style="list-style-type: none"> • If you run the command in operating mode, the CLI commands that were executed in operating mode are displayed. • If you run the command in configuration mode, the CLI commands that were executed in configuration mode are displayed. <p>You use the <code>number</code> to specify how many entries are to be displayed.</p> <p>The 10 last CLI commands are saved. After the maximum number of CLI commands has been reached, the oldest command in the list is deleted when a further CLI command is run.</p> <p>The CLI command history is not saved permanently. The CLI command history is empty after a restart.</p> |
| <p>show configuration commit changes</p> | <p>Displays the last configuration changes.</p> <p>When the following message is shown, the corresponding configuration change cannot be displayed: <code>% No configuration changes found.</code></p> |
| <p>show configuration commit changes ?</p> | <p>Displays a list of saved configuration changes. The saved changes are assigned a number. The larger the number, the older the change.</p> |

| Command | Description |
|--|---|
| <code>show configuration commit changes { number }</code> | <p>Displays the configuration changes that were committed for the selected entry. If you specify a "0", the last configuration changes are displayed.</p> <p>Example:</p> <pre>localhost(config)# show configuration commit changes 1 ! ! Created by: admin ! Date: 2019-03-25 00:08:00 ! Client: cli ! system hostname SWITCH-VPM6002848</pre> <p>When you load a configuration file that does not result in configuration changes that must be committed, an empty entry is created, and the following message displayed:</p> <pre>localhost(config)# show configuration commit changes 0 ! ! Created by: admin ! Date: 2019-03-25 00:10:00 ! Client: load-and-save ! % No configuration changes found.</pre> <p>This can happen when you load the same configuration file twice.</p> |
| <code>show configuration commit changes diff { number }</code> | <p>Displays the configuration changes that were committed for the selected entry. The values that were active before the commitment are also displayed. The newly configured values are marked with a "+". The obsolete values are marked with a "-".</p> <p>Example:</p> <pre>localhost(config)# show configuration commit changes diff 1 ! ! Created by: admin ! Date: 2019-03-25 00:08:00 ! Client: cli ! -system hostname localhost +system hostname SWITCH-VPM6002848</pre> |
| <code>show configuration commit list</code> | Displays the history of configuration changes. |
| <code>show configuration commit list { Number }</code> | <p>Displays the last configuration changes according to the specified number. If you specify a "0", the complete history of the configuration changes is displayed.</p> |
| <code>show configuration commit list { function }</code> | Displays the configuration changes in which the specified function was configured. |
| <code>show configuration rollback changes { number }</code> | <p>Displays saved configurations that you can restore. The stored configurations are assigned a number. The larger the number, the older the configuration. Specify a number to indicate what changes will be made when you restore this configuration.</p> <p>To view the last configuration changes, enter a "0" or no number.</p> <p>To display a list of all configurations, enter ? instead of a number.</p> |

3.1 Basic commands

3.1.2 General commands in operational mode

To run the following commands, you need to be in operating mode.

| Command | Description |
|--|--|
| <code>clear counters</code> | Deletes the counters for all interfaces. |
| <code>clear counters { interface }</code> | Deletes the counters of the selected interface. |
| <code>config [exclusive terminal]</code> | Opens the configuration mode. If you do not specify a parameter, the <code>terminal</code> parameter is used. Options include: <ul style="list-style-type: none"> <code>terminal</code> The shared configuration mode is active. <code>exclusive</code> The exclusive configuration mode is active. For more information on the configuration mode, refer to "Select a configuration mode (Page 52)". |
| <code>exit</code> | Closes the CLI session. |
| <code>show terminal</code> | Displays the CLI environment settings. |
| <code>system</code> | Key command for functions with which you can make changes to the system |
| <code>terminal</code> | Key command for functions that you can use to configure the CLI environment |
| <code>who</code> | Displays the logged-on users. For more information, refer to "Displaying active users (Page 174)". |

3.1.3 General commands in configuration mode

To run the following commands, you need to be in configuration mode.

| Command | Description |
|--------------------|---|
| <code>abort</code> | Exits the configuration mode without saving the changes. |
| <code>clear</code> | Deletes all configuration changes. |
| <code>do</code> | Runs a command from operating mode in configuration mode. Example: The following command runs a <code>show</code> command in configuration mode: <code>localhost(config)# do show system firmware</code> |
| <code>end</code> | Exits the configuration mode. When you execute the command with outstanding changes, you are asked whether you want to apply the changes. |

| Command | Description |
|---|--|
| <code>exit [configuration-mode level no-confirm]</code> | <p>Ends the current mode. If you do not specify a parameter, the <code>level</code> parameter is used. You can call the command with the following parameters:</p> <ul style="list-style-type: none">• <code>configuration-mode</code> Exits the configuration mode regardless of your position in the CLI structure. After you have executed the command, you are in operating mode. When you execute the command with outstanding changes, you are asked whether you want to apply the changes.• <code>level</code> Ends the current mode. After you execute the command, you are in the context in which you were before. If you run this command at the top level, configuration mode terminates and you are in operating mode. When you execute the command with outstanding changes, you are asked whether you want to apply the changes.• <code>no-confirm</code> Exits configuration mode and discards pending configuration changes. There is no query. |
| <code>no</code> | <p>Negates a command or resets it to its default setting. For more information, refer to "Using the no command (Page 53)".</p> |

3.1 Basic commands

| Command | Description |
|----------|---|
| resolved | <p>If conflicts occur when the configuration changes are committed, an error message is output.</p> <p>You have the following options for dealing with conflicts:</p> <ul style="list-style-type: none"> • The conflicts must be cleared up before you can commit the changes. <ul style="list-style-type: none"> – Show the conflicts with the <code>show configuration</code> command. Configuration changes with a conflict are displayed with a preceding <code>!</code>. – Go to the top level of the command hierarchy (<code>top</code>) and run the <code>resolved</code> command. – Commit the configuration changes (<code>commit</code>). Your changes are applied. • Exit configuration mode with the <code>abort</code> command and discard your configuration changes. Note that all configuration changes are discarded in this case. <p>Example:</p> <p>In this example, the <code>lldp hold</code> parameter is configured in two different CLI sessions. CLI session A configured the value 6 and CLI session B the value 8. CLI session A committed the changes. If CLI session B wants to commit the changes, an error message is output.</p> <pre>localhost(config)# lldp hold 8 localhost(config-lldp)# System message at 2020-03-25 09:00:47... Commit performed by admin via ssh using cli. localhost(config-lldp)# commit Aborted: there are conflicts. ----- Resolve needed before configuration can be committed. View conflicts with the command 'show configuration' and execute the command 'resolved' when done, or exit configuration mode to abort. Conflicting configuration items are indicated with a leading '!' Conflicting users: admin ----- localhost(config-lldp)# show configuration lldp ! hold 8 exit localhost(config-lldp)# top localhost(config)# resolved localhost(config)# commit Commit complete. localhost(config)# do show running-config lldp hold lldp hold 8 exit</pre> <p>CLI session B has resolved the conflict and was able to commit the configuration changes. The value of CLI session B (8) is configured for the <code>lldp hold</code> parameter.</p> |

| Command | Description |
|---|--|
| <code>rollback</code> | Restores an older version of the configuration. For more information, refer to "Restoring a configuration (Rollback) (Page 57)". |
| <code>show configuration</code> | Displays uncommitted configuration changes. Commands that are executed when the changes are committed are displayed. If you execute the command in a context, only the uncommitted configuration changes that affect that context are displayed. Example: localhost(config)# show configuration lldp hold 10 exit system hostname SWITCH-VPM6002848 exit |
| <code>show configuration { function }</code> | Displays the uncommitted configuration changes of a function. Commands that are executed when the changes are committed are displayed. Example: localhost(config-lldp)# show configuration lldp hold 10 exit |
| <code>show configuration diff</code> | Compares unconfirmed configuration changes with the currently running configuration. If the values of the default settings differ, the current value is shown with a - and the newly configured value is shown with a +. If you run the command in a context, only the values that affect that context are displayed. Example: localhost(config-lldp)# show configuration diff lldp - hold 10 + hold 8 exit |
| <code>show configuration diff { function }</code> | Compares uncommitted configuration changes of a function with the currently running configuration. If the values of the default settings differ, the current value is shown with a - and the newly configured value is shown with a +. Example: localhost(config)# show configuration diff system hostname system - hostname localhost + hostname SWITCH-VPM6002848 exit |
| <code>show configuration merge</code> | Shows how the configuration appears after the current configuration changes are committed. Only configuration changes that deviate from the default setting are displayed. If you run the command in a context, only the configuration that affects that context is displayed. Example: localhost(config-lldp)# show configuration merge lldp hold 10 exit |

3.1 Basic commands

| Command | Description |
|--|---|
| <pre>show configuration merge { function }</pre> | <p>Shows how the configuration of a function appears after the current configuration changes are committed. Only configuration changes that deviate from the default setting are displayed.</p> <p>To display the entire configuration including the default settings, use and the customization parameter details.</p> <p>Example:</p> <pre>localhost(config)# show configuration merge lldp lldp hold 10 exit</pre> <pre>localhost(config)# show configuration merge lldp details lldp tx-interval 5 hold 10 reinit-delay 1 tx-delay 1 exit</pre> |
| <pre>show configuration running</pre> | <p>Displays the current configuration. Uncommitted configuration changes are ignored. Only configuration changes that deviate from the default setting are displayed.</p> <p>If you run the command in a context, only the configuration that affects that context is displayed.</p> <p>Example:</p> <pre>localhost(config-lldp)# show configuration running lldp hold 10 exit</pre> |
| <pre>show configuration running { function }</pre> | <p>Shows the current configuration of a function. Uncommitted configuration changes are ignored. Only configuration changes that deviate from the default setting are displayed.</p> <p>Example:</p> <pre>localhost(config)# show configuration running lldp lldp hold 10 exit</pre> |
| <pre>show full-configuration</pre> | <p>Shows how the configuration appears after the current configuration changes are committed. Only configuration changes that deviate from the default setting are displayed.</p> <p>If you run the command in a context, only the configuration that affects that context is displayed.</p> <p>Example:</p> <pre>localhost(config-lldp)# show full-configuration lldp hold 10 exit</pre> |

| Command | Description |
|---|---|
| <pre>show full-configuration { function }</pre> | <p>Shows how the configuration of a function appears after the current configuration changes are committed. Only configuration changes that deviate from the default setting are displayed.</p> <p>To display the entire configuration including the default settings, use " " and the customization parameter details.</p> <p>Example:</p> <pre>localhost(config)# show full-configuration lldp lldp hold 10 exit localhost(config)# show full-configuration lldp details lldp tx-interval 5 hold 10 reinit-delay 1 tx-delay 1 exit</pre> |
| top | Goes to the top level of the command hierarchy. |
| validate | Checks whether there are conflicts between the current configuration and configuration changes. The first conflict found is output. |

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 "General commands in operational mode (Page 46)".

3.2.2 Displaying the current configuration

Execute the following command in operating mode to show the current configuration of the device:

```
show running-config
```

To display the current configuration of a function, execute the following command in operating mode:

```
show running-config { function }
```

Only configuration data that deviates from the default setting is displayed.

To display the complete configuration including default settings, execute the following command in operating mode:

```
show running-config | details
```

Note

The output of the `show running-config` command corresponds to valid CLI commands. You can copy the output, paste it in configuration mode and execute it.

Example

In this example the current configuration of LLDP is shown without default values.

```
localhost# show running-config lldp
lldp
  hold          10
exit
```

Example

In this example the current configuration of LLDP is shown with the default values.

```
localhost# show running-config lldp | details
lldp
  tx-interval 5
  hold 10
  reinit-delay 1
  tx-delay 1
exit
```

3.2.3 Using the no command

The `no` form of a command is used to disable a function, delete an entry, or reset the value of a parameter to the default setting. The `no` must always be at the beginning of a command sequence.

If the `no` form is not available for a command, the description of the command will include a note to this effect.

Example

The existing VLAN 7 is deleted in this example.

```
localhost# show running-config switch vlan
switch
  vlan 1
    name vlan1
    no igmp-snooping enabled
  exit

  vlan 2
    name VLAN2
    no igmp-snooping enabled
  exit

  vlan 7
    no igmp-snooping enabled
  exit

exit

localhost# config
Entering configuration mode terminal
localhost(config)# no switch vlan 7
localhost(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config switch vlan
switch
  vlan 1
    name vlan1
    no igmp-snooping enabled
```

3.2 Configuration transactions

```
exit

vlan 2
  name VLAN2
  no igmp-snooping enabled
exit
```

```
exit
```

Example

The NTP global function is disabled in this example.

```
localhost# show running-config system time-sync ntp enabled
system
  time-sync
    ntp
      enabled
    exit
```

```
exit
```

```
exit
```

```
localhost# config
Entering configuration mode terminal
localhost(config)# no system time-sync ntp enabled
localhost(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config system time-sync ntp enabled
system
  time-sync
    ntp
      no enabled
    exit
```

```
exit
```

```
exit
```

Example

The send interval for LLDPDUs is reset to its default setting in this example.

```
localhost# show running-config lldp tx-interval
lldp
  tx-interval 50
exit
```

```
localhost# config
Entering configuration mode terminal
localhost(config)# no lldp tx-interval
localhost(config)# commit
Commit complete.
localhost(config)# end
```

```
localhost# show running-config lldp tx-interval
lldp
  tx-interval 5
exit
```

3.2.4 Committing configuration changes (Commit)

Use the `commit` command to commit configuration changes.

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 ID to list the changes later and restore the previous configuration. The label can be automatically generated or defined by the user.

The table below shows the different versions of the command.

| Command | Description |
|---|--|
| <code>commit check</code> | Checks whether there are conflicts between the current configuration and configuration changes. The first conflict found is output. |
| <code>commit</code> | Commits the current configuration changes together with an automatically generated identifier. |
| <code>commit comment { comment }</code> | Commits the current configuration changes along with a custom comment. The comment is displayed together with the configuration change in the output of the <code>show configuration commit list</code> command. |
| <code>commit label { label }</code> | Commits the current configuration changes along with a custom label. The label is displayed together with the configuration change in the output of the <code>show configuration commit list</code> command. |
| <code>commit and-quit</code> | Commits the current configuration changes and exits configuration mode. |

3.2 Configuration transactions

| Command | Description |
|--|--|
| <code>commit confirmed { time period in minutes }</code> | <p>Commits configuration changes temporarily for a specific time period to be able to test a configuration.</p> <p>Only available in exclusive configuration mode.</p> <p>Only users with the <code>admin</code> user profile can commit configuration changes in tests.</p> <p>Enter the <code>time period</code> for which configuration changes should remain in effect.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Min. 1 minute • Max. 1440 minutes <p>Default: 10 minutes</p> <p>For changes to remain in effect permanently, you need to commit the changes before the time period ends. If the changes are not committed before the end of the period or you close the CLI session, the changes are automatically discarded and the previous settings are restored.</p> <p>While a test period is running, you can make further configuration changes and commit these in tests. The timer to be counted down is discarded and a new timer starts with the new time period. In this way, you extend the time period for existing temporary changes.</p> <p>The time period starts as soon as the configuration changes have been successfully applied to the current configuration. The changes remain in effect for the specified period.</p> <p>You can permanently commit or discard changes within this time period:</p> <ul style="list-style-type: none"> • To permanently commit changes, run the following command before the timer elapses: <code>commit</code> The changes can only be committed in the session in which they were committed by tests. If you do not commit the changes before the timer elapses, the changes are automatically discarded and the previous settings are restored. • To discard changes before the timer elapses, run the following command: <code>commit abort</code> |
| <code>commit abort</code> | <p>Discards temporary configuration changes before the time period elapses.</p> <p>For more information, refer to the command <code>commit confirmed { time period in minutes }</code>.</p> |

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.

Two users in shared configuration mode change the same element

For example, user 1 is connected to the device via the Web user interface. The **Exclusive rights on/off** function is disabled. A second user is connected to the same device via the CLI. The user has used the `config terminal` command to enter the configuration mode.

1. User 1 changes the host name to `webui-private`.
2. User 2 changes the host name to `cli-terminal`.

3. User 1 confirms the changes made. The changes are applied. The new host name is `webui-private`.
 4. User 2 confirms the changes made. The changes are rejected.
- The later confirmation is rejected.

Two users in shared configuration mode violate a configuration rule

1. User 1 (Web UI, **Exclusive rights on/off** disabled) changes the IP address of VLAN 3 to 192.168.1.1.
2. User 2 (CLI, `config terminal`) changes the IP address of VLAN 4 to 192.168.1.1.
3. User 1 confirms the changes made. The changes are applied. The IP address of VLAN 3 is 192.168.1.1.
4. User 2 confirms the changes made. The changes are rejected.

The later confirmation violates a configuration rule, the IP address of VLAN 4 would be a duplicate.

Commit and discard configuration changes temporarily for a specific time period

In this example, the hostname is first changed and committed for eight minutes. Within the eight minutes, the contact partner is changed and committed for twelve minutes. With the second temporary commit, the changed hostname is also committed for a longer time period. The temporary configuration changes are discarded before the time period elapses.

```
localhost# config exclusive
Entering configuration mode exclusive
Warning: uncommitted changes will be discarded on exit
localhost(config)# system hostname sec01
localhost(config-system)# commit confirmed 8
Warning: The configuration will be reverted if you exit the CLI
without performing the commit operation within 8 minutes.
sec01(config-system)# top
sec01(config)# system contact "Winston Smith"
sec01(config-system)# commit confirmed 12
Warning: The configuration will be reverted if you exit the CLI
without performing the commit operation within 12 minutes.
sec01(config-system)# commit abort
Confirmed commit has been aborted. Old configuration will now be
restored.
localhost(config)#
Message from system at 2019-03-25 14:50:50...
confirmed commit operation not confirmed by admin from cli
configuration rolled back
localhost(config)#
```

3.2.5 Restoring a configuration (Rollback)

Before you confirm 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 confirmed change appears as element "0" in the list.

3.2 Configuration transactions

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

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, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | [Optional] Display a list of saved configurations that you can restore. | <code>show configuration rollback changes ?</code> |
| 2 | [Optional] Indicate what changes are made when you restore a particular configuration. | <code>show configuration rollback changes { 0 - 49 }</code> |
| 3 | Enter configuration mode. | <code>config</code> |
| 4 | Select the configuration you want to restore. To restore a specific configuration, enter the appropriate number. If you do not specify a number or enter "0", you restore the last configuration. Options include: <ul style="list-style-type: none"> <code>configuration</code> All changes made since confirming the specified configuration are undone. <code>selective</code> Only the changes of the specified configuration are undone. | <code>rollback [configuration selective] { 0 - 49 }</code> |
| 5 | Commit the changes. | <code>commit</code> |
| 6 | Exit configuration mode. | <code>end</code> |

Basic configuration for examples

The following basic configuration is assumed for the examples:

- The host name was changed to: SWITCH-VPM6002848
- The DHCP client ID `sys-name` was configured for the VLAN interface `vlan1`.
- The lease time 8 was configured for LLDP.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system hostname SWITCH-VPM6002848
localhost(config-system)# commit
Commit complete.
SWITCH-VPM6002848(config-system)# top
SWITCH-VPM6002848(config)# dhcp client ipv4 vlan1 client-id sys-name
SWITCH-VPM6002848(config-vlan1)# commit
Commit complete.
SWITCH-VPM6002848(config-system)# top
```

```
SWITCH-VPM6002848(config)# lldp hold 8
SWITCH-VPM6002848(config-lldp)# commit
Commit complete.
SWITCH-VPM6002848(config-lldp)# end
SWITCH-VPM6002848#
```

First, a list of saved configurations is displayed.

```
SWITCH-VPM6002848# show configuration rollback changes ?
```

Possible completions:

```
0      2019-03-25 00:08:00 by admin via cli
1      2019-03-25 00:07:47 by admin via cli
2      2019-03-25 00:07:34 by admin via cli
.
.
.
```

The changes made when restoring the last three configurations are displayed for an overview. The commands that are executed to restore the corresponding configuration are listed.

```
SWITCH-VPM6002848# show configuration rollback changes 0
lldp
no hold 8
exit
```

```
SWITCH-VPM6002848# show configuration rollback changes 1
lldp
no hold 8
exit
```

```
dhcp
client
ipv4 vlan1
client-id mac-address
exit
```

```
exit
```

```
exit
```

```
SWITCH-VPM6002848# show configuration rollback changes 2
lldp
no hold 8
exit
```

```
dhcp
client
ipv4 vlan1
client-id mac-address
exit
```

```
exit
```

```
exit
```

3.2 Configuration transactions

```
system
  hostname localhost
exit
```

Example

In this example, the configuration "2" is restored with the parameter `configuration` from the basic configuration, i.e. all changes made since configuration "2" was confirmed are undone. In this example, this means:

- The LLDP lease time is reset to the default setting.
- The change of the DHCP client ID is undone for the VLAN interface `vlan1`.
- The change of the host name is undone.

```
SWITCH-VPM6002848# config
SWITCH-VPM6002848(config)# rollback configuration 2
SWITCH-VPM6002848(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config dhcp client ipv4 vlan1
dhcp
  client
    ipv4 vlan1
      client-id mac-address
    exit
  exit
exit

localhost# show running-config lldp
% No entries found.
localhost#
```

Example

In this example, the configuration "2" with the parameter `selective` is restored from the basic configuration, i.e. only the changes of configuration "2" are undone. In this example, this means the change of host name is undone.

```
SWITCH-VPM6002848# config
SWITCH-VPM6002848(config)# rollback selective 2
SWITCH-VPM6002848(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config dhcp client ipv4 vlan1
dhcp
  client
    ipv4 vlan1
      client-id sys-name
    exit
  exit
exit
```

```

exit

localhost# show running-config lldp
lldp
  hold 8
exit

```

3.3 Basic operation

This section describes the basic operation of the CLI.

3.3.1 Operating the CLI with the keyboard

Depending on the terminal program, some key combinations may vary.

Moving the cursor

| Action | Key/shortcut |
|--|------------------------------------|
| Move the cursor back one character | [Ctrl] + [B] or arrow to the left |
| Move the cursor forward one character | [Ctrl] + [F] or arrow to the right |
| Move the cursor back one word | [Alt] + [B] |
| Move the cursor forward one word | [Alt] + [F] |
| Move the cursor to the beginning of the command line | [Ctrl] + [A] or [Home] |
| Move the cursor to the end of the command line | [Ctrl] + [E] or [End] |

Deleting characters

| Action | Key/shortcut |
|---|--|
| Delete the character before the cursor | [Ctrl] + [H], [Del] or backspace |
| Delete the currently selected character | [Ctrl] + [D] |
| Delete the entire command line | [Ctrl] + [U] or [Ctrl] + [X] |
| Delete all characters from the cursor until the end of the command line | [Ctrl] + [K] |
| Delete all characters of a word before the cursor | [Ctrl] + [W], [Esc] + [Backspace] or [Alt] + [Backspace] |
| Delete all characters of a word after the cursor | [Alt] + [D] |

Inserting recently deleted text

| Action | Key/shortcut |
|---|--------------|
| Insert the most recently deleted text at the position of the cursor Only works with text that has been deleted with one of the following key combinations: <ul style="list-style-type: none"> • Delete the entire command line [Ctrl] + [U] or [Ctrl] + [X] • Delete all characters from the cursor until the end of the command line [Ctrl] + [K] • Delete all characters of a word before the cursor [Ctrl] + [W], [Esc] + [Backspace] or [Alt] + [Backspace] • Delete all characters of a word after the cursor [Alt] + [D] | [Ctrl] + [Y] |

Upper and lower case

| Action | Key/shortcut |
|---|--------------|
| Capitalize the currently selected letter and lowercase all following characters of the word | [Esc] + [C] |
| Set a word to lower case starting with the currently selected letter. | [Esc] + [L] |
| Set a word to uppercase starting with the currently selected letter. | [Esc] + [U] |

Showing previously entered commands

| Action | Key/shortcut |
|---|----------------------------|
| Show the previous command in the command history | [Ctrl] + [P] or arrow up |
| Show the next command in the command history | [Ctrl] + [N] or arrow down |
| Search for commands in the command history <ol style="list-style-type: none"> 1. Press the key combination. (reverse-i-search) ` `: 2. Enter the command you are looking for. 3. To browse the command history, press the key combination again. | [Ctrl] + [R] |

Special actions

| Action | Key/shortcut |
|--|--------------|
| Cancel a command | [Ctrl] + [C] |
| Empty the screen | [Ctrl] + [L] |
| Swaps the selected character with the preceding character. | [Ctrl] + [T] |
| Switch to multiline mode | [Esc] + [M] |
| End multiline mode | [Ctrl] + [D] |
| Exit configuration mode When you execute the command with outstanding changes, you are asked whether you want to apply the changes. | [Ctrl] + [Z] |

3.3.2 Permitted characters

In this section, you can find the permissible ASCII character sets with their hexadecimal code. The characters permitted for the configuration of user names, passwords, parameters and texts are explicitly stated in the respective configuration.

Standard characters

- 0x30 - 0x39
0 1 2 3 4 5 6 7 8 9
- 0x41 - 0x5A
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- 0x61 - 0x7A
a b c d e f g h i j k l m n o p q r s t u v w x y z

Special characters

- 0x21 - 0x2F
! " # \$ % & ' () * + , - . /
- 0x3A - 0x40
: ; < = > ? @
- 0x5B - 0x60
[\] ^ _ `
- 0x7B - 0x7E
{ | } ~

3.3.3 Using regular expressions

Regular expressions are a generalized search pattern for strings to search for matches in strings. This allows you, for example, to check command outputs to see whether they correspond to certain patterns.

Regular expressions can be used as filter criteria in the text search by comparing the text with the model of the regular expression.

The following regular expressions can be used together with some customization parameters. For more information about using customization parameters, refer to "Customizing the output of a command (Page 73)".

| Character | Description | Example |
|-----------|---|--------------------|
| . | Matches any single character. The ".ab" example finds all strings with three characters where the last two characters are "a" and "b", e.g. "Aab", "aab" or "1ab". The example "ab." finds all strings with three characters where the first two characters are "a" and "b", e.g. "ab4", "abb" or "ab?". The example "a..b" finds all strings with four characters where the first character is an "a" and the last character is a "b", e.g. "a12b" or "aabb". | .ab ab. a..b |
| ^ | Matches the beginning of a string or line. The example finds all strings or lines beginning with "a". | ^a |

| Character | Description | Example |
|-----------|--|-----------------|
| \$ | Matches the end of a string or line. The example finds all strings or lines ending with "a". | a\$ |
| [] | Character class. A sequence of arbitrary characters in square brackets finds all the characters that contain one of the specified characters. Two characters separated by "-" in the parentheses stand for all characters of this range. The example [abc] finds all "a", "b" and "c". The example [ab-f] finds all "a", "b", "c", "d", "e" and "f". | [abc] [ab-f] |
| [^] | A circumflex character after the opening square bracket creates a negated character class. This finds any character that is not contained in the specified string. The example finds all characters except "a". | [^a] |
| | Alternative. Matches the first or second string. The example finds all "abc" and "def". | abc def |
| + | The preceding character occurs at least once. With the example, "ab", "abb" or "abbb" are found, for example. | ab+ |
| * | The preceding character does not occur or occurs as often as desired. With the example, "a", "ab" or "abbb" are found, for example. | ab* |
| ? | The preceding character does not occur or occurs exactly once. The example finds "a" and "ab". | ab? |
| () | Grouping. The grouping can be used to apply operators to all characters in the brackets. The example finds one or more repetitions of "ab", e.g. "ab", "abab" or "ababab". | (ab)+ |

3.3.4 Configuring parameters in different ways

If you are in configuration mode, you have various options for configuring parameters.

Example with multiple parameters

The following examples show two procedures for configuring multiple parameters of LLDP. The result is the same with both procedures.

You can enter and execute a command with parameters contiguously.

```
localhost# config
localhost(config)# lldp hold 6 tx-interval 50 tx-delay 10
localhost(config-lldp)#
```

You can switch to the context of LLDP first and execute the parameters individually.

```
localhost# config
localhost(config)# lldp
localhost(config-lldp)# hold 6
localhost(config-lldp)# tx-interval 50
localhost(config-lldp)# tx-delay 10
localhost(config-lldp)#
```

Note

The entry <cr> shows you if you can switch to a context. If you log on with ? to view a list of available command options and <cr> is in the list, you can execute the previously entered command with **Enter**.

Example with one parameter

The following examples show two procedures for adding a static VLAN and assigning a name. The result is the same with both procedures.

You can enter and execute a command contiguously.

```
localhost# config
localhost(config)# switch vlan 8 name subst8
localhost(config-switch-vlan-8)#
```

You can execute the command in smaller units. A unit must always consist of a context.

```
localhost# config
localhost(config)# switch
localhost(config-switch)# vlan 8
localhost(config-switch-vlan-8)# name subst8
localhost(config-switch-vlan-8)#
```

3.3.5 Processing a series of commands

To call multiple commands one after the other, list the commands in one line separated by semicolons ";". To start processing the command sequence, press **Enter**.

Example

```
localhost# config; system hostname "sec01"; commit
sec01(config)# end
```

This series of commands has the same result as the following input:

```
localhost# config
localhost(config)# system hostname sec01
localhost(config)# commit
sec01(config)# end
```

3.3.6 Executing commands as script

To apply the same configuration to multiple devices or to configure the new device during a device replacement, you can run CLI commands like a script.

You can write the required CLI commands together, copy them and insert them in the CLI. The device processes the command autonomously.

To create the script, you can also use the output of the `show running-config` command. This corresponds to valid CLI commands.

Note**Configuration risk**

If you use one script for different devices, note that you are modifying parameters that could lead to conflicts (e.g. IP addresses).

Example script

The following CLI commands create the following configuration:

- NTP server
 - 192.168.113.10
 - burst
 - iburst
- Keystore
 - Key pair AK1
 - Certificate CN1
- Truststore
 - Certificate folder BN1
 - Certificate BN1
- Remote Syslog server S1
 - 192.168.113.10
 - Reference to the keystore
 - Reference to the truststore

Note

Long inputs, such as keys or certificates, are truncated (. . .) to make examples clearer.

```
=====
config
system time-sync ntp enabled unicast-configuration ipv4
192.168.113.10 burst iburst
system certificates local asymmetric-key AK1
public-key-format subject-public-key-info-format
public-key MIIBIjANBgkqhkiG9w0B...
private-key-format rsa-private-key-format
private-key MIIEowIBAAKCAQEAvLw...
certificate CN1 cert-data MIIIEwYJKoZIhvcNAQcCo...
system certificates remote certificate-bag BN1 certificate BN1 cert-
data MIIESQYJKoZIhv...
system logging action remote destination S1 tls ipv4 192.168.113.10
```

```

system logging action remote destination S1 facility-filter
facility-list all all
system logging action remote destination S1 tls client-identity
certificate keystore-reference asymmetric-key AK1 certificate CN1
system logging action remote destination S1 tls server-
authentication ca-certs truststore-reference BN1
commit
=====

```

Example

In this example, the previously described script is inserted in the CLI and run automatically.

```

localhost# config
Entering configuration mode terminal
localhost(config)# system time-sync ntp enabled unicast-
configuration ipv4 192.168.113.10 burst iburst
localhost(config-ipv4-192.168.113.10)# system certificates local
asymmetric-key AK1
localhost(config-asymmetric-key-AK1)# public-key-format subject-
public-key-info-format
localhost(config-asymmetric-key-AK1)#public-key
MIIBIjANBgkqhkiG9w0B...
localhost(config-asymmetric-key-AK1)# private-key-format rsa-
private-key-format
localhost(config-asymmetric-key-AK1)# private-key
MIIEowIBAAKCAQEAvLw...
localhost(config-asymmetric-key-AK1)# certificate CN1 cert-data
MIIEwYJKoZIhvcNAQcCo...
localhost(config-certificate-CN1)# system certificates remote
certificate-bag BN1 certificate BN1 cert-data MIIESQYJKoZIhvcN...
localhost(config-certificate-BN1)# system logging action remote
destination S1 tls ipv4 192.168.113.10
localhost(config-destination-S1)# system logging action remote
destination S1 facility-filter facility-list all all
localhost(config-facility-list-all/all)# system logging action
remote destination S1 tls client-identity certificate keystore-
reference asymmetric-key AK1 certificate CN1
localhost(config-keystore-reference)# system logging action remote
destination S1 tls server-authentication ca-certs truststore-
reference BN1
localhost(config-destination-S1)# commit
Commit complete.
localhost(config-destination-S1)#

```

3.3.7 Specifying a URL

The URL is needed if you want to load and save files via a remote server.

For special characters, SINEC OS supports URL encoding (also known as percent encoding), for example %23 for #.

A URL is composed as follows:

- **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

Note

Security risk - Danger of unauthorized access and/or misuse

Of the available protocols, only SFTP transfers the files encrypted. The other protocols are not protected against interception and manipulation.

To prevent unauthorized access and/or misuse, use SFTP.

- **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.

Scheme

Protocol://User name:Password@IP address of the server:Port/path to the file/file name

Example

The firmware is loaded from an FTP server in this example. User name `ftpuser` and password `password` are required. The default port is used.

```
localhost# system firmware update source ftp://
ftpuser:password@192.168.1.1/sinec-os_V02.00.00.00.sfw
```

Example

This example shows you how to save the configuration of the device on an SFTP server. A connection to the SFTP server is established for the first time. User name `sftpuser` and password `password` are required. The default port is used.

```
localhost# system configuration save target sftp://
sftpuser:password@192.168.1.1/home/user/config.xml
Are you sure you want to backup the current configuration? This may
take several minutes. [no,yes] yes
Transferring file...
The authenticity of host '192.168.1.1' cannot be verified.
ecdsa key fingerprint is SHA256: a0EWGzsLe...
Are you sure you want to continue connecting? [no,yes] yes
The key has been successfully committed to the database.
File transfer done.
```

Example

The firmware is loaded from a TFTP server in this example. User name and password are not supported by TFTP. The default port is used.

```
localhost# system firmware update source tftp://192.168.1.1/sinec-
os_V02.00.00.00.sfw
```

Example

The firmware is loaded from an HTTP server in this example. User name and password are not required. The TCP port 8081 is used.

```
localhost# system firmware update source http://192.168.200.10:8081/
sinec-os_V02.00.00.00.sfw
```

3.3.8 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.

3.3 Basic operation

- **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. |

3.3.9 Showing operative data

Execute the following command in operating mode to show operative data of the device:

```
show { function }
```

Use "?" to display a list of available functions.

Example

```
localhost# show lldp local-system-data
  LLDP local-system-data
    Local System Name           localhost
    Local System Description    Siemens, SIMATIC NET, ...
    Local Device ID             20:87:56:8c:94:09
    Local Chassis ID Subtype    macAddress
    Capabilities Enabled        bridge
```

3.3.10 Using wildcards to specify interfaces in show commands

If you want to display the configuration of all interfaces with a `show` command, use "*" instead of the number of the Ethernet or VLAN interface.

Example:

```
localhost# show running-config interface ethernet0/* enabled
% The following list contains 34 entries.
interface ethernet0/1
  enabled
exit

interface ethernet0/2
  enabled
exit

interface ethernet0/3
  enabled
exit
.
.
.
```

3.3.11 Multiple selection of interfaces

Use multiple selection of interfaces for the following actions:

- For identical configuration of multiple bridge ports.
- For simultaneous creation and identical configuration of multiple static VLANs.
- To display the configuration of multiple interfaces with `show` commands.

Specify the interfaces you want and run configuration commands for the selected interfaces.

It is not possible to create multiple VLAN interfaces using multiple selection. This restriction also applies when the required static VLANs have already been created.

Example

In this example, the bridge ports `ethernet0/1` to `ethernet0/8` are selected. All configuration commands that you run in this context are applied to all selected bridge ports.

```
localhost# config
```

3.3 Basic operation

```
localhost(config)# interface ethernet0/1-8
localhost(config-interface-ethernet0/1-8)#
```

Example

In this example, the bridge ports ethernet0/2, ethernet0/3 and ethernet0/6 to ethernet0/8 are selected. All configuration commands that you run in this context are applied to all selected bridge ports.

```
localhost# config
localhost(config)# interface ethernet0/2,3,6-8
localhost(config-interface-ethernet0/2,3,6-8)#
```

Example

In this example, the static VLANs 6 to 9 are created and selected. All configuration commands that you run in this context are applied to all selected static VLANs.

```
localhost# config
localhost# switch vlan 6-9
localhost(config-switch-vlan-6-9)# commit
Commit complete.
localhost(config-switch-vlan-6-9)#
```

Example

In this example, the static VLANs 10 and 17 to 19 are created and selected. All configuration commands that you run in this context are applied to all selected static VLANs.

```
localhost# config
localhost# switch vlan 10,17-19
localhost(config-switch-vlan-10,17-19)# commit
Commit complete.
localhost(config-switch-vlan-10,17-19)#
```

Example

This example shows the multiple selection of interfaces cannot be used to create VLAN interfaces.

```
localhost# config
localhost(config)# interface vlan6-9
Error: no matching instances found
localhost(config)#
```

Example

In this example, a show command is executed for the interfaces ethernet0/2, ethernet0/3 and ethernet0/6 to ethernet0/8.

```
localhost# show running-config interface ethernet0/2,3,6-8 enabled
% The following list contains 5 entries.
interface ethernet0/2
  enabled
exit

interface ethernet0/3
  enabled
exit

interface ethernet0/6
```



```
    enabled
  exit

interface ethernet0/7
  enabled
  exit

interface ethernet0/8
  enabled
  exit
```

Example

In this example, a `show` command is executed for the VLAN interfaces 1 to 6. The information is displayed for the existing VLAN interfaces.

```
localhost# show interface vlan1-6 admin-status
% The following list contains 4 entries.
interface vlan1
  admin-status up
interface vlan3
  admin-status up
interface vlan4
  admin-status up
interface vlan6
  admin-status up
```

3.3.12 Customizing the output of a command

Data output via a CLI command can be adapted and filtered in various ways. To adapt an output, enter `|` after the CLI command followed by an customization parameter. You can combine several customization parameters. To do this, each customization parameter must begin with a `|`. To view the available customization parameters, enter `| ?` after a CLI command.

3.3 Basic operation

For some customizations, you can use regular expressions. For more information on regular expressions, refer to "Using regular expressions (Page 63)".

| Command | Description |
|-----------------------------|---|
| <code>begin { text }</code> | <p>Starts the output with the line containing the specified text. Regular expressions can be used in this adaptation.</p> <p>Example:</p> <pre>localhost# show running-config dhcp dhcp client ipv4 vlan1 client-id sys-name lease 06:40 hostname exit exit exit localhost# show running-config dhcp begin lease lease 06:40 hostname exit exit exit</pre> |

| Command | Description |
|-----------------------------------|---|
| <pre>context-match { text }</pre> | <p>Returns only lines that contain the specified text. Higher-level data is also output. Regular expressions can be used in this adaptation.</p> <p>Example:</p> <pre>localhost# show running-config dhcp dhcp client ipv4 vlan1 client-id sys-name lease 06:40 hostname exit ipv4 vlan2 client-id name-of-station lease 10:00 hostname exit exit exit localhost# show running-config dhcp context-match name dhcp client ipv4 vlan1 client-id sys-name dhcp client ipv4 vlan1 hostname dhcp client ipv4 vlan2 client-id name-of-station dhcp client ipv4 vlan2 hostname</pre> |
| <pre>count</pre> | <p>Displays the number of lines returned by the command.</p> <p>Example:</p> <pre>localhost# show running-config dhcp count Count: 14 lines</pre> |
| <pre>csv</pre> | <p>Outputs the data as a table in csv format.</p> <p>Example:</p> <pre>localhost# show dhcp client ipv4 bindings csv INTERFACE,HW ADDRESS,IP ADDRESS,PREFIX LENGTH,LEASE GRANTED vlan1,20:87:56:8c:94:09,0.0.0.0,-,- vlan2,20:87:56:8c:94:09,0.0.0.0,-,-</pre> |

3.3 Basic operation

| Command | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------------------|--|-------------|---------------|-----------------|-----------------|---------------|-------|-------------------|---------|---|---|-------|-------------------|---------|---|---|-----------|------------|------------|---------------|-------|-------------------|---------|---|-------|-------------------|---------|---|-----------|----------|-------|-------------|----------|-----------------|--------|-------|------|-------|---|---|---|---|-------|------|-------|---|---|---|---|-----------|-------|-------------|----------|-----------------|--------|-------|-------|---|---|---|---|-------|-------|---|---|---|---|
| <pre>de-select { column }</pre> | <p>The specified column is not output. To be able to use this customization parameter, the output must be made as a table. If necessary, use the <code>tab</code> customization parameter first.</p> <p>Example:</p> <pre>localhost# show dhcp client ipv4 bindings</pre> <table border="1"> <thead> <tr> <th>INTERFACE</th> <th>HW ADDRESS</th> <th>IP ADDRESS</th> <th>PREFIX LENGTH</th> <th>LEASE GRANTED</th> </tr> </thead> <tbody> <tr> <td>vlan1</td> <td>20:87:56:8c:93:f8</td> <td>0.0.0.0</td> <td>-</td> <td>-</td> </tr> <tr> <td>vlan2</td> <td>20:87:56:8c:93:f8</td> <td>0.0.0.0</td> <td>-</td> <td>-</td> </tr> </tbody> </table> <pre>localhost# show dhcp client ipv4 bindings de-select lease-granted</pre> <table border="1"> <thead> <tr> <th>INTERFACE</th> <th>HW ADDRESS</th> <th>IP ADDRESS</th> <th>PREFIX LENGTH</th> </tr> </thead> <tbody> <tr> <td>vlan1</td> <td>20:87:56:8c:93:f8</td> <td>0.0.0.0</td> <td>-</td> </tr> <tr> <td>vlan2</td> <td>20:87:56:8c:93:f8</td> <td>0.0.0.0</td> <td>-</td> </tr> </tbody> </table> <p>Example:</p> <pre>localhost# show running-config dhcp client ipv4 vlan* tab</pre> <table border="1"> <thead> <tr> <th>INTERFACE</th> <th>HOSTNAME</th> <th>LEASE</th> <th>MAC ADDRESS</th> <th>SYS NAME</th> <th>NAME OF STATION</th> <th>STRING</th> </tr> </thead> <tbody> <tr> <td>vlan1</td> <td>true</td> <td>06:40</td> <td>-</td> <td>X</td> <td>-</td> <td>-</td> </tr> <tr> <td>vlan2</td> <td>true</td> <td>10:00</td> <td>-</td> <td>-</td> <td>X</td> <td>-</td> </tr> </tbody> </table> <pre>exit</pre> <pre>localhost# show running-config dhcp client ipv4 vlan* tab de-select hostname</pre> <table border="1"> <thead> <tr> <th>INTERFACE</th> <th>LEASE</th> <th>MAC ADDRESS</th> <th>SYS NAME</th> <th>NAME OF STATION</th> <th>STRING</th> </tr> </thead> <tbody> <tr> <td>vlan1</td> <td>06:40</td> <td>-</td> <td>X</td> <td>-</td> <td>-</td> </tr> <tr> <td>vlan2</td> <td>10:00</td> <td>-</td> <td>-</td> <td>X</td> <td>-</td> </tr> </tbody> </table> <pre>exit</pre> | INTERFACE | HW ADDRESS | IP ADDRESS | PREFIX LENGTH | LEASE GRANTED | vlan1 | 20:87:56:8c:93:f8 | 0.0.0.0 | - | - | vlan2 | 20:87:56:8c:93:f8 | 0.0.0.0 | - | - | INTERFACE | HW ADDRESS | IP ADDRESS | PREFIX LENGTH | vlan1 | 20:87:56:8c:93:f8 | 0.0.0.0 | - | vlan2 | 20:87:56:8c:93:f8 | 0.0.0.0 | - | INTERFACE | HOSTNAME | LEASE | MAC ADDRESS | SYS NAME | NAME OF STATION | STRING | vlan1 | true | 06:40 | - | X | - | - | vlan2 | true | 10:00 | - | - | X | - | INTERFACE | LEASE | MAC ADDRESS | SYS NAME | NAME OF STATION | STRING | vlan1 | 06:40 | - | X | - | - | vlan2 | 10:00 | - | - | X | - |
| INTERFACE | HW ADDRESS | IP ADDRESS | PREFIX LENGTH | LEASE GRANTED | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan1 | 20:87:56:8c:93:f8 | 0.0.0.0 | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan2 | 20:87:56:8c:93:f8 | 0.0.0.0 | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| INTERFACE | HW ADDRESS | IP ADDRESS | PREFIX LENGTH | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan1 | 20:87:56:8c:93:f8 | 0.0.0.0 | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan2 | 20:87:56:8c:93:f8 | 0.0.0.0 | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| INTERFACE | HOSTNAME | LEASE | MAC ADDRESS | SYS NAME | NAME OF STATION | STRING | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan1 | true | 06:40 | - | X | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan2 | true | 10:00 | - | - | X | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| INTERFACE | LEASE | MAC ADDRESS | SYS NAME | NAME OF STATION | STRING | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan1 | 06:40 | - | X | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan2 | 10:00 | - | - | X | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>details</pre> | <p>Creates a more detailed output.</p> <p>Example:</p> <pre>localhost# show running-config lldp</pre> <pre>lldp tx-interval 50 tx-delay 10 exit</pre> <pre>localhost# show running-config lldp details</pre> <pre>lldp tx-interval 50 hold 4 reinit-delay 1 tx-delay 10 exit</pre> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Command | Description |
|--|--|
| <pre>display [curly-braces json keypath xml xpath]</pre> | <p>Output options include:</p> <ul style="list-style-type: none"> • curly-braces - Output with curly brackets • json - Output in JSON format • keypath - Output with path specifications • xml - Output in XML format • xpath - Output in XPath format <p>Example:</p> <pre>localhost# show running-config dhcp client ipv4 vlan* display curly-braces ipv4 vlan1 { lease 06:40; client-id { sys-name; } } ipv4 vlan2 { lease 10:00; client-id { name-of-station; } }</pre> |
| <pre>exclude { text }</pre> | <p>Excludes lines that contain the specified text. Regular expressions can be used in this adaptation.</p> <p>Example:</p> <pre>localhost# show running-config dhcp dhcp client ipv4 vlan1 client-id sys-name lease 06:40 hostname exit exit exit localhost# show running-config dhcp exclude name dhcp client ipv4 vlan1 lease 06:40 exit exit exit</pre> |

3.3 Basic operation

| Command | Description |
|---------|--|
| force | <p>When you switch to the exclusive configuration mode and another user is already in the exclusive configuration mode, you can use this adaptation parameter to end the exclusive configuration mode of the other user.</p> <p>Example:</p> <p>In the following example, admin2 is in the exclusive configuration mode. The user admin uses the adaptation parameter force to switch to the exclusive configuration mode. admin receives a query whether the exclusive configuration mode is to be ended for admin2. When admin confirms the query, admin2 will receive a corresponding message and is in the operating mode.</p> <pre>admin# config exclusive force Error: configuration database locked by: admin2 ssh (cli from 192.168.16.1) on since 1970-01-06 18:05:46 exclusive Attempt to end blocking session? [yes,no] yes Forcing admin2 out of configure mode Entering configuration mode exclusive Warning: uncommitted changes will be discarded on exit admin(config)# ----- admin2(config)# You are forced out of configure mode by admin. admin2#</pre> |
| icount | <p>Counts the number of entries output by the preceding command. Use this adaptation only for outputs in list form. If an output is in table form as standard, No instance found is displayed</p> <p>Example:</p> <p>In the following example, all entries in the MAC address table are counted.</p> <pre>localhost# show switch mac-address-tables filtering-database entry icount Found 1000 instances.</pre> <p>Example:</p> <p>In the following example, all configured VLANs are counted.</p> <pre>localhost# show switch vlan icount Found 1 instance.</pre> <p>Example:</p> <p>In the following example, all enabled bridge ports are counted.</p> <pre>localhost# show running-config interface ethernet* enabled icount Found 8 instances.</pre> <p>Example:</p> <p>In the following example, all critical entries in the logfile are counted.</p> <pre>localhost# show system logging logbook log-list severity critical icount Found 0 instances.</pre> |

| Command | Description |
|--|---|
| <pre>include [-a -b -c] { text }</pre> | <p>Returns only lines that contain the specified text. Higher-level data is not output automatically. You can output higher-level data with one of the following parameters:</p> <ul style="list-style-type: none"> -a - Specify how many lines are to be output after the specified text. -b - Specify how many lines are to be output before the specified text. -c - Specify how many lines are to be output before and after the specified text. <p>Regular expressions can be used in this adaptation.</p> <p>Example:</p> <pre>localhost# show running-config dhcp dhcp client ipv4 vlan1 hostname lease 06:40 client-id sys-name exit ipv4 vlan2 client-id name-of-station exit exit exit localhost# show running-config dhcp include name hostname client-id sys-name client-id name-of-station localhost# show running-config dhcp include -a 2 name 4: hostname 5- lease 06:40 6: client-id sys-name 7- exit 8- -- 10: client-id name-of-station 11- exit 12-</pre> |

3.3 Basic operation

| Command | Description |
|-----------|---|
| linnum | <p>Numbers the lines in the output.</p> <p>Example:</p> <pre>localhost# show running-config dhcp linnum 1: dhcp 2: client 3: ipv4 vlan1 4: client-id sys-name 5: lease 06:40 6: hostname 7: exit 8: 9: ipv4 vlan2 10: client-id name-of-station 11: lease 10:00 12: hostname 13: exit 14: 15: exit 16: 17: exit 18:</pre> |
| match-all | <p>All set filters must apply. If you combine several customization parameters, you receive an output by default if at least one of the filters applies. If you also specify the customization parameter <code>match-all</code>, you only get an output if all filters match. If there is no entry for which all filters apply, you obtain the corresponding information.</p> <p>Example:</p> <pre>localhost# show running-config dhcp client ipv4 vlan* select lease 06:40 select client-id name-of-station dhcp client ipv4 vlan1 client-id sys-name lease 06:40 hostname exit ipv4 vlan2 client-id name-of-station lease 10:00 hostname exit exit exit localhost# show running-config dhcp client ipv4 vlan* select lease 06:40 select client-id name-of-station match-all % No entries found.</pre> |
| more | <p>Displays the output page-by-page. When the output reaches the screen length, you are prompted to press a key to display the next output. Enter allows you to move forward line-by-line, the space key allows you to scroll page-by-page.</p> |
| nomore | <p>Suppresses the page output.</p> |

| Command | Description |
|-------------------------|--|
| notab | <p>Suppresses the output as a table.</p> <p>Example:</p> <pre>localhost# show system firmware versions SOFTWARE VERSION DATE ----- Running SINEC OS Firmware V02.00.00.00 2021-06-01_00:00:00 Backup SINEC OS Firmware V02.00.00.00 2021-06-01_00:00:00 Running after Restart V02.00.00.00 2021-06-01_00:00:00 Bootloader V02.00.00.00 2021-06-01_00:00:00</pre> <pre>localhost# show system firmware versions notab firmware versions "Running SINEC OS Firmware" version V02.00.00.00 date 2021-06-01_00:00:00 firmware versions "Backup SINEC OS Firmware" version V02.00.00.00 date 2021-06-01_00:00:00 firmware versions "Running after Restart" version V02.00.00.00 date 2021-06-01_00:00:00 firmware versions Bootloader version V02.00.00.00 date 2021-06-01_00:00:00</pre> |
| repeat | <p>Repeats the output in the specified interval. Enter an interval in seconds. If you do not specify an interval, the output is updated every 10 seconds by default. The printout is repeated until you cancel it with [Ctrl] + [C].</p> <p>Example:</p> <p>The show dhcp client repeat 15 command repeats the show dhcp client command every 15 seconds.</p> |
| select { parameter } | <p>Only the specified parameter is displayed. You must specify the exact parameter name.</p> <p>Example:</p> <pre>localhost# show dhcp client ipv4 bindings select ip-address IP INTERFACE ADDRESS ----- vlan1 0.0.0.0 vlan2 0.0.0.0</pre> <pre>localhost# show running-config dhcp client ipv4 vlan* select hostname dhcp client ipv4 vlan1 hostname exit ipv4 vlan2 hostname exit exit exit</pre> |

3.3 Basic operation

| Command | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------|--|-----------|-------------|----------|-----------------|----------|-----------------|--------|-------|------|-------|---|---|---|---|-------|------|-------|---|---|---|---|-------|------|-------|---|---|---|---|
| sort-by | <p>Sorts the output according to the specified parameter.</p> <p>Example:</p> <pre>localhost# show running-config dhcp client ipv4 vlan* tab sort-by lease</pre> <table border="1"> <thead> <tr> <th>INTERFACE</th> <th>HOSTNAME</th> <th>LEASE</th> <th>MAC ADDRESS</th> <th>SYS NAME</th> <th>NAME OF STATION</th> <th>STRING</th> </tr> </thead> <tbody> <tr> <td>vlan7</td> <td>true</td> <td>02:00</td> <td>X</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>vlan1</td> <td>true</td> <td>04:60</td> <td>-</td> <td>X</td> <td>-</td> <td>-</td> </tr> <tr> <td>vlan2</td> <td>true</td> <td>10:00</td> <td>-</td> <td>-</td> <td>X</td> <td>-</td> </tr> </tbody> </table> | INTERFACE | HOSTNAME | LEASE | MAC ADDRESS | SYS NAME | NAME OF STATION | STRING | vlan7 | true | 02:00 | X | - | - | - | vlan1 | true | 04:60 | - | X | - | - | vlan2 | true | 10:00 | - | - | X | - |
| INTERFACE | HOSTNAME | LEASE | MAC ADDRESS | SYS NAME | NAME OF STATION | STRING | | | | | | | | | | | | | | | | | | | | | | | |
| vlan7 | true | 02:00 | X | - | - | - | | | | | | | | | | | | | | | | | | | | | | | |
| vlan1 | true | 04:60 | - | X | - | - | | | | | | | | | | | | | | | | | | | | | | | |
| vlan2 | true | 10:00 | - | - | X | - | | | | | | | | | | | | | | | | | | | | | | | |

| Command | Description |
|---------|--|
| tab | <p>Forces the output as a table.</p> <p>Example:</p> <pre>localhost# show running-config dhcp client ipv4 vlan* dhcp client ipv4 vlan1 client-id sys-name lease 06:40 hostname exit dhcp client ipv4 vlan2 client-id name-of-station lease 10:00 hostname exit exit exit localhost# show running-config dhcp client ipv4 vlan* tab MAC SYS NAME OF INTERFACE HOSTNAME LEASE ADDRESS NAME STATION STRING ----- vlan1 true 04:60 - X - - vlan2 true 10:00 - - X -</pre> |

3.3 Basic operation

| Command | Description |
|-----------------------------|--|
| <code>until { text }</code> | <p>Returns all lines until a line with the specified text appears. Regular expressions can be used in this output.</p> <p>Example:</p> <pre>localhost# show running-config dhcp dhcp client ipv4 vlan1 client-id sys-name lease 01:00:00 hostname exit ipv4 vlan2 client-id name-of-station lease 02:00:00 hostname exit exit localhost# show running-config dhcp until lease dhcp client ipv4 vlan1 client-id sys-name lease 06:40</pre> |

3.3.13 Adapting the output of lists

When outputting lists, you can influence which items are displayed. An existing output is not filtered retroactively in this case; rather, the desired output is generated directly.

To adapt the output of lists, execute the following command in operational mode:

```
show { CLI path } { Key element } [Range][Number of characters]*
```

Conditions:

- As range, enter the characters which the displayed key elements should contain.
- Options for the range include:
 - 0-9
 - A-Z
 - a-z
 - / . _ :-
- If you combine numbers, letters and symbols for the range, they are strung together directly, e.g. [0-9a-z] or [0-9a-z/].

- Specify the number of characters of the keyword the range information must match, starting with the first character of the keyword. The `[A-F]{6}` specification means that only key elements with the first 6 characters in the range A-F are displayed.
- Use the placeholder `"*"`.
- If the entire expression contains spaces, it needs to be placed in quotation marks (`"`), e.g. `"LED* [A-Z]{2}"`.

Restrictions:

- You can only apply the adaptation to a data structure of the data type "List".
- You can only apply the adaptation to the key element(s) of a list.

Refer to the data model for the corresponding information on data types and keywords.

Example

In this example, all MAC addresses on VLAN 1 that begin with two letters are displayed.

```
localhost# show switch mac-address-tables filtering-database entry
1 [a-f]{2}*
```

| VID | MAC ADDRESS | TRAFFIC CLASS | ENTRY TYPE | FORWARDING PORT |
|-----|-------------------|---------------|------------|-----------------|
| 1 | ee:00:00:00:00:01 | unprioritized | static | ethernet0/1 |

Example

In this example, the two LEDs for the display mode are shown.

```
localhost# show system hardware component LED*DM[1-2]
```

| NAME | CLASS | DESCRIPTION | PARENT | REV | HARDWARE NUM | SERIAL | OPER STATE | STATUS |
|---------|-------|-------------|--------|-----|--------------|--------|------------|--------|
| LED DM1 | led | Type: Green | CPU | 0 | - | - | enabled | OFF |
| LED DM2 | led | Type: Green | CPU | 0 | - | - | enabled | OFF |

Example

In this example, all LEDs with two letters are displayed.

```
localhost# show system hardware component "LED*[A-Z]{2}"
```

| NAME | CLASS | DESCRIPTION | PARENT | REV | HARDWARE NUM | SERIAL | OPER STATE | STATUS |
|--------|-------|-------------|--------|-----|--------------|--------|------------|--------|
| - | | | | | | | | |
| LED RM | led | Type: Green | CPU | 0 | - | - | enabled | OFF |
| LED CM | led | Type: Green | CPU | 0 | - | - | enabled | OFF |

Example

In this example, all LEDs with one character are displayed.

```
localhost# show system hardware component "LED* [A-Z0-9]{1}"
```

| NAME | CLASS | DESCRIPTION | PARENT | REV | HARDWARE NUM | SERIAL | OPER STATE | STATUS |
|-------|-------|-------------|--------|-----|--------------|--------|------------|--------|
| - | | | | | | | | |
| LED A | led | Type: Red | CPU | 0 | - | - | enabled | OFF |

3.4 Help commands

This section describes commands that support you in the operation of the CLI.

3.4.1 Displaying all available options for a command

The syntax of a command consists of required and optional parameters. To view the possible command options, enter a question mark `?` directly in the command prompt or after a part of the command with a space. You do not have to press **Enter**. A list and short description of all currently allowed command options is immediately displayed.

The `<cr>` entry stands for *carriage return*. If the `<cr>` entry is at the end of the list, you can execute the previously entered command with **Enter**. The listed parameters are optional. If the `<cr>` entry stands alone, no further parameters are available. You must execute the command with **Enter**.

If the `|` entry is in the list, you can use customization parameters to adjust the output of the CLI command. For additional information, see also "Customizing the output of a command (Page 73)".

Example

In this example, all commands available to you in operating mode are displayed.

```
localhost# ?
Possible completions:
  admin      Administrative commands.
  clear      Clear parameter
  ...
localhost#
```

Example

This example shows all the parameters that are available to you for the `lldp` command. You can also execute the command without `<cr>` parameters.

```
localhost(config)# lldp ?
Possible completions:
  hold          The multiplier ..
  reinit-delay  The time in seconds (s) ..
  ...
  <cr>
localhost(config)# lldp
```

Example

In this example, date and system time are configured. The `?` is used to indicate which parameters must be entered next.

```
localhost# system clock set-current-datetime ?
Possible completions:
  date  The system date in the form of YYYY-MM-DD.
  time  The system time in hours (24-hour clock), ...
localhost# system clock set-current-datetime date ?
Description: The system date in the form of YYYY-MM-DD.
Possible completions:
```

```

    <string>    Date, format is YYYY-MM-DD.
localhost# system clock set-current-datetime date 2019-03-25 ?
Possible completions:
    time      The system time in hours (24-hour clock), ...
localhost# system clock set-current-datetime date 2019-03-25 time ?
Description: The system time in hours (24-hour clock), ...
Possible completions:
    <string>    Time, format is HH:MM:SS.
localhost# system clock set-current-datetime date 2019-03-25 time
12:00:00 ?
Possible completions:
    <cr>
localhost# system clock set-current-datetime date 2019-03-25 time
12:00:00
localhost#

```

3.4.2 Showing the infotext for a command

To show the infotext for a specific command, execute the following command:

```
help {command}
```

If the command consists of multiple parameters, the infotext for the last parameter is displayed.

Example

```

localhost# help system
Help for command: system
    General system management configuration settings.
localhost# help system clock set-current-datetime
Help for command: set-current-datetime
    System date and time settings.

```

3.4.3 Completing a command

You do not need to enter commands and parameters completely for the CLI to recognize them. If you type the first letters of a command and press the Tab key, the command is completed or the possible additions are displayed.

Example

This example shows a simple completion.

If the first letters of a command are unique, the command is completed automatically.

```

localhost# con[Tab key]
localhost# config

```

Example

This example shows a list of possible additions.

3.5 Configuration of the user interfaces

If the first letters correspond to more than one possible command, a list with the possible completions appears. The letters entered are retained in the next command line so that you can continue entering the command.

```
localhost# system rest[Tab key]
Possible completions:
  restart          Restart the device.
  restore-defaults Restore factory defaults and restart the
device.
localhost# system rest
```

Example

This example shows multi-level completion.

If multiple commands are possible and their first letters are the same, the command is completed to the extent that the commands match. If you press the Tab key again, a list with the possible additions appears. The letters entered are retained in the next command line so that you can continue entering the command.

```
localhost# system r[Tab key]
localhost# system rest[Tab key]
Possible completions:
  restart          Restart the device.
  restore-defaults Restore factory defaults and restart the
device.
localhost# system rest
```

3.5 Configuration of the user interfaces

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

For more information on the SNMP user interface, refer to "SNMP (Page 475)".

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).

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 485)".

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 in CLI | default |
| Name in Web UI | SSH |
| Endpoint enabled | Yes |
| IP address | 0.0.0.0 |
| Port | 22 |

Web UI HTTP

| Endpoint | Default |
|------------------|----------|
| Name in CLI | unsecure |
| Name in Web UI | HTTP |
| Endpoint enabled | No |
| IP address | 0.0.0.0 |
| Port | 80 |

Web UI HTTPS

| Endpoint | Default |
|------------------|---------|
| Name in CLI | secure |
| Name in Web UI | HTTPS |
| Endpoint enabled | Yes |
| IP address | 0.0.0.0 |
| Port | 443 |

NETCONF SSH

| Endpoint | Default |
|------------------|---------|
| Name in CLI | default |
| Name in Web UI | NETCONF |
| Endpoint enabled | Yes |
| IP address | 0.0.0.0 |
| Port | 830 |

3.5.1 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 90)".
2. [Optional] Change the inactivity timeout for NETCONF sessions.
For more information, refer to "Changing the inactivity timeout for NETCONF sessions (Page 91)".
3. Configure a server endpoint for NETCONF.
For more information, refer to "Configuring a server endpoint for NETCONF (Page 92)".
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 93)".
5. Enable a server endpoint for NETCONF.
For more information, refer to "Enabling a server endpoint for NETCONF (Page 95)".

3.5.1.1 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:

| Step | Instruction | Command |
|------|------------------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the NETCONF user interface. | <code>system management-services netconf enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services netconf enabled</code> |

Example

```
localhost# config
localhost(config)# system management-services netconf enabled
localhost(config-netconf)# commit
Commit complete.
localhost(config-netconf)# end
localhost# show running-config system management-services netconf
enabled
system
  management-services
    netconf
      enabled
    exit
  exit
```

exit

3.5.1.2 Changing the inactivity timeout for NETCONF sessions

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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Change the inactivity timeout for NETCONF sessions. Conditions: <ul style="list-style-type: none"> Formatted as <code>nYnMnDnhnmns</code>, where <code>n</code> is a user-defined number Minimum 0 seconds (<code>0s</code>) Maximum 49 days 17 hours 2 minutes 47 seconds (<code>49D17h2m47s</code>) Default: <code>5m</code> (5 minutes) If you set the value to <code>0s</code> , automatic logoff is disabled. If you set the value <code>1M</code> (1 month), the device calculates the inactivity timeout as follows: 365 days/12 months. Accordingly, a value of 30.4167 days is configured. | <code>system management-services netconf idle-timeout [0s - 49D17h2m47s]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services netconf idle-timeout</code> |

Example

```
localhost# config
localhost(config)# system management-services netconf idle-timeout
30m
localhost(config-netconf)# commit
Commit complete.
localhost(config-netconf)# end
localhost# show running-config system management-services netconf
idle-timeout
system
management-services
```

3.5 Configuration of the user interfaces

```

netconf
  idle-timeout 30m
exit

exit

exit

```

3.5.1.3 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:

- 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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the IP address and the port for a server endpoint. Default IP address: 0.0.0.0 The default IP address allows client requests on all local addresses. Default port: 830 | <code>system management-services netconf endpoint default ssh tcp ipv4 { IP address } port [830, 5355 - 49151]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services netconf endpoint default</code> |

Example

```

localhost# config
localhost(config)# system management-services netconf endpoint
default ssh tcp ipv4 192.168.1.1 port 5830
localhost(config-netconf-endpoint-default)# commit

```

```
Commit complete.
localhost(config-netconf-endpoint-default)# end
localhost# show running-config system management-services netconf
endpoint default
system
management-services
netconf
endpoint default
ssh
tcp
port 5830
ipv4 192.168.1.1
exit

exit

exit

exit

exit

exit
```

3.5.1.4 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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Configure the SSH key exchange method for a NETCONF server endpoint.</p> <p>Options include:</p> <ul style="list-style-type: none"> • <code>curve448-sha512</code> For more information, refer to RFC8731 (https://www.ietf.org/rfc/rfc8731.html) • <code>curve25519-sha256</code> For more information, refer to RFC8731 (https://www.ietf.org/rfc/rfc8731.html) • <code>diffie-hellman-group14-sha1</code> For more information, refer to RFC4253 (https://www.ietf.org/rfc/rfc4253.html) • <code>diffie-hellman-group16-sha512</code> For more information, refer to RFC8268 (https://www.ietf.org/rfc/rfc8268.html) • <code>ecdh-sha2-nistp256</code> For more information, refer to RFC5656 (https://www.ietf.org/rfc/rfc5656.html) • <code>ecdh-sha2-nistp384</code> For more information, refer to RFC5656 (https://www.ietf.org/rfc/rfc5656.html) • <code>ecdh-sha2-nistp521</code> For more information, refer to RFC5656 (https://www.ietf.org/rfc/rfc5656.html) <p>Default:</p> <ul style="list-style-type: none"> • <code>curve25519-sha256</code> • <code>diffie-hellman-group16-sha512</code> • <code>ecdh-sha2-nistp256</code> | <pre>system management-services netconf endpoint default ssh ssh transport-params key-exchange- alg [curve448-sha512 curve25519-sha256 diffie- hellman-group14-sha1 diffie- hellman-group16-sha512 ecdh- sha2-nistp256 ecdh-sha2- nistp384 ecdh-sha2-nistp521]</pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <pre>show running-config system management-services netconf endpoint default ssh ssh transport-params key-exchange-alg</pre> |

Example

In this example, the key exchange method **diffie-hellman-group14-sha1** is configured in addition.

```
localhost# config
localhost(config)# system management-services netconf endpoint
default ssh ssh transport-params key-exchange-alg diffie-hellman-
group14-sha1
localhost(config-transport-params)# commit
Commit complete.
```

```

localhost(config-transport-params)# end
localhost# show running-config system management-services netconf
endpoint default ssh ssh transport-params key-exchange-alg
system
management-services
netconf
endpoint default
ssh
ssh
transport-params
key-exchange-alg [ curve25519-sha256 diffie-hellman-group16-
sha512 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 ]
exit

exit

exit

exit

exit

exit

exit

```

3.5.1.5 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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the server endpoint for NETCONF. | <code>system management-services netconf endpoint default enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services netconf endpoint default enabled</code> |

Example

```

localhost# config
localhost(config)# system management-services netconf endpoint
default enabled
localhost(config-netconf-endpoint-default)# commit
Commit complete.
localhost(config-netconf-endpoint-default)# end

```

3.5 Configuration of the user interfaces

```
localhost# show running-config system management-services netconf
endpoint default enabled
system
management-services
netconf
endpoint default
enabled
exit

exit

exit

exit
```

3.5.2 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 96)".
2. Configure a server endpoint for the CLI.
For more information, refer to "Configuring a server endpoint for the CLI (Page 98)".
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 99)".
4. Enable a server endpoint for the CLI.
For more information, refer to "Enabling a server endpoint for the CLI (Page 101)".
5. [Optional] Change the settings for local CLI sessions.
For more information, refer to "Configuring the local CLI environment (Page 102)".

3.5.2.1 Changing the inactivity timeout for CLI sessions

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 configure 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 "Configuring the local CLI environment (Page 102)".

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Change the inactivity timeout for CLI sessions. Conditions: <ul style="list-style-type: none"> Formatted as <code>nYnMnDnHnmns</code>, where <code>n</code> is a user-defined number Minimum 0 seconds (<code>0s</code>) Maximum 49 days 17 hours 2 minutes 47 seconds (<code>49D17h2m47s</code>) Default: <code>15m</code> (15 minutes) If you set the value to <code>0s</code> , automatic logout is disabled. If you set the value <code>1M</code> (1 month), the device calculates the inactivity timeout as follows: 365 days/12 months. Accordingly, a value of <code>30.4167</code> days is configured. | <code>system management-services cli idle-timeout [0s - 49D17h2m47s]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services cli idle- timeout</code> |

Example

```
localhost# config
localhost(config)# system management-services cli idle-timeout 30m
localhost(config-cli)# commit
Commit complete.
localhost(config-cli)# end
localhost# show running-config system management-services cli idle-
timeout
system
  management-services
    cli
      idle-timeout 30m
    exit
  exit
exit
```

3.5.2.2 Configuring a server endpoint for the CLI

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

| NOTICE |
|--|
| <p>Configuration hazard - risk of connection loss</p> <p>If the device is assigned its IP address dynamically via DHCP, not the following:</p> <p>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.</p> <p>You have the following options to prevent connection loss:</p> <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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the IP address and the port for a server endpoint. Default IP address: 0.0.0.0 The default IP address allows client requests on all local addresses. Default port: 22 | <code>system management-services cli endpoint default ssh tcp ipv4 { IP address } port [22, 5355 - 49151]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services cli endpoint default</code> |

Example

```
localhost# config
localhost(config)# system management-services cli endpoint default
ssh tcp ipv4 192.168.1.1 port 6022
localhost(config-cli-endpoint-default)# commit
Commit complete.
localhost(config-cli-endpoint-default)# end
localhost# show running-config system management-services cli
endpoint default
system
management-services
cli
endpoint default
ssh
tcp
```

```
port 6022
ipv4 192.168.1.1
exit

exit

exit

exit

exit

exit
```

3.5.2.3 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.

3.5 Configuration of the user interfaces

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

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the SSH key exchange method for a CLI server endpoint. Options include: <ul style="list-style-type: none"> • <code>curve448-sha512</code> For more information, refer to RFC8731 (https://www.ietf.org/rfc/rfc8731.html) • <code>curve25519-sha256</code> For more information, refer to RFC8731 (https://www.ietf.org/rfc/rfc8731.html) • <code>diffie-hellman-group14-sha1</code> For more information, refer to RFC4253 (https://www.ietf.org/rfc/rfc4253.html) • <code>diffie-hellman-group16-sha512</code> For more information, refer to RFC8268 (https://www.ietf.org/rfc/rfc8268.html) • <code>ecdh-sha2-nistp256</code> For more information, refer to RFC5656 (https://www.ietf.org/rfc/rfc5656.html) • <code>ecdh-sha2-nistp384</code> For more information, refer to RFC5656 (https://www.ietf.org/rfc/rfc5656.html) • <code>ecdh-sha2-nistp521</code> For more information, refer to RFC5656 (https://www.ietf.org/rfc/rfc5656.html) Default: <ul style="list-style-type: none"> • <code>curve25519-sha256</code> • <code>diffie-hellman-group16-sha512</code> • <code>ecdh-sha2-nistp256</code> | <pre>system management-services cli endpoint default ssh ssh transport-params key-exchange- alg [curve448-sha512 curve25519-sha256 diffie- hellman-group14-sha1 diffie- hellman-group16-sha512 ecdh- sha2-nistp256 ecdh-sha2- nistp384 ecdh-sha2-nistp521]</pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <pre>show running-config system management-services cli endpoint default ssh ssh transport-params key-exchange-alg</pre> |

Example

In this example, the key exchange method **diffie-hellman-group14-sha1** is configured in addition.

```
localhost# config
localhost(config)# system management-services cli endpoint default
ssh ssh transport-params key-exchange-alg diffie-hellman-group14-
sha1
localhost(config-transport-params)# commit
Commit complete.
```

```

localhost(config-transport-params)# end
localhost# show running-config system management-services cli
endpoint default ssh ssh transport-params key-exchange-alg
system
management-services
cli
endpoint default
ssh
ssh
transport-params
key-exchange-alg [ curve25519-sha256 diffie-hellman-group16-
sha512 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 ]
exit

exit

exit

exit

exit

exit

exit

```

3.5.2.4 Enabling a server endpoint for the CLI

The server endpoint for the CLI is enabled by default.

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 the USB console interface.

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

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the server endpoint for the CLI. | <code>system management-services cli endpoint default enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services cli endpoint default enabled</code> |

Example

```
localhost# config
```

3.5 Configuration of the user interfaces

```
localhost(config)# system management-services cli endpoint default
enabled
localhost(config-cli-endpoint-default)# commit
Commit complete.
localhost(config-cli-endpoint-default)# end
localhost# show running-config system management-services cli
endpoint default enabled
system
management-services
cli
endpoint default
enabled
exit

exit

exit

exit
```

3.5.2.5 Configuring the local CLI environment

To run the following commands, you need to be in operating mode. Enter the `terminal` command followed by one of the following commands.

| Command | Description |
|--|--|
| <pre>idle-timeout { 0 - 4294967 } Default: 900</pre> | <p>The timeout in seconds after the CLI session is automatically terminated. If you set the value to "0", automatic logout is disabled.</p> <p>You can set the timeout only for the current CLI session. The setting is not saved. When you open a new CLI session, the default value is set again for this session.</p> <p>For more information about configuring the global timeout for CLI sessions, refer to "Changing the inactivity timeout for CLI sessions (Page 96)".</p> |
| <pre>paginate [true false] Default: true</pre> | <p>The output is page-by-page by default. When the output reaches the configured screen length, you are prompted to press a key to display the next output. Enter allows you to move forward line-by-line, the space key allows you to scroll page-by-page. When disabled, page-by-page output is suppressed.</p> |
| <pre>screen-length { Length } Default: Set automatically</pre> | <p>Defines the length of a terminal page in pixels (px). If you set the smallest value "0", the terminal sets the maximum available value for the length and suppresses page-by-page output (<code>paginate false</code>). The greatest value depends on the terminal being used.</p> |
| <pre>screen-width { Width } Default: Set automatically</pre> | <p>Defines the width of a terminal page in pixels (px). If you set the smallest value "0", the terminal sets the maximum available value for the width. The greatest value depends on the terminal being used.</p> |
| <pre>timestamp [enable disable] Default: disable</pre> | <p>Enables/disables the display of a time stamp for every command.</p> |

3.5.3 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 103)".
2. [Optional] Change the inactivity timeout for Web UI sessions.
For more information, refer to "Changing the inactivity timeout for Web UI sessions (Page 104)".
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 105)".
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 106)".
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 107)".
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 108)".
7. [Optional] Reference a user-defined HTTPS certificate.
For more information, refer to "Using a user-defined HTTPS certificate (Page 109)".

3.5.3.1 Enabling the Web user interface

The Web user interface is enabled by default.

Note

When the Web user interface is enabled, you can also configure the device via the Web UI. For more information, refer to the **SINEC OS Web UI Configuration Manual**.

Only users with the `admin` user profile can enable the Web user interface.

To enable the Web user interface, do the following:

| Step | Instruction | Command |
|------|--------------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the Web user interface. | <code>system management-services webui enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services webui enabled</code> |

Example

```
localhost# config
localhost(config)# system management-services webui enabled
```

3.5 Configuration of the user interfaces

```
localhost(config-webui)# commit
Commit complete.
localhost(config-webui)# end
localhost# show running-config system management-services webui
enabled
system
management-services
webui
enabled
exit

exit

exit
```

3.5.3.2 Changing the inactivity timeout for Web UI sessions

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Change the inactivity timeout for Web UI sessions. Conditions: <ul style="list-style-type: none"> Formatted as <code>nYnMnDnHnmns</code>, where <code>n</code> is a user-defined number Minimum 0 seconds (<code>0s</code>) Maximum 49 days 17 hours 2 minutes 47 seconds (<code>49D17h2m47s</code>) Default: <code>15m</code> (15 minutes) If you set the value to <code>0s</code> , automatic logoff is disabled. If you set the value <code>1M</code> (1 month), the device calculates the inactivity timeout as follows: 365 days/12 months. Accordingly, a value of 30.4167 days is configured. | <code>system management-services webui idle-timeout [0s - 49D17h2m47s]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services webui idle-timeout</code> |

Example

```

localhost# config
localhost(config)# system management-services webui idle-timeout 30m
localhost(config-webui)# commit
Commit complete.
localhost(config-webui)# end
localhost# show running-config system management-services webui
idle-timeout
system
  management-services
    webui
      idle-timeout 30m
    exit
  exit
exit
exit

```

3.5.3.3 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:

- 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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the IP address and the port for an HTTP server endpoint. Default IP address: 0.0.0.0 The default IP address allows client requests on all local addresses. Default port: 80 | <code>system management-services webui endpoint unsecure http tcp ipv4 { IP address } port [80, 5355 - 49151]</code> |
| 3 | Commit the change. | <code>commit</code> |

3.5 Configuration of the user interfaces

| Step | Instruction | Command |
|------|---------------------------|--|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system management-services webui endpoint unsecure |

Example

```
localhost# config
localhost(config)# system management-services webui endpoint
unsecure http tcp ipv4 192.168.1.1 port 8080
localhost(config-webui-endpoint-unsecure)# commit
Commit complete.
localhost(config-webui-endpoint-unsecure)# end
localhost# show running-config system management-services webui
endpoint unsecure
system
management-services
webui
endpoint unsecure
http
tcp
port 8080
ipv4 192.168.1.1
exit

exit

exit

exit

exit

exit
```

3.5.3.4 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 an HTTP server endpoint.

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

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable the HTTP server endpoint for the Web UI. | system management-services webui endpoint unsecure enabled |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------|--|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system management-services webui endpoint unsecure enabled |

Example

```
localhost# config
localhost(config)# system management-services webui endpoint
unsecure enabled
localhost(config-webui-endpoint-unsecure)# commit
Commit complete.
localhost(config-webui-endpoint-unsecure)# end
localhost# show running-config system management-services webui
endpoint unsecure enabled
system
  management-services
    webui
      endpoint unsecure
        enabled
      exit
    exit
  exit
exit
exit
```

3.5.3.5 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.

3.5 Configuration of the user interfaces

To configure an HTTPS server endpoint, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the IP address and the port for an HTTPS server endpoint. Default IP address: 0.0.0.0 The default IP address allows client requests on all local addresses. Default port: 443 | <code>system management-services webui endpoint secure https tcp ipv4 { IP address } port [443, 5355 - 49151]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services webui endpoint secure</code> |

Example

```
localhost# config
localhost(config)# system management-services webui endpoint secure
https tcp ipv4 192.168.1.1 port 5443
localhost(config-webui-endpoint-secure)# commit
Commit complete.
localhost(config-webui-endpoint-secure)# end
localhost# show running-config system management-services webui
endpoint secure
system
management-services
webui
endpoint secure
https
tcp
port 5443
ipv4 192.168.1.1
exit

exit

exit

exit

exit

exit
```

3.5.3.6 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 an HTTPS server endpoint.

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

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the HTTPS server endpoint for the Web UI. | <code>system management-services webui endpoint secure enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services webui endpoint secure enabled</code> |

Example

```
localhost# config
localhost(config)# system management-services webui endpoint secure
enabled
localhost(config-webui-endpoint-secure)# commit
Commit complete.
localhost(config-webui-endpoint-secure)# end
localhost# show running-config system management-services webui
endpoint secure enabled
system
management-services
webui
endpoint secure
enabled
exit

exit

exit

exit
```

3.5.3.7 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 201)".

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.

3.5 Configuration of the user interfaces

To use an HTTPS certificate, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Reference an HTTPS certificate from the key-store. | system management-services webui endpoint secure https tls server-identity certificate keystore-reference asymmetric-key { Name } certificate { Name } |
| 3 | Commit the change. | commit |
| 4 | Exit to the top level. | top |
| 5 | To apply the loaded certificate, restart the HTTPS server endpoint. Disable the HTTPS server endpoint. | no system management-services webui endpoint secure enabled |
| 6 | Commit the change. | commit |
| 7 | Enable the HTTPS server endpoint. | system management-services webui endpoint secure enabled |
| 8 | Commit the change. | commit |
| 9 | Exit configuration mode. | end |

Example

```
localhost# config
localhost(config)# system management-services webui endpoint secure
https tls server-identity certificate keystore-reference asymmetric-
key my-https-server certificate my-https
localhost(config-keystore-reference)# commit
Commit complete.
localhost(config-keystore-reference)# top
localhost(config)# no system management-services webui endpoint
secure enabled
localhost(config)# commit
Commit complete.
localhost(config)# system management-services webui endpoint secure
enabled
localhost(config-webui-endpoint-secure)# commit
Commit complete.
localhost(config-webui-endpoint-secure)# end
localhost#
```

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 Calling the CLI

You can access the Command Line Interface (CLI) via a direct connection between a client PC and a device or via a remote connection over the network.

4.1.1 Accessing the CLI through the USB console interface

You can access the CLI by using a virtual serial connection (115200 8N1) between the USB console interface of the device and a client PC. Access to the device is possible independently of the Ethernet ports and without the device having an IP configuration.

Requirements

The following requirements must be met:

- The device is connected to the client PC via the USB console interface.
You need a cable with USB type B connector and USB type A connector. The connecting cable for the USB console interface can be ordered as accessory (article number: 7ML1930-1FN).
- The **Custom SCALANCE/RUGGEDCOM Driver** is installed on the client PC.
To use the USB console interface under Windows, you must install the driver on the client PC. You can download the driver via SIOS (<https://support.industry.siemens.com/cs/at/en/view/109798927>).
- Terminal software for establishing serial connections is available on the client PC.

Establishing a connection to a device

To access the CLI, do the following:

1. Make the following connection settings in the terminal software:

| | |
|--------------------------|--------|
| Connection type | Serial |
| Transmission rate | 115200 |
| Data rate | 8 bits |
| Parity | None |
| Stop | 1 bit |
| Flow control | None |

2. Select the **SCALANCE USB Serial Console** COM port.

3. Establish a connection to the device.
4. Log in.
For more information, refer to "Logging in (Page 112)".

4.1.2 Accessing the CLI via a network connection

You can access the CLI using an SSH client.

Requirements

The following requirements must be met:

- The device has an IP address.

Note

Assign an IP address for the device using DHCP, the USB console interface or SINEC PNI.

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

Note

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

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

Establishing a connection to a device

To access the CLI, do the following:

1. Make the following connection settings in the terminal software:

| | |
|-----------------|------------------------------|
| Connection type | SSH |
| IP address | The IP address of the device |
| TCP port | 22 |

2. Establish a connection to the device.
3. Log in.
For more information, refer to "Logging in (Page 112)".

4.2 Logging in

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:

| |
|---|
| NOTICE |
| Security hazard - risk of unauthorized access and/or exploitation |
| To prevent unauthorized access, default passwords must be changed before commissioning the device. For more information, refer to "Changing the password of a user (Page 171)". |

| Profile | Password |
|---------|----------|
| admin | admin |

4.2.2 Logging in to a device with default settings

| |
|--|
| NOTICE |
| Configuration hazard - risk of connection loss |
| Note that the access rights of some functions change after the first login with the default user profile admin and the assignment of a new password. |
| For more information, refer to: |
| <ul style="list-style-type: none"> • Requesting a configuration file from the DHCP server (option 66, 67) (Page 329) • Configuring the access rights of DCP (Page 452) |

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

1. Set up a connection to the device and call the CLI.
The logon prompt is displayed.
For more information, refer to "Calling the CLI (Page 111)".
2. Enter the factory default user name.
For more information, refer to "Default user profiles and passwords (Page 113)".
3. Enter the factory default password.
If the entries are incorrect, the user is denied access.

4. If the entries are correct, 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: \$5\$ (SHA-256) or \$6\$ (SHA-512)
 - As plain text password
If a password begins with a character combination other than \$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 viewed as a plain text 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 8 and 255 characters long
 - Must contain at least 1 number
 - All standard characters are allowed, plus the following special characters:
\$ % & () * + , - . / : < = > @ [] ^ _ { } ~

5. Enter the new password again.
The CLI verifies the entries.
 - If the entries are correct, you are in operating mode.
To apply the changes, the CLI session is closed automatically after a few seconds.
 - If the entries are incorrect, an error message is generated. Repeat the last steps.
6. Call up the CLI and log in with the user name and the new password.

Example

```
login as: admin
admin@192.168.16.15's password: admin
```

```
      Welcome to the SINEC OS Command Line Interface
      Copyright (c) 2019 Siemens AG
```

```
admin connected from 192.168.16.1 using ssh on localhost
The default password must be changed before access to the device is
granted.
Enter the new password: *****
Confirm the new password: *****
The default password has been changed.
To apply the changes, you will be logged out automatically in a few
seconds.
localhost#
```

4.2.3 Logging in to a configured device

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

1. Set up a connection to the device and call the CLI.
The logon prompt is displayed.
For more information, refer to "Calling the CLI (Page 111)".
2. Enter the user name.
3. Enter the password.
The CLI verifies the entries.
 - If the entries are correct, you are in operating mode.
 - If the entries are incorrect, an error message is generated. Repeat the last steps.

Example

```
login as: admin
admin@192.168.16.15's password: *****
```

```
Welcome to the SINEC OS Command Line Interface
Copyright (c) 2019 Siemens AG
```

```
admin connected from 192.168.16.1 using ssh on localhost
localhost#
```

4.3 Logging out

To log out and end the CLI session, execute the following command in operating mode:

```
exit
```

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 116)".
2. Specify the physical location of the device.
For more information, refer to "Specifying the device location (Page 117)".

3. Specify a contact person for the device.
For more information, refer to "Specifying the contact person for the device (Page 117)".
4. [Optional] Define the default gateway manually.
For more information, refer to "Defining the default gateway manually (Page 118)".

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.

By default, the host name is the device family name combined with the serial number.

```
{ device family }-{ serial number }#
```

If the host name is cleared, the host name changes automatically to "localhost".

```
localhost#
```

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

The host name uses the same data source as the sysName MIB object. The two elements differ only in their default setting and after a reset or deletion. If a concrete value is configured for either element, both elements contain the same value. For more information about the MIB object, refer to "sysName MIB object (Page 480)".

To change the host name, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Change the host name for the device. Conditions: <ul style="list-style-type: none"> • Must be between 1 and 253 characters long • Must not contain spaces | system hostname { Name } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system hostname |

Example

The following changes the host name to sec01.

```
localhost# config
localhost(config)# system hostname sec01
localhost(config-system)# commit
Commit complete.
sec01(config-system)# end
sec01# show running-config system hostname
system
hostname sec01
exit
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Specify the location of the device. If the string includes spaces, it must either be wrapped in double-quotes (") or you can press Enter after <code>location</code> to enter wizard mode. Condition: <ul style="list-style-type: none"> • Must be between 1 and 255 characters long | <code>system location "{ Description }"</code> <code>system location(<string, min: 0 chars, max: 255 chars>): { Description }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system location</code> |

Example

```
localhost# config
localhost(config)# system location "telephone case, 3rd floor"
localhost(config)# commit
localhost(config)# end
localhost# show running-config system location
system location "telephone case, 3rd floor"
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Specify the contact person for the device. If the string includes spaces, it must either be wrapped in double-quotes (") or you can press Enter after <code>contact</code> to enter wizard mode. Conditions: <ul style="list-style-type: none"> • Can be between 0 and 255 characters long | <code>system contact "{ Name }"</code> <code>system contact(<string, min: 0 chars, max: 255 chars>): { Name }</code> |
| 3 | Commit the change. | <code>commit</code> |

| Step | Instruction | Command |
|------|---------------------------|------------------------------------|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system contact |

Example

```
localhost# config
localhost(config)# system contact "Winston Smith
(wsmith@company.com)"
localhost(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config system contact
system contact "Winston Smith (wsmith@company.com)"
```

Example

```
localhost# config
localhost(config)# system contact
(<string, min: 0 chars, max: 255 chars>): Winston Smith
(wsmith@company.com)
localhost(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config system contact
system contact "Winston Smith (wsmith@company.com)"
```

4.4.1.4 Defining 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 e.g. via DHCP. When multiple default gateways are configured for a device, the distance value decides which default gateway is used.

By default, no default gateway is configured.

To configure the default gateway manually, do the following:

| Step | Instruction | Command |
|------|---|---------------------------------------|
| 1 | Enter configuration mode. | config |
| 2 | Configure the default gateway for the device. The specified IPv4 address must be in an active subnet. | routing gateway ipv4 { IPv4 address } |

| Step | Instruction | Command |
|------|--|---|
| 3 | <p>[Optional] Configure the distance value of the default gateway.</p> <p>When there are multiple routes to the same destination, the device uses the distance value to determine the best path. The path with the shortest distance is preferred.</p> <p>The value 240 is reserved for a default gateway that was configured via DHCP. To avoid conflicts when selecting the default gateway, the value 240 is not permitted for default gateways that are configured manually.</p> <p>Default: 1</p> | <code>distance { 1 - 254 }</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config routing gateway ipv4</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# routing gateway ipv4 192.168.10.1
localhost(config-routing-gateway)# distance 100
localhost(config-routing-gateway)# commit
Commit complete.
localhost(config-routing-gateway)# end
localhost# show running-config routing gateway ipv4
routing
 gateway
  ipv4      192.168.10.1
  distance 100
exit

exit
```

4.4.2 Displaying the basic settings

To display the basic settings of the device, execute the following commands in the operating mode:

```
show system info
show routing gateway ipv4
```

Example

```
localhost# show system info
info hostname localhost
info contact "Winston Smith (wsmith@company.com)"
info location "telephone case, 3rd floor"
localhost# show routing gateway ipv4
routing
 gateway
```

```
ipv4 192.168.10.1  
exit
```

```
exit
```

Description

The following information is shown:

| Parameter | Description |
|----------------------|--|
| info hostname | Displays the configured hostname. |
| info contact | Displays the configured contact. |
| info location | Displays the configured device location. |
| routing gateway ipv4 | Shows the IPv4 default gateway. |

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 Restarting and shutting down the device

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

Note

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

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.

To restart the device, do the following:

| Step | Instruction | Command |
|------|---|-----------------------------|
| 1 | Restart the device. | <code>system restart</code> |
| 2 | Respond to the security prompt. To cancel the restart, answer the security prompt with <code>no</code> . | <code>yes</code> |

Example

```
localhost# system restart
Are you sure you want to restart the device? [no,yes] yes
```

5.1.3 Shutting down the device

Note

If you shut down the device while it is connected to a SCALANCE LPE, the SCALANCE LPE is not shut down. The SCALANCE LPE is still supplied with voltage, but can only be reached via its serial interface.

Note

If you shut down the device with this command, you can only put the device back into operation on site by disconnecting and reconnecting the power supply (cold restart).

Remote access to the device is not possible.

Note

If the device shuts down while you commit configuration changes, check the configuration changes as soon as the device can be reached again.

To shut down the unit, do the following:

| Step | Instruction | Command |
|------|---|------------------------------|
| 1 | Shut down the unit. | <code>system shutdown</code> |
| 2 | Respond to the security prompt. If you respond to the prompt with <code>yes</code> , the device switches off. The device is permanently switched off. To cancel the shutdown, answer the security prompt with <code>no</code> . | <code>yes</code> |

Example

```
localhost# system shutdown
Are you sure you want to shut down the device? [no,yes] yes
```

5.2 Resetting the device to default settings

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.

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 users
- 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, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Reset the device to its default settings. | <code>system restore-defaults factory</code> |
| 2 | Respond to the security prompt. To cancel the reset to default settings, answer the security prompt with <code>no</code> . | <code>yes</code> |

Example

```
localhost# system restore-defaults factory
Are you sure you want to restore factory defaults and reboot? The
configuration will be lost. [no,yes] yes
```

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 Product 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 126)".
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 129)".
3. Shut down the device.
For more information, refer to "Shutting down the device (Page 122)".

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 (<https://support.industry.siemens.com/cs/search?t=all&search=%22SCALANCE%20XRM-300%22%2C%20%22SCALANCE%20XCM-300%22&type=Download&lc=en-DE>).

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, execute the following command in operating mode:
`show system firmware versions`

Example

```
localhost# show system firmware versions
SOFTWARE                VERSION                DATE
-----
Running SINEC OS Firmware  V02.00.00.00         2021-06-01_00:00:00
Backup SINEC OS Firmware   V02.00.00.00         2021-06-01_00:00:00
```

| | | |
|-----------------------|--------------|---------------------|
| Running after Restart | V02.00.00.00 | 2021-06-01_00:00:00 |
| Bootloader | V02.00.00.00 | 2021-06-01_00:00:00 |

Description

The following information is shown:

| Parameter | Description |
|-----------|---|
| SOFTWARE | <p>Software components available on the device</p> <p>Possible values include:</p> <ul style="list-style-type: none"> Running SINEC OS Firmware - Firmware version that is active on the device Backup SINEC OS Firmware - Firmware version that is inactive on the device Running after Restart Firmware version that is active after the next device restart Bootloader - The version of the bootloader running on the device |
| VERSION | Installed version of the firmware or bootloader |
| DATE | <p>Date and time at which the firmware or bootloader was successfully created</p> <p>The data displayed does not relate to the time at which the firmware or boot loader was loaded to the device.</p> |

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/search?search=%22SINEC%20OS%22&type=Download&lc=en-DE>)). Alternatively, you can also request firmware packages from the Siemens customer service.

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

- 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
- 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.
- Extract the contents of the compressed file and make sure the content is not changed.
- Depending on the firmware version, you are either performing a firmware upgrade or downgrade.
For the further procedure, see "Upgrading the firmware (Page 127)" or "Downgrading the firmware (Page 129)".

5.4.4 Upgrading the firmware

Requirements

- You have configured a server accordingly.

Note

Configuration hazard - risk of connection loss

While SINEC OS is downloading a firmware file from a remote server, there are pauses in the file transfer during which SINEC OS processes parts of the received firmware file in the background.

To prevent interruptions in the transmission of firmware files, you can set a timeout on the remote server.

If your remote server supports timeout configuration, set a value of at least two minutes.

- The firmware file (.sfw) is located on the server.
- There is a network 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

Operating risk - Danger of damage to property

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.

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

| Step | Instruction | Command |
|------|--|--|
| 1 | Make sure the documentation is valid for the version currently installed on your device. | <code>show system firmware</code> |
| 2 | Obtain the desired firmware package. For more information, refer to "Obtaining a firmware package (Page 126)". Note the requirements and restrictions that were published for this firmware version. | - |
| 3 | Load the firmware file. For more information on the URL, see "Specifying a URL (Page 67)". | <code>system firmware update source { URL }</code> |
| 4 | Respond to the security prompt. The firmware is loaded. | <code>yes</code> |

| Step | Instruction | Command |
|------|--|-----------------------------------|
| 5 | To activate the updated firmware, restart the device. 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 131)". The updated firmware is also activated during a cold restart (due to a loss of power). There is no confirmation prompt. | <code>system restart</code> |
| 6 | Respond to the security prompt. The device restarts with the updated firmware. To cancel the restart, answer the security prompt with <code>no</code> . When you have restarted the device, you can activate the backup firmware. For more information, refer to "Activating the backup firmware (Page 131)". | <code>yes</code> |
| 7 | [Optional] Call up the CLI and log in. For more information, refer to "Calling the CLI (Page 111)" and "Logging in to a configured device (Page 115)". | - |
| 8 | [Optional] Verify the firmware version. | <code>show system firmware</code> |

Example

The firmware is loaded from a TFTP server in this example.

```
localhost# system firmware update source tftp://192.168.1.1/sinec-
os_V02.00.00.00.sfw
The backup firmware will be discarded and updated with the new
firmware. Are you sure you want to continue? [yes,no] yes
Preparing update... done
Transferring file... done
Waiting for the update being applied... done
.
.
.
localhost# system restart
Are you sure you want to restart the device? [no,yes] yes
.
.
.
login as: admin
admin@192.168.16.15's password: *****
Welcome to the SINEC OS Command Line Interface
Copyright (c) 2019 Siemens AG
admin connected from 192.168.16.1 using ssh on localhost
localhost#
```


5.4.5 Downgrading the firmware

Requirements

- You have configured a server accordingly.

Note

Configuration hazard - risk of connection loss

While SINEC OS is downloading a firmware file from a remote server, there are pauses in the file transfer during which SINEC OS processes parts of the received firmware file in the background.

To prevent interruptions in the transmission of firmware files, you can set a timeout on the remote server.

If your remote server supports timeout configuration, set a value of at least two minutes.

- The firmware file (.sfw) is located on the server.
- There is a network 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

Operating risk - Danger of damage to property

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.

To load an older firmware file into the device, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Make sure the documentation is valid for the version currently installed on your device. | <code>show system firmware</code> |
| 2 | Obtain the desired firmware package. For more information, refer to "Obtaining a firmware package (Page 126)". Note the requirements and restrictions that were published for this firmware version. | - |
| 3 | Load the firmware file. For more information on the URL, see "Specifying a URL (Page 67)". | <code>system firmware update source { URL }</code> |
| 4 | Respond to the security prompt. The firmware is loaded. | <code>yes</code> |

| Step | Instruction | Command |
|------|---|--|
| 5 | Reset the device to its default settings. The device restarts when it is reset to default settings. The updated firmware is activated. 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 131)". | <code>system restore-defaults factory</code> |
| 6 | Respond to the security prompt. The device restarts with the updated firmware and default settings. When you have restarted the device, you can activate the backup firmware. For more information, refer to "Activating the backup firmware (Page 131)". | <code>yes</code> |
| 7 | [Optional] Call up the CLI and log in. For more information, refer to "Calling the CLI (Page 111)" and "Logging in to a device with default settings (Page 113)". | <code>-</code> |
| 8 | [Optional] Verify the firmware version. | <code>show system firmware</code> |

Example

The firmware is loaded from a TFTP server in this example.

```
localhost# system firmware update source tftp://192.168.1.1/sinec-os_V02.00.00.00.sfw
```

```
The backup firmware will be discarded and updated with the new
firmware. Are you sure you want to continue? [yes,no] yes
```

```
Preparing update... done
```

```
Transferring file... done
```

```
Waiting for the update being applied... done
```

```
localhost# system restore-defaults factory
```

```
Are you sure you want to restore factory defaults and restart? The
configuration will be lost. [no,yes] yes
```

```
.
```

```
.
```

```
.
```

```
login as: admin
```

```
admin@192.168.16.15's password: admin
```

```
Welcome to the SINEC OS Command Line Interface
```

```
Copyright (c) 2019 Siemens AG
```

```
admin connected from 192.168.16.1 using ssh on localhost
```

```
The default password must be changed before access to the device is
granted.
```

```
Enter the new password: *****
```

```
Confirm the new password: *****
```

```
The default password has been changed.
```

```
To apply the changes, you will be logged out automatically in a few
seconds.
```

```
.
```

```

.
.
localhost#

```

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.

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:

| Step | Instruction | Command |
|------|---|--------------------------------------|
| 1 | Reject the firmware file. | <code>system firmware decline</code> |
| 2 | Respond to the security prompt. The previously firmware used remains active. | <code>yes</code> |

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.

To activate the backup firmware, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Activate the backup firmware. The associated configuration database is restored together with the backup firmware. | <code>system firmware rollback</code> |
| 2 | Respond to the security prompt. The backup firmware is activated. | <code>yes</code> |
| 3 | Restart the device. | <code>system restart</code> |
| 4 | Respond to the security prompt. The device restarts with the backup firmware and the associated configuration database. To cancel the restart, answer the security prompt with <code>no</code> . | <code>yes</code> |
| 5 | [Optional] Call up the CLI and log in. For more information, refer to "Calling the CLI (Page 111)" and "Logging in to a configured device (Page 115)". | - |
| 6 | [Optional] Verify the firmware version to ensure the previously inactive firmware version (Backup Firmware) is now active (Running Firmware). | <code>show system firmware versions</code> |

Example

```
localhost# system firmware rollback
Are you sure you want to switch to the backup firmware release?
[yes,no] yes
localhost# system restart
Are you sure you want to restart the device? [no,yes] yes
.
.
.
login as: admin
admin@192.168.16.15's password: *****

Welcome to the SINEC OS Command Line Interface
Copyright (c) 2019 Siemens AG

admin connected from 192.168.16.1 using ssh on localhost
localhost# show system firmware versions
```

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, execute the following command in operational mode:

```
show system hardware component
```

Example

```
localhost# show system hardware component | notab
hardware component "{ Product Name }"
  class          chassis
  description    "Family: { Product Family }"
  hardware-rev  1
  serial-num     { Serial Number }
  state oper-state enabled
  article-num    "{ Order Number }"
.
.
.
hardware component SELECT/SET
  class          button
  parent         CPU
  hardware-rev  0
  state oper-state enabled
hardware component "SIGNALING CONTACT"
  class          relay
  parent         CPU
  hardware-rev  0
  state oper-state enabled
  state status  CLOSE
.
.
.
```

Description

The following information is displayed when applicable:

| Parameter | Description |
|------------------|--|
| class | The type of component. |
| description | A description of the component. |
| parent | The parent component. |
| state oper-state | The operational state of the component. Possible values include: <ul style="list-style-type: none"> enabled - The component is operational disabled - The component has been disabled unknown - The status of the component cannot be determined |

| Parameter | Description |
|--------------|--|
| state status | Additional information about the current state of the component. Possible values may include: <ul style="list-style-type: none"> • OFF - The component is off • ON - The component is on • OPEN - The component is open. Applies to relay components. • CLOSE - The component is closed. Applies to relay components. • { color } - The color of the component. Applies to LED components. |
| hardware-rev | The hardware revision. |
| serial-num | The hardware serial number. |
| article-num | The article (or order) number. |

5.5.2 Displaying the Last Time the Hardware Information Was Changed

To display the time when the hardware information of the device was last changed (e.g. a component was added/removed, the state of an LED changed, etc.), execute the following command in operational mode:

```
show system hardware last-change
```

Note

If a time source is not configured, the time and date will default to the system time (1970-01-01T00:00:53-00:00).

Example

```
localhost# show system hardware last-change
hardware last-change 1970-01-01T00:00:53-00:00
```

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).

In modular devices, the configuration can only be loaded successfully into a device whose hardware configuration (interfaces) corresponds to what is saved in the configuration file. When a configuration file is loaded, the entire interface configuration is overwritten and may not correspond to the existing hardware otherwise.

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.
- In modular devices, pay attention to a suitable hardware configuration (interfaces).

5.6.1 Saving the current configuration as a file on a remote server

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.

Note

Save the current configuration as a file on an SFTP server

During the initial connection setup to an SFTP server, the device must save the fingerprint of the public key in the truststore.

When saving a configuration file is the first time a connection is set up to an SFTP server, the fingerprint of the SFTP server is saved as well. However, the device only saves the fingerprint after the configuration file has already been saved.

The fingerprint of the SFTP server is not included in the saved configuration file.

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

| Step | Instruction | Command |
|------|---|---------------------|
| 1 | Change to the shared configuration mode. For more information, refer to section "General commands in operational mode (Page 46)". | <code>config</code> |
| 2 | Make sure that no other user has enabled the exclusive configuration. For more information, refer to section "Displaying active users (Page 174)". | <code>do who</code> |

| Step | Instruction | Command |
|------|--|--|
| 3 | <p>Save the configuration to a file in XML format. For more information on the URL, see "Specifying a URL (Page 67)".</p> <p>Only execute this command when you are in the shared configuration mode.</p> <p>[Optional] When you use the <code>protected</code> parameter, 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.</p> | <pre>system configuration save format xml target { URL } protected</pre> |
| 4 | <p>[Optional] When you use the <code>protected</code> parameter, assign a password.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Must be between 1 and 255 characters long • All standard characters are allowed, plus the following special characters: # \$ % & () * + , - . / : < = > @ [] ^ _ { } ~ | <pre>{ Password }</pre> |
| 5 | <p>[Optional] When you use the <code>protected</code> parameter, confirm the password.</p> <p>To enter a plain text password encrypted and not in plain text, press Enter after <code>password-confirm</code>. This will put you in Wizard mode.</p> | <pre>password-confirm { password }</pre> |
| 6 | <p>Respond to the security prompt.</p> <p>During the save operation, the device briefly changes to exclusive configuration mode. Other users in configuration mode receive a corresponding message at this time.</p> <p>Wait until the save operation is complete before making changes to the device configuration. When the command prompt is displayed again in the CLI, this indicates the operation is complete (default: <code>localhost (config) #</code>).</p> | <pre>yes</pre> |

Example

In this example, the configuration is saved in a file with the name `backup.xml` in XML format on a TFTP server. No checksum is added to the file.

```
localhost# config
Entering configuration mode terminal
localhost(config)# do who
Session User Context From Proto Date Mode
*126 admin cli 192.0.2.1 ssh 2020-03-25 config-terminal
localhost(config)# system configuration save format xml target
tftp://192.0.2.10/backup.xml
```



```
Are you sure you want to backup the current configuration? This may
take severel minutes. [no,yes] yes
Transferring file... done
localhost(config)#
```

Example

In this example, the configuration is saved in a file with the name `backup.xml` in XML format on a TFTP server in protected mode.

```
localhost# config
Entering configuration mode terminal
Current configuration users:
admin https (webui from 192.0.2.2) on since 2020-03-25 10:55:00
terminal mode
localhost(config)# do who
Session User Context From Proto Date Mode
188 admin webui 192.0.2.2 https 2020-03-25 config-terminal
*126 admin cli 192.0.2.1 ssh 2020-03-25 config-terminal
localhost(config)# system configuration save format xml target
tftp://192.0.2.10/backup.xml protected
Value for 'password' (<string, min: 0 chars, max: 255 chars>):
*****
Value for 'password-confirm' (<string, min: 0 chars, max: 255
chars>): *****
Are you sure you want to backup the current configuration? This may
take several minutes. [no,yes] yes
Transferring file... done
localhost(config)#
```

5.6.2 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.
- Plugged SFP transceivers correspond to what is saved in the configuration file.

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 123)".

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, do the following:

| Step | Instruction | Command |
|------|---|---------------------|
| 1 | Change to the shared configuration mode. For more information, refer to section "General commands in operational mode (Page 46)". | <code>config</code> |
| 2 | Make sure that no other user has enabled the exclusive configuration. For more information, refer to section "Displaying active users (Page 174)". | <code>do who</code> |

| Step | Instruction | Command |
|------|---|---|
| 3 | <p>Load a configuration file in XML format.</p> <p>For more information on the URL, see "Specifying a URL (Page 67)".</p> <p>Only execute this command when you are in the shared configuration mode.</p> <p>Wait until the load operation is complete before making changes to the configuration.</p> <p>When the command prompt is displayed again in the CLI, this indicates the operation is complete (default: <code>localhost(config)#</code>).</p> <p>Possible options for loading behavior:</p> <ul style="list-style-type: none"> • <code>merge</code> - 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. • <code>replace</code> - 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. <p>When the configuration was saved in protected mode, you must use the <code>protected</code> parameter and enter the associated password to load the configuration.</p> | <pre>system configuration load format xml mode [merge replace] source { URL } protected</pre> |
| 4 | [Optional] When you use the <code>protected</code> parameter, enter a password. | <code>{ Password }</code> |
| 5 | <p>Respond to the security prompt.</p> <p>During the load operation, the device briefly changes to exclusive configuration mode. Other users in configuration mode receive a corresponding message at this time.</p> | <code>yes</code> |
| 6 | <p>[Optional] If plugged SFP transceivers do not correspond to what is saved in the configuration file, pull and plug the deviating SFP transceivers or restart the device.</p> <p>For more information, refer to section "Restarting the device (Page 122)".</p> | <code>-</code> |

Basic configuration and configuration file for examples

The following basic configuration is assumed for the examples:

- The following users are configured:

- **Admin1** user
- **Guest1** user

The following VLANs are configured:

- VLAN 1
- VLAN 2

The `backup.xml` configuration file contains the following configuration:

- **Maint** user
- **User1** user

Example

In this example, the configuration file `backup.xml` with the load behavior `merge` is loaded.

First, the basic configuration is checked.

```
localhost# show running-config switch vlan
```

```
switch
vlan 1
.
.
.
exit
```

```
vlan 2
.
.
.
exit
```

```
exit
```

```
localhost# show running-config system authentication user
```

```
system
authentication
user Admin1
.
.
.
exit
```

```
user Guest1
.
.
.
exit
```

```
exit
```

```
exit
```

Then, the configuration file `backup.xml` with the load behavior `merge` is loaded.

```
localhost# config
Entering configuration mode terminal
localhost(config)# do who
Session User Context From Proto Date Mode
*126 admin cli 192.0.2.1 ssh 2020-03-25 config-terminal
localhost(config)# system configuration load format xml mode merge
source tftp://192.0.2.10/backup.xml
Are you sure you want to load the configuration file? This action
will take several minutes to complete and will modify the current
running system configuration. [no,yes] yes
Transferring file... done
localhost(config)#
```

Next, the new configuration is checked as compared to the basic configuration.

```
localhost# show running-config switch vlan
switch
vlan 1
.
.
.
exit

vlan 2
.
.
.
exit

exit
```

```
localhost# show running-config system authentication user
system
authentication
user Admin1
.
.
.
exit

user Guest1
.
.
.
exit

user Maint
.
.
```

```
.
exit

user User1
.
.
exit

exit

exit
```

Example

In this example, the configuration file `backup.xml` with the load behavior `replace` is loaded.

First, the basic configuration is checked.

```
localhost# show running-config switch vlan
switch
vlan 1
.
.
.
exit

vlan 2
.
.
.
exit

exit

localhost# show running-config system authentication user
system
authentication
user Admin1
.
.
.
exit

user Guest1
.
.
.
exit

exit

exit
```

Then, the configuration file `backup.xml` with the load behavior `replace` is loaded.

```
localhost# config
Entering configuration mode terminal
localhost(config)# do who
Session User Context From Proto Date Mode
*126 admin cli 192.0.2.1 ssh 2020-03-25 config-terminal
localhost(config)# system configuration load format xml mode
replace source tftp://192.0.2.10/backup.xml
Are you sure you want to load the configuration file? This action
will take several minutes to complete and will modify the current
running system configuration. [no,yes] yes
Transferring file... done
localhost(config)#
```

Next, the new configuration is checked as compared to the basic configuration.

```
localhost# show running-config switch vlan
switch
vlan 1
.
.
.
exit

vlan 2
.
.
.
exit

exit

localhost# show running-config system authentication user
system
authentication
user Maint
.
.
.
exit

user User1
.
.
.
exit

exit

exit
```

Example

In this example, the configuration file `backup.xml` is loaded with the load behavior `replace` and a password.

```
localhost# config
Entering configuration mode terminal
localhost(config)# do who
Session User Context From Proto Date Mode
*126 admin cli 192.0.2.1 ssh 2020-03-25 config-terminal
localhost(config)# system configuration load format xml mode
replace source tftp://192.0.2.10/backup.xml protected
Value for 'password' (<string, min: 0 chars, max: 255 chars>):
*****
Are you sure you want to load the configuration file? This action
will take several minutes to complete and will modify the current
running system configuration. [no,yes] yes
Transferring file... done
localhost(config)#
```

5.6.3 Displaying the header information of a configuration file

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

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Call the header information of a configuration file. For more information on the URL, see "Specifying a URL (Page 67)". When the configuration was saved in protected mode, you must use the <code>protected</code> parameter and enter the associated password to load the configuration. | <code>system configuration view-info format xml source { URL } protected</code> |
| 3 | [Optional] When you use the <code>protected</code> parameter, enter a password. | <code>{ Password }</code> |

Example

In this example, the header information of the configuration file with the name `backup.xml` is displayed. No checksum has been added to the file.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system configuration view-info source tftp://
192.168.200.10/backup.xml
Transferring file... done
backup-time 2020-03-25T09:00:00+00:00
backup-by admin
device-type SCALANCE XCM332
serial-number VPM6002848
article-number 6GK5 332-0GA01-2AC2
hw-revision 1
```



```
firmware-version V02.00.00.00
hostname localhost
localhost(config)#
```

Example

In this example, the header information of the configuration file with the name `backup.xml` is displayed. A checksum has been added to the file.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system configuration view-info source tftp://
192.168.200.10/backup.xml protected
Value for 'password' (<string, min: 0 chars, max: 255 chars>):
*****
Transferring file... done
backup-time 2020-03-25T09:00:00+00:00
backup-by admin
device-type SCALANCE XCM332
serial-number VPM6002848
article-number 6GK5 332-0GA01-2AC2
hw-revision 1
firmware-version V02.00.00.00
hostname localhost
checksum cf2ed44c50d8c3ecac2...
localhost(config)#
```

Description

The following information is shown:

| Parameter | Description |
|-------------------------------|---|
| <code>backup-time</code> | Date and time at which the configuration file was saved |
| <code>backup-by</code> | User who saved the configuration file |
| <code>device-type</code> | Device name |
| <code>serial-number</code> | Serial number of the hardware |
| <code>article-number</code> | Article number (order number) |
| <code>hw-revision</code> | Hardware version |
| <code>firmware-version</code> | Firmware version that is active on the device |
| <code>hostname</code> | Configured hostname |
| <code>checksum</code> | 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 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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Save and transfer the file with OSS information. For more information on the URL, see "Specifying a URL (Page 67)". | <code>system service oss-info save target { URL }</code> |
| 2 | Respond to the security prompt. | <code>yes</code> |

Example

In this example, the OSS information with the name `oss-info.pdf` is saved on a TFTP server.

```
localhost# system service oss-info save target tftp://192.168.1.1/
oss-info.pdf
Uploading the OSS license documents may take several minutes
depending on the available bandwidth. Do you wish to continue?
[no,yes] yes
Transferring file... done
```

5.8 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

5.8.1 Setting the signaling contact mode

To define the signaling contact mode, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the signaling contact mode. Options include: <ul style="list-style-type: none"> • <code>event-driven</code> - The signaling contact is controlled by alarms that are configured to open or close the relay when a specific event occurs • <code>open</code> - The signaling contact is always open • <code>closed</code> - The signaling contact is always closed Default: <code>event-driven</code> | <code>system signaling-contact mode</code> <code>[event-driven open closed]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system signaling-contact mode</code> <code>or</code> <code>show running-config system signaling-contact details</code> |

Example

```
localhost# config
localhost(config)# system signaling-contact mode event-driven
localhost(config-system-signaling-contact)# commit
Commit complete.
localhost(config-system-signaling-contact)# end
localhost# show running-config system signaling-contact mode
system
  signaling-contact
    mode event-driven
  exit

exit
localhost# show running-config system signaling-contact | details
system
  signaling-contact
    mode event-driven
  exit

exit
```

5.8.2 Displaying the current signaling contact state

To display the current state of the signaling contact, enter the following command:

```
show system hardware component FAULT
```

Example

```
localhost# show system hardware component FAULT
hardware component FAULT
  class relay
  parent CPU
  state oper-state enabled
  state status CLOSE
```

Description

Possible values for `state status` include:

- OPEN - The signaling contact is currently open
- CLOSE - The signaling contact is currently closed

5.9 Button function

The functions of the button and the associated configuration option are described in greater detail in this section.

5.9.1 Understanding the button functions

The device has a button with the following functions:

- **Reset the device to default settings**
You can reset the device to its default settings using the button.
Note that the button function distinguishes between the startup phase and running operation. To be able to use the button during operation, the **Reset to default settings** button function must be enabled. The button function is always active in the startup phase. You will find more information on the button in the Product Manual for the device.
- **Load a firmware file via TFTP**
You can switch to rescue mode with the button and load a firmware file into the device via TFTP.
For more information, refer to "The device cannot be reached via CLI and Web UI (loading a firmware file via TFTP) (Page 689)".
- **Change 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. You will find more information on the display modes and LEDs in the Product Manual for the device.

5.9.2 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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the Reset to default settings button function. | <code>system device-panel button-capabilities restore-factory-defaults</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system device-panel button-capabilities restore-factory-defaults</code> |

Example

```
localhost# config
localhost(config)# system device-panel button-capabilities restore-
factory-defaults
localhost(config-system)# commit
Commit complete.
localhost(config-system)# end
localhost# show running-config system device-panel button-
capabilities restore-factory-defaults
system
  device-panel button-capabilities restore-factory-defaults
exit
```

5.10 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

5.10.1 Understanding the CLP

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

5.10.1.1 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 151)".

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.

5.10.1.2 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 and firmware of the device are 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).

5.10.1.3 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. Take note of exceptions due to the encryption method (Page 152).

5.10.1.4 Encryption methods

As of SINEC OS firmware version 2.4, the CLP is encrypted with a different encryption method.

If you plug a CLP with an older encryption method into a device with a firmware version ≥ 2.4 , the new encryption method is automatically applied during the startup phase. The same happens with a plugged CLP during a firmware update to a version ≥ 2.4 . All data stored on the CLP are retained.

Devices with a firmware version ≤ 2.3 cannot read a CLP that was written by a device with a firmware version ≥ 2.4 .

You cannot use a CLP with a configuration and firmware version ≥ 2.4 to transfer this data to a device with a firmware version ≤ 2.3 . A device with older firmware cannot decrypt the CLP and starts with the configuration and firmware from its internal memory. The CLP has the `not-accepted` status.

To be able to use a CLP with new encryption method in a device with older firmware, you have the following options:

- After a CLP is plugged (`not-accepted` status): Reset the CLP to default settings. All saved data of the CLP, including licenses, is deleted. For more information, refer to "Resetting the CLP (Page 155)".
- Load a firmware version ≥ 2.4 before you plug a CLP with the new encryption method.

5.10.1.5 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.

5.10.1.6 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. |
| EventCPlugPluggedIn | Info | CLP plugged in 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. |
| EventCPlugInvalidContent | Notice | Unexpected file content on CLP detected. |

5.10.2 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:

| Step | Instruction | Command |
|------|---|-----------------------------------|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Save the current firmware of the device to the CLP. | <code>clp firmware-on-plug</code> |

| Step | Instruction | Command |
|------|---------------------------|--|
| 3 | Commit the changes. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config clp firmware-on-plug |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# clp firmware-on-plug
localhost(config-clp)# commit
Commit complete.
localhost(config-clp)# end
localhost# show running-config clp firmware-on-plug
clp
  firmware-on-plug
exit
```

5.10.3 Saving the device configuration on the CLP

Use this command to delete all saved data from the CLP and save the current device configuration.

To save the current device configuration to the CLP, execute the following command in operational mode:

```
clp write
```

Example

```
localhost# clp write
Are you sure you want to format and write to the CLP? [no,yes] yes
localhost#
```

5.10.4 Deleting data on the CLP

Use this command to delete all saved data from the CLP, apart from the saved licenses.

To delete the data from the CLP, execute the following command in operational mode:

```
clp clean
```

Example

```
localhost# clp clean
Are you sure you want to erase the contents of the CLP, with the
exception of key licenses? [no,yes] yes
localhost#
```

5.10.5 Resetting the CLP

Use this command to delete all stored data on the CLP, including licenses, and reset it 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 data on the CLP (Page 154)" and "Resetting the device to default settings (Page 123)".

To reset the CLP to default settings, execute the following command in operational mode:

```
clp factoryclean
```

Example

```
localhost# clp factoryclean
Are you sure you want to perform a factory reset on the CLP?
[no,yes] yes
localhost#
```

5.10.6 Showing the status of the CLP

To display the status of CLP, execute the following command in operational mode:

```
show clp
```

Example

```
localhost# show clp

CLP Configuration State:      accepted
Device Group:                 "{ Product line }"
Device Type:                  "{ Device type }"
Config Revision:              1
Filesystem:                   fs-ext4
Filesystem Size MB:           918
Filesystem Usage MB:          7
Info String:                   "{ Article number }"
                               HW 01
                               SW V02.03.00.00

CLP License State:            not-present
Order ID:                      -
Serial Number:                 -
Info String:                   -

FW on CLP State:              enabled
Status:                         fw-present
```

Description

The following information is shown:

| Parameter | Description |
|-------------------------|--|
| CLP Configuration State | Shows the status of the CLP. Possible values: <ul style="list-style-type: none"> 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. empty - The data of a CLP was deleted with the <code>clp clean</code> command. |
| 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. |
| Config Revision | Shows the output state of the configuration that exists on the CLP. |
| 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. |
| 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 <code>not-accepted</code> status, further information on the cause of the problem is displayed. |
| CLP License State | Shows only one value in the current version: <code>not-present</code> A CLP without licenses is plugged into the device. |
| Order ID | Not relevant in the current version (-). |
| Serial Number | |
| Info String | |
| FW on CLP State | If the function is enabled (<code>enabled</code>), the firmware is stored on the CLP. |
| Status | Shows whether firmware is stored on the CLP (<code>fw-present</code>) or not (<code>fw-not-present</code>). |

System administration

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

6.1 Configuring a banner for login

You can display a user-defined greeting message, device information or other information with the login prompt of the CLI.

Only users with the `admin` user profile can configure a banner.

To configure a banner, follow these steps:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure a user-specific banner. If the string contains spaces, they must either be placed in quotation marks (") or you can press the Enter key after <code>banner</code> to open wizard mode. Condition: <ul style="list-style-type: none"> Must be between 1 and 12800 characters long | <code>system banner "{ banner text }"</code> <code>system banner</code> <code>(<string>):</code> <code>[Multiline mode, exit with ctrl-D.]</code> <code>> { banner text }</code> |
| 3 | [Optional] Exit wizard mode. | <code>[Ctrl] + [D]</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |

Example

A banner with security information is configured in this example.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system banner
(<string>):
[Multiline mode, exit with ctrl-D.]
> #####
> #           # #   #####   # #   #####   #
> #           # # #   #   #   #   #
> #           ##### #   ###   ###   #
> #           #   # #   #   #   #
> #           #   # ##### ##### #   #
> #
> # You are entering into a secured area! Your IP, Login Time, #
> # Username has been noted and has been sent to the server #
> # administrator! #
> # This service is restricted to authorized users only. All #
```

```

> #                 activities on this system are logged.                 #
> #  Unauthorized access will be fully investigated and reported  #
> #                 to the appropriate law enforcement agencies.      #
> #####
>
localhost(config-system)# commit
Commit complete.
localhost(config-system)# end
localhost# exit
login as: admin
Pre-authentication banner message from server:
| #####
| #                 # #       #### ### #####                        #
| #                 # # #     #   # #   #                           #
| #                 ##### #    ### ###   #                          #
| #                 #   # #    #   # #   #                           #
| #                 #   # ##### ##### #   #                         #
| #
| #  You are entering into a secured area! Your IP, Login Time,      #
| #  Username has been noted and has been sent to the server         #
| #                          administrator!                           #
| #  This service is restricted to authorized users only. All        #
| #  activities on this system are logged.                            #
| #  Unauthorized access will be fully investigated and reported     #
| #  to the appropriate law enforcement agencies.                      #
| #####
End of banner message from server
admin@192.168.16.34's password: *****

```

6.2 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.

6.2.1 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 159)".
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 160)".
3. [Optional] Configure that a password must include at least one number.
For more information, refer to "Configuring the condition for numbers (Page 161)".
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 161)".
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 162)".
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 163)".
7. Enable the password policy.
For more information, refer to "Enabling the password policy (Page 163)".

6.2.1.1 Configuring the minimum number of characters

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

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the minimum number of characters that must be included in a password. Default: 8 | <code>system authentication password-policy min-length { 1 - 255 }</code> |
| 3 | Commit the changes. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system authentication password-policy min-length</code> |

Example

In this example, you define that a password must include at least 10 characters.

```
localhost# config
localhost(config)# system authentication password-policy min-length
10
localhost(config-password-policy)# commit
Commit complete.
localhost(config-password-policy)# end
localhost# show running-config system authentication password-
policy min-length
system
```

6.2 Password policy

```

authentication
 password-policy
  min-length 10
 exit

exit

exit

```

6.2.1.2 Configuring the maximum number of characters

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

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the maximum number of characters that may be included in a password. Default: 255 The value range starts at 4 to prevent invalid password policies when all conditions are enabled: <ul style="list-style-type: none"> • At least 1 number • At least 1 lowercase letter • At least 1 uppercase letter • At least 1 special character | <code>system authentication password-policy max-length { 4 - 255 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system authentication password-policy max-length</code> |

Example

In this example, you define that a password may include up to 200 characters.

```

localhost# config
localhost(config)# system authentication password-policy max-length
200
localhost(config-password-policy)# commit
Commit complete.
localhost(config-password-policy)# end
localhost# show running-config system authentication password-
policy max-length
system
 authentication
  password-policy
    max-length 200
 exit

exit

```



```
exit
```

6.2.1.3 Configuring the condition for numbers

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

To configure that a password must include at least one number, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Configure that a password must include at least one number. | system authentication password-policy number |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system authentication password-policy number |

Example

In this example, you define that a password is not required to include a number.

```
localhost# config
localhost(config)# no system authentication password-policy number
localhost(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config system authentication password-
policy number
system
 authentication
  password-policy
    no number
  exit
exit
exit
```

6.2.1.4 Configuring the condition for lowercase letters

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

To configure that a password must include at least one lowercase letter, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Configure that a password must include at least one lowercase letter. | system authentication password-policy lowercase |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------|---|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system authentication password-policy lowercase |

Example

In this example, you define that a password must include at least one lowercase letter.

```
localhost# config
localhost(config)# system authentication password-policy lowercase
localhost(config-password-policy)# commit
Commit complete.
localhost(config-password-policy)# end
localhost# show running-config system authentication password-
policy lowercase
system
 authentication
  password-policy
   lowercase
  exit

exit

exit
```

6.2.1.5 Configuring the condition for uppercase letters

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

To configure that a password must include at least one uppercase letter, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Configure that a password must include at least one uppercase letter. | system authentication password-policy uppercase |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system authentication password-policy uppercase |

Example

In this example, you define that a password must include at least one uppercase letter.

```
localhost# config
localhost(config)# system authentication password-policy uppercase
localhost(config-password-policy)# commit
Commit complete.
localhost(config-password-policy)# end
localhost# show running-config system authentication password-
policy uppercase
```

```

system
 authentication
  password-policy
   uppercase
  exit

exit

exit

```

6.2.1.6 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 that a password must include at least one special character, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Configure that a password must include at least one special character. | system authentication password-policy special |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system authentication password-policy special |

Example

In this example, you define that a password must include at least one special character.

```

localhost# config
localhost(config)# system authentication password-policy special
localhost(config-password-policy)# commit
Commit complete.
localhost(config-password-policy)# end
localhost# show running-config system authentication password-
policy special
system
 authentication
  password-policy
   special
  exit

exit

exit

```

6.2.1.7 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:

| Step | Instruction | Command |
|------|-----------------------------|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the password policy. | <code>system authentication password-policy enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system authentication password-policy enabled</code> |

Example

```
localhost# config
localhost(config)# system authentication password-policy enabled
localhost(config-password-policy)# commit
Commit complete.
localhost(config-password-policy)# end
localhost# show running-config system authentication password-policy enabled
system
 authentication
  password-policy
    enabled
  exit
exit
exit
```

6.2.2 Displaying the password policy

You can show which conditions are active for the password policy.

To display the active password policy, execute the following command in operational mode:
`show running-config system authentication password-policy | details`

Example

```
localhost# show running-config system authentication password-policy | details
system
 authentication
  password-policy
    enabled
    min-length 10
    max-length 200
    no number
    lowercase
```

```

    uppercase
    special
    exit

```

```

exit

```

```

exit

```

Description

The following information is shown:

| Parameter | Description |
|------------|--|
| enabled | Specifies whether the password policy is enabled. When the password policy is disabled (<code>no enabled</code>), the only condition is that a password must contain at least one character. Other configured conditions do not need to be met. |
| min-length | Specifies the minimum number of characters in a password. |
| max-length | Specifies the maximum number of characters in a password. |
| number | Specifies whether numbers must be used. |
| lowercase | Specifies whether lowercase letters must be used. |
| uppercase | Specifies whether uppercase letters must be used. |
| special | Specifies whether special characters must be used. |

6.3 User administration

This section describes the creation and management of users.

6.3.1 Understanding user management

This section describes special features of user management.

6.3.1.1 User profiles

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 37)".

6.3.1.2 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**.

6.3.1.3 Deleting a user

NOTICE

Security hazard - Risk of unauthorized access and/or misuse

When you delete a user, existing CLI, Web UI and NETCONF sessions of the affected user are not automatically terminated. Sessions that were opened before the user is deleted are retained.

Users with malicious intent can exploit this.

To prevent unauthorized access and/or misuse, check open sessions and terminate sessions of deleted users.

To delete a user, follow these steps:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Delete the user. | <code>no system authentication user { user name }</code> |
| 3 | Commit the changes. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Check which users are currently logged into the device. For more information, refer to "Displaying active users (Page 174)". | <code>who</code> |
| 6 | Close the sessions of the deleted user. For more information, refer to "Logging off a user (Page 175)". | <code>admin logout [session { session ID } user { user name }]</code> |

Example

In this example, the user `guest` is deleted and this user's open CLI session is closed.

```

localhost# config
Entering configuration mode terminal
localhost(config)# no system authentication user user1
localhost(config)# commit
Commit complete.
localhost(config)# end
localhost# who
Session User Context From Proto Date Mode
-----
180 guest cli 192.0.2.10 ssh 01:45:32 operational
179 admin webui 192.0.2.1 https 01:44:59 config-terminal
*75 admin cli 192.0.2.1 ssh 1970-01-01 operational
localhost# admin logout user guest

```

6.3.2 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 167)".

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 169)".
3. [Optional] Change the password of a user.
For more information, refer to "Changing the password of a user (Page 171)".
4. [Optional] Change the user profile of a user.
For more information, refer to "Changing the user profile of a user (Page 173)".

6.3.2.1 Configuring a new user

Only users with the `admin` user profile can configure a new user.

To create a new user, follow these steps:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define a new user. Conditions: <ul style="list-style-type: none"> • Must be unique • Must be between 1 and 250 characters long • All standard characters are allowed, plus the following special characters: _ - | <code>system authentication user { user name }</code> |
| 3 | Assign a password for the user. You can enter a password as follows: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – \$5\$ (SHA-256) – \$6\$ (SHA-512) • As plain text password If a password begins with a character combination other than \$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 viewed as a plain text password. Use this combination of characters if you want to configure a password that begins with the character \$. Example: \$0\$\$iemens123 To enter a plain text password encrypted and not in plain text, press Enter after <code>password</code>. This will put you in Wizard mode. By default, a password must fulfill the following conditions: <ul style="list-style-type: none"> • 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 164)". | <code>password { password }</code> |

| Step | Instruction | Command |
|------|--|---|
| 4 | Confirm the password. To enter a plain text password encrypted and not in plain text, press Enter after <code>password-confirm</code> . This will put you in Wizard mode. | <code>password-confirm { password }</code> |
| 5 | Assign the user a user profile. Options include: <ul style="list-style-type: none"> <code>admin</code> - Users with the <code>admin</code> user profile have read and write access to the device functions. <code>guest</code> - Users with the <code>guest</code> user profile have read access to the device functions and can change their own password. | <code>role [admin guest]</code> |
| 6 | Commit the changes. | <code>commit</code> |
| 7 | Exit configuration mode. | <code>end</code> |
| 8 | Verify the configuration. | <code>show running-config system authentication user { user name }</code> |

Example

In this example, a user is created with the user name `user1` and the user profile `guest`.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication user user1
localhost(config-user-user1)# password
(<string>): *****
localhost(config-user-user1)# password-confirm
(<string>): *****
localhost(config-user-user1)# role guest
localhost(config-user-user1)# commit
Commit complete.
localhost(config-user-user1)# end
localhost# show running-config system authentication user user1
system
 authentication
  user user1
    password          $6$NBrh127y0q2Zzjgx$Bg...
    password-confirm  $6$NBrh127y0q2Zzjgx$Bg...
    role              guest
  exit
exit
exit
```

6.3.2.2 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 apply the changes, the CLI session is closed automatically 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 apply the changes, the CLI session is closed automatically 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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable that a user needs to assign a new password. | <code>system authentication user { user name } change-of-password-required</code> |
| 3 | Commit the changes. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system authentication user { user name } change-of-password-required</code> |

Example

In this example, the function is enabled for the existing user `user1`.

```
localhost# config
Entering configuration mode terminal
```

```
localhost(config)# system authentication user user1 change-of-  
password-required  
localhost(config-user-user1)# Warning: change-of-password-required  
was changed. When the change is committed, active session(s) of the  
*affected user* will be terminated.  
localhost(config-user-user1)#                If you don't wish to  
proceed, use the 'abort' command to cancel the transaction.  
localhost(config-user-user1)# commit  
Commit complete.  
localhost(config-user-user1)# end  
localhost# show running-config system authentication user user1  
change-of-password-required  
system  
  authentication  
    user user1  
      change-of-password-required  
    exit  
  
exit  
  
exit
```

If the user `user1` has an active CLI session while the function is enabled, the following messages are output:

```
login as: user1  
user1@192.0.2.2's password:
```

```
Welcome to the SINEC OS Command Line Interface  
Copyright (c) 2019 Siemens AG
```

```
user1 connected from 192.0.2.2 using ssh on switch02  
switch02# ...  
System message at 2021-01-01 00:08:00...  
Commit performed by admin via ssh using cli.  
switch02# Session will close in 3 seconds  
switch02# Session will close in 2 seconds  
switch02# Session will close in 1 second  
switch02# Connection to 192.168.16.34 closed.
```

6.3.2.3 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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Change the password for a user. To enter the password encrypted and not in plain text, press Enter after <code>password</code> . This will put you in Wizard mode. | <code>system authentication user { user name } password</code> |
| 3 | Enter the password. You can enter a password as follows: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> – <code>\$5\$</code> (SHA-256) – <code>\$6\$</code> (SHA-512) As plain text password If a password begins with a character combination other than <code>\$5\$</code> or <code>\$6\$</code>, 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 <code>\$0\$</code>, it is also viewed as a plain text password. Use this combination of characters if you want to configure a password that begins with the character <code>\$</code>. Example: <code>\$0\$\$iemens123</code> <p>By default, a password must fulfill the following conditions:</p> <ul style="list-style-type: none"> Must be between 8 and 255 characters long Must contain at least 1 number All standard characters are allowed, plus the following special characters: <code># \$ % & () * + , - . / : < = > @ [] ^ _ { } ~</code> <p>Note any deviating conditions due to the configurable password policy. For more information, refer to "Displaying the password policy (Page 164)".</p> | <code>{ Password }</code> |
| 4 | Confirm the password. To enter a plain text password encrypted and not in plain text, press Enter after <code>password-confirm</code> . This will put you in Wizard mode. | <code>password-confirm { password }</code> |
| 5 | Enter the password again. | <code>{ Password }</code> |
| 6 | Commit the changes. | <code>commit</code> |
| 7 | Exit configuration mode. | <code>end</code> |

Example

```

In this example, the password for the user with the user name user1 is changed.
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication user user1 password
(<string>): *****
localhost(config-user-user1)# password-confirm
(<string>): *****
localhost(config-user-user1)# commit
Commit complete.
localhost(config-user-user1)# end

```

6.3.2.4 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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Change the user profile for a user. Options include: <ul style="list-style-type: none"> <code>admin</code> - Users with the <code>admin</code> user profile have read and write access to the device functions. <code>guest</code> - Users with the <code>guest</code> user profile have read access to the device functions and can change their own password. | <code>system authentication user { user name } role [admin guest]</code> |
| 3 | Commit the changes. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system authentication user { user name } role</code> |

Example

```

In this example, the user profile for the user with the user name user1 is changed.
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication user user1 role guest
localhost(config-user-user1)# commit
Commit complete.
localhost(config-user-user1)# end
localhost# show running-config system authentication user user1 role
system
 authentication
  user admin3
  role guest
 exit

exit

```

```
exit
```

6.3.3 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.

6.3.3.1 Displaying active users

To show which users are currently logged on to the device, execute the following command in operational mode:

```
who
```

Example

```
localhost# who
Session User Context From Proto Date Mode
*188 admin cli 192.0.2.1 ssh 2020-03-25 operational
```

Description

The following information is shown:

| Parameter | Description |
|-----------|---|
| Session | Number of the session Your own session is marked with a *. |
| User | User name |
| Context | User interface via which the user is logged on |
| From | The IP address with which the user is logged on |
| Proto | The protocol with 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"> <code>operational</code> - The user is in operational mode. <code>config-terminal</code> - The user is in the shared configuration mode. <code>config-exculsive</code> - The user is in the exclusive configuration mode. |

6.3.3.2 Displaying user details

To show the configuration of all users, execute the following command in operational mode:

```
show running-config system authentication user
```

To show the configuration of one user, execute the following command in operational mode:

```
show running-config system authentication user { user name }
```

Example

This example shows the configuration of all users.

```
localhost# show running-config system authentication user | details
system
authentication
  user admin
    password                    $5$ViooGsb.$0vCqsxZ/5Q...
    password-confirm            $5$ViooGsb.$0vCqsxZ/5Q...
    role                         admin
    change-of-password-required
  exit

  user guest
    password                    $5$EzntQ/IV$hL9amGK5/1...
    password-confirm            $5$EzntQ/IV$hL9amGK5/1...
    role                         guest
    change-of-password-required
  exit

  user user1
    password                    $6$nBrh127yOq2Zzjgx$Bg...
    password-confirm            $6$nBrh127yOq2Zzjgx$Bg...
    role                         guest
    no change-of-password-required
  exit

exit

exit
```

Description

The following information is shown:

| Parameter | Description |
|-----------------------------|---|
| password | The password displayed is a hash value. |
| password-confirm | |
| role | Displays the user profile of the user. |
| change-of-password-required | Shows whether the user will be prompted on the next login to assign a new password. |

6.3.3.3 Logging off a user

If you are logged on with the `admin` user profile, you can log off users from the device. Logoff takes place using the session ID or the user name.

To log off a user from the device, execute the following command in operational mode:

```
admin logout [ session { session ID } | user { user name } ]
```

Example

```
localhost# admin logout user guest
```

6.3.3.4 Sending messages to users

You can send messages to users logged on to the device.

To send messages to all users or a specific user, execute the following command in operational mode:

```
send { user name } { message }
```

Example

```
localhost# send guest "Rebooting at midnight!"
localhost#
Message from admin@localhost at 2019-03-25 15:00:00...
Rebooting at midnight!
```

6.4 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.

6.4.1 Saving debug information on a remote server

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 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 debug information

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

| Step | Instruction | Command |
|------|--|---|
| 1 | Save and transfer a ZIP file with debug information. For more information on the URL, see "Specifying a URL (Page 67)". | <code>system service debug save target { URL }</code> |
| 2 | Respond to the security prompt. | <code>yes</code> |
| 3 | If the debug information has been saved before, there will be another query. Options include: <ul style="list-style-type: none"> <code>yes</code> - No new ZIP file is generated. The existing ZIP file is transferred. <code>no</code> - A new ZIP file with current debug information is generated and transferred. The existing ZIP file is overwritten. | <code>[yes no]</code> |

Example

In this example, the debug information is saved for the first time.

```
localhost# system service debug save target tftp://192.168.1.1/
debug-information.zip
Generating the Debug Info file may take several minutes. Do you
wish to continue? [no,yes] yes
Transferring file... done
```

6.4.2 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.

To enable the Debug user account, do the following:

| Step | Instruction | Command |
|------|--------------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the Debug user account. | <code>system authentication allow-debug-user</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system authentication allow-debug-user</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication allow-debug-user
```

6.4 Preparing the device for troubleshooting

```
localhost(config-system-authentication)# commit
Commit complete.
localhost(config-system-authentication)# end
localhost# show running-config system authentication allow-debug-
user
system
  authentication
    allow-debug-user
  exit
exit
```

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 30)".

7.1 Brute-Force Attack (BFA) 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.

7.1.1 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.

7.1.1.1 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.

User's and services that 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

7.1.1.2 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 |

7.1.2 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 180)".
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 181)".
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 183)".
4. Enable BFA prevention. For more information, refer to "Enabling BFA prevention (Page 184)".

7.1.2.1 Changing the auto-reset timer

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

Note

Unblocking a username or IP address

The auto-reset timer must be set to 0 before any username or IP address can be unblocked manually.

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

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the auto-reset timer. Conditions: <ul style="list-style-type: none"> Formatted as nYnMnDnhnmns, where n is a user-defined number Minimum 0 seconds Maximum 255 minutes (15300 seconds) Default: 10m | <code>system authentication brute-force-prevention auto-reset-timer { time }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system authentication brute-force-prevention auto-reset-timer</code> |

Example

The following sets the auto-reset timer to 15 minutes.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication brute-force-prevention auto-reset-timer 15m
localhost(config-brute-force-prevention)# commit
Commit complete.
localhost(config-brute-force-prevention)# end
localhost# show running-config system authentication brute-force-prevention auto-reset-timer
system
 authentication
  brute-force-prevention
    auto-reset-timer 15m
  exit
exit
exit
```

7.1.2.2 Changing the maximum number of failed login attempts

When a user or service fails to log in, their username or IP address is tracked and a timer starts. If the user or service fails again before the timer has expired, a counter is incremented by one.

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

This feature can also be disabled for either users or services by setting the limit to zero (0).

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

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Set the maximum number of failed log in attempts for users. Default: 10 | system authentication brute-force-prevention user-specific-login-attempts { 0 - 255 } |
| 3 | Set the maximum number of failed log in attempts for services. Default: 10 | system authentication brute-force-prevention ip-specific-login-attempts { 0 - 255 } |
| 4 | Commit the change. | commit |
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config system authentication brute-force-prevention [user-specific-login-attempts ip-specific-login-attempts] |

Example

The following sets a maximum of five failed log in attempts for users and 15 failed log in attempts for services.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication brute-force-prevention user-
specific-login-attempts 5
localhost(config-brute-force-prevention)# ip-specific-login-attempts 15
localhost(config-brute-force-prevention)# commit
Commit complete.
localhost(config-brute-force-prevention)# end
localhost# show running-config system authentication brute-force-
prevention user-specific-login-attempts
system
 authentication
  brute-force-prevention
    user-specific-login-attempts 5
  exit
exit

exit
localhost# show running-config system authentication brute-force-
prevention ip-specific-login-attempts
system
 authentication
  brute-force-prevention
    ip-specific-login-attempts 15
  exit
exit

exit
```

7.1.2.3 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.

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

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the time between failed log in attempts. Conditions: <ul style="list-style-type: none"> Formatted as nYnMnDnHnmns, where n is a user-defined number Minimum 5 minutes (300 seconds) Maximum 255 minutes (15300 seconds) Default: 5m | <code>system authentication brute-force-prevention trigger-interval { time }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system authentication brute-force-prevention trigger-interval</code> |

Example

The following sets the window between failed log in attempts to 10 minutes.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication brute-force-prevention trigger-
interval 10m
localhost(config-brute-force-prevention)# commit
Commit complete.
localhost(config-brute-force-prevention)# end
localhost# show running-config system authentication brute-force-
prevention trigger-interval
system
 authentication
  brute-force-prevention
    trigger-interval 10m
  exit
exit
exit
```

7.1.2.4 Enabling BFA prevention

To enable the BFA prevention mechanism, do the following:

Note

BFA prevention is enabled by default.

| Step | Instruction | Command |
|------|--------------------------------------|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable the BFA prevention mechanism. | system authentication brute-force-prevention enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system authentication brute-force-prevention |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication brute-force-prevention enabled
localhost(config-brute-force-prevention)# commit
Commit complete.
localhost(config-brute-force-prevention)# end
localhost# show running-config system authentication brute-force-prevention
system
 authentication
  brute-force-prevention
  enabled
 exit
exit
exit
```

7.1.3 Unblocking a user or IP address

Username and IP addresses can be unblocked manually.

Note

Unblocking a username or IP address

The auto-reset timer must be set to 0 before any username or IP address can be unblocked manually.

For more information, refer to Changing the auto-reset timer (Page 180).

To unblock a username or IP address that is currently blocked, execute the following command in operating mode:

```
system authentication brute-force-prevention reset [ user | ip ] { username
| IP address }
```

Example

The following unblocks IP address 172.30.145.142.

```
localhost# system authentication brute-force-prevention reset ip
172.30.145.142
```

7.1.4 Monitoring BFA prevention

To review which usernames and/or IP addresses are currently being monitored by the BFA protection mechanism, enter the following command in operating mode:

```
show system authentication brute-force-prevention
```

If any username or IP address is currently monitored, the following information is displayed:

| 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 | The IP address that is currently monitored. |
| failed-logins | The current number of failed login attempts. |
| 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

```
localhost# show system authentication brute-force-prevention | tab
```

| | FAILED | LAST | |
|--------------|--------|--------|---------|
| USERNAME | LOGINS | FAILED | BLOCKED |
| Unknown User | 5 | 3s | 0s |
| admin | 2 | 44s | 0s |
| guest | 10 | 1m38s | 8m22s |
| wsmith | 0 | 0s | 0s |

| | FAILED | LAST | |
|----------------|--------|--------|---------|
| IP | LOGINS | FAILED | BLOCKED |
| 192.168.128.31 | 3 | 2m58s | 0s |
| 192.168.128.30 | 12 | 3s | 9m57s |

7.2 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.

7.2.1 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 625)".

7.2.1.1 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.

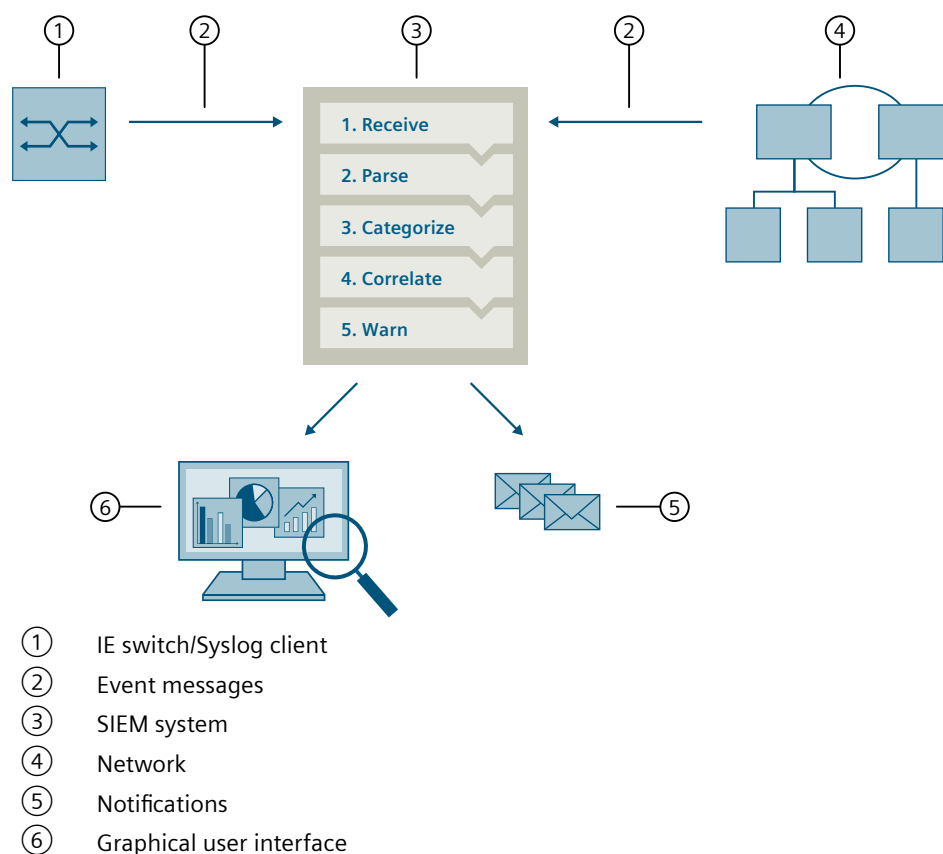


Figure 7-1 SIEM system

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 189)".

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.

7.2.1.2 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 627)". 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 | |
| timeQuality | Information on the system time Example: [timeQuality tzKnown="0" isSynced="0"] The tzKnown parameter indicates whether the sender knows its time zone. Options include: <ul style="list-style-type: none"> Value "1" = The time zone is known. Value "0" = The time zone is unknown. The isSynced parameter specifies whether the source device is synchronized with a reliable external time source, e.g. via NTP. Options include: <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>).

7.2.1.3 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 190)" (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 |
| 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 that identifies an authenticated user by name, without spaces Format: %s | maier |
| Group | String that identifies a group by name, without spaces Format: %s | it-service |

| Variable | Description | Example |
|------------------------|---|------------------------|
| Local interface | Symbolic name of a local interface Format: %s | Console ethernet0/4 |
| 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) |
| Config detail | String for a configuration (configuration path), without spaces Format: %s | /switch/vlan{2} |
| License key | String that represents an ALM license or an article number in the case of a CLP Format: %s | SISLSOXTST0100 |
| Vlan id | VLAN ID Range of values: 1 ... 4094 Format: %d | 7 |

7.2.2 Monitoring security-relevant events

This section describes the security-relevant event messages. The categorization of the messages is based on the IEC 62443 standard.

7.2.2.1 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}: SSH authentication attempt was not completed within {timeout} seconds from {IP address}.

| | |
|-------------|--|
| Example | SSH: SSH authentication attempt was not completed within 120 seconds from 192.168.0.1. |
| Explanation | An SSH authentication attempt via a network interface on the SINEC OS device was not completed within the defined time. In the example, the SSH authentication attempt from network address "192.168.0.1" was not completed within 120 seconds. |
| Severity | Info |
| 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}: {IP address} - No response from the RADIUS server.

| | |
|-------------|--|
| Example | RADIUS: 192.168.1.105 - No response from the RADIUS server. |
| 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 |

7.2.2.2 Identification and authentication of devices

The following event messages provide information about successful and failed device accesses.

{Protocol}: {IP address} access granted.

| | |
|-------------|--|
| Example | SSH: 192.0.2.2 access granted. |
| Explanation | Device access is granted due to successful authentication. In the example, access of the device with the IP address "192.0.2.2" is granted. |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.2 |

{Protocol}: {IP address} access denied.

| | |
|-------------|--|
| Example | SSH: 192.0.2.2 access denied. |
| Explanation | Device access is denied due to unsuccessful authentication. In the example, access of the device with the IP address "192.0.2.2" is denied. |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.2 |

{Protocol}: Device {Src mac} access granted on {Local interface} in vlan {Vlan id}.

| | |
|-------------|---|
| Example | 802.1X: Device 10:00:00:00:00:29 access granted on ethernet0/3 in vlan 12. |
| Explanation | Device access is granted due to successful port authentication. In the example, access for the device with the source MAC address "10:00:00:00:00:29" is granted via bridge port 3 in VLAN 12. |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.2 |

{Protocol}: Device {Src mac} access denied on {Local interface} in vlan {Vlan id}.

| | |
|-------------|--|
| Example | 802.1X: Device 10:00:00:00:00:29 access denied on ethernet0/3 in vlan 7. |
| Explanation | Device access is denied due to unsuccessful port authentication. In the example, access for the device with the source MAC address "10:00:00:00:00:29" is denied via bridge port 3 in VLAN 7. |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.2 |

7.2.2.3 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} changed user-account {Destination user name} with role {Role}.

| | |
|-------------|---|
| Example | SSH: User admin changed user-account admin2 with role Administrator. |
| Explanation | A user has changed the user account of another user. In the example, the "admin" user changed the "admin2" user account with the "Administrator" user profile. |
| 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 |

7.2.2.4 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 |

7.2.2.5 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 |

7.2.2.6 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 |

7.2.2.7 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 /switch/vlan{2} configuration. |
| Explanation | A user has changed specific configuration values. In the example, the user "admin" has changed the configuration of VLAN 2. |
| 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 |

7.2.2.8 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 |

7.2.2.9 Software and information integrity

The following event messages provide information about failed integrity verification when loading the firmware.

Firmware integrity verification failed.

| | |
|-------------|---|
| Example | Firmware integrity verification failed. |
| Explanation | An integrity fault was detected while the firmware integrity was being checked. |
| Severity | Error |

| | |
|----------|---------------------------------|
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 3.4 |

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 |

Configuration integrity verification failed.

| | |
|-------------|--|
| Example | Configuration integrity verification failed. |
| Explanation | An integrity fault was detected while the configuration integrity was being checked. |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 3.4 |

7.2.2.10 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 |

7.2.2.11 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 |

7.2.2.12 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 |

7.2.2.13 Restoring 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}: 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 |

7.3 Keys and certificates

This section describes how to configure and manage keys and certificates.

7.3.1 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

7.3.1.1 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.

7.3.1.2 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.

7.3.1.3 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.

7.3.1.4 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.

7.3.1.5 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.

7.3.1.6 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.

7.3.1.7 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.

7.3.1.8 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.

7.3.1.9 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.

7.3.1.10 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. |

7.3.2 Managing the keystore

To configure the keystore, do the following:

1. [Optional] Add key pairs in the keystore.
For more information, refer to "Manually configuring a key pair (Page 207)" and "Importing a key pair (Page 209)".
2. [Optional] Add certificates in the keystore to sign the public key.
For more information, refer to "Manually configuring a certificate (Page 213)" and "Importing a certificate (Page 214)".

7.3.2.1 Manually configuring a key pair

Note

It is recommended that you import key pairs.

If you manually configure a key pair in the keystore, you are recommended to use Wizard mode.

To manually configure a key pair, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Assign a name for the key pair. Condition: <ul style="list-style-type: none"> • Must be between 1 and 32 characters long | <code>system certificates local asymmetric-key { Name }</code> |
| 3 | Define the format of the public key. Options include: <ul style="list-style-type: none"> • <code>ssh-public-key-format</code> - Format for SSH keys • <code>subject-public-key-info-format</code> - Format for TLS keys | <code>public-key-format [ssh-public- key-format subject-public-key- info-format]</code> |
| 4 | Enter the public key (Base64-coded DER format). The format depends on the configuration of the <code>public-key-format</code> parameter. Condition: <ul style="list-style-type: none"> • Must be between 1 and 2048 bytes long To enter the key encrypted, press Enter after <code>public-key</code> . This will put you in Wizard mode. | <code>public-key { Public key }</code> |

| Step | Instruction | Command |
|------|---|--|
| 5 | Define the format of the private key. Options include: <ul style="list-style-type: none"> • <code>ec-private-key-format</code> - The private key must be available in the syntax defined in the following RFC: RFC 5915 Elliptic Curve Private Key Structure (https://tools.ietf.org/html/rfc5915) • <code>one-asymmetric-key-format</code> - The private key must be available in the syntax defined in the following RFC: RFC 5958 Asymmetric Key Packages (https://tools.ietf.org/html/rfc5958) • <code>rsa-private-key-format</code> - The private key must be available in the syntax defined in the following RFC: RFC 3447 Public-Key Cryptography Standards (PKCS) #1 (https://tools.ietf.org/html/rfc3447) | <code>private-key-format [ec-private-key-format one-asymmetric-key-format rsa-private-key-format]</code> |
| 6 | Enter the encrypted private key (Base64-coded DER format). The format depends on the configuration of the <code>private-key-format</code> parameter. Condition: <ul style="list-style-type: none"> • Must be between 1 and 8192 bytes long To enter the key encrypted, press Enter after <code>private-key</code> . This will put you in Wizard mode. | <code>private-key { Private key }</code> |
| 7 | Commit the changes. | <code>commit</code> |
| 8 | Exit configuration mode. | <code>end</code> |
| 9 | Verify the configuration. | <code>show running-config system certificates local asymmetric-key { Name }</code> |

Example

```

localhost# config
localhost(config)# system certificates local asymmetric-key my-
https-server
localhost(config-asymmetric-key-my-https-server)# public-key-format
subject-public-key-info-format
localhost(config-asymmetric-key-my-https-server)# public-key
(<base64Binary, min: 1 octets, max: 2048 octets>):
MIIBIjANBgkqhkiG9...
localhost(config-asymmetric-key-my-https-server)# private-key-
format one-asymmetric-key-format
localhost(config-asymmetric-key-my-https-server)# private-key
(<AES encrypted string, min: 1 units, max: 8192 units>):
*****...
localhost(config-asymmetric-key-my-https-server)# commit
Commit complete.

```



```
localhost(config-asymmetric-key-my-https-server)# end
localhost# show running-config system certificates local asymmetric-
key my-https-server
system
 certificates
  local
    asymmetric-key my-https-server
      public-key-format  subject-public-key-info-format
      public-key          MIIBIjANBgkqhkiG9...
      private-key-format one-asymmetric-key-format
      private-key         "$8$sGE795EWikian...
    exit
  exit
exit
exit
exit
```

7.3.2.2 Importing a key pair

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 file 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 key pair, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Assign a name for the key pair. Condition: <ul style="list-style-type: none"> • Must be between 1 and 32 characters long | <code>system certificates local asymmetric-key { Name }</code> |
| 3 | Load a file in the appropriate format. Options for the format include: <ul style="list-style-type: none"> • <code>pem</code> - The file is available in PEM format. • <code>pkcs12</code> - The file is available in PKCS#12 format. For more information on the URL, see "Specifying a URL (Page 67)". [Optional] With the <code>certificate-name</code> parameter, enter the name of the user certificate to be created or overwritten. Condition: <ul style="list-style-type: none"> • Must be between 1 and 64 characters long If you do not specify this parameter, all certificates contained in the file are ignored. [Optional] If a PKCS#12 file is encrypted, enter the password for the file with the <code>password</code> parameter. Condition: <ul style="list-style-type: none"> • Must be between 1 and 255 characters long [Optional] If a CA certificate is contained in a PKCS#12 file and it is to be stored in the trust-store, enter the name of the certificate folder with the <code>bag-name</code> parameter and the name of the certificate with the <code>bag-certificate-name</code> parameter. Condition for the name of the certificate folder: <ul style="list-style-type: none"> • Must be between 1 and 32 characters long Condition for the name of the certificate: <ul style="list-style-type: none"> • Must be between 1 and 64 characters long The file transfer starts immediately and the new key pair is displayed as an unconfirmed configuration change. | <code>load format [pem pkcs12] source { URL } certificate-name { User certificate } password { Password } bag-name { Certificate folder } bag- certificate-name { Certificate }</code> |
| 4 | [Optional] Verify the imported key pair. | <code>show configuration</code> |
| 5 | Commit the changes. | <code>commit</code> |
| 6 | Exit configuration mode. | <code>end</code> |

| Step | Instruction | Command |
|------|--|--|
| 7 | Verify the configuration. | show running-config system certificates local asymmetric- key { Name } |
| 8 | [Optional] If a CA certificate from a PKCS#12 file was stored in the truststore, check this configuration. | show running-config system certificates remote certificate- bag { Certificate folder } |

Example

In this example, a file is imported in PEM format with a self-signed user certificate.

```
localhost# config
localhost(config)# system certificates local asymmetric-key my-
https-server
localhost(config-asymmetric-key-my-https-server)# load format
pem source tftp://192.168.2.68/privkey.pem certificate-name self-
signed-1
Transferring file... done
localhost(config-asymmetric-key-my-https-server)# show configuration
system
certificates
local
asymmetric-key my-https-server
public-key-format subject-public-key-info-format
public-key MIIBIjANBgkqhk...
private-key-format one-asymmetric-key-format
private-key "$8$eUWJ/CSj9f...
certificate self-signed-1
cert-data MIICYgYJKoZIhvcNAQcCoIICU...
exit

exit

exit

exit

localhost(config-asymmetric-key-my-https-server)# commit
Commit complete.
localhost(config-asymmetric-key-my-https-server)# end
localhost# show running-config system certificates local asymmetric-
key my-https-server
system
certificates
local
asymmetric-key my-https-server
public-key-format subject-public-key-info-format
public-key MIIBIjANBgkqhk...
private-key-format one-asymmetric-key-format
private-key "$8$eUWJ/CSj9f...
certificate self-signed-1
cert-data MIICYgYJKoZIhvcNAQcCoIICU...
```

```
exit

exit

exit

exit

exit
```

Example

In this example, a file in PKCS#12 format is imported with a CA certificate. The CA certificate is displayed in the truststore.

```
localhost# config
localhost(config)# system certificates local asymmetric-key my-
https-server
localhost(config-asymmetric-key-my-https-server)# load format
pkcs12 source tftp://192.168.2.68/client1.p12 certificate-name my-
end-entity bag-name my-trusted-cas bag-certificate-name my-ca-1
Transferring file... done
localhost(config-asymmetric-key-my-https-server)# show configuration
system
certificates
local
asymmetric-key my-https-server
public-key-format subject-public-key-info-format
public-key          MIIBIjANBgkqhk...
private-key-format one-asymmetric-key-format
private-key          "$8$eUWJ/CSj9f...
certificate my-end-entity
cert-data MIIHFwYJKoZIhvcNAQcCo...
exit

exit

exit

exit

exit
localhost(config-asymmetric-key-my-https-server)# commit
Commit complete.
localhost(config-asymmetric-key-my-https-server)# end
localhost# show running-config system certificates local asymmetric-
key my-https-server
system
certificates
local
asymmetric-key my-https-server
public-key-format subject-public-key-info-format
public-key          MIIBIjANBgkqhk...
private-key-format one-asymmetric-key-format
```

```

private-key      "$8$eUWJ/CSj9f...
certificate my-end-entity
  cert-data MIIHFwYJKoZIhvcNAQcCo...
exit

exit

exit

exit

localhost# show running-config system certificates remote
certificate-bag
system
certificates
  remote
  certificate-bag my-trusted-cas
  certificate my-ca-1
    cert-data MIIDjwYJKoZIhvcNAQcC...
  exit

exit

exit

exit

exit

```

7.3.2.3 Manually configuring a certificate

Note

It is recommended that you import certificates.

If you manually configure a certificate or a certificate chain in the keystore for a key pair, you are recommended to use Wizard mode.

To manually configure a certificate in the keystore, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enter the name of the key pair for which you want to configure the certificate or the certificate chain. | <code>system certificates local asymmetric-key { Name }</code> |
| 3 | Assign a name for the certificate or the certificate chain. Condition: <ul style="list-style-type: none"> • Must be between 1 and 64 characters long | <code>certificate { Name }</code> |

| Step | Instruction | Command |
|------|--|---|
| 4 | Enter the DER-coded certificate or the certificate chain in PKCS#7 format. The entry must comprise either a self-signed user certificate or the entire certificate chain from the user certificate to the root certificate. Condition: <ul style="list-style-type: none"> • Must be between 1 and 8192 bytes long To enter the certificate encrypted, press Enter after <code>cert-data</code> . This will put you in Wizard mode. | <code>cert-data { Certificate }</code> |
| 5 | Commit the changes. | <code>commit</code> |
| 6 | Exit configuration mode. | <code>end</code> |
| 7 | Verify the configuration. | <code>show running-config system certificates local asymmetric- key { Name } certificate</code> |

Example

```
localhost# config
localhost(config)# system certificates local asymmetric-key my-
https-server
localhost(config-asymmetric-key-my-https-server)# certificate my-
selfsigned-1
localhost(config-certificate-my-selfsigned-1)# cert-data
(<base64Binary, min: 1 octets, max: 8192 octets>): MIIHRwYJKoZIh...
localhost(config-certificate-my-selfsigned-1)# commit
Commit complete.
localhost(config-certificate-my-selfsigned-1)# end
localhost# show running-config system certificates local asymmetric-
key my-https-server certificate
system
 certificates
  local
    asymmetric-key my-https-server
      certificate my-selfsigned-1
        cert-data MIIHFwYJKoZIHvcNAQcCo...
      exit
    exit
  exit
exit
```

7.3.2.4 Importing a certificate

You can load a file from a file server and import a certificate or a certificate chain into the keystore to an existing key pair.

Requirements

- You have configured a server accordingly.
- The file 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

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, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enter the name of the key pair for which you want to import the certificate or the certificate chain. | <code>system certificates local asymmetric-key { Name }</code> |
| 3 | Assign a name for the certificate or the certificate chain. Condition: • Must be between 1 and 64 characters long | <code>certificate { Name }</code> |
| 4 | Load the file in the appropriate format. Options for the format include: • <code>pem</code> - The file is available in PEM format. • <code>pkcs7</code> - The file is available in PKCS#7 format. For more information on the URL, see "Specifying a URL (Page 67)". The file transfer starts immediately and the new certificate is displayed as an unconfirmed configuration change. | <code>load format [pem pkcs7] source { URL }</code> |
| 5 | [Optional] Verify the imported certificate. | <code>show configuration</code> |
| 6 | Commit the changes. | <code>commit</code> |
| 7 | Exit configuration mode. | <code>end</code> |
| 8 | Verify the configuration. | <code>show running-config system certificates local asymmetric-key { Name } certificate</code> |

Example

```
localhost# config
localhost(config)# system certificates local asymmetric-key my-
https-server
localhost(config-asymmetric-key-my-https-server)# certificate my-
selfsigned-2
localhost(config-certificate-my-selfsigned-2)# load format pkcs7
source tftp://192.168.2.68/cert-chain.p7
Transferring file... done
localhost(config-certificate-my-selfsigned-2)# show configuration
system
certificates
local
asymmetric-key my-https-server
certificate selfsigned-2
cert-data MIICYgYJKoZIhvcNAQcCoIICU...
exit

exit

exit

exit

localhost(config-certificate-my-selfsigned-2)# commit
Commit complete.
localhost(config-certificate-my-selfsigned-2)# end
localhost# show running-config system certificates local asymmetric-
key my-https-server certificate
system
certificates
local
asymmetric-key my-https-server
certificate my-selfsigned-2
cert-data MIIHFwYJKoZIhvcNAQcCo...
exit

exit

exit

exit
```


7.3.3 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 "Manually configuring a certificate (Page 217)" and "Importing a certificate (Page 218)".
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 "Manually configuring a known host (Page 221)".
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 "Specifying a URL (Page 67)".

7.3.3.1 Manually configuring a certificate

If you manually configure a certificate or a certificate chain in the truststore, you are recommended to use Wizard mode.

To manually configure a certificate in the truststore, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | If you want to add a certificate to an existing certificate folder, enter the name of the certificate folder. If you want to create a new certificate folder, assign a name to the certificate folder. Condition: <ul style="list-style-type: none"> • Must be between 1 and 32 characters long | <code>system certificates remote certificate-bag { Name }</code> |
| 3 | [Optional] Enter a description for the certificate folder. Condition: <ul style="list-style-type: none"> • Must be between 1 and 256 characters long | <code>description { Description }</code> |
| 4 | Assign a name for the certificate or the certificate chain. Condition: <ul style="list-style-type: none"> • Must be between 1 and 64 characters long | <code>certificate { Name }</code> |

| Step | Instruction | Command |
|------|--|---|
| 5 | Enter the DER-coded certificate or the certificate chain in PKCS#7 format. The entry must comprise either a self-signed user certificate or the entire certificate chain from the user certificate to the root certificate. Condition: <ul style="list-style-type: none"> • Must be between 1 and 8192 bytes long To enter the certificate encrypted, press Enter after <code>cert-data</code> . This will put you in Wizard mode. | <code>cert-data { Certificate }</code> |
| 6 | Commit the changes. | <code>commit</code> |
| 7 | Exit configuration mode. | <code>end</code> |
| 8 | Verify the configuration. | <code>show running-config system certificates remote certificate-bag { Name } certificate { Name }</code> |

Example

```
localhost# config
localhost(config)# system certificates remote certificate-bag my-trusted-cas
localhost(config-certificate-bag-my-trusted-cas)# certificate my-ca-1
localhost(config-certificate-my-ca-1)# cert-data
(<base64Binary, min: 1 octets, max: 8192 octets>):
MIIDjwYJKoZIhvc...
localhost(config-certificate-my-ca-1)# commit
Commit complete.
localhost(config-certificate-my-ca-1)# end
localhost# show running-config system certificates remote
certificate-bag my-trusted-cas certificate my-ca-1
system
certificates
remote
certificate-bag my-trusted-cas
certificate my-ca-1
cert-data MIIDjwYJKoZIhvcNA...
exit

exit

exit

exit

exit
```

7.3.3.2 Importing a certificate

You can load a file from a file server and import a certificate or a certificate chain into the truststore.

Requirements

- You have configured a server accordingly.
- The file 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

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, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | If you want to add a certificate to an existing certificate folder, enter the name of the certificate folder. 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 | <code>system certificates remote certificate-bag { Name }</code> |
| 3 | [Optional] Enter a description for the certificate folder. Condition: • Must be between 1 and 256 characters long | <code>description { Description }</code> |
| 4 | Assign a name for the certificate or the certificate chain. Condition: • Must be between 1 and 64 characters long | <code>certificate { Name }</code> |

| Step | Instruction | Command |
|------|---|--|
| 5 | Load the file in the appropriate format. Options for the format include: <ul style="list-style-type: none"> • pem - The file is available in PEM format. • pkcs7 - The file is available in PKCS#7 format. For more information on the URL, see "Specifying a URL (Page 67)". The file transfer starts immediately and the new certificate is displayed as an unconfirmed configuration change. | <pre>load format [pem pkcs7] source { URL }</pre> |
| 6 | [Optional] Verify the imported certificate. | <pre>show configuration</pre> |
| 7 | Commit the changes. | <pre>commit</pre> |
| 8 | Exit configuration mode. | <pre>end</pre> |
| 9 | Verify the configuration. | <pre>show running-config system certificates remote certificate- bag { Name } certificate { Name }</pre> |

Example

```
localhost# config
localhost(config)# system certificates remote certificate-bag my-
trusted-cas
localhost(config-certificate-bag-my-trusted-cas)# certificate my-
ca-1
localhost(config-certificate-bag-my-trusted-cas)# load format pkcs7
source tftp://192.168.2.68/cert-chain.p7
Transferring file... done
localhost(config-certificate-bag-my-trusted-cas)# show configuration
system
certificates
remote
certificate-bag my-trusted-cas
certificate my-ca-1
cert-data MIIDjwYJKoZIhvcNA...
exit

exit

exit

exit

exit
localhost(config-certificate-bag-my-trusted-cas)# commit
Commit complete.
localhost(config-certificate-bag-my-trusted-cas)# end
localhost# show running-config system certificates remote
certificate-bag my-trusted-cas certificate my-ca-1
system
certificates
remote
```

```

certificate-bag my-trusted-cas
certificate my-ca-1
cert-data MIIDjwYJKoZIhvcNA...
exit

exit

exit

exit

exit

```

7.3.3.3 Manually configuring a known host

When you manually configure a known host in the truststore, you are recommended to use Wizard mode.

To manually configure a known host in the truststore, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | If you want to add a known host to an existing key bag, enter the name of the key bag. If you want to create a new key bag, assign a name to the key bag. Condition: <ul style="list-style-type: none"> Must be between 1 and 259 characters long | <code>system certificates remote public-key-bag { Name }</code> |
| 3 | [Optional] Enter a description for the key bag. Condition: <ul style="list-style-type: none"> Must be between 1 and 256 characters long | <code>description { Description }</code> |
| 4 | Assign a name for the known host. Condition: <ul style="list-style-type: none"> Must be between 1 and 64 characters long | <code>public-key { Name }</code> |
| 5 | Define the format of the public key. Options include: <ul style="list-style-type: none"> <code>ssh-public-key-format</code> - Format for SSH keys <code>subject-public-key-info-format</code> - Format for TLS keys | <code>public-key-format [ssh-public-key-format subject-public-key-info-format]</code> |

| Step | Instruction | Command |
|------|---|--|
| 6 | Enter the public key (Base64-coded DER format). The format depends on the configuration of the <code>public-key-format</code> parameter. Condition: <ul style="list-style-type: none"> • Must be between 1 and 2048 bytes long To enter the key encrypted, press Enter after <code>public-key</code> . This will put you in Wizard mode. | <code>public-key { Public key }</code> |
| 7 | [Optional] Enter the fingerprint of the public key (Base64-coded DER format). Condition: <ul style="list-style-type: none"> • Must be between 1 and 2048 bytes long To enter the fingerprint encrypted, press Enter after <code>fingerprint</code> . This will put you in Wizard mode. | <code>fingerprint { Fingerprint }</code> |
| 8 | Commit the changes. | <code>commit</code> |
| 9 | Exit configuration mode. | <code>end</code> |
| 10 | Verify the configuration. | <code>show running-config system certificates remote public-key- bag { Name } public-key { Name }</code> |

Example

```
localhost# config
localhost(config)# system certificates remote public-key-bag my-
known-hosts
localhost(config-public-key-bag-my-known-hosts)# public-key my-sftp-
host-1
localhost(config-public-key-my-sftp-host-1)# public-key-format ssh-
public-key-format
localhost(config-public-key-my-sftp-host-1)# public-key
(<base64Binary>): AAAAC3NzaC1lZDI1NTE5AAAAI...
localhost(config-public-key-my-sftp-host-1)# fingerprint
(<base64Binary, min: 1 octets, max: 64 octets>):
n2/4+VLG5oQ4NURiYtAr2WMR140BQ+7aeImEV...
localhost(config-public-key-my-sftp-host-1)# commit
Commit complete.
localhost(config-public-key-my-sftp-host-1)# end
localhost# show running-config system certificates remote public-
key-bag my-known-hosts public-key my-sftp-host-1
system
certificates
remote
public-key-bag my-known-hosts
public-key my-sftp-host-1
public-key-format ssh-public-key-format
public-key AAAAC3NzaC1lZDI1NTE5AAAAI...
fingerprint n2/4+VLG5oQ4NURiYtAr2WMR140BQ+7aeImEV...
exit
```

```
exit
exit
exit
exit
```

7.3.4 Monitoring certificates

This section describes how to monitor keys and certificates and view detailed information.

7.3.4.1 Showing fingerprints

To display the fingerprints of public keys or certificates, execute the following command in operational mode:

```
show system certificates
```

Example

```
localhost# show system certificates
certificates
local
  asymmetric-key vendor-ssh
  key-info fingerprint md5
  value 7c:ba:86:57:c9:...
  key-info fingerprint sha1
  value Xw/fxhAYdIzRK+K...
  key-info fingerprint sha256
  value y4JzVpySYToOFdP...
  asymmetric-key vendor-tls
  certificate vendor-signed
  cert-info
  fingerprint sha1
  value 12:4d:fd:44:...
  fingerprint sha256
  value 43:17:2f:1e:...
  key-info fingerprint sha1
  value c4:6c:8d:cd:07:...
  key-info fingerprint sha256
  value a6:68:3f:a2:e3:...
```

Description

The following information is shown:

| Parameter | Description |
|-------------|---|
| fingerprint | Shows the hash algorithm with which the fingerprint was created. Possible values: <ul style="list-style-type: none"> • md5 - Bit length 128 • sha1 - Bit length 160 • sha256 - Bit length 256 |
| value | Shows the fingerprint. |

7.4 User authentication

SINEC OS offers various options for authenticating users attempting to access the device.

7.4.1 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.

7.4.1.1 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 235)".

7.4.1.2 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.

Authentication types

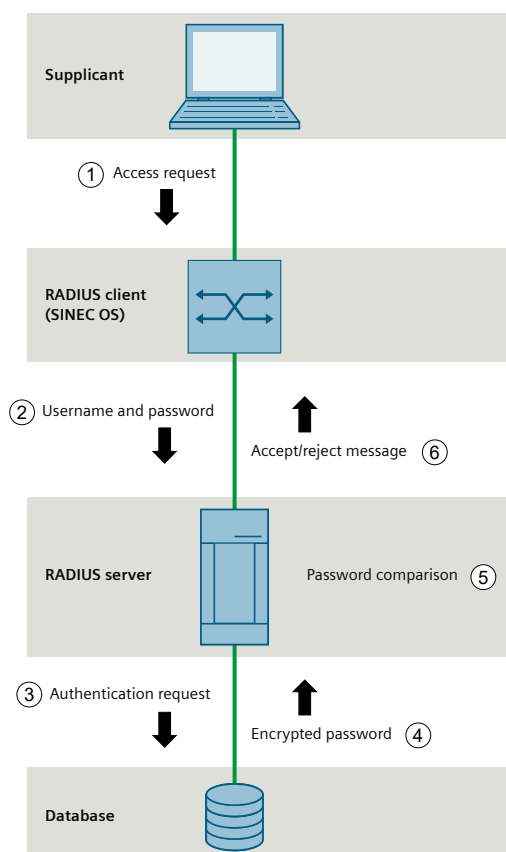
SINEC OS supports the following types of RADIUS authentication:

- **Password Authentication Protocol (PAP)**

PAP uses a two-way handshake approach for validating users based on their username and password.

When a user requests access, their supplicant forwards their username and password to the RADIUS client (SINEC OS). The RADIUS client then forwards the user's credentials in plaintext to the RADIUS server as part of an access-request packet. These steps are repeated until the RADIUS server responds with an access-accept or access-reject packet.

The RADIUS server includes an encrypted database of last known valid passwords. It encrypts the received password and compares it to the stored password. If the passwords match, the server forwards an access-accept message back to the client. Otherwise, the server forwards an access-reject message.



- ① The supplicant forwards an access-request packet to the RADIUS client containing the user's username and password.
- ② The RADIUS client forwards the username and password to the RADIUS server as plaintext.
- ③ The RADIUS server queries the RADIUS database.
- ④ The RADIUS database forwards the stored password to the server. Stored passwords are encrypted.
- ⑤ The RADIUS server encrypts the received password and compares it to the stored password.
- ⑥ The RADIUS server forwards an accept or reject message to the client depending on the comparison result.

Figure 7-2 PAP authentication method

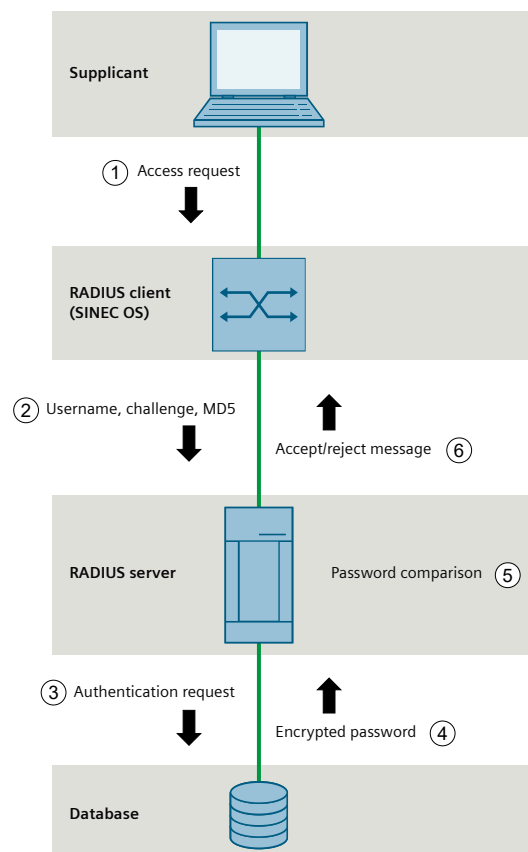
- **Challenge-Handshake Authentication Protocol (CHAP)**

CHAP uses a similar process to PAP, except the information forwarded to the RADIUS client is encrypted at the beginning.

When a user requests access, their supplicant combines the user's password with a random string of numbers (the challenge) received from the RADIUS client (SINEC OS). This combination is then run through an MD5 hash to render it unreadable.

The username, challenge, and MD5 hash are then forwarded to the RADIUS client and then on to the RADIUS server.

Passwords, in this case, are stored unencrypted in the server's database. The server must first apply the challenge and MD5 hash to the stored password before comparing it to the encrypted password received. If the encrypted passwords match, the server forwards an access-accept message back to the client. Otherwise, the server forwards an access-reject message.



- ① The supplicant forwards an access-request packet to the RADIUS client containing the user's username, challenge, and an MD5 hash of the user's password.
- ② The RADIUS client forwards the username, challenge, and encrypted password to the RADIUS server.
- ③ The RADIUS server queries the RADIUS database.
- ④ The RADIUS database forwards the stored password to the server as plaintext.
- ⑤ The RADIUS server applies the MD5 hash and challenge to the stored password.
- ⑥ The RADIUS server forwards an accept or reject message to the client depending on the comparison result.

Figure 7-3 CHAP authentication

When a new RADIUS server profile is defined for SINEC OS, the PAP authentication method is applied by default.

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. |

7.4.2 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 229)".
2. Set the user authentication mode.
For more information, refer to "Selecting the user authentication mode (Page 235)".

7.4.3 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 229)".
2. Configure the remote RADIUS server(s).
For more information, refer to "Configuring a RADIUS server (Page 232)".
3. Test the connection to the RADIUS server(s).
For more information, refer to "Testing a RADIUS server connection (Page 235)".

7.4.3.1 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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the name of the server profile. Condition: <ul style="list-style-type: none"> Must be between 1 and 256 characters long | <code>system radius server { name }</code> |
| 3 | Set the authentication key required by the server. Conditions: <ul style="list-style-type: none"> Must be between 1 and 128 characters long Allowed ASCII signs are 0x21 to 0x7E The key is AES encrypted once committed. | <code>shared-secret { key }</code> |
| 4 | Set the authentication key again. Conditions: <ul style="list-style-type: none"> Must be between 1 and 128 characters long Allowed ASCII signs are 0x21 to 0x7E The key is AES encrypted once committed. | <code>shared-secret-confirm { key }</code> |
| 5 | Specify the RADIUS server type. Options include: <ul style="list-style-type: none"> <code>login</code> - Select this option to authenticate users logging in via SSH. <code>dot1x</code> - Select this option to authenticate users logging in through a secure bridge port. For this option, port security must be enabled and the security mode must be set to <code>dot1x</code> or <code>dot1x_mac_auth</code> for one or more bridge ports. These options can be combined (in any order) if the RADIUS server supports both authentication types. Combinations include: <ul style="list-style-type: none"> <code>login dot1x</code> <code>dot1x login</code> Either combination specifies the server supports both LOGIN and IEEE 802.1X user authentication. Default: <code>login</code> | <code>server-type [login dot1x]</code> or <code>server-type < Enter ></code> [list] ({ Current Mode } : [login dot1x] [login dot1x] |
| 6 | Specify whether the server is reached via IP address or domain name. Condition: <ul style="list-style-type: none"> Must be between 1 and 253 characters long A domain name can only be defined if <code>server-type</code> is set strictly to <code>login</code> | <code>ipv4 { IP address }</code> or <code>host { domain }</code> |

| Step | Instruction | Command |
|------|---|---|
| 7 | <p>[Optional] Set the authentication type.</p> <p>Options include:</p> <ul style="list-style-type: none"> radius-pap - Use PAP based authentication radius-chap - Use CHAP based authentication <p>Default: radius-pap</p> | <pre>authentication-type [radius-pap radius-chap]</pre> |
| 8 | <p>[Optional] Set the destination UDP port to use when communicating with the server.</p> <p>Condition:</p> <ul style="list-style-type: none"> A number between 1 and 65535 <p>Default: 1812</p> | <pre>udp-port { 1 - 65535 }</pre> |
| 9 | <p>[Optional] Specify if the server is the primary server.</p> <p>If a server profile is not explicitly designated as primary, the first profile defined will be automatically designated as the primary.</p> <p>The server cannot be set as primary if the other server profile is already set as primary.</p> | <pre>primary</pre> |
| 10 | <p>[Optional] Set the number of times the RADIUS client will attempt to reach the server.</p> <p>Condition:</p> <ul style="list-style-type: none"> A number between 1 and 5 <p>Default: 3</p> | <pre>attempts { 1 - 5 }</pre> |
| 11 | <p>[Optional] Set the time in seconds (s) the RADIUS client will wait for a response after each attempt to reach the server.</p> <p>Conditions:</p> <ul style="list-style-type: none"> Formatted as nYnMnDnHnMnS, where n is a user-defined number Minimum 1 second (1s) Maximum 255 seconds (255s) <p>Default: 5s (5 seconds)</p> | <pre>timeout { 1s - 255s }</pre> |
| 12 | Commit the changes. | <pre>commit</pre> |
| 13 | Exit configuration mode. | <pre>end</pre> |
| 14 | Verify the configuration. | <pre>show running-config system radius server</pre> |

Example

The following configures a basic server profile for a primary RADIUS server available to at 172.30.141.141.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system radius server RADIUS1
localhost(config-server-radius-RADIUS1)# shared-secret sharedkey123
localhost(config-server-radius-RADIUS1)# shared-secret-confirm sharedkey123
localhost(config-server-radius-RADIUS1)# server-type
[list] (login): login dot1x
localhost(config-server-radius-RADIUS1)# ipv4 172.30.141.141
localhost(config-server-radius-RADIUS1)# primary
localhost(config-server-radius-RADIUS1)# commit
Commit complete.
localhost(config-server-radius-RADIUS1)# end
localhost# show running-config system radius server
system
radius
  server RADIUS1
    shared-secret          $8$dOzis+dFAghd4v+QJxRrkq+Io9lu4O...
    shared-secret-confirm $8$zXSRr0CqJswX1Q9XjYNJsgZdxihIki...
    ipv4 172.30.141.141
    server-type [ dot1x login ]
    authentication-type radius-pap
    primary
  exit
exit
exit
```

7.4.3.2 Configuring a RADIUS server

Before communicating with your RADIUS server(s), you need to first define the following on the server side:

- Which IP subnets to listen on
- Which certificates and keys to use for authentication
- Which users and/or MAC addresses to authenticate

While most RADIUS servers are configured in the same way, the following describes how to configure a server using FreeRADIUS. For specific instructions, refer to the vendor's user documentation.

To install and configure FreeRADIUS, do the following:

Step 1: Download and install FreeRADIUS

Download and install FreeRADIUS on your PC according to the instructions provided by the vendor.

Note

Instructions may vary based on the product version.

For more information, visit freeradius.org (<https://freeradius.org>).

Step 2: Add the SINEC OS dictionary file

Save the SINEC OS dictionary file (`dictionary.sinecos`) under `/etc/freeradius`.

This file provides information about SINEC OS privilege levels necessary for FreeRADIUS to properly interpret authentication requests.

Step 3: Edit the `clients.conf` file

The `clients.conf` file defines the IP subnets that will be used for communication between the authenticator (SINEC OS) and the RADIUS server.

A client must be defined for every IP subnet that will be used, including the shared secret.

To edit the `clients.conf` file, do the following:

1. Edit the `client.conf` file.

```
# sudo nano /etc/freeradius/client.conf
```

2. Add each device that will communicate with the RADIUS server, including the correct shared secret.

```
client { network } {  
    ipaddr      = { IP address }  
    secret      = { secret }  
}
```

3. Save and exit the file.

Step 4: Define authorized users and MAC addresses

The users file defines each user that can be authenticated. Any user not defined will be automatically rejected.

1. Edit the users file.

```
# sudo nano users
```

2. Add an entry for each authorized user as follows:

```
{ username } Cleartext-Password := "{ password }"
    Service-Type = Login-User,
    Siemens-Automation-Privileged-User-Group = { admin |
guest }
```

For example:

```
newadmin Cleartext-Password := "$ecurePa8sword"
    Service-Type = Login-User,
    Siemens-Automation-Privileged-User-Group = admin
```

3. Add an entry for each authorized MAC address as follows:

```
"{ MAC address }" Cleartext-Password := "{ password }"
    Service-Type == Call-Check,
    Tunnel-Type = 13,
    Tunnel-Medium-Type = 6,
    Tunnel-Private-Group-ID = "{ ID }"
```

For example:

```
"00-13-3B-21-0F-60" Cleartext-Password := "00-13-3B-21-0F-60"
    Service-Type == Call-Check,
    Tunnel-Type = 13,
    Tunnel-Medium-Type = 6,
    Tunnel-Private-Group-ID = "4099"
```

Step 5: Configure EAP-TLS authentication

1. Update certificates used by the EAP-TLS/PEAP-MSCHAPv2 authentication process. Replace the following certificates under `/etc/freeradius/{ version }/certs`:

- ca.crt
- server_rt.crt
- server_rt.key

2. Open the **eap.conf** file.

```
# sudo nano /etc/freeradius/{ version }/mods-available/eap
```

3. Make sure the following default settings are configured:

- `default_eap_type` - Set to `tls`
- `Private_key_password` - Set to the private key password that is used to generate the private key for the server certificate
- `Private_key_file` - Set to the location for the server certificate's private key file
- `Certificate_file` - The location of the server certificate
- `Ca_file` - The location of the CA certificate

4. Save and exit the file.

Step 6: Restart the FreeRADIUS service

Execute the following command to restart the FreeRADIUS service:

```
# freeradius -X
```

7.4.3.3 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, enter the following command in operational mode:

```
system radius server { name } check-server-credentials
```

Example

The following is a successful test.

```
localhost# system radius server MY-RADIUS check-server-credentials  
server-credential-verification true
```

Example

The following is an unsuccessful test.

```
localhost# system radius server MY-RADIUS check-server-credentials  
server-credential-verification false
```

7.4.4 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 the connection with an external RADIUS server.

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Set the user authentication mode.</p> <p>Options include:</p> <ul style="list-style-type: none"> <code>local-users</code> - Users are authenticated locally <code>radius</code> - Users are authenticated by an external RADIUS server <p>These options can be combined to define a fallback scenario should one authentication service fail (e.g. server is unreachable). Combinations include:</p> <ul style="list-style-type: none"> <code>local-users radius</code> Users are first authenticated locally. If the user is unknown, credentials are forwarded to an external RADIUS server. <code>radius local-users</code> Users are first authenticated by an external RADIUS server. If the server is unreachable, users are then authenticated locally. <p>Default: <code>local-users</code></p> <p>To enter the authentication mode, press Enter after <code>auth-order</code> and then enter the authentication modes in order. The first mode listed is the primary mode.</p> | <pre>system authentication auth-order < Enter > [list] ({ Current Mode }): [local-users radius] [local- users radius]</pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <pre>show running-config system authentication auth-order</pre> |

Example

The following enables RADIUS authentication for all users.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication auth-order
[list] (local-users): radius
localhost(config-system-authentication)# commit
Commit complete.
localhost(config-system-authentication)# end
localhost# show running-config system authentication auth-order
system
 authentication
  auth-order [ radius ]
exit

exit
```

Example

The following enables RADIUS authentication for all users, but also enables local authentication should the RADIUS server(s) be unreachable.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication auth-order
[list] (local-users): radius local-users
localhost(config-system-authentication)# commit
Commit complete.
localhost(config-system-authentication)# end
localhost# show running-config system authentication auth-order
system
  authentication
    auth-order [ radius local-users ]
  exit

exit
```

Example

The following enables local authentication for all users, but also enables RADIUS authentication should local authentication fail.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system authentication auth-order
[list] (local-users): local-users radius
localhost(config-system-authentication)# commit
Commit complete.
localhost(config-system-authentication)# end
localhost# show running-config system authentication auth-order
system
  authentication
    auth-order [ local-users radius ]
  exit

exit
```

7.4.5 Monitoring user authentication

This section describes how to monitor aspects of user authentication.

7.4.5.1 Displaying RADIUS statistics

The RADIUS client collects the following statistics for each RADIUS server defined.

Note

All RADIUS statistics are cleared automatically when the device is reset.

To display RADIUS client statistics, enter one of the following commands in operational mode:

- `show system radius server statistics`
Displays the statistics for all RADIUS servers.
- `show system radius server statistics [accepted | rejected | lost]`
Displays only the statistic specified for all RADIUS servers.
- `show system radius server { server } statistics`
Displays the statistics for a specific RADIUS server.
- `show system radius server { server } statistics [accepted | rejected | lost]`
Displays only the statistic specified for the selected RADIUS server.

Examples

The following displays statistics for all RADIUS server profiles defined.

```
localhost# show system radius server statistics
server RADIUS1
  statistics accepted 3
  statistics rejected 5
  statistics lost 0
server RADIUS2
  statistics accepted 0
  statistics rejected 0
  statistics lost 0
```

The following displays only the number of rejected logins for all RADIUS server profiles.

```
localhost# show system radius server statistics rejected
server RADIUS1
  statistics rejected 5
server RADIUS2
  statistics rejected 0
```

The following displays statistics only for the **RADIUS1** server profile.

```
localhost# show system radius server RADIUS1 statistics
  statistics accepted 3
  statistics rejected 5
  statistics lost 0
```

The following displays only the number of accepted logins for the **RADIUS1** server profile.

```
localhost# show system radius server RADIUS1 statistics accepted
server RADIUS1
  accepted 3
```

Description

The following information is shown:

| Statistic | Description |
|-----------|---|
| 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. |

7.5 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.

7.5.1 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 specific 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 limits access to the CLI. A second rule applies specifically to a remote host within that range, 1.1.1.16/32, and limits 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.

7.5.2 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 240)".
2. Enable the management ACL.
For more information, refer to "Enabling the management ACL (Page 245)".

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 242)".
- Restrict the authorized manager to accessing a specific user interface or interfaces
For more information, refer to "Restricting access based on user interface (Page 243)".

7.5.2.1 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 34)".

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Add the rule by entering the IP address and prefix length of a remote host.</p> <p>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.</p> <p>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.</p> | <pre>system management-acl ip-source ipv4 { IP address }/{ prefix length }</pre> |

| Step | Instruction | Command |
|------|---|--|
| 3 | <p>[Optional] Limit the authorized manager to using one or more VLANs by specifying the VLAN interface or interfaces.</p> <p>By default, inbound traffic from an authorized manager is permitted on all VLAN interfaces.</p> <p>Repeat this step as needed to allow the authorized manager to use multiple VLAN interfaces.</p> <p>A VLAN interface can also be added after the authorized manager is added.</p> <p>For more information about changing the interface used by an existing authorized manager, refer to "Restricting access based on VLAN interface (Page 242)".</p> | <pre>interface { VLAN interface }</pre> |
| 4 | <p>[Optional] Limit the authorized manager to use a specific user interface or interfaces when accessing the device.</p> <p>By default, authorized managers can use any of the following user interfaces:</p> <ul style="list-style-type: none"> • Web UI • NETCONF • SNMP • CLI <p>Only select the user interfaces you want the authorized manager to access. All others are inaccessible.</p> <p>Multiple management interfaces can be selected at the same time by writing a comma-separated list.</p> <p>For example, the following restricts the authorized managers from accessing the Web UI: <code>netconf, snmp, cli</code></p> <p>Allowed user interfaces can also be redefined after the authorized manager is added.</p> <p>For more information about redefining allowed user interfaces for an existing authorization manager, refer to "Restricting access based on user interface (Page 243)".</p> | <pre>service [webui netconf snmp cli]</pre> |
| 5 | Commit the change. | <code>commit</code> |
| 6 | Exit configuration mode. | <code>end</code> |
| 7 | Verify the configuration. | <pre>show running-config system management-acl ip-source ipv4 { IP address }/{ prefix length }</pre> |

Example

The following adds a rule that restricts a remote host to sending traffic on VLANs 10 and 11. It also prevents the host from accessing the Web UI (webui) and SNMP user interfaces.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-acl ip-source ipv4 172.30.145.145/32
localhost(config-mgmt-acl-172.30.145.145/32)# interface vlan10
localhost(config-mgmt-acl-172.30.145.145/32)# interface vlan11
localhost(config-mgmt-acl-172.30.145.145/32)# service netconf,cli
localhost(config-mgmt-acl-172.30.145.145/32)# commit
Commit complete.
localhost(config-mgmt-acl-172.30.145.145/32)# end
localhost# show running-config system management-acl
system
management-acl
no enabled
ip-source ipv4 172.30.145.145/32
interface [ vlan10 vlan11 ]
service netconf,cli
exit

exit

exit
```

7.5.2.2 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:

Note

To allow an authorized manager to use more than one VLAN, repeat the following procedure for each VLAN interface.

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Select a VLAN interface for the target authorized manager. | system management-acl ip-source ipv4 { IP address }/{ prefix length } interface { VLAN interface } |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------|---|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system management-acl ip-source ipv4 { IP address }/{ prefix length } |

Example

The following restricts an existing authorized manager to VLAN 10.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-acl ip-source ipv4 172.30.145.145/32
interface vlan10
localhost(config-mgmt-acl-172.30.145.145/32)# commit
Commit complete.
localhost(config-mgmt-acl-172.30.145.145/32)# end
localhost# show running-config system management-acl ip-source ipv4
172.30.145.145/32
system
management-acl
  enabled
  ip-source ipv4 172.30.145.145/32
  interface [ vlan10 ]
    service cli,netconf,snmp,webui
  exit
exit
exit
```

7.5.2.3 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

To restrict or allow an existing authorized manager to use a specific user interface or interfaces, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Restrict the authorized manager to use a specific user interface or interfaces when accessing the device. Multiple user interfaces can be selected at the same time by writing a comma-separated list. For example, the following restricts the authorized managers from accessing the Web UI: <code>netconf, snmp, cli</code> | <code>system management-acl ip-source ipv4 { IP address }/{ prefix length } service [webui netconf snmp cli]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-acl ip-source ipv4 { IP address }/{ prefix length }</code> |

Example

The following restricts an existing authorized manager from using the NETCONF and SNMP user interfaces.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-acl ip-source ipv4 172.30.145.145/32
service webui,cli
localhost(config-mgmt-acl-172.30.145.145/32)# commit
Commit complete.
localhost(config-mgmt-acl-172.30.145.145/32)# end
localhost# show running-config system management-acl ip-source ipv4
172.30.145.145/32
system
management-acl
enabled
ip-source ipv4 172.30.145.145/32
service webui,cli
exit

exit

exit
```

7.5.2.4 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.

| Step | Instruction | Command |
|------|----------------------------|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable the management ACL. | system management-acl enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system management-acl |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-acl enabled
localhost(config-mgmt-acl)# commit
Commit complete.
localhost(config-mgmt-acl)# end
localhost# show running-config system management-acl
system
management-acl
  enabled
  ip-source ipv4 172.30.145.145/32
  interface [ vlan10 vlan11 ]
  service netconf,cli
exit

exit
```

7.5.3 Monitoring the management ACL

This section describes the various methods for monitoring the management ACL.

7.5.3.1 Displaying the operational state of the management ACL

To display the operational state of the management ACL, enter the following command in operating mode:

```
show system management-acl
```

Example

```
localhost# show system management-acl
management-acl
admin true
ip-source ipv4 172.30.145.145/32
service-id cli,netconf,snmp
interface-name [ vlan10 vlan11 ]
```

Description

The following information is displayed, if configured:

| Parameter | Description |
|-------------------------------|--|
| admin | Indicates the status of the management ACL. Possible values include: <ul style="list-style-type: none"> • true - The management ACL is enabled • false - The management ACL is disabled |
| ip-source ipv4 { IP address } | The IP address of an authorized manager. |
| service-id | The management interface or interfaces the authorized manager can use when accessing the device. Possible values include: <ul style="list-style-type: none"> • webui • netconf • snmp • cli |
| interface-name | The VLAN interface or interfaces on which the authorized manager send traffic to a management interface. |

7.5.4 Configuration examples

The following configuration examples demonstrate different ways to configure authorized managers in the management ACL.

7.5.4.1 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:

| IP address | VLAN interface | Management interfaces |
|-------------|----------------|-----------------------|
| 1.1.1.0/24 | all | netconf,snmp,cli |
| 1.1.1.10/32 | all | webui |
| 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.

Configuration

```
localhost# config
localhost(config)# system management-acl ip-source ipv4 1.1.1.0/24
service netconf, snmp, cli
localhost(config-mgmt-acl-1.1.1.0/24)# top
localhost(config)# system management-acl ip-source ipv4 1.1.1.10/32
service webui
localhost(config-mgmt-acl-1.1.1.10/32)# top
localhost(config)# system management-acl ip-source ipv4 2.2.2.20/32
service cli
localhost(config-mgmt-acl-2.2.2.20/32)# top
localhost(config)# system management-acl ip-source ipv4 2.2.2.0/24
service netconf, snmp
localhost(config-mgmt-acl-2.2.2.0/24)# commit
Commit complete.
localhost(config-mgmt-acl-2.2.2.0/24)# end
localhost# show system management-acl
management-acl
  admin true
  ip-source ipv4 1.1.1.0/24
    service-id netconf, snmp, cli
  ip-source ipv4 1.1.1.10/32
    service-id webui
  ip-source ipv4 2.2.2.20/32
    service-id cli
  ip-source ipv4 2.2.2.0/24
    service-id netconf, snmp
```

7.6 Port security

SINEC OS supports port security, or Port Access Control (PAC), to control network access through specific bridge ports.

Note

Port security and RADIUS authentication

You must enable port security for one or more bridge ports if the server type for either the primary or secondary RADIUS server is set to `dot1x`.

For more information about configuring a RADIUS server profile, refer to "Configuring RADIUS authentication (Page 229)".

7.6.1 Understanding port security

Port security provides the ability to authenticate network access via individual bridge ports through one of the following methods:

- **Static MAC address-based authentication**
This method authenticates frames based on their source MAC address. If the source MAC address is listed in the Static MAC Address table, the endpoint is authenticated.
A secure bridge port can be configured to accept frames from MAC addresses in the Static MAC Address table, or configured to learn *N* number of MAC addresses from the frames it receives. Learned MAC addresses are added automatically to the Static MAC Address table and can only be removed explicitly manually.
For more information, refer to "Static MAC address-based authentication (Page 249)".
- **IEEE 802.1X authentication**
This method authenticates an endpoint or user against a external RADIUS authentication server. Access is granted if the endpoint or user provides the proper credentials.
For more information, refer to "IEEE 802.1X authentication (Page 249)".
- **IEEE 802.1X authentication with MAB**
This method first employs IEEE 802.1X authentication. If the endpoint does not support IEEE 802.1X, SINEC OS uses MAC Authentication Bypass (MAB) to authenticate the device based on its MAC address.
For more information, refer to "IEEE 802.1X authentication with MAB (Page 250)".

| |
|--|
| NOTICE |
| Security hazard - risk of unauthorized access and/or exploitation |
| Do not apply port security on core switch connections. Port security is applied at the network edge to restrict external access to specific devices. |

7.6.1.1 Static MAC address-based authentication

The static MAC address-based authentication method validates the source MAC address of each received frame against the contents of the Static MAC Address table. SINEC OS also supports a highly flexible port security configuration that provides a convenient means for network administrators to use the feature in various network scenarios.

A static MAC address can be added to the Static MAC Address table without explicitly specifying a bridge port. In this case, the configured MAC address will be automatically authorized on the bridge port where it is detected. This allows endpoints to be connected to any secure bridge port on the switch without requiring any reconfiguration.

SINEC OS can also be programmed to learn (and, thus, authorize) a pre-configured number of source MAC addresses first encountered by a secure bridge port. This enables the capture of the appropriate secure addresses when first configuring MAC address-based authorization on a port. Those MAC addresses are automatically inserted into the Static MAC Address table and remain there until they are removed manually.

7.6.1.2 IEEE 802.1X authentication

The IEEE 802.1X standard defines a mechanism for port-based network access control and provides a means of authenticating and authorizing endpoints connected to secure bridge ports.

Although IEEE 802.1X is mostly used in wireless networks, this method is also implemented in wired switches.

The IEEE 802.1X standard defines three major components of the authentication method: supplicant, authenticator, and authentication server. SINEC OS functions as the authenticator.

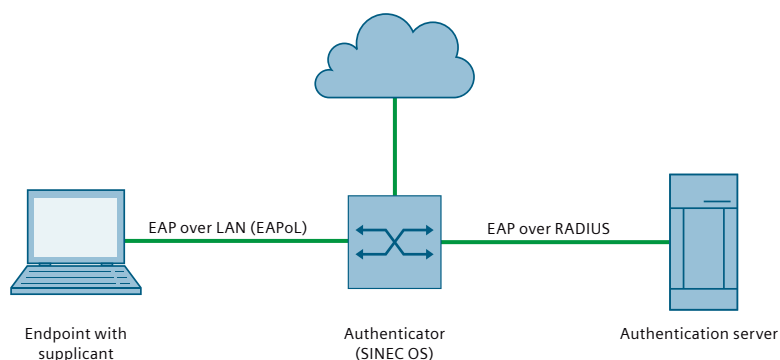


Figure 7-4 IEEE 802.1X authentication components

IEEE 802.1X makes use of the Extensible Authentication Protocol (EAP), an authentication protocol that expands the authentication methods used by the Point-to-Point Protocol (PPP). IEEE 802.1X defines a protocol for communication between the supplicant and the authenticator, referred to as EAP over LAN (EAPoL).

SINEC OS communicates with the authentication server using EAP over RADIUS.

NOTICE

Security hazard - risk of unauthorized access and/or exploitation

SINEC OS supports both Protected Extensible Authentication Protocol (PEAP), EAP Transport Layer Security (EAP-TLS), and EAP-MD5. The MD5 hash function in EAP-MD5 is vulnerable to dictionary attacks and man-in-the-middle attacks. PEAP and EAP-TLS are more secure and are recommended over EAP-MD5 if supported by the supplicant.

Note

If the MAC address of the source device is configured in the Static MAC Address table, it will be authorized, even if the endpoint is rejected by the authentication server.

7.6.1.3 IEEE 802.1X authentication with MAB

This method combines IEEE 802.1X authentication with MAC Authentication Bypass (MAB). MAB is an access control protocol that uses an endpoint's MAC address to verify the supplicant's identity before authorizing access. It is used as a fallback when a supplicant does not support IEEE 802.1X, such as a printer or IP phone.

IEEE 802.1X with MAB works as follows:

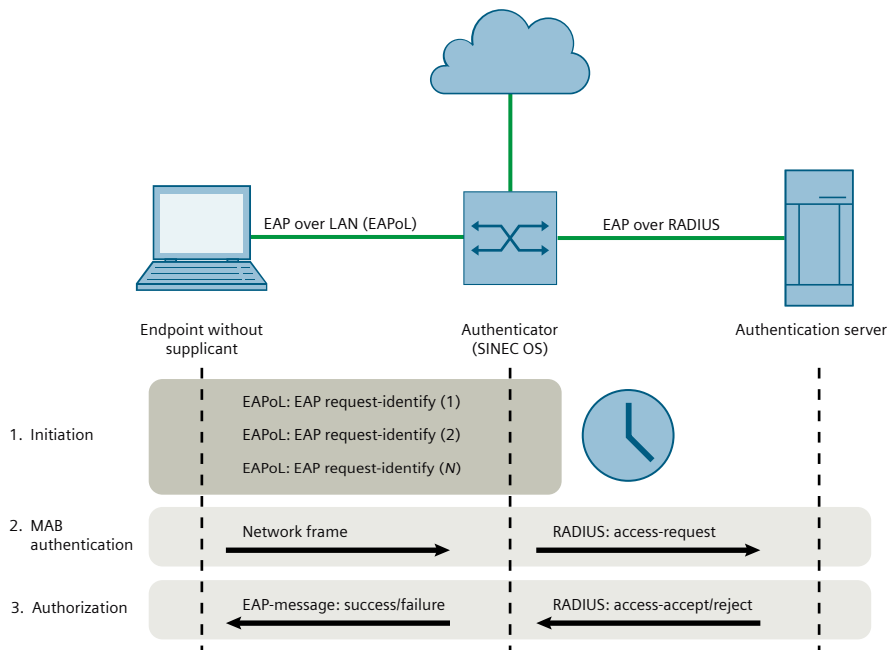


Figure 7-5 IEEE 802.1X authentication with MAB

1. Initiation

SINEC OS forwards an EAPoL identity request to the endpoint. If the endpoint responds within the allotted time, the IEEE 802.1X authentication method is applied. However, if the endpoint does not respond within the allotted time and after the maximum number of attempts are reached, SINEC OS determines the endpoint does not have a supplicant. SINEC OS then attempts to use MAB to authenticate the endpoint.

2. MAB authentication

SINEC OS accepts a single frame from the bridge port to determine the endpoint's MAC address. Once the MAC address is determined, the frame is discarded and SINEC OS forwards a RADIUS access-request message to the authentication server. The message includes the MAC address as the username and password.

3. Authorization

The authentication server determines if the supplicant can be granted access and at what level. It communicates its decision back to the authenticator (SINEC OS) by forwarding either a RADIUS access-accept or access-reject message.

NOTICE

Security hazard - risk of unauthorized access and/or exploitation

SINEC OS supports both Protected Extensible Authentication Protocol (PEAP), EAP Transport Layer Security (EAP-TLS), and EAP-MD5. The MD5 hash function in EAP-MD5 is vulnerable to dictionary attacks and man-in-the-middle attacks. PEAP and EAP-TLS are more secure and are recommended over EAP-MD5 if supported by the supplicant.

Note

SINEC OS only supports single-host mode for MAB authentication. A security violation is flagged if more than one source MAC address is detected on a secure bridge port after an endpoint has been authenticated using MAB.

7.6.1.4 Restricted VLANs

You can configure secure bridge ports to go into Quarantine or Guest VLAN mode when the authentication of a supplicant with IEEE 802.1X or IEEE 802.1X with MAB fails. This automatically limits services to the supplicant.

For example, an administrator may choose to restrict access to only printers, Internet, or specific downloads for unauthenticated users. When a supplicant fails to authenticate after a set number of attempts, the configured bridge port will switch automatically to either

Quarantine or Guest VLAN mode, depending on the port security mode and the supplicant's security setup:

- If the supplicant supports IEEE 802.1X but has failed to authenticate, the bridge port will become a member of the Quarantine VLAN
- If the supplicant does not support IEEE 802.1X and the bridge port is set to use IEEE 802.1X authentication protocols, the bridge port will become a member of the Guest VLAN after the authentication fails
- If the supplicant does not support IEEE 802.1X and the bridge port is set to use IEEE 802.1X authentication with MAB authentication protocols, the bridge port will become a member of the Quarantine VLAN after the authentication fails

An alarm is generated when a secure bridge port becomes a member of the Quarantine or Guest VLAN.

When a secure bridge port is a member of the Quarantine VLAN, SINEC OS will attempt to reauthenticate the supplicant at configured intervals. If the supplicant supports IEEE 802.1X, the IEEE 802.1X authentication method will be used. Otherwise, the IEEE 802.1X authentication with MAB will be used.

Supplicants that fail to authenticate remain in the Quarantine VLAN until successfully re-authenticated, or until the physical link goes down. If re-authentication fails, the port remains a member of the Quarantine VLAN.

There are no re-authentication attempts for supplicants when a secure bridge port is a member of the Guest VLAN.

When an EAPoL start frame is received from the supplicant, the bridge port will revert to the unauthenticated state and revoke its membership with the Guest VLAN. The authentication process can then begin anew.

The following outlines Quarantine vs Guest VLAN membership behavior following authentication failure:

| Security mode | Supplicant support for IEEE 802.1X | VLAN after authentication failure |
|-------------------------------------|------------------------------------|-----------------------------------|
| IEEE 802.1X authentication | IEEE 802.1X compatible | Quarantine VLAN |
| | IEEE 802.1X incompatible | Guest VLAN |
| IEEE 802.1X authentication with MAB | IEEE 802.1X compatible | Quarantine VLAN |
| | IEEE 802.1X incompatible | Quarantine VLAN |

7.6.1.5 Assigning VLANs with tunnel attributes

SINEC OS supports assigning a VLAN to a secure bridge port using tunnel attributes, as defined in RFC 3850 (<http://tools.ietf.org/html/rfc3580>), when the security mode is set to either:

- IEEE 802.1X authentication
- IEEE 802.1X authentication with MAB

In some cases, it may be desirable to allow a secure bridge port to be placed in a specific VLAN, based on the authentication result. For example:

- To allow a specific endpoint, based on its source MAC address, to remain on the same VLAN as it moves within a network, configure SINEC OS devices to use either security mode
- To allow a specific user, based on the user's login credentials, to remain on the same VLAN when the user logs in from different locations, configure SINEC OS devices to use the IEEE 802.1X authentication with MAB security mode

When a RADIUS authentication server wants to use this feature, it indicates the desired VLAN by including tunnel attributes in the RADIUS access-accept message. The server uses the following tunnel attributes for VLAN assignment:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Note the VLANID is 12-bits and takes a value between 1 and 4094, inclusive. The Tunnel-Private-Group-ID is a string as defined in RFC 2868 (<http://tools.ietf.org/html/rfc2868>), so the VLANID integer value is encoded as a string.

If the tunnel attributes are not returned by the authentication server, the VLAN assigned to the bridge port remains unchanged.

7.6.1.6 Static VLAN requirement

A RADIUS server may require an IEEE 802.1X client on a given port be assigned to a static VLAN. Review the configuration of your RADIUS server to confirm.

If the required static VLAN does not exist on the switch or the VLAN is dynamically created (by GVRP), client authentication will fail.

7.6.2 Configuring port security

Port security is configurable for individual bridge ports.

To configure port security for a bridge port, do the following:

1. Enable port security.
Port security is disabled by default for each bridge port.
For more information, refer to "Enabling port security (Page 254)".
2. Set the security mode.
For more information, refer to "Setting the security mode (Page 255)".
3. Set the Quarantine VLAN ID.
Only applicable when the IEEE 802.1X authentication or IEEE 802.1X authentication with MAB security mode is set.
For more information, refer to "Setting the Quarantine VLAN ID (Page 256)".
4. Set the Guest VLAN ID.
Only applicable when the security mode is set to IEEE 802.1X authentication.
For more information, refer to "Setting the Guest VLAN ID (Page 257)".

5. Review and configure the IEEE 802.1X settings.
Only applicable when the IEEE 802.1X authentication or IEEE 802.1X authentication with MAB security mode is set.
For more information, refer to "Configuring IEEE 802.1X (Page 262)".
6. [Optional] Enable sticky mode.
Only applicable when the static MAC addressed-based security mode is set.
Sticky mode makes sure MAC addresses dynamically learned by the bridge port are not switched to another secure bridge port.
This option is enabled by default.
For more information, refer to "Enabling sticky mode (Page 258)".
7. [Optional] Limit the number of MAC addresses the port can learn dynamically.
Only applicable when the static MAC addressed-based security mode is set.
For more information, refer to "Setting the maximum number of dynamically learned MAC addresses (Page 259)".
8. [Optional] Enable administrative shutdown mode.
This mode shuts down the bridge port in case of a security violation.
This option is disabled by default.
For more information, refer to "Enabling administrative shutdown mode (Page 260)".
9. [Optional] Set the administrative shutdown timer.
Secure bridge ports that were shutdown previously as the result of a security violation are re-enabled once the timer expires.
For more information, refer to "Setting the administrative shutdown timer (Page 261)".

7.6.2.1 Enabling port security

Port security is disabled by default for all bridge ports.

To enable port security for a bridge port, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable port security for the selected bridge port. | <code>interface { bridge port } port-security enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } port-security</code> |

Example

The following enables port security for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security enabled
localhost(config-interface-ethernet0/1-port-security)# commit
Commit complete.
localhost(config-interface-ethernet0/1-port-security)# end
localhost# show running-config interface ethernet0/1 port-security enabled
interface ethernet0/1
  port-security
    enabled
  exit

exit
```

7.6.2.2 Setting the security mode

To set the security mode, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the security mode for the selected bridge port. Options include: <ul style="list-style-type: none"> • <code>per-macaddress</code> - The static MAC address-based authentication method is used • <code>dot1x</code> - The IEEE 802.1X authentication method is used • <code>dot1x-mac-auth</code> - IEEE 802.1X with MAB authentication is used Default: <code>dot1x</code> For more information about these modes, refer to "Understanding port security (Page 248)". | <code>interface { bridge port } port-security security-mode [dot1x dot1x_mac_auth per-macaddress]</code> |
| 3 | If the security mode is set to either <code>dot1x</code> or <code>dot1x-mac-auth</code> , make sure the RADIUS server type is set to <code>dot1x</code> for the primary and secondary RADIUS server profiles. For more information, refer to "Configuring a RADIUS server profile (Page 229)". | - |
| 4 | Commit the change. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config interface { bridge port } port-security security-mode</code> |

Example

The following configures ethernet0/1 to use the IEEE 802.1X authentication (dot1x) security mode.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security security-mode dot1x
localhost(config-interface-ethernet0/1-port-security)# commit
Commit complete.
localhost(config-interface-ethernet0/1-port-security)# end
localhost# show running-config interface ethernet0/1 port-security
security-mode
interface ethernet0/1
  port-security
    security-mode dot1x
  exit

exit
```

7.6.2.3 Setting the Quarantine VLAN ID

The Quarantine VLAN ID indicates the VLAN the bridge port will switch to when a supplicant fails to authenticate. A bridge port will switch to a Quarantine VLAN under the following conditions:

- The security mode is set to either `dot1x` or `dot1x-mac-auth`
- The supplicant fails to authenticate with the authentication server

For more information about Quarantine VLANs, refer to "Restricted VLANs (Page 251)".

Note

The Quarantine VLAN ID must be different from the Guest VLAN ID.

To set the Quarantine VLAN ID, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Make sure the security mode is set to either <code>dot1x</code> or <code>dot1x-mac-auth</code> for the selected bridge port. For more information, refer to "Setting the security mode (Page 255)". | <code>show running-config interface { bridge port } port-security security-mode</code> |
| 2 | Enter configuration mode. | <code>config</code> |
| 3 | Set the Quarantine VLAN ID for the selected bridge port. Condition: • A number between 1 and 4096 | <code>interface { bridge port } port-security quarantine-vid { 1 - 4096 }</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config interface { bridge port } port-security quarantine-vid</code> |

Example

The following sets the Quarantine VLAN ID to 2 for ethernet0/1.

```

localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security quarantine-vid 2
localhost(config-interface-ethernet0/1-port-security)# commit
Commit complete.
localhost(config-interface-ethernet0/1-port-security)# end
localhost# show running-config interface ethernet0/1 port-security
quarantine-vid
interface ethernet0/1
  port-security
    quarantine-vid 2
  exit

exit

```

7.6.2.4 Setting the Guest VLAN ID

The Guest VLAN ID indicates the VLAN the bridge port will switch to when a supplicant fails to authenticate. A bridge port will switch to a Guest VLAN under the following conditions:

- The security mode is set to `dot1x`
- The supplicant does not support IEEE 802.1X
- The supplicant fails to authenticate with the authentication server

For more information about Guest VLANs, refer to "Restricted VLANs (Page 251)".

Note

The Guest VLAN ID must be different from the Quarantine VLAN ID.

To set the Guest VLAN ID, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Make sure the security mode is set to <code>dot1x</code> for the selected bridge port. For more information, refer to "Setting the security mode (Page 255)". | <code>show running-config interface { bridge port } port-security security-mode</code> |
| 2 | Enter configuration mode. | <code>config</code> |
| 3 | Set the Guest VLAN ID for the selected bridge port. Condition: <ul style="list-style-type: none"> • A number between 1 and 4096 | <code>interface { bridge port } port-security guest-vid { 1 - 4096 }</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config interface { bridge port } port-security guest-vid</code> |

Example

The following sets the Guest VLAN ID to 3 for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security guest-vid 3
localhost(config-interface-ethernet0/1-port-security)# commit
Commit complete.
localhost(config-interface-ethernet0/1-port-security)# end
localhost# show running-config interface ethernet0/1 port-security guest-
vid
interface ethernet0/1
  port-security
    guest-vid 3
  exit

exit
```

7.6.2.5 Enabling sticky mode

Sticky mode is available when the security mode is set to `per-macaddress`.

When enabled for a bridge port, supplicants whose MAC addresses were dynamically learned by the port can only access the network via that port. They cannot attempt to access the network through another port.

Sticky mode is enabled by default for each bridge port, but can be disabled per port as needed.

To enable sticky mode, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Make sure the security mode is set to <code>per-macaddress</code> for the selected bridge port. For more information, refer to "Setting the security mode (Page 255)". | <code>show running-config interface { bridge port } port-security security-mode</code> |
| 2 | Enter configuration mode. | <code>config</code> |
| 3 | Enable sticky mode for the selected bridge port. | <code>interface { bridge port } port-security sticky</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config interface { bridge port } port-security sticky</code> |

Example

The following enables sticky mode for ethernet0/1.

```

localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security sticky
localhost(config-interface-ethernet0/1-port-security)# commit
Commit complete.
localhost(config-interface-ethernet0/1-port-security)# end
localhost# show running-config interface ethernet0/1 port-security sticky
interface ethernet0/1
  port-security
    sticky
  exit

exit

```

7.6.2.6 Setting the maximum number of dynamically learned MAC addresses

When the security mode for a secure bridge port is set to `per-macaddress` or `dot1x`, only frames from authorized MAC addresses are forwarded. Frames from all other sources are dropped.

By default, only static MAC addresses mapped to a secure bridge port are authorized. However, some MAC addresses (or the port to which they will be connected) may not be known in advance. For these cases, you can enable a secure bridge port to receive traffic from a limited number of client devices and dynamically learn their MAC addresses. Once learned, these MAC addresses do not age out until either the device is reset or the link goes down.

A secure bridge port can dynamically learn up to 16 MAC addresses, minus any static MAC addresses mapped to the bridge port.

When the maximum number of dynamically learned MAC addresses has been reached, only frames from those MAC addresses and any static MAC addresses mapped to the port are forwarded.

To limit the number of MAC address that can be learned dynamically by a secure bridge port, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Make sure the security mode is set to either <code>per-macaddress</code> or <code>dot1x</code> for the selected bridge port. For more information, refer to "Setting the security mode (Page 255)". | <code>show running-config interface { bridge port } port-security security-mode</code> |
| 2 | Enter configuration mode. | <code>config</code> |

| Step | Instruction | Command |
|------|--|---|
| 3 | <p>Set the maximum number of MAC addresses that can be learned by the selected bridge port.</p> <p>If static MAC addresses are configured and mapped to the bridge port, the actual number of dynamically learned MAC addresses is the configured number minus the number of static MAC addresses.</p> <p>For example, if the number is set to 10 and there are 4 static MAC addresses mapped to the port, the actual number of MAC addresses that can be learned dynamically is 6.</p> <p>If the maximum number of MAC addresses that can be learned dynamically is 0, only static MAC addresses mapped to the port are permitted to forward traffic.</p> <p>Condition:</p> <ul style="list-style-type: none"> • A number between 0 and 16 <p>Default: 0</p> | <pre>interface { bridge port } port- security auto-learn { 0 - 16 }</pre> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <pre>show running-config interface { bridge port } port-security auto-learn</pre> |

Example

The following sets the maximum number of dynamically learned MAC addresses to 10 for ethernet0/1. The bridge port will learn this many MAC addresses from supplicants, minus any static MAC addresses mapped to the port.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security auto-learn 10
localhost(config-interface-ethernet0/1-port-security)# commit
Commit complete.
localhost(config-interface-ethernet0/1-port-security)# end
localhost# show running-config interface ethernet0/1 port-security auto-
learn
interface ethernet0/1
  port-security
    auto-learn 10
  exit
exit
```

7.6.2.7 Enabling administrative shutdown mode

Administrative shutdown mode automatically shuts down a secure bridge port when an ingress frame violates the port security settings. The port is either re-enabled automatically after a configurable time or reset manually.

A security violation occurs when:

- The maximum number of MAC addresses has been reached and a new endpoint (whose MAC address is not in the Static MAC Address table) sends traffic to the bridge port
- A learned MAC address is seen in the address table of another secure bridge port that is a member of the same VLAN

Administrative shutdown mode is disabled by default for each bridge port.

To enable administrative shutdown for a bridge port, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable administrative shutdown for the selected bridge port. | <code>interface { bridge port } port-security violation-shutdown</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } port-security violation-shutdown</code> |

Example

The following enables administrative shutdown mode for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security violation-shutdown
localhost(config-interface-ethernet0/1-port-security)# commit
Commit complete.
localhost(config-interface-ethernet0/1-port-security)# end
localhost# show running-config interface ethernet0/1 port-security
violation-shutdown
interface ethernet0/1
  port-security
    violation-shutdown
exit

exit
```

7.6.2.8 Setting the administrative shutdown timer

The administration shutdown timer re-enables secure bridge ports that had been shut down due to a security violation when the timer expires.

A timer is not defined by default. When the timer is not defined, the bridge port will remain shut down until manually reset by a user.

To set the administration shutdown timer, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the administration shutdown timer for the selected bridge port. Conditions: <ul style="list-style-type: none"> Formatted as nYnMnDnhmns, where n is a user-defined number Minimum of 1 second (1s) Maximum of 1 day (1d) A blank value indicates the bridge port will remain shut down until manually reset. | <code>interface { bridge port } port-security shutdown-time { time }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } port-security shutdown-time</code> |

Example

The following sets the shutdown timer to 25 minutes and 34 seconds for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security shutdown-time 25m34s
localhost(config-interface-ethernet0/1-port-security)# commit
Commit complete.
localhost(config-interface-ethernet0/1-port-security)# end
localhost# show running-config interface ethernet0/1 port-security
shutdown-time
interface ethernet0/1
  port-security
    shutdown-time 25m34s
  exit
exit
```

7.6.3 Configuring IEEE 802.1X

IEEE 802.1X settings must be configured if the security mode is set to either IEEE 802.1X authentication or IEEE 802.1X with MAB authentication.

To configure the IEEE 802.1X settings, do the following:

1. [Optional] Set the held period.
This is the time to wait for a supplicant's EAP response/identity packet before retransmitting an EAP request/identify packet.
For more information, refer to "Setting the held period (Page 263)".
2. [Optional] Set the quiet period.
This is the time to wait after a failed authorization session failed before reattempting to acquire a supplicant.
For more information, refer to "Setting the quiet period (Page 264)".
3. [Optional] Set the maximum number of times to retransmit the authentication server's EAP request/identity packet to a supplicant.
For more information, refer to "Enabling the periodic reauthentication of supplicants (Page 265)".
4. [Optional] Set the time to wait for a supplicant's response to the authentication server's EAP packet.
For more information, refer to "Setting the supplicant reauthentication timeout period (Page 266)".
5. [Optional] Set the time to wait for the authenticator's response to the authentication server's EAP packet.
For more information, refer to "Setting the maximum number of reauthentication attempts (Page 267)".
6. [Optional] Enable the periodic authentication of supplicants.
This option is disabled by default.
For more information, refer to "Setting the supplicant timeout period (Page 268)".
7. [Optional] Set the time to wait between supplicant reauthentication attempts.
For more information, refer to "Setting the authenticator timeout period (Page 269)".

7.6.3.1 Setting the held period

The held period is the configurable time SINEC OS will wait for a supplicant to respond to an authentication request. If the supplicant does not forward an EAP response/identity packet before the timer expires, SINEC OS will automatically retransmit an EAP request/identity packet to the supplicant.

To set the held period, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the held period for the selected bridge port. Conditions: <ul style="list-style-type: none"> • Formatted as nYnMnDnhmns, where n is a user-defined number • Minimum of 1 second (1s) • Maximum of 18 hours, 12 minutes, and 15 seconds (18h12m15s) Default: 1m | <code>interface { bridge port } port-security ieee802-dot1x tx-period { time }</code> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } port-security ieee802-dot1x tx-period |

Example

The following sets the held period to five minutes and 30 seconds for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security ieee802-dot1x tx-
period 5m30s
localhost(config-ieee802-dot1x)# commit
Commit complete.
localhost(config-ieee802-dot1x)# end
localhost# show running-config interface ethernet0/1 port-security ieee802-
dot1x tx-period
interface ethernet0/1
  port-security
    ieee802-dot1x
      tx-period 5m30s
    exit
  exit
exit
```

7.6.3.2 Setting the quiet period

The quiet period is the configurable time SINEC OS will wait after attempting to acquire a supplicant before attempting to acquire the supplicant again.

To set the quiet period, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Set the quiet period for the selected bridge port. Conditions: <ul style="list-style-type: none"> Formatted as nYnMnDnhmns, where n is a user-defined number Minimum of 1 second (1s) Maximum of 18 hours, 12 minutes, and 15 seconds (18h12m15s) Default: 1m | interface { bridge port } port- security ieee802-dot1x quiet- period { time } |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------|--|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } port-security ieee802-dot1x quiet-period |

Example

The following sets the quiet period to 25 minutes and 34 seconds for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security ieee802-dot1x quiet-
period 25m34s
localhost(config-ieee802-dot1x)# commit
Commit complete.
localhost(config-ieee802-dot1x)# end
localhost# show running-config interface ethernet0/1 port-security ieee802-
dot1x quiet-period
interface ethernet0/1
port-security
  ieee802-dot1x
  quiet-period 25m34s
exit

exit

exit
```

7.6.3.3 Enabling the periodic reauthentication of supplicants

Periodic reauthentication of supplicants is disabled by default for each secure bridge port. When enabled, SINEC OS will attempt to reauthenticate supplicants that were previously rejected by the authentication server. The interval and maximum number of attempts is configurable.

To enable the periodic reauthentication of supplicants, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable reauthentication of supplicants for the selected bridge port. | interface { bridge port } port- security ieee802-dot1x reauth- enable |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } port-security ieee802-dot1x reauth-enable |

Example

The following enables the reauthentication of supplicants for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security ieee802-dot1x
reauth-enable
localhost(config-ieee802-dot1x)# commit
Commit complete.
localhost(config-ieee802-dot1x)# end
localhost# show running-config interface ethernet0/1 port-security ieee-
dot1x reauth-enable
interface ethernet0/1
  port-security
    ieee802-dot1x
    reauth-enable
  exit
exit
exit
```

7.6.3.4 Setting the supplicant reauthentication timeout period

When the periodic reauthentication of supplicant's is enabled, the time between reauthentication attempts can be configured.

To set the time period between periodic authentication attempts, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Make sure the periodic reauthentication of supplicants is enabled for the selected bridge port. For more information, refer to "Enabling the periodic reauthentication of supplicants (Page 265)". | show running-config interface { bridge port } port-security ieee802-dot1x reauth-enable |
| 2 | Enter configuration mode. | config |
| 3 | Set the time between periodic authentication attempts for the selected bridge port. Condition: <ul style="list-style-type: none"> Formatted as nYnMnDnhmns, where n is a user-defined number Minimum of 1 minute (1m) Maximum of 1 day (1d) Default: 1h | interface { bridge port } port-security ieee802-dot1x reauth-period { time } |
| 4 | Commit the changes. | commit |
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config interface { bridge port } port-security ieee802-dot1x reauth-period |

Example

The following sets the reauthentication interval to 24 minutes and 30 seconds for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security ieee802-dot1x
reauth-period 25m34s
localhost(config-ieee802-dot1x)# commit
Commit complete.
localhost(config-ieee802-dot1x)# end
localhost# show running-config interface ethernet0/1 port-security ieee802-
dot1x reauth-period
interface ethernet0/1
port-security
  ieee802-dot1x
    reauth-period 24m34s
  exit
exit
exit
```

7.6.3.5 Setting the maximum number of reauthentication attempts

The number of times the authentication server's EAP request packet to the supplicant is limited. Once the maximum number of attempts has been exceeded, the authentication period times out and the supplication is not acquired.

To set the maximum number of reauthentication attempts, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Make sure the periodic reauthentication of supplicants is enabled for the selected bridge port. For more information, refer to "Enabling the periodic reauthentication of supplicants (Page 265)". | show running-config interface { bridge port } port-security ieee802-dot1x reauth-enable |
| 2 | Enter configuration mode. | config |
| 3 | Set the maximum number of reauthentication attempts for the selected bridge port. Conditions: • A number between 1 and 10 Default: 2 | interface { bridge port } port-security ieee802-dot1x max-request { 1 - 10 } |
| 4 | Commit the changes. | commit |
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config interface { bridge port } port-security ieee802-dot1x max-request |

Example

The following sets the maximum number of reauthentication attempts to three for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security ieee802-dot1x max-
request 3
localhost(config-ieee802-dot1x)# commit
Commit complete.
localhost(config-ieee802-dot1x)# end
localhost# show running-config interface ethernet0/1 port-security ieee802-
dot1x max-request
interface ethernet0/1
  port-security
    ieee802-dot1x
      max-request 3
  exit

exit

exit
```

7.6.3.6 Setting the supplicant timeout period

To set the time SINEC OS waits for a supplicant's response to an EAP request from the authentication server, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Set the time to wait for a supplicant's response for the selected bridge port. Conditions: <ul style="list-style-type: none"> Formatted as nYnMnDnhmns, where n is a user-defined number Minimum of 1 second (1s) Maximum of 18 hours, 12 minutes, and 15 seconds (18h12m15s) Default: 30s | interface { bridge port } port- security ieee802-dot1x supp- timeout { time } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } port-security ieee802-dot1x supp-timeout |

Example

The following sets the wait time to 25 minutes and 34 seconds for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security ieee802-dot1x supp-
timeout 25m 34s
localhost(config-ieee802-dot1x)# commit
Commit complete.
localhost(config-ieee802-dot1x)# end
localhost# show running-config interface ethernet0/1 port-security ieee802-
dot1x supp-timeout
interface ethernet0/1
port-security
  ieee802-dot1x
    supp-timeout 25m34s
  exit
exit
exit
```

7.6.3.7 Setting the authenticator timeout period

To set the time to wait for the authentication server's response to a supplicant's EAP packet, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Set the time to wait for a response from the authentication server for the selected bridge port. Condition: <ul style="list-style-type: none"> Formatted as nYnMnDnhmns, where n is a user-defined number Minimum of 1 second (1s) Maximum of 5 minutes (5m) Default: 30s | interface { bridge port } port-security ieee802-dot1x server-timeout { time } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } port-security ieee802-dot1x server-timeout |

Example

The following sets the wait time to three minutes for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 port-security ieee802-dot1x
server-timeout 3m
localhost(config-ieee802-dot1x)# commit
Commit complete.
localhost(config-ieee802-dot1x)# end
localhost# show running-config interface ethernet0/1 port-security ieee802-
dot1x server-timeout
interface ethernet0/1
  port-security
    ieee802-dot1x
      server-timeout 3m
  exit
exit
exit
```

7.6.4 Monitoring port security

This section describes how to monitor aspects of port security.

7.6.4.1 Displaying the security status of a bridge port

To display the security status of a bridge port, enter the following command in operational mode:

```
show interface { bridge port } port-security status
```

Example

```
localhost# show interface ethernet0/1 port-security
port-security
  status "Unauthorized; Connecting  "
```

Description

Various status messages may be displayed based on the authentication method used and the port security state.

| Authentication method | Port security state | Message |
|---|---------------------|--------------------------------|
| - | - | "Disabled" |
| Static MAC address-based authentication | Unsecure | "Unsecure" |
| | Unauthorized | "Unauthorized; Learning" |
| | Authorized | "Authorized; N MACs; Learning" |
| | Shutdown | "Shutdown" |

| Authentication method | Port security state | Message |
|---|-----------------------|--------------------------------|
| IEEE 802.1X authentication | Unsecure | "Unsecure" |
| IEEE 802.1X with MAC address-based authentication | Unauthorized | "Unauthorized; Initialize" |
| | | "Unauthorized; Disconnected" |
| | | "Unauthorized; Connecting" |
| | | "Unauthorized; Authenticating" |
| | | "Unauthorized; Authenticated" |
| | | "Unauthorized; Aborting" |
| | | "Unauthorized; Held" |
| | | "Unauthorized; Force Auth" |
| | | "Unauthorized; Quarantined" |
| | "Unauthorized; Guest" | |
| | Authorized | "Authorized;" |
| | Shutdown | "Shutdown" |

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. Slot number zero (0) indicates the port is a fixed physical port. Slot numbers 1 and greater represent the module slot where the port is located. |
| vlan{ ID } | vlan1, vlan2 | Interfaces for VLANs are named based on the VLAN ID. |
| extender0/{ Port } | extender0/1, extender0/2 | Function Extender Interface (FEI) ports are named extender , followed by the slot number (0) and associated port number. |

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, duplex mode, etc.) 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 that are initialized when a link failure occurs. 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.

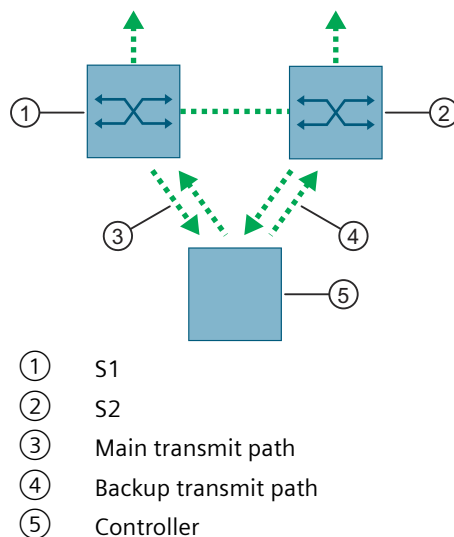


Figure 8-3 Scenario

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 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
 - 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 |

8.1.1.6 Hot swapping/hot plugging

Hot swapping allows you to exchange a media component with an exact replacement while the device is operational.

Hot plugging allows you to exchange a media component with a different component while the device is operational.

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.

Replacement/exchange during operation

SINEC OS supports replacing and exchanging SFP transceivers while the device is in operation.

After you have replaced an SFP transceiver with another SFP transceiver of the same or a different type, the new SFP transceiver is automatically configured in such a way that it works in the same operating state as the previous SFP transceiver.

Automatic detection

SINEC OS actively monitors every SFP transceiver port to determine whether a transceiver was plugged or pulled. 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 is inserted in a slot that supports 100Base-X and 1000Base-X, 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

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 279)".
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 10/100/1000Base-T copper Ethernet ports.
For more information, refer to "Enabling auto-negotiation (Page 280)".
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 more information, refer to "Selecting the bridge port speed (Page 281)".
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.
For more information, refer to "Selecting the duplex mode (Page 283)".
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 285)".
6. [Optional] Configure the interface to disable automatically on a link down event.
For more information, refer to "Configuring the action for link down events (Page 286)".
7. [Optional] Enable Link Fault Indication (LFI).
This feature detects link fault conditions at the other end of the link. It is only compatible with 1000Base-X and 100Base-FX bridge ports.
For more information, refer to "Enabling Link Fault Indication (LFI) (Page 286)".
8. [Optional] Enable alarms to be triggered on a link down/up event.
For more information, refer to "Enabling link up/down traps (Page 287)".
9. [Optional] Enable Smart SFP (for SFP ports only).
For more information, refer to "Enabling Smart SFP (for SFP ports only) (Page 288)".
10. Make sure the bridge port is enabled.
For more information, refer to "Enabling a bridge port (Page 289)".

See also

Configuring a static IPv4 address (Page 315)

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Add a description for the selected bridge port. Conditions: <ul style="list-style-type: none"> • Must be between 0 and 64 characters long • Quotation marks are required if the description contains spaces | <code>interface { bridge port } description { description }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } description</code> |

Example

The following adds a description for `ethernet0/1`.

```
localhost# config
localhost(config)# interface ethernet0/1 description "1G Server Link"
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 description
interface ethernet0/1
  description "1G Server Link"
exit
```

8.1.2.2 Enabling auto-negotiation

To enable auto-negotiation for a bridge port, do the following:

| NOTICE |
|---|
| <p>Restrictions</p> <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 "Displaying the auto-negotiation capability of each bridge port (Page 300)". • 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 automatically for all bridge 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`).

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable auto-negotiation for the selected bridge port. | <code>interface { bridge port } ethernet auto-negotiation</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } ethernet auto- negotiation</code> |

Example

```
localhost# config
localhost(config)# interface ethernet0/1 ethernet auto-negotiation
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 ethernet auto-
negotiation
interface ethernet0/1
  ethernet
    auto-negotiation
  exit
exit
```

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/requirements**

Some restrictions/requirements apply based on the port's media type. Note the following:

- Auto-negotiation must be enabled for bridge ports that have a port speed of 1 Gbps or higher
- The speed must be set to 0.1 for all 100BASE-FX bridge ports
- The speed must be set to 1.0 for all 1000BASE-X bridge ports
- The speed must be set to 10.0 for all 10GBASE-X bridge ports

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Select the speed for the selected bridge port. Based on the maximum speed supported by the port, options may include:</p> <ul style="list-style-type: none"> • 0.0 - Frames are sent at the speed determined through auto-negotiation • 0.01 - Frames are sent at 10 Mbps • 0.1 - Frames are sent at 100 Mbps • 1.0 - Frames are sent at 1 Gbps • 2.5 - Frames are sent at 2.5 Gbps • 5.0 - Frames are sent at 5 Gbps • 10.0 - Frames are sent at 10 Gbps <p>If auto-negotiation is enabled, the interface advertises the selected option as its speed capability to its link partner.</p> <p>If auto-negotiation is disabled, the interface operates at the speed in which it is capable.</p> <p>Default: dependant on media type</p> | <pre>interface { bridge port } ethernet speed [0 0.01 0.1 1 2.5 5.0 10.0]</pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } ethernet speed</code> |

Example

The following sets the speed for ethernet0/1 to 1.0, or 1 Gbps.

```
localhost# config
localhost(config)# interface ethernet0/1 ethernet speed 1.0
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 ethernet speed
interface ethernet0/1
  ethernet
    speed 1.0
  exit

exit
```

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

Restrictions/requirements

Some restrictions/requirements apply based on the port's media type. Note the following:

- Duplex must be set to `full` for all bridge ports that have a port speed of 1 Gbps or higher
- Duplex must cannot be set to `auto` for 100Base-X bridge ports

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select the duplex mode for the selected bridge port. Options include: <ul style="list-style-type: none"> • <code>auto</code> - The duplex mode is determined through auto-negotiation. • <code>half</code> - 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 <code>speed</code> is set to <code>1.0</code>. • <code>full</code> - Communication between the interface and its link partner can occur simultaneously in both directions (bi-directional). Default: dependant on media type | <code>interface { bridge port }</code> <code>ethernet duplex [auto half full]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } ethernet speed</code> |

Example

The following sets `ethernet0/1` into full duplex mode.

```
localhost# config
localhost(config)# interface ethernet0/1 ethernet duplex full
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# exit
localhost# show running-config interface ethernet0/1 ethernet duplex
interface ethernet0/1
  ethernet
    duplex full
  exit

exit
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable downshift for the selected bridge port. | <code>interface { bridge port } ethernet down-shift</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } ethernet down- shift</code> |

Example

```
localhost# config
localhost(config)# interface ethernet0/1 ethernet down-shift
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 ethernet down-shift
interface ethernet0/1
  ethernet
  down-shift
  exit
exit
```

8.1.2.6 Enabling Link Fault Indication (LFI)

Link Fault Indication (LFI) allows a 1000BASE-X or 100BASE-FX bridge port to detect faults that occur on the other end of the link.

NOTICE

Requirements

- LFI is only compatible with 1000Base-X and 100Base-FX bridge ports. LFI is disabled for all other media types.
- Auto-negotiation must be disabled on any bridge port that has LFI enabled.
- 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.

To enable LFI for a bridge port, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Make sure auto-negotiation is disabled for the selected bridge port | <code>no interface { bridge port } ethernet auto-negotiation</code> |
| 3 | Enable LFI for the selected bridge port. | <code>interface { bridge port } ethernet lfi</code> |
| 4 | Commit the change. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config interface { bridge port } ethernet lfi</code> |

Example

```
localhost# config
localhost(config)# no interface ethernet0/1 ethernet auto-negotiation
localhost(config)# interface ethernet0/1 ethernet lfi
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 ethernet lfi
interface ethernet0/1
  ethernet
    lfi
  exit
exit
```

8.1.2.7 Configuring the action for link down events

A bridge port can be configured to perform a specific action when its link partner is down.

To configure a bridge port to perform a specific action on a link down event, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Set the selected bridge port to perform a specific action on a link down event. Options include: <ul style="list-style-type: none"> • none - The interface performs no action. • disable-port - The interface administratively disables itself. This prevents the physical port from being connected to unauthorized link partner. The port can only be re-enabled by an administrator. Default: none | interface { bridge port } ethernet link-down-action [none disable-port] |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } ethernet link-down-action |

Example

```
localhost# config
localhost(config)# interface ethernet0/1 ethernet link-down-action disable-port
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 ethernet link-down-action
interface ethernet0/1
  ethernet
    link-down-action disable-port
  exit
exit
```

8.1.2.8 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:

| Step | Instruction | Command |
|------|----------------------------------|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable the selected bridge port. | interface { bridge port } link-up-down-trap |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } link-up-down-trap |

Example

```
localhost# config
localhost(config)# interface ethernet0/1 link-up-down-trap-enable enabled
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 link-up-down-trap-enable
interface ethernet0/1
  link-up-down-trap
exit
```

8.1.2.9 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.

To enable Smart SFP, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable Smart SFP for an SFP transceiver port. | interface { SFP transceiver port } sfp autoconfig |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { SFP transceiver port } sfp autoconfig |

Example

In this example, Smart SFP is enabled for ethernet0/11.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/11 sfp autoconfig
localhost(config-interface-ethernet0/11-sfp)# commit
Commit complete.
```



```
localhost(config-interface-ethernet0/11-sfp)# end
localhost# show running-config interface ethernet0/11 sfp autoconfig
interface ethernet0/11
  sfp
  autoconfig
  exit

exit
```

8.1.2.10 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. | |

| Step | Instruction | Command |
|------|----------------------------------|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable the selected bridge port. | interface { bridge port } enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } enabled |

Example

```
localhost# config
localhost(config)# interface ethernet0/1 enabled
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1
interface ethernet0/1
  enabled
  exit
```

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.

8.1 Interfaces

To configure a VLAN interface, do the following:

1. Define a VLAN interface.
For more information, refer to "Adding a VLAN interface (Page 290)".
2. [Optional] Add a description for the interface.
For more information, refer to "Adding a description for a VLAN interface (Page 291)".
3. [Optional] Configure the MTU size.
For more information, refer to "Configuring the MTU size (Page 291)".
4. [Optional] Enable alarms to be triggered on a link down/up event.
For more information, refer to "Enabling link up/down traps (Page 292)".
5. [Optional] Assign a static IPv4 address to the interface or enable DHCP.
For more information, refer to "Configuring a static IPv4 address (Page 315)".
6. Enable the VLAN interface.
For more information, refer to "Enabling a VLAN interface (Page 293)".

8.1.3.1 Adding a VLAN interface

To adding a VLAN interface, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | 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 531)". | <code>switch vlan { VLAN ID }</code> |
| 3 | Add the VLAN interface. Each VLAN interface is associated with a static VLAN through its name. For example, <code>vlan10</code> is associated with VLAN 10. VLAN interfaces must be added individually. A range (e.g. <code>interface vlan1-3</code>) cannot be used to add multiple interfaces. | <code>interface vlan{ VLAN ID }</code> |
| 4 | Commit the change. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config interface vlan{ VLAN ID }</code> |

Example

The following adds a VLAN interface for the VLAN 10 interface.

```
localhost# config
localhost(config)# switch vlan 10
localhost(config-switch-vlan-10)# top
localhost(config)# interface vlan10
localhost(config-interface-vlan10)# commit
Commit complete.
localhost(config)# end
localhost# show running-config interface vlan10
```

```
interface vlan10
  enabled
  no link-up-down-trap
exit
```

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 the description for VLAN interface, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Add a description to the interface. Conditions: <ul style="list-style-type: none"> • Can be between 0 and 64 characters long • Quotation marks are required if the description contains spaces | interface vlan{ VLAN ID } description { description } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface vlan{ VLAN ID } description |

Example

The following adds a description for the VLAN 10 interface.

```
localhost# config
localhost(config)# interface vlan10 description "Interface to production
network"
localhost(config-interface-vlan10)# commit
Commit complete.
localhost(config)# end
localhost# show running-config interface vlan10 description
interface vlan10
  description "Interface to production network"
exit
```

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 configure the MTU size for a VLAN interface, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the MTU size in bytes for the selected VLAN interface. Multiple VLAN interfaces can be affected by defining a range (e.g. <code>vlan1-3</code>). However, only interfaces that exist will be configured. If an interface within the range does not exist, the interface will be ignored. Condition: <ul style="list-style-type: none"> A number between 68 and 1500 Default: 1500 | <code>interface vlan{ VLAN ID } mtu { 68 - 1500 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface vlan{ VLAN ID } mtu</code> |

Example

The following sets the MTU size to 1500 for the VLAN 10 interface.

```
localhost# config
localhost(config)# interface vlan10 mtu 1500
localhost(config-interface-vlan1)# commit
Commit complete.
localhost(config-interface-vlan1)# end
localhost# show running-config interface vlan10 mtu
interface vlan1
  mtu 1500
exit
```

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the selected VLAN interface. Multiple VLAN interfaces can be affected by defining a range (e.g. <code>vlan1-3</code>). However, only existing interfaces in the defined range will be configured. If an interface within the range does not exist, the interface will be ignored. | <code>interface vlan{ VLAN ID } link-up-down-trap</code> |

| Step | Instruction | Command |
|------|---------------------------|--|
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface vlan{ VLAN ID } link-up-down- trap |

Example

```
localhost# config
localhost(config)# interface vlan1 link-up-down-trap
localhost(config-interface-vlan1)# commit
Commit complete.
localhost(config-interface-vlan1)# end
localhost# show running-config interface vlan1 link-up-down-trap
interface vlan1
  link-up-down-trap
exit
```

8.1.3.5 Enabling a VLAN interface

To enable a VLAN interface, do the following:

Note

All VLAN interfaces are enabled by default.

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable the selected VLAN interface. Multiple VLAN interfaces can be affected by defining a range (e.g. vlan1-3). However, only existing interfaces in the defined range will be configured. If an interface within the range does not exist, the interface will be ignored. | interface vlan{ VLAN ID } enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface vlan{ VLAN ID } |

Example

```
localhost# config
localhost(config)# interface vlan1 enabled
localhost(config-interface-vlan1)# commit
Commit complete.
localhost(config-interface-vlan1)# end
localhost# show running-config interface vlan1
interface vlan1
  enabled
```

```
exit
```

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, execute the following command in operational mode:

```
interface { bridge port } ethernet reset
```

Example

```
localhost# interface ethernet0/1 ethernet reset
```

8.1.5 Monitoring interfaces

This section describes the various ways to look up information about the available interfaces, including their configuration, capabilities, and status.

8.1.5.1 Displaying interface characteristics

To display the characteristics of an interface, including port speed, media type, duplex mode, etc., execute one of the following commands in operational mode:

| Command | Description |
|--|--|
| <code>show running-config interface ethernet details</code> | Shows the characteristics for all interfaces. |
| <code>show runningconfig interface [Interface] ethernet details</code> | Shows the characteristics for the specified interface. |

Example

The following displays the characteristics of ethernet0/1.

```
localhost# show running-config interface ethernet0/1 ethernet |
details
interface ethernet0/1
 ethernet
  speed 0.0
  duplex auto
  auto-negotiation
  media 1000BASE-T
  no lfi
```

```
link-down-action none
down-shift
no rate-control ingress enabled
rate-control ingress traffic-type all
rate-control ingress rate-type kbps
rate-control ingress rate 0
no rate-control egress enabled
rate-control egress traffic-type all
rate-control egress rate-type kbps
rate-control egress rate 0
exit

exit
```

8.1.5.2 Displaying receive/transmit statistics for all interfaces

To display statistics collected for all interfaces, execute the following command in operational mode:

```
show interface statistics
```

Alternatively, to display only a specific statistic, execute the same command with the relevant option:

```
show interface statistics [ in-octets | in-unicast-pkts | in-
broadcast-pkts | in-multicast-pkts | in-discards | in-errors | out-
octets | out-unicast-pkts | out-broadcast-pkts | out-multicast-pkts
| out-discards | out-errors ]
```

Example

The following displays statistics for each interface.

```
localhost# show interface statistics
interface ethernet0/1
  statistics in-octets 6820
  statistics in-unicast-pkts 33
  statistics in-multicast-pkts 0
  statistics in-discards 0
  statistics in-errors 0
  statistics out-octets 3086
  statistics out-unicast-pkts 18
  statistics out-multicast-pkts 0
  statistics out-discards 15
  statistics out-errors 0
Interface ethernet0/2
.
.
.
interface vlan1
  statistics in-octets 5430
  statistics in-unicast-pkts 26
  statistics in-multicast-pkts 0
  statistics in-discards 0
  statistics in-errors 0
  statistics out-octets 1980
```

8.1 Interfaces

```

statistics out-unicast-pkts 14
statistics out-multicast-pkts 0
statistics out-discards 12
statistics out-errors 0
interface vlan10
.
.
.

```

Example

The following displays a specific statistic (out-unicast-pkts) for each interface.

```
localhost# show interface statistics out-unicast-pkts | tab
```

```

          OUT
          UNICAST
NAME          PKTS
-----
ethernet0/1  18
ethernet0/2   0
ethernet0/3   0
ethernet0/4   0
ethernet0/5   0
ethernet0/6   0
ethernet0/7   0
ethernet0/8   0
vlan1         14
vlan2         0

```

Description

The following information can be displayed for each interface:

| Statistic | Description |
|--------------------|--|
| 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-multicast-pkts | The number of multicast frames successfully received by the interface. |
| in-discards | The number of frames received by the interface that were dropped due to congestion at the input queue. |
| in-errors | 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-unicast-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 |

| Statistic | Description |
|--------------|---|
| out-discards | The number of frames the interface due to congestion at the output queue. |
| out-errors | The number of invalid frames forwarded by the interface. |

8.1.5.3 Displaying receive/transmit statistics for only bridge ports

To display statistics collected for only bridge ports, execute the following command in operational mode:

```
show interface ethernet statistics
```

Alternatively, to display only a specific statistic, execute the same command with the relevant option:

```
show interface ethernet statistics frame [ in-total-frames | in-total-
octets | in-frames | in-multicast-frames | in-broadcast-frames | in-error-
fcs-frames | in-error-undersize-frames | in-error-oversize-frames | out-
frames | out-multicast-frames | out-broadcast-frames | in-unicast-frames |
in-errors | out-octets | out-unicast-frames | pkt-64-octets | pkt-65-to-127-
octets | pkt-128-to-255-octets | pkt-256-to-511-octets | pkt-512-to-1023-
octets | pkt-1024-to-1536-octets ]
```

Example

The following displays statistics for each bridge port.

```
localhost# show interface ethernet statistics
interface ethernet0/1
  ethernet
    statistics frame in-total-frames 49229
    statistics frame in-total-octets 7587869
    statistics frame in-frames 49229
    statistics frame in-multicast-frames 41015
    statistics frame in-broadcast-frames 578
    statistics frame in-error-fcs-frames 0
    statistics frame in-error-undersize-frames 0
    statistics frame in-error-oversize-frames 0
    statistics frame out-frames 690364
    statistics frame out-multicast-frames 683625
    statistics frame out-broadcast-frames 18
    statistics frame in-unicast-frames 7636
    statistics frame in-errors 0
    statistics frame out-octets 58156529
    statistics frame out-unicast-frames 6721
    statistics frame pkt-64-octets 3057239
    statistics frame pkt-65-to-127-octets 1020377
    statistics frame pkt-128-to-255-octets 667286
    statistics frame pkt-256-to-511-octets 415077
    statistics frame pkt-512-to-1023-octets 23045
    statistics frame pkt-1024-to-1536-octets 382544
  interface ethernet0/2
    .
    .
    .
```

Example

The following displays a specific statistics (out-unicast-frames) for each bridge port.

```
localhost# show interface ethernet statistics frame out-unicast-frames | tab
          OUT
          UNICAST
NAME      FRAMES
-----
ethernet0/1  7160
ethernet0/2   0
ethernet0/3   0
ethernet0/4   0
ethernet0/5   0
ethernet0/6   0
ethernet0/7   0
ethernet0/8   0
```

Description

The following information can be displayed for each bridge port:

| 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 <code>max-frame-length</code>). |
| 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. |

| Statistic | Description |
|-------------------------|---|
| pkt-64-octets | The number of 64 octet packets received and transmitted, including dropped packets |
| pkt-65-to-127-octets | The number packets between 65 and 127 octets received and transmitted, including dropped packets |
| pkt-128-to-255-octets | The number packets between 128 and 255 octets received and transmitted, including dropped packets |
| pkt-256-to-511-octets | The number packets between 256 and 511 octets received and transmitted, including dropped packets |
| pkt-512-to-1023-octets | The number packets between 512 and 1023 octets received and transmitted, including dropped packets |
| pkt-1024-to-1536-octets | The number packets between 1024 and 1536 octets received and transmitted, including dropped packets |

8.1.5.4 Displaying negotiated settings for each bridge port

To display for each bridge port the settings agreed upon with its link partner following negotiation (i.e. speed and duplex mode), execute the following command in operational mode:
`show interface ethernet duplex-status | select ethernet speed-status`

Example

```
localhost# show interface ethernet duplex-status | select ethernet
speed-status | tab
```

```

NAME                SPEED    DUPLEX
                   STATUS   STATUS
-----
ethernet0/1         0.0     unknown
ethernet0/2         0.0     unknown
ethernet0/3         0.1     full
.
.
.
```

Description

The following information is displayed for each bridge port:

| Column | Description |
|---------------|---|
| NAME | The name of the interface. |
| SPEED STATUS | The negotiated maximum speed in Gigabit per second (Gbps). |
| DUPLEX STATUS | The negotiated duplex setting. Possible values include: <ul style="list-style-type: none"> <code>unknown</code> - The duplex mode is undefined <code>half</code> - Communication between the sender and receiver occurs in both directions, but only one at a time <code>full</code> - Communication between the sender and receiver occurs simultaneously in both directions |

8.1.5.5 Displaying the MAC address for each interface

To display the MAC address (or physical address) of each interface, execute the following command in operational mode:

```
show interface phys-address
```

Example

```
localhost# show interface phys-address | tab
NAME                PHYS ADDRESS
-----
ethernet0/1         20:87:56:8c:9b:e0
ethernet0/2         20:87:56:8c:9b:e1
ethernet0/3         20:87:56:8c:9b:e2
.
.
.
vlan1                20:87:56:8c:9b:df
vlan10               20:87:56:8c:9b:df
vlan2                20:87:56:8c:9b:df
```

Description

The following information is displayed for each interface:

| Column | Description |
|--------------|------------------------------|
| NAME | The name of the interface. |
| PHYS ADDRESS | The interface's MAC address. |

8.1.5.6 Displaying the auto-negotiation capability of each bridge port

To determine which bridge ports support auto-negotiation, execute the following command in operational mode:

```
show interface ethernet capabilities
```

Example

```
localhost# show interface ethernet capabilities | tab
                AUTO
NAME           NEGOTIATION
-----
ethernet0/1    true
ethernet0/2    false
ethernet0/3    true
.
.
.
```

Description

The following information is displayed for each bridge port:

| Column | Description |
|------------------|---|
| NAME | The name of the bridge port. |
| AUTO NEGOTIATION | The auto-negotiation capability of the interface. Possible values include: <ul style="list-style-type: none"> <code>true</code> - Auto-negotiation is supported <code>false</code> - Auto-negotiation is not supported |

8.1.5.7 Displaying the administrative state of each interface

The administrative state of an interface is the configured state of the interface, as opposed to the operational state, which is the running state of the interface.

At times, the administrative state of an interface will be up, while the operational state is down.

To display the administrative state of all interfaces, execute the following command:

```
show interface admin-status
```

To display only interfaces that have a specific status, execute the following command:

```
show interface admin-status | select admin-status { status }
```

Example

The following displays the administrative status of each interface.

```
localhost# show interface admin-status | tab
                ADMIN
NAME           STATUS
-----
ethernet0/1   up
ethernet0/2   down
ethernet0/3   down
.
.
.
vlan1          up
vlan10         up
vlan2          up
```

Example

The following only displays interfaces whose administrative status is "up".

```
localhost# show interface admin-status | select admin-status up | tab
                ADMIN
NAME            STATUS
-----
ethernet0/1    up
vlan1          up
vlan10         up
vlan2          up
```

Description

The following information is displayed for each interface:

| Column | Description |
|--------------|--|
| NAME | The name of the interface. |
| ADMIN STATUS | The current administrative state of the interface. Possible values include: <ul style="list-style-type: none"> • down - The interface is administratively down • testing - The interface is being tested by an administrator • up - The interface is administratively up |

8.1.5.8 Displaying the link state of each interface

The link state of an interface indicates the running state of the interface, as opposed to the administrative state, which is a configured state.

At times, the link state of an interface will be down, while the administrative state is up.

To display the link state of all interfaces, execute the following command:

```
show interface link-status
```

To display only interfaces that have a specific status, execute the following command:

```
show interface link-status | select link-status { status }
```

Example

The following displays the link status for each interface.

```
localhost# show interface link-status | tab
                LINK
NAME            STATUS
-----
ethernet0/1    up
ethernet0/2    down
ethernet0/3    down
.
.
.
vlan1          up
vlan10         up
vlan2          up
```

Example

The following only displays interfaces whose link status is "up".

```
localhost# show interface link-status | select link-status up | tab
                LINK
NAME            STATUS
-----
ethernet0/1    up
vlan1          up
vlan10         up
vlan2          up
```

Description

The following information is displayed for each interface:

| Column | Description |
|-------------|---|
| NAME | The name of the interface. |
| LINK STATUS | <p>The current state of the interface.</p> <p>Possible values include:</p> <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 |

8.1.5.9 Monitoring SFP transceivers

To show the status of SFP transceivers, you can execute different commands in operational mode:

| Command | Description |
|--|---|
| <code>show interface sfp</code> | Shows the status of all SFP transceivers. |
| <code>show interface { SFP transceiver port } sfp</code> | Shows the status of a specific SFP transceiver. |

Example

```
localhost# show interface ethernet0/11 sfp
sfp present          true
sfp model            SFP992-1LD
sfp vendor           SIEMENS
sfp article-num      "6GK5 992-1AM00-8AA0"
sfp description      "1 x 1000 Mbit/s LC-Port ..."
sfp part-rev         2
sfp speed            1.0
sfp serial-num       N65BYDL
sfp rx-power         -27.5
sfp rx-min-power     -19
sfp rx-max-power     -3
sfp tx-power         -29.9
sfp tx-min-power     -9.5
sfp tx-max-power     -3
sfp max-len-9um     10000
sfp temp             35.04
```

Description

Note

If an SFP transceiver does not offer a value, the parameter is not shown in the output.

The following information is displayed when a readable SFP transceiver is plugged:

| Parameter | Description |
|--------------------------|--|
| <code>present</code> | Shows whether an SFP transceiver is plugged (<code>true</code>) or not (<code>false</code>). |
| <code>model</code> | Shows the name/type of the SFP transceiver. |
| <code>vendor</code> | Shows the manufacturer of the SFP transceiver. |
| <code>article-num</code> | Shows the article number of the SFP transceiver. |
| <code>description</code> | Displays a description of the SFP transceiver. |
| <code>part-rev</code> | Shows the hardware version of the SFP transceiver. |

| Parameter | Description |
|--------------|---|
| speed | Shows the transmission speed with which frames are transmitted at the SFP transceiver port. Possible values: <ul style="list-style-type: none"> 0.0 - Frames are sent with the speed determined by autonegotiation. 0.01 - Frames are sent with 10 Mbps. 0.1 - Frames are sent with 100 Mbps. 1.0 - Frames are sent with 1 Gbps. 2.5 - Frames are sent with 2.5 Gbps. 5.0 - Frames are sent with 5 Gbps. 10.0 - Frames are sent with 10 Gbps. |
| serial-num | Shows the serial number of the SFP transceiver. |
| rx-power | Shows the current value of the receive power in decibel-milliwatts (dBm). |
| rx-min-power | Shows the smallest possible value of the receive power of the SFP transceiver in decibel-milliwatts (dBm). |
| rx-max-power | Shows the largest possible value of the receive power of the SFP transceiver in decibel-milliwatts (dBm). |
| tx-power | Shows the current value of the sent power in decibel-milliwatts (dBm). |
| tx-min-power | Shows the smallest possible value of the send power of the SFP transceiver in decibel-milliwatts (dBm). |
| tx-max-power | Shows the largest possible value of the send power of the SFP transceiver in decibel-milliwatts (dBm). |
| max-len-9um | Shows the maximum cable length with a fiber core diameter of 9 μm in meters (m). |
| max-len-50um | Shows the maximum cable length with a fiber core diameter of 50 μm in meters (m). |
| max-len-62um | Shows the maximum cable length with a fiber core diameter of 62.5 μm in meters (m). |
| temp | Shows the current temperature of the SFP transceiver in degrees Celsius ($^{\circ}\text{C}$). |

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).

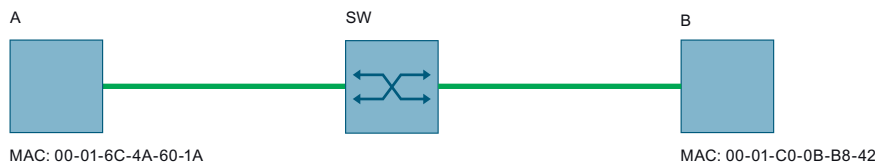


Figure 8-4 Learning MAC addresses from two hosts

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 307)".
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 308)".

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the time that dynamically learned MAC addresses are kept in the MAC address table. Conditions: <ul style="list-style-type: none"> • Formatted as <code>nYnMnDnHnmns</code>, where <code>n</code> is a user-defined number • Minimum of 15 seconds (<code>15s</code>) • Maximum of 13 minutes (<code>13m</code>) or 800 seconds (<code>800s</code>) Default: <code>5m</code> (5 minutes) | <code>switch mac-address-tables filtering-database aging-time [15s - 13m]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch mac- address-tables filtering- database aging-time</code> |

Example

The following sets the aging time to 9 minutes and 30 seconds.

```
localhost# config
```

```

localhost(config)# switch mac-address-tables filtering-database
aging-time 9m30s
localhost(config-switch)# commit
Commit complete.
localhost(config-switch)# end
localhost# show running-config switch mac-address-tables filtering-
database aging-time
switch
 mac-address-tables
  filtering-database aging-time 9m30s
exit

exit

```

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.

This feature 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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable the age upon link loss feature. | switch mac-address-tables filtering-database age-upon- link-loss |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch mac- address-tables filtering- database age-upon-link-loss |

Example

```

localhost# config
localhost(config)# switch mac-address-tables filtering-database age-
upon-link-loss
localhost(config-switch)# commit
Commit complete.
localhost(config-switch)# end
localhost# show running-config switch mac-address-tables filtering-
database age-upon-link-loss
switch
 mac-address-tables
  filtering-database age-upon-link-loss
exit

exit

```

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 309)".
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 310)".

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Add the static MAC filtering entry. Each entry must be given a VLAN ID and a valid MAC address. | <code>switch mac-address-tables static { 1 - 4094 } { address }</code> |
| 3 | Map the entry to a forwarding port. Ingress frames associated with the MAC address will be forwarded to the specified bridge port. | <code>forwarding-port-map { bridge port }</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config switch mac- address-tables static</code> |

Example

The following adds an entry and selects ethernet0/1 as the forwarding port.

```
localhost# config
localhost(config)# switch mac-address-tables static 10 3A:34:52:C4:69:B8
forwarding-port-map ethernet0/1
localhost(config-forwarding-port-map-ethernet0/1)# commit
Commit complete.
localhost(config)# end
localhost# show running-config switch mac-address-tables static | tab
VIDS  ADDRESS                TRAFFIC CLASS  PORT REF
-----
10    3A:34:52:C4:69:B8  unprioritized  ethernet0/1
exit

exit
```

Example

The following adds two entries for the same MAC address and selects ethernet0/1 as the forwarding port for both.

Note

Each MAC address filtering entry must exist first before a forwarding port can be mapped to each entry in a single command.

```
localhost(config)# switch mac-address-tables static 10 3A:34:52:C4:69:B8
localhost(config-static-10/3a:34:52:c4:69:b8)# top
localhost(config)# switch mac-address-tables static 11 3A:34:52:C4:69:B8
localhost(config-static-11/3a:34:52:c4:69:b8)# top
localhost(config)# switch mac-address-tables static 10,11
3A:34:52:C4:69:B8 forwarding-port-map ethernet0/1
localhost(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config switch mac-address-tables static | tab
VIDS  ADDRESS                TRAFFIC CLASS  PORT REF
-----
10    3A:34:52:C4:69:B8  unprioritized  ethernet0/1
11    3A:34:52:C4:69:B8  unprioritized  ethernet0/1
exit

exit
```

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Assign a traffic class queue to the selected static MAC filtering entry. Options include: <ul style="list-style-type: none"> 0 - 7 - A traffic class queue unprioritized - No traffic class queue is assigned Default: unprioritized | <code>switch mac-address-tables static { 1 - 4094 } { address } traffic-class [{ 0 - 7 } unprioritized]</code> |
| 4 | Commit the change. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config switch mac-address-tables static</code> |

Example

The following assigns queue 7 to a static entry.

```
localhost# config
localhost(config)# switch mac-address-tables static 10 3A:34:52:C4:69:B8
localhost(config-static-10/3A:34:52:C4:69:B8)# traffic-class 7
localhost(config-static-10/3A:34:52:C4:69:B8)# commit
Commit complete.
localhost(config)# end
localhost# show running-config switch mac-address-tables static | tab
VIDS  ADDRESS                TRAFFIC CLASS  PORT REF
-----
10    3A:34:52:C4:69:B8    7              ethernet0/1
exit

exit
```

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, execute the following command:
`show switch mac-address-tables filtering-database`

Example

```
localhost# show switch mac-address-tables filtering-database | notab
filtering-database entry 1 00:01:6C:4A:60:1A
  traffic-class unprioritized
  entry-type    dynamic
  port-map     ethernet0/1
```

```

filtering-database entry 10 3A:34:52:C4:69:B8
  traffic-class 7
  entry-type    static
  port-map ethernet0/1
filtering-database entry 2 00:01:C0:0B:B8:42
  traffic-class unprioritized
  entry-type    dynamic
  port-map ethernet0/1
3 entries in the list.

```

Note

A total count of MAC addresses is shown when the filtering database is displayed in a table format. The total count is not displayed when the `notab` customization is applied.

For example:

```
Total MAC Addresses Displayed: 127
```

Description

The following information is displayed for each entry:

| Parameter | Description |
|--|--|
| <code>mac-address-tables filtering-database entry 1</code> | The VLAN ID associated with the MAC address. |
| <code>mac-address-tables filtering-database entry 1 00:00:00:00:00:01</code> | The destination MAC address. |
| <code>entry-type</code> | The type of entry. Possible values include: <ul style="list-style-type: none"> <code>dynamic</code> - The entry was added dynamically <code>static</code> - The entry was added statically |
| <code>traffic-class</code> | The traffic class queue assigned to the entry. Possible values include: <ul style="list-style-type: none"> <code>[0 - 7]</code> - The traffic queue number <code>unprioritized</code> - No traffic class queue is assigned to the entry |
| <code>port-map</code> | The forwarding interface assigned to the entry. When frames match the entry, they are forwarded on this interface. |

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, execute the following command:

```
switch mac-address-tables filtering-database purge-dynamic-entries
```


Example

```
localhost# switch mac-address-tables filtering-database purge-  
dynamic-entries  
localhost# show switch mac-address-tables | tab  
DATABASE          ENTRY  
ID      VIDS  ADDRESS      TYPE      TRAFFIC CLASS  PORT REF  STATE  
-----  
%No entries found%
```


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 "Configuring VLANs (Page 531)".
2. Configure a static IPv4 address.
For more information, refer to "Configuring a static IPv4 address (Page 315)".

9.1.1 Configuring a static IPv4 address

To configure a static IPv4 address, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Make sure DHCP is disabled on the IP interface to which you want to assign a static IPv4 address. | <code>no interface { IP interface } ipv4 dhcp</code> |
| 3 | Configure a static IPv4 address with prefix or subnet mask for the IP interface. | <code>interface { IP interface } ipv4 address { IP address } prefix- length { Prefix length }</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show interface { IP interface } ipv4 address</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# no interface vlan7 ipv4 dhcp
localhost(config)# interface vlan7 ipv4 address 192.168.1.10
localhost(config-address-192.168.1.10)# prefix-length 16
localhost(config-address-192.168.1.10)# commit
Commit complete.
localhost(config-address-192.168.1.10)# end
localhost# show interface vlan7 ipv4 address
% The following list contains 1 entry.
```

9.1 Static IP address assignment

```

IP                ORIGIN PREFIX IPV4 STATUS VALID LIFETIME
-----
192.168.1.10 static 16      preferred  forever

```

9.1.2 Listing the IPv4 address configuration

To display all IP interfaces that are assigned an IP address, execute the following command in the operating mode:

```
show interface ipv4 address
```

To show a specific IP interface that is assigned an IP address, execute the following command in the operating mode:

```
show interface { IP interface } ipv4 address
```

Example

This example shows the IPv4 address configuration of all IP interfaces.

```
localhost# show interface ipv4 address
```

```

NAME   IP                ORIGIN PREFIX IPV4 STATUS VALID
-----
vlan1  192.0.2.2         dhcp   24     preferred 7200s
vlan6  198.51.100.20    static 24     preferred forever
vlan7  203.0.113.10     static 25     preferred forever

```

Description

The following information is shown:

| Parameter | Description |
|----------------|--|
| name | Name of the IP interface |
| ip | IP address of the IP interface |
| prefix-length | Subnet displayed as prefix length |
| origin | Type of IP address configuration Possible values: <ul style="list-style-type: none"> static - The IP address was configured statically. dhcp - The IP address was assigned dynamically via DHCP. |
| ipv4 status | Status of the IP address Possible values: <ul style="list-style-type: none"> preferred - The IP address is valid. It can be used as the source or destination IP address in packets. inaccessible - The IP address is not reachable. The IP interface to which the IP address is assigned is not ready for operation. |
| valid lifetime | Shows the lease time in seconds for dynamically assigned IP addresses. With statically configured IP addresses, <code>forever</code> is listed. |

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> |
| DNS server | <p>A DNS server or name server has information that resolves a domain name into an IP address.</p> <p>A DNS server can provide the information of one or more DNS zones:</p> <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 | <p>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).</p> |
| DNS resolver | <p>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.</p> <p>For the DNS resolver to work, it needs the IP address of at least one DNS server.</p> |

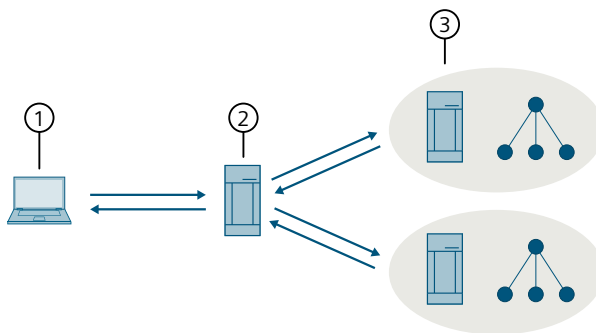
| Term | Explanation |
|---------------|--|
| Search domain | A search domain is used to avoid having to manually enter the entire address of frequently used domains. The search domains you configure are automatically appended to the names you enter. DNS resolvers use search domains to create an FQDN 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.



- ① DNS client
- ② DNS resolver
- ③ Authoritative DNS server

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 319)".
2. [Optional] Configure how often to request a DNS server before requesting the next DNS server.
For more information, refer to "Configuring the number of request attempts to a DNS server (Page 320)".
3. [Optional] Configure the length of time the DNS resolver waits for a response from the DNS server.
For more information, refer to "Configuring the waiting time for a DNS server to respond (Page 321)".
4. [Optional] Configure a search domain.
For more information, refer to "Configuring a search domain (Page 321)".

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, the 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:

| Step | Instruction | Command |
|------|---------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure a DNS server. | <code>system dns-resolver server { server name } ipv4 { IP address }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system dns- resolver server</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system dns-resolver server server1 ipv4
192.168.1.1
localhost(config-server-server1)# commit
Commit complete.
localhost(config-server-server1)# end
localhost# show running-config system dns-resolver server
system
  dns-resolver
    server server1
      ipv4 192.168.1.1
    exit
```

```
exit
```

```
exit
```

9.2.2.2 Configuring the number of request attempts to a DNS server

To configure after how many unsuccessful requests to a DNS server another DNS server should be requested, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the number of requests that a DNS resolver sends to a DNS server. If the DNS server does not respond within the specified time, the DNS resolver sends the request to the next available DNS server. If no DNS server responds, the DNS resolver returns an error message. Default: 2 | <code>system dns-resolver options attempts { 1 - 5 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system dns-resolver options attempts</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system dns-resolver options attempts 3
localhost(config-system-dns-resolver)# commit
Commit complete.
localhost(config-system-dns-resolver)# end
localhost# show running-config system dns-resolver options attempts
system
  dns-resolver
    options attempts 3
  exit
exit
```


9.2.2.3 Configuring the waiting time for a DNS server to respond

To configure the wait time for a DNS server to respond, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the length of time in seconds the DNS resolver waits for a response from the DNS server. When the time has expired, the DNS resolver resends the request or, when the maximum number of requests is reached, sends it to another DNS server. Default: 5 | <code>system dns-resolver options timeout { 1 - 30 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system dns-resolver options timeout</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system dns-resolver options timeout 10
localhost(config-system-dns-resolver)# commit
Commit complete.
localhost(config-system-dns-resolver)# end
localhost# show running-config system dns-resolver options timeout
system
  dns-resolver
    options timeout 10
  exit
exit
```

9.2.2.4 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. If there is more than one search domain, the index specifies the order in which the search domains are used. 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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure a search domain. Condition: <ul style="list-style-type: none"> Must be between 1 and 251 characters long | <code>system dns-resolver search { search domain }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system dns-resolver search</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system dns-resolver search example.com
localhost(config-system-dns-resolver)# commit
Commit complete.
localhost(config-system-dns-resolver)# end
localhost# show running-config system dns-resolver search
system
  dns-resolver
    search [ example.com ]
  exit

exit
```

9.2.3 Displaying the DNS configuration

To view the configuration of DNS, execute the following command in operational mode:

```
show system dns
```

Example

```
localhost# show system dns
dns search [ example.com example.org ]
dns server [ 192.168.1.1 ]
dns origin static
dns options timeout 10
dns options attempts 3
```

Description

The following information is shown:

| Parameter | Description |
|-------------------------|---|
| <code>dns search</code> | Shows the configured search domains. |
| <code>dns server</code> | Shows the IP addresses of the configured DNS servers. |

| Parameter | Description |
|-----------------------------------|--|
| <code>dns origin</code> | Indicates how the DNS server was added. Possible values: <ul style="list-style-type: none"> <code>static</code> - The DNS server was added manually. <code>dynamic</code> - The DNS server was learned dynamically. |
| <code>dns options timeout</code> | Lists the configured time in seconds that the DNS resolver waits for a DNS server to respond. |
| <code>dns options attempts</code> | Lists the configured number of requests a DNS resolver sends to each available DNS server before returning an error message. |

9.3 DHCP

This section describes how to configure a device to obtain its IP configuration from a DHCP server.

9.3.1 Understanding DHCP

The DHCP (Dynamic Host Configuration Protocol (DHCP)) is a communication protocol for central management and assignment of TCP/IP configuration parameters.

DHCP enables the integration of a terminal device into an existing network without manual configuration. All required parameters such as IP address and subnet mask are assigned to the client by the server. The server also transmits optional parameters such as a gateway or DNS server.

Note

A part of the DHCP communication is transmitted as a broadcast. This informs all other clients and servers about the configuration.

For a client to be able to communicate with a server, both devices must be in the same broadcast domain. If the client and the server are in different broadcast domains, which means communication takes place via router, you must use a DHCP relay agent.

9.3.1.1 DHCP communication

DHCP is familiar with the following types of messages for communication between client and server.

| | DHCP message type | Meaning |
|---|-------------------|---|
| ① | DHCPDiscover | When a DHCP client needs an IP address for the first time, it sends a broadcast to test its local network for DHCP servers. |
| ② | DHCPOffer | The available DHCP servers respond to the DHCP client with corresponding configuration parameters as unicast. |

| | DHCP message type | Meaning |
|---|-------------------|--|
| 3 | DHCPRequest | The DHCP client selects one of the configurations and uses a broadcast to inform the DHCP server with the configuration for which it has decided. It implicitly rejects all other configurations. Other reasons why a DHCP client sends a DHCPRequest to a DHCP server: <ul style="list-style-type: none"> • The DHCP client checks the correctness of a previously received IP address (e.g. after a restart). • The DHCP client extends the validity of a specific network address. |
| 4 | DHCPAck | The selected DHCP server commits its offer and transfers the configuration parameters. |
| | DHCPNak | The selected DHCP server rejects the DHCPRequest. |
| | DHCPDecline | The DHCP client rejects a configuration if it determines that there is a conflict with the offered IP address. Before the DHCP client uses an IP address on an IP interface, it checks whether the IP address is already being used by sending an ARP request. |
| 5 | DHCPRelease | When a DHCP client no longer needs an IP address, it is released. |

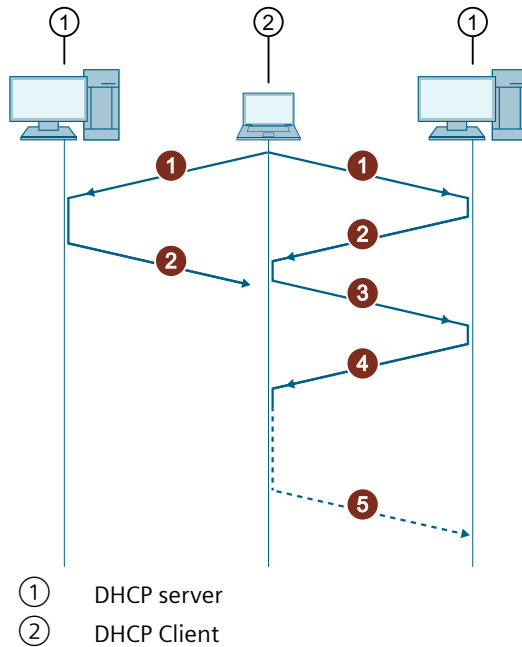


Figure 9-2 DHCP communication

9.3.1.2 DHCP server

The assignment of IP addresses can be dynamic or static:

- **Dynamic assignment**

With dynamic assignment, IP address ranges are configured in the DHCP server. An IP address is only assigned temporarily to a client when it logs in. The client now has the option of extending the lease time of its assigned IP address. To do so, it must send a request to the server again. If the client no longer extends the IP address, it becomes free and can be assigned to other clients.

- **Static assignment**

For static assignment, the IP addresses in the DHCP server are reserved for specific client IDs. The MAC address, the host name or the device name can be used as the client ID for example. This is best for clients that should always be accessible under the same IP address. For more information on the definition of the client ID, refer to "Changing the client ID of an interface (Page 327)".

9.3.2 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 325)".
2. [Optional] Set a lease time.
For more information, refer to "Requesting a lease time (Page 326)".
3. [Optional] Change the client ID of a DHCP client interface.
For more information, refer to "Changing the client ID of an interface (Page 327)".
4. [Optional] Enable the use of the hostname.
For more information, refer to "Including the hostname in DHCP messages (Page 328)".
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 (option 66, 67) (Page 329)".

9.3.2.1 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 the DHCP client interface, do the following:

| Step | Instruction | Command |
|------|-----------------------------------|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the DHCP client interface. | <code>interface { IP interface } ipv4 dhcp</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show dhcp client ipv4 bindings { IP interface }</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface vlan5 ipv4 dhcp
localhost(config-interface-vlan5-ipv4)# commit
Commit complete.
localhost(config-interface-vlan5-ipv4)# end
localhost# show dhcp client ipv4 bindings vlan5
  DHCP Bindings vlan5
  .
  .
  .
  Dhcp                               true
  .
  .
  .
```

9.3.2.2 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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define the lease time in seconds that a DHCP client interface requests from the DHCP server. Conditions: <ul style="list-style-type: none"> Formatted as <code>nYnMnDnhnmns</code>, where <code>n</code> is a user-defined number Minimum 2 minutes (2m) Maximum 136 years 2 months 10 days 6 hours 28 minutes 15 seconds (136Y2M10D6h28m15s) | <code>dhcp client ipv4 { IP interface } lease { 2m - 136Y2M10D6h28m15s }</code> |
| 3 | Commit the change. | <code>commit</code> |

| Step | Instruction | Command |
|------|---------------------------|--|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show dhcp client ipv4 bindings { IP interface } lease-requested |

Example

In this example, a lease time of 1 hour is configured.

```
localhost# config
Entering configuration mode terminal
localhost(config)# dhcp client ipv4 vlan5 lease 1h
localhost(config-vlan5)# commit
Commit complete.
localhost(config-vlan5)# end
localhost# show dhcp client ipv4 bindings vlan5 lease-requested
lease-requested 1h
```

9.3.2.3 Changing the client ID of an interface

The client-ID is used to assign a specific IP address to a particular DHCP client. In a DHCP server, IP addresses can be associated and thus reserved with client IDs. Every time a DHCP server receives a request with a known client ID, it offers the corresponding IP address to the requesting DHCP client. This ensures that a client is always reachable under the same IP address.

To change the client ID of a DHCP client interface, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | <p>Define the client ID of a DHCP client interface.</p> <p>Options include:</p> <ul style="list-style-type: none"> • <code>string { string }</code> - Freely selectable ID. The DHCP client identifies itself to the DHCP server with the ID. <p>Conditions:</p> <ul style="list-style-type: none"> - At least 1 character - Maximum of 152 characters - All standard characters are allowed, plus the following special characters: _ - . : < = > @ () <ul style="list-style-type: none"> • <code>mac-address</code> - The DHCP client identifies to the DHCP server with its MAC address. • <code>name-of-station</code> - The DHCP client identifies to the DHCP server with its PRO-FINET device name. • <code>sys-name</code> - The DHCP client identifies to the DHCP server with its hostname. For more information, refer to "Changing the host name (Page 116)". <p>Default: <code>mac-address</code></p> | <pre>dhcp client ipv4 { IP interface } client-id [string { string } mac-address name-of-station sys-name]</pre> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show dhcp client ipv4 bindings { IP interface } client-id-type |
| | | show dhcp client ipv4 bindings { IP interface } client-id |

Example

In this example, the string `MonitoringPC` is defined as the client ID for the DHCP client interface "vlan5".

```
localhost# config
Entering configuration mode terminal
localhost(config)# dhcp client ipv4 vlan5 client-id string
MonitoringPC
localhost(config-vlan5)# commit
Commit complete.
localhost(config-vlan5)# end
localhost# show dhcp client ipv4 bindings vlan5 client-id-type
client-id-type string
localhost# show dhcp client ipv4 bindings vlan5 client-id
client-id MonitoringPC
```

9.3.2.4 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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable the use of the hostname of a client in messages to the server. | dhcp client ipv4 { IP interface } hostname |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show dhcp client ipv4 bindings { IP interface } hostname |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# dhcp client ipv4 vlan5 hostname
localhost(config-vlan5)# commit
Commit complete.
```



```
localhost(config-vlan5)# end
localhost# show dhcp client ipv4 bindings vlan5 hostname
hostname localhost
```

9.3.2.5 Requesting a configuration file from the DHCP server (option 66, 67)

This feature allows DHCP clients to download their configuration from a TFTP server.

If you enable this function, a DHCP client sends a request with options 66 and 67 to a DHCP server to retrieve the following information:

- DHCP option 66: IP address or FQDN of a TFTP server
- DHCP option 67: Name of the configuration file

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. The loading and applying of the file is recorded in the system log (Syslog).

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.

If the function is enabled for multiple DHCP clients and the device receives multiple answers from multiple DHCP servers, the device uses the configuration file whose information is received first.

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Configure whether the DHCP client requests a configuration file.</p> <p>Options include:</p> <ul style="list-style-type: none"> • <code>off</code> - The function is disabled. The DHCP client does not request a configuration file. • <code>on</code> - The function is enabled. The DHCP client requests a configuration file with the next DHCP query. • <code>setup</code> - The function depends on the status of the device. <p>In the delivery state and after reset to default settings, the function behaves as with the setting <code>on</code>. 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 <code>off</code>. This means the function is disabled for all DHCP client interfaces.</p> <p>The status change takes place automatically and once.</p> <p>Default: <code>setup</code></p> | <pre>dhcp client ipv4 { IP interface } config-file-request [off on setup]</pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <pre>show dhcp client ipv4 bindings { IP interface } config-file- requested</pre> |

Example

In this example the function is disabled for the DHCP client interface `vlan5`.

```
localhost# config
```

```

Entering configuration mode terminal
localhost(config)# dhcp client ipv4 vlan5 config-file-request off
localhost(config-vlan5)# commit
Commit complete.
localhost(config-vlan5)# end
localhost# show dhcp client ipv4 bindings vlan5 config-file-
requested
config-file-requested off

```

9.3.3 Monitoring DHCP client interfaces

This section describes how you can view DHCP configuration data and monitor DHCP messages.

9.3.3.1 Listing configuration data of DHCP client interfaces

To list the configuration data of DHCP client interfaces, you can execute different commands in operating mode:

| Command | Description |
|--|---|
| show dhcp client ipv4 bindings | Shows the configuration data of all DHCP client interfaces. |
| show dhcp client ipv4 bindings { interface } | Shows the configuration data of a specific DHCP client interface. |

Example

The configuration data of the DHCP client interface `vlan1` are listed in detail in this example.

```

localhost# show dhcp client ipv4 bindings vlan1
  DHCP Bindings vlan1

Interface-enabled      true
Dhcp                   true
Client-id-type        mac-address
Client-id              10:00:00:00:00:01
Mac-address            10:00:00:00:00:01
Hostname-option-set   true
Hostname               SWITCH-VPM6002848
Ip-address             192.0.2.2
Netmask                -
Prefix-length         24
Broadcast-address     192.0.2.255
Domain-name            example.com
Domain-name-servers   [ 10.0.0.1 10.0.0.2 ]
Routers                [ 192.0.2.1 ]
Server-id              [ 192.0.2.1 ]
Lease-requested       2h

```

```

Lease-granted          2h
Lease-renew            2019-01-02 01:00:00 [YYYY-MM-DD HH:MM:SS]
Lease-rebind           2019-01-02 01:45:00 [YYYY-MM-DD HH:MM:SS]
Lease-expire           2019-01-02 02:00:00 [YYYY-MM-DD HH:MM:SS]
Config-file-requested  on
Tftp-server-name       tftp-server.com
Bootfile-name          sinec.xml

```

Description

The following information is shown:

| Parameter | Description |
|-----------------------|---|
| Interface-enabled | Indicates whether the interface at which the DHCP client sends DHCP requests to the DHCP server is enabled. |
| Dhcp | Indicates whether DHCP client is enabled for the above interface. |
| Client-id-type | Type of client ID |
| Client-id | ID the DHCP client uses to log in to the DHCP server |
| Mac-address | MAC address of the interface |
| Hostname-option-set | Indicates whether the host name of the DHCP client is used in communication with the DHCP server. |
| Hostname | Name of the host |
| Ip-address | IPv4 address of the interface |
| Netmask | Subnet displayed as subnet mask |
| Prefix-length | Subnet displayed as prefix length |
| Broadcast-address | Broadcast address that is used in the subnet of the DHCP client |
| Domain-name | Name of the domain |
| Domain-name-servers | List of DNS servers that the DHCP server offers to the DHCP client when it issues the lease to the DHCP client |
| Routers | List of assigned routers |
| Server-id | ID of the DHCP server |
| Lease-requested | Validity period formatted as nYnMnDnhnmns the DHCP client requested from the DHCP server |
| Lease-granted | Validity period formatted as nYnMnDnhnmns assigned by the DHCP server |
| Lease-renew | Date and time until which a DHCP client can unicast the validity of its current IP configuration to the DHCP server. |
| Lease-rebind | Date and time until which a DHCP client can extend the validity of its current IP configuration via broadcast to the DHCP server. |
| Lease-expire | Date and time at which the validity of the current IP configuration expires. |
| Config-file-requested | 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 |

9.3.3.2 Monitoring DHCP messages

To list the sent and received DHCP messages, you can execute different commands in operating mode:

| Command | Description |
|--|--|
| <code>show dhcp client ipv4 packet-statistics</code> | Shows the received and sent DHCP messages of all DHCP client interfaces. |
| <code>show dhcp client ipv4 packet-statistics receive</code> | Shows the received DHCP messages of all DHCP client interfaces. |
| <code>show dhcp client ipv4 packet-statistics send</code> | Shows the sent DHCP messages of all DHCP client interfaces. |
| <code>show dhcp client ipv4 packet-statistics { interface }</code> | Shows the received and sent DHCP messages of a specific DHCP client interface. |
| <code>show dhcp client ipv4 packet-statistics { interface } receive</code> | Shows the received DHCP messages of a specific DHCP client interface. |
| <code>show dhcp client ipv4 packet-statistics { interface } send</code> | Shows the sent DHCP messages of a specific DHCP client interface. |

Example

In this example, the received and sent DHCP messages of all DHCP client interfaces are displayed.

```
localhost# show dhcp client ipv4 packet-statistics
INTER- OFFER ACK NAK DECLINE DISCOVER REQUEST RELEASE
FACE PACKET PACKET PACKET PACKET PACKET PACKET PACKET
-----
vlan1 1 41 - - 1 41 -
vlan2 - - - - - - -
```

Example

Only the received DHCP messages of all DHCP client interfaces are listed in this example.

```
localhost# show dhcp client ipv4 packet-statistics receive
INTER- OFFER ACK NAK
FACE PACKET PACKET PACKET
-----
vlan1 1 41 -
vlan2 - - -
```

Description

The following information is shown:

| Parameter | Description |
|-----------------|--|
| OFFER PACKET | Number of received DHCP Offer messages |
| ACK PACKET | Number of received DHCP Ack messages |
| NAK PACKET | Number of received DHCP Nak messages |
| DECLINE PACKET | Number of sent DHCP Decline messages |
| DISCOVER PACKET | Number of sent DHCP Discover messages |

| Parameter | Description |
|----------------|-------------------------------------|
| REQUEST PACKET | Number of sent DHCPRequest messages |
| RELEASE PACKET | Number of sent DHCPRelease messages |

9.3.3.3 Clearing the statistics of DHCP messages

To clear the statistics of DHCP messages from all DHCP client interfaces, execute the following command in operating mode:

```
clear dhcp client
```

To clear the statistics of DHCP messages from a specific DHCP client interface, execute the following command in operating mode:

```
clear dhcp client { interface }
```

Example

```
localhost# clear dhcp client
Are you sure you want to clear the client packet statistics?
[yes,no] yes
```

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).

| |
|--|
| NOTICE |
| Configuration hazard - risk of traffic storms |
| If transitioning your network configuration from MRP to STP, make sure to completely disable MRP and then commit the changes before configuring STP. |

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

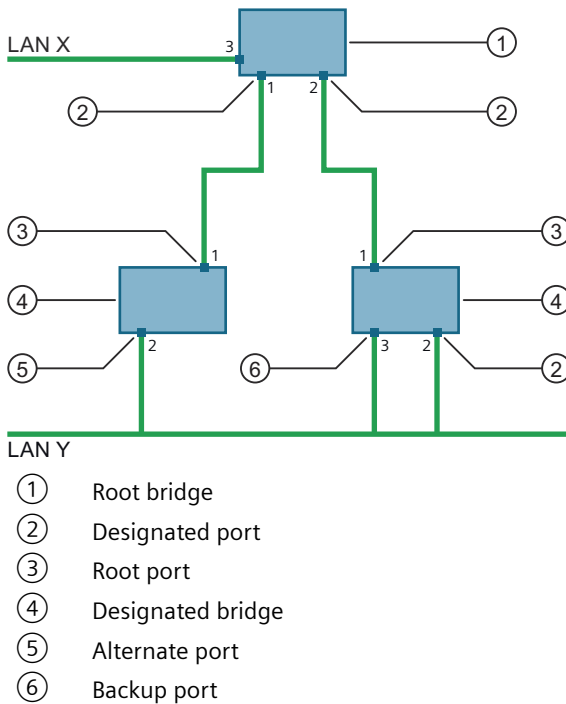


Figure 10-1 RSTP states and roles

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.
- **Master**
A port in the **master** role is an MST region boundary port. This role is only applicable to MSTP. Ports assigned the master role are the only port on the bridge that provides connectivity for the MSTI towards the CST root bridge.

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.
- **Blocking**
In the **blocking** state, the port is blocking all STP traffic.

Edge ports

A port may be designated as an **edge port** if it is directly connected to an end station. As such, it cannot create bridging loops in the network and can thus directly transition to the forwarding state, skipping the listening and learning states.

A port will lose its edge port status 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.

Since edge ports only service end stations, topology changes are not communicated to the root bridge when its link toggles.

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 (BID), an 8 byte field comprised of the assigned 2 byte bridge priority and the bridge's 6 byte MAC address.

The BID is important mainly at network startup when the bridge with the lowest ID is elected as the root bridge.

After startup, when all bridges agree on the root bridge's ID, 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 BID is selected.

Finally, if candidate root ports have the same path cost and peer bridge ID, the port ID of the peer bridge is used to select the root port. In all cases the lower BID, path cost, or port ID 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 ¼ of a second. The value of the maximum bridge diameter is thus four times the configured maximum age parameter.

Enhanced Passive Listening Compatibility (EPLC)

Enhanced Passive Listening Compatibility (EPLC) is an extension of Passive Listening. Like Passive Listening, EPLC is also a proprietary Siemens solution.

Both protocols are required for a redundant coupling between (R)STP networks and ring topologies to prevent network loops and reduce switchover times.

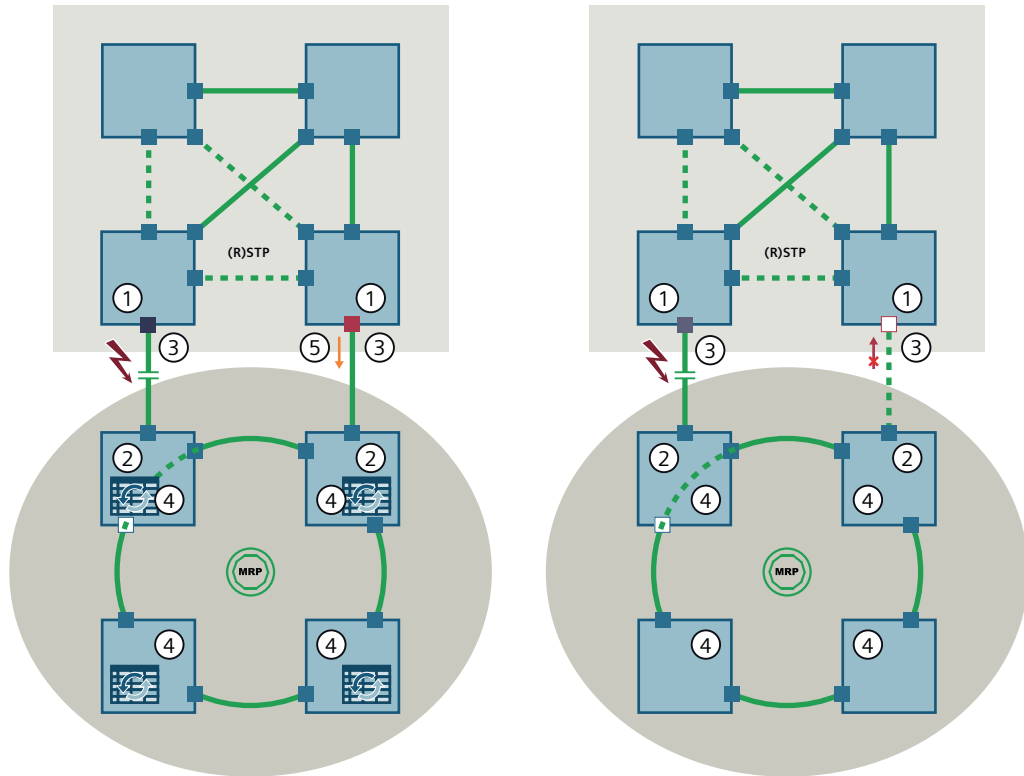
For more information about Passive Listening, refer to "Passive Listening (Page 436)".

If the active connection is dropped in a redundantly coupled (R)STP network and MRP ring with Passive Listening, the (R)STP coupling port in Blocking status does not receive any more (R)STP BPDUs. The port becomes the Edge port and switches to Forwarding status. Because an Edge port expects an end station as its connection partner, it does not send a Topology Change Notification (TCN) by default.

10.1 Spanning Tree Protocol (STP)

If EPLC is enabled for the port, the port sends a TCN. The connected ring devices react to the TCN, reduce their aging time temporarily, and update their MAC address table. This reduces the switchover time.

Enable EPLC on both (R)STP coupling ports.



Failure of the active connection

Sending of a TCN via an Edge port

- ① Coupling devices that belong to the (R)STP network
- ② Coupling devices that belong to the MRP ring
- ③ (R)STP ports with enabled EPLC
- ④ Ring device with enabled Passive Listening
- ⑤ Topology change message (TCN)
- Port in Link down status
- (R)STP port in Blocking status
- (R)STP port in Forwarding status

Figure 10-2 EPLC and topology changes

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.

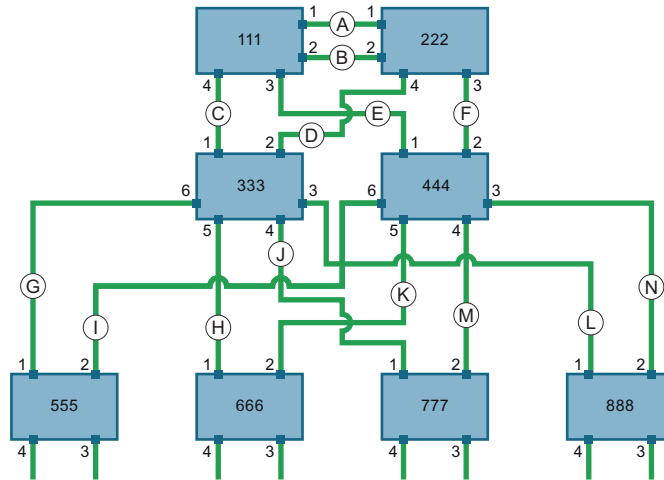


Figure 10-3 Example - RSTP structured wiring configuration

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.

10.1 Spanning Tree Protocol (STP)

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.

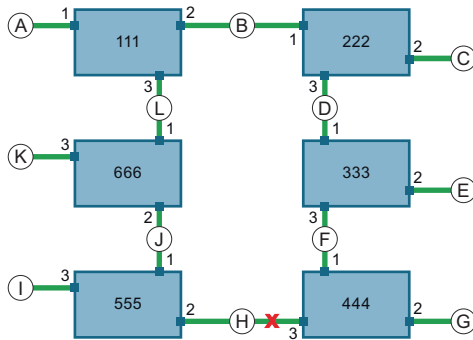


Figure 10-4 Example - RSTP ring backbone configuration

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, 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.
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.

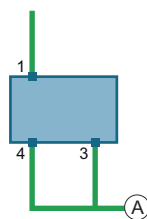


Figure 10-5 Example - Port redundancy

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 351)".
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 373)".
3. Create static VLANs and map them to the MSTIs.
For more information, refer to "Mapping a VLAN to an MSTI (Page 375)".

10.1 Spanning Tree Protocol (STP)

4. Set the STP protocol version to MSTP.
For more information, refer to "Selecting the STP version (Page 352)".
5. Configure the region revision level.
For more information, refer to "Configuring the region revision level (Page 373)".
6. Enable STP.
For more information, refer to "Enabling STP (Page 351)".

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 644)".

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 351)".
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 352)".
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 353)".
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 354)".
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 355)".
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 358)".

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 356)".
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 357)".

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 366)".
- For MSTP, configure the global MSTP settings and define MSTIs.
For more information, refer to "Configuring MSTP (Page 371)".

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.

| Step | Instruction | Command |
|------|-----------------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the Spanning Tree service. | <code>switch spanning-tree enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch spanning-tree</code> |

10.1 Spanning Tree Protocol (STP)

Example

The following enables the Spanning Tree services.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree enabled
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show running-config switch spanning-tree
switch
  spanning-tree
    enabled
  exit

exit
```

10.1.2.2 Selecting the STP version

To control which version of Spanning Tree the bridge uses, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select which version of STP the bridge will use. Options include: <ul style="list-style-type: none"> <code>rstp</code> - The bridge will operate using the Rapid Spanning Tree Protocol (RSTP) <code>mstp</code> - The bridge will operate using the Multiple Spanning Tree Protocol (MSTP) Default: <code>rstp</code> | <code>switch spanning-tree version [rstp mstp]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch spanning-tree version</code> |

Example

The following example sets the Spanning Tree version to mstp for Multiple Spanning Tree Protocol.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree version mstp
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show running-config switch spanning-tree version
switch
 spanning-tree
  version mstp
exit

exit
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Select the bridge priority for the bridge. Default: 32768 | switch spanning-tree priority [0 4096 8192 12288 16384 20480 24576 28672 32768 36864 40960 45056 49152 53248 57344 61440] |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch spanning-tree priority |

10.1 Spanning Tree Protocol (STP)

Example

The following sets the bridge priority to 4096. If the bridge priority for another bridge is 0, that bridge will be made the root bridge and this bridge will be second in line. If no other bridge has a lower bridge priority, this bridge will be made the root bridge.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree priority 4096
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show running-config switch spanning-tree priority
switch
 spanning-tree
  priority 4096
exit

exit
```

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.

To configure the Hello time for the bridge, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the Hello time in seconds. Default: 2 | <code>switch spanning-tree hello-time { 1 - 10 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch spanning-tree hello-time</code> |

Example

The following configuration sets the time between configuration messages to 4 seconds.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree hello-time 4
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show running-config switch spanning-tree hello-time
switch
 spanning-tree
  hello-time 4
exit

exit
```

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the maximum aging time in seconds for all bridges. 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 | <code>switch spanning-tree max-age-time { 6 - 40 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch spanning-tree max-age-time</code> |

Example

The following changes the maximum aging time to 30 seconds for all bridges.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree max-age-time 30
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show running-config switch spanning-tree max-age-time
switch
  spanning-tree
    max-age-time 20
  exit

exit
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the transmit hold count. Options include: <ul style="list-style-type: none"> • { number } - A number between 3 and 100 • unlimited - There is no limit to the number of BPDUs that can be sent Default: unlimited | <code>switch spanning-tree transmit-count [{ 3 - 100 } unlimited]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch spanning-tree transmit-count</code> |

Example

The following changes the transmit hold count to four BPDUs per second for each interface.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree transmit-count 4
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show running-config switch spanning-tree transmit-count
switch
 spanning-tree
  transmit-count 4
exit

exit
```

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Configure the forward delay timer. Default: 15 | switch spanning-tree forward-delay { 4 - 30 } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch spanning-tree forward-delay |

Example

The following sets the forward delay timer to 10 seconds. Ports will transition to the forwarding state after 10 seconds.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree forward-delay 10
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show running-config switch spanning-tree forward-delay
switch
 spanning-tree
  forward-delay 10
exit

exit
```

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 358)".
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 359)".
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 360)".
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 361)".
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 362)".
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 363)".
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 364)".
8. [Optional] Enable Enhanced Passive Listening Compatibility (EPLC) for two (R)STP coupling ports.
EPLC must be enabled for two (R)STP coupling ports.
For more information, refer to "Enabling Enhanced Passive Listening Compatibility (EPLC) (Page 365)".

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.

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable Spanning Tree for the selected bridge port. | interface { bridge port } spanning-tree enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. Make sure to use the detail command. Information will not be displayed otherwise. | show running-config interface { bridge port } spanning-tree detail |

Example

The following enables Spanning Tree for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 spanning-tree enabled
localhost(config-interface-ethernet0/1-spanning-tree)# commit
Commit complete.
localhost(config-interface-ethernet0/1-spanning-tree)# end
localhost# show running-config interface ethernet0/1 spanning-tree | detail
interface ethernet0/1
 spanning-tree
  enabled
  port-priority 128
  cost auto
  edge-port auto
  link-type auto
  no restricted-role
  no restricted-tcn
exit

exit
```

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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the port cost for the selected bridge port. Options include: <ul style="list-style-type: none"> • { 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: 20000 (physical interfaces) or 199999 (port channels) | <code>interface { bridge port } spanning-tree cost [{ 1 - 2147483647 } auto]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } spanning-tree cost</code> |

Example

The following sets the port cost to 1000 for bridge port ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 spanning-tree cost 1000
localhost(config-interface-ethernet0/1-spanning-tree)# commit
Commit complete.
localhost(config-interface-ethernet0/1-spanning-tree)# end
localhost# show running-config interface ethernet0/1 spanning-tree cost
interface ethernet0/1
  spanning-tree
    cost 1000
  exit
exit
```

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.

To select the port priority for a bridge port, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Select the port priority for the selected bridge port. Default: 128 | interface { bridge port } spanning-tree port-priority [0 16 32 48 64 80 96 112 128 144 160 176 194 208 224 240] |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } spanning-tree port-priority |

Example

The following sets the port priority to 240 for bridge port ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 spanning-tree port-priority 240
localhost(config-interface-ethernet0/1-spanning-tree)# commit
Commit complete.
localhost(config-interface-ethernet0/1-spanning-tree)# end
localhost# show running-config interface ethernet0/1 spanning-tree port-
priority
interface ethernet0/1
 spanning-tree
  port-priority 240
exit

exit
```

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select the edge port state for the selected bridge port. Options include: <ul style="list-style-type: none"> • <code>enabled</code> - The bridge port is designated as an edge port • <code>disabled</code> - The edge port state is removed from the bridge port • <code>auto</code> - The bridge port is designated as an edge port automatically Default: <code>auto</code> | <code>interface { bridge port } spanning-tree edge-port [enabled disabled auto]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } spanning-tree edge-port</code> |

Example

The following explicitly makes `ethernet0/1` an edge port.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 spanning-tree edge-port enable
localhost(config-interface-ethernet0/1-spanning-tree)# commit
Commit complete.
localhost(config-interface-ethernet0/1-spanning-tree)# end
localhost# show running-config interface ethernet0/1 spanning-tree edge-
port
interface ethernet0/1
 spanning-tree
  edge-port enable
exit

exit
```

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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select the port link type for the selected bridge port. Options include: <ul style="list-style-type: none"> <code>point-to-point</code> - The bridge port operates in half-duplex mode, but is a point-to-point link <code>shared</code> - The bridge port operates in full-duplex mode, but it is a shared link <code>auto</code> - Automatically sets the port link type to <code>point-to-point</code> if the bridge port is in full-duplex mode, or <code>shared</code> if the port is in half-duplex mode Default: <code>auto</code> | <code>interface { bridge port } spanning-tree link-type [point-to-point shared auto]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } spanning-tree link-type</code> |

Example

The following sets the port link type to point-to-point for bridge port `ethernet0/1`.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 spanning-tree link-type point-to-point
localhost(config-interface-ethernet0/1-spanning-tree)# commit
Commit complete.
localhost(config-interface-ethernet0/1-spanning-tree)# end
localhost# show running-config interface ethernet0/1 spanning-tree link-type
interface ethernet0/1
 spanning-tree
  link-type point-to-point
exit

exit
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Restrict the role of the selected bridge port. | interface { bridge port } spanning-tree restricted-role |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } spanning-tree restricted-role |

Example

The following marks ethernet0/1 as **restricted**.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 spanning-tree restricted-role
localhost(config-interface-ethernet0/1-spanning-tree)# commit
Commit complete.
localhost(config-interface-ethernet0/1-spanning-tree)# end
localhost# show running-config interface ethernet0/1 spanning-tree
restricted-role
interface ethernet0/1
  spanning-tree
    restricted-role
  exit

exit
```

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Restrict the selected bridge port from forwarding TCNs. | interface { bridge port } spanning-tree restricted-tcn |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } spanning-tree restricted-tcn |

Example

The following prevents ethernet0/1 from forwarding TCNs.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 spanning-tree restricted-tcn
localhost(config-interface-ethernet0/1-spanning-tree)# commit
Commit complete.
localhost(config-interface-ethernet0/1-spanning-tree)# end
localhost# show running-config interface ethernet0/1 spanning-tree
restricted-tcn
interface ethernet0/1
 spanning-tree
  restricted-tcn
exit

exit
```

10.1.3.8 Enabling Enhanced Passive Listening Compatibility (EPLC)

By default, EPLC is disabled for all bridge ports.

Enable EPLC on both (R)STP coupling ports.

To enable EPLC for a bridge port, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable EPLC for the selected bridge port. | <code>interface { bridge port } spanning-tree enhanced-passive-listening-compatibility</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } spanning-tree enhanced-passive-listening- compatibility</code> |

Example

In this example, EPLC is enabled for ethernet0/9.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/9 spanning-tree enhanced-passive-
listening-compatibility
localhost(config-interface-ethernet0/9-spanning-tree)# commit
Commit complete.
localhost(config-interface-ethernet0/9-spanning-tree)# end
localhost# show running-config interface ethernet0/9 spanning-tree
enhanced-passive-listening-compatibility
interface ethernet0/9
 spanning-tree
  enhanced-passive-listening-compatibility
exit

exit
```

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 367)".
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 368)".

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 369)".
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 370)".

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 355)".

To select the maximum network diameter, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select the maximum network diameter. Options include: <ul style="list-style-type: none"> • <code>max-age-time</code> - The maximum network diameter is equal to the maximum aging time • <code>4x-max-age-time</code> - The maximum network diameter is four times (4x) larger than the maximum aging time Default: <code>4x-max-age-time</code> | <code>switch spanning-tree erstp max-network-diameter [max-age-time 4x-max-age-time]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show switch spanning-tree erstp max-network-diameter</code> |

10.1 Spanning Tree Protocol (STP)

Example

The following sets the maximum network diameter to the standard RSTP, which is equal to the value of the maximum aging time.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree erstp max-network-diameter max-age-
time
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show switch spanning-tree erstp max-network-diameter
switch
spanning-tree
  erstp max-network-diameter max-age-time
exit

exit
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Configure BPDU Guard Timeout. Options include: <ul style="list-style-type: none"> • { seconds } - Disables ports for the specified number of seconds if they receive a BPDU from an unexpected device • until-reset - Disables ports until they are re-enabled if they receive a BPDU from an unexpected device • do-not-shutdown - Disables BPDU Guard Timeout Default: do-not-shutdown | switch spanning-tree erstp bpdu-guard-timeout [{ 1 - 86400 } until-reset do-not-shutdown] |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------|---|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show switch spanning-tree erstp max-age-time |

Example

The following configures BPDU Guard Timeout to disable ports for 30 seconds if they receive a BPDU from an unexpected device.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree erstp bpdu-guard-timeout 30
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show switch spanning-tree erstp bpdu-guard-timeout
switch
 spanning-tree
  erstp bpdu-guard-timeout 30
exit

exit
```

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Select the Fast Root Failover mechanism. Options include: <ul style="list-style-type: none"> • on - Enables Fast Root Failover in robust mode • on-with-standard-root - Enables Fast Root Failover in relaxed mode • off - Disables Fast Root Failover Default: on | switch spanning-tree erstp fast- root-failover [on on-with- standard-root off] |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------|---|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show switch spanning-tree erstp fast-root-failover |

Example

The following enables Fast Root Failover in **relaxed** mode. This is required if the root bridge does not support the Fast Root Failover mechanism.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree erstp fast-root-failover on-with-
standard-root
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show switch spanning-tree erstp fast-root-failover
switch
  spanning-tree
    erstp fast-root-failover on-with-standard-root
  exit
exit
```

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:

| Step | Instruction | Command |
|------|--------------------------------------|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable IEEE 802.1w interoperability. | switch spanning-tree erstp ieeedot1w-interoperability |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show switch spanning-tree erstp ieeedot1w-interoperability |

Example

The following enables IEEE 802.1w interoperability.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree erstp ieee8021w-interoperability
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show switch spanning-tree erstp ieee8021w-interoperability
switch
  spanning-tree
    erstp ieee8021w-interoperability
  exit

exit
```

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 371)".
2. Add the name of the region.
For more information, refer to "Adding the region name (Page 372)".
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 373)".
4. Configure one or more Multiple Spanning Tree Instances (MSTIs).
For more information, refer to "Configuring Multiple Spanning Tree Instances (MSTIs) (Page 373)".

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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Select the maximum number of hops. Default: 20 | switch spanning-tree mstp max-hops { 6 - 40 } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show switch spanning-tree mstp max-hops |

10.1 Spanning Tree Protocol (STP)

Example

The following sets the maximum number of hops to 10. If a BPDU traverses more than 10 bridges, it will be dropped by the eleventh bridge.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree mstp max-hops 10
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show switch spanning-tree mstp max-hops
switch
  spanning-tree
    mstp max-hops 10
  exit

exit
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enter the name of the MSTP region. Default: 00-0A-DC-92-00-00 | <code>switch spanning-tree mstp region name { name }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show switch spanning-tree mstp region name</code> |

Example

The following sets the MSTP region name to `sinecos`.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree mstp region name sinecos
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show switch spanning-tree mstp region name
switch
  spanning-tree
    mstp region name sinecos
  exit

exit
```

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the revision level. Default: 0 | <code>switch spanning-tree mstp region revision { 0 - 65535 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show switch spanning-tree mstp region revision</code> |

Example

The following sets the revision level for the device to 2.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree mstp region revision 2
localhost(config-switch-spanning-tree)# commit
Commit complete.
localhost(config-switch-spanning-tree)# end
localhost# show switch spanning-tree mstp region revision
switch
 spanning-tree
  mstp region revision 2
exit

exit
```

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 374)".
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 375)".
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 375)".
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 376)".
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 377)".

10.1.6.1 Creating an MSTI

To create an MSTI, do the following:

| Step | Instruction | Command |
|------|---------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Create the MSTI. | <code>switch spanning-tree mstp mst { 1 - 16 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show switch spanning-tree mstp mst</code> |

Example

The following creates an MSTI with an ID of 2.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree mstp mst 2
localhost(config-mst-2)# commit
Commit complete.
localhost(config-mst-2)# end
localhost# show switch spanning-tree mstp mst
mstp mst 2
  bridge-status          unknown

  root-cost              0
  total-topology-changes 0
```

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Select the bridge priority for the selected MSTI. Default: 32768 | switch spanning-tree mstp mst { MSTI ID } bridge [0 4096 8192 12288 16384 20480 24576 28672 32768 36864 40960 45056 49152 53248 57344 61440] |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show switch spanning-tree mstp mst { MSTI ID } bridge |

Example

The following sets the bridge priority for MST 2 to 4096.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch spanning-tree mstp mst 2 bridge 4096
localhost(config-mstp)# commit
Commit complete.
localhost(config-mstp)# end
localhost# show switch spanning-tree mstp mst 2 bridge
spanning-tree
 mstp
  mst 2
    bridge 4096
  exit
exit
exit
```

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.

10.1 Spanning Tree Protocol (STP)

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Map the selected VLAN to an MSTI. Default: 0 | switch vlan { VLAN ID } msti { MSTI ID } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch vlan { VLAN ID } msti |

Example

The following maps VLAN 10 to MST 2.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch vlan 10 msti 2
localhost(config-switch-vlan-10)# commit
Commit complete.
localhost(config-switch-vlan-10)# end
localhost# show running-config switch vlan 10 msti
switch
  vlan 10
    msti 2
  exit

exit
```

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.

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Configure the MSTI port priority for the bridge port. Default: 128 | interface { bridge port } spanning-tree mst { MSTI ID } port-priority [0 16 32 48 64 80 96 112 128 144 160 176 194 208 224 240] |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } spanning-tree mst { MSTI ID } port-priority |

Example

The following sets the port priority for ethernet0/1 on MSTI 1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 spanning-tree mst 1 port-priority
144
localhost(config-mst-1)# commit
Commit complete.
localhost(config-mst-1)# end
localhost# show running-config interface ethernet0/1 spanning-tree mst 1
port-priority
interface ethernet0/1
spanning-tree
mst 1
port-priority 144
exit

exit

exit
```

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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Configure the MSTI cost for the bridge port. Options include: <ul style="list-style-type: none"> { 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 | interface { bridge port } spanning-tree mst { MSTI ID } cost { { 1 - 2147483647 } auto } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } spanning-tree mst { MSTI ID } cost |

10.1 Spanning Tree Protocol (STP)

Example

The following sets the cost to 30,000 for ethernet0/1 on MSTI 1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 spanning-tree mst 1 cost 30000
localhost(config-mst-1)# commit
Commit complete.
localhost(config-mst-1)# end
localhost# show running-config interface ethernet0/1 spanning-tree mst 1
cost
interface ethernet0/1
 spanning-tree
  mst 1
    cost 30000
  exit
exit
exit
```

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, execute the following command in operational mode:

```
show switch spanning-tree
```

Alternatively, to display only specific information, execute the same command with the relevant option:

```
show switch spanning-tree [ bridge-status | bridge-id | root-id | root-port
| root-cost | learned-hello-time | learned-forward-delay | learned-max-age
| total-topology-changes | time-since-last-tc ]
```

Example

The following displays the status and statistics for the Spanning Tree service:

```
localhost# show switch spanning-tree
spanning-tree
  bridge-status          designated-bridge
  bridge-id              32768/D4:F5:27:5A:1B:B0
  root-id                0/94:B8:C5:12:E7:00
  root-port              ethernet0/3
  root-cost               220000
  learned-hello-time     2
  learned-forward-delay  15
  learned-max-age        20
  total-topology-changes 5436
  time-since-last-tc     56m20.47s
  mstp regional-root-id  32768/D4:F5:27:5A:1B:B0
  mstp regional-root-cost 0
  mstp region digest     AC36177F50283CD4B83821D8AB26DE62
```

Example

The following displays only the bridge ID:

```
localhost# show switch spanning-tree bridge-id
bridge-id 32768/D4:F5:27:5A:1B:B0
```

Description

The following information can be displayed:

| 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. |

| Parameter | Description |
|-------------------------|--|
| 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. |
| total-topology-change | 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-last-tc | 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 |
| mstp regional-root-id | The MSTP regional root ID. This is a combination of the priority and the device's MAC address. |
| mstp regional-root-cost | The root cost of the MST region. |
| mstp region digest | The 16-octet signature that details characteristics of the device's MST region. 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, each BPDU forwarded by a bridge includes this region (or configuration) digest. 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. |

10.1.7.2 Displaying the status of STP per bridge port

To display the status of a bridge port for which Spanning Tree is enabled, execute the following command in operational mode:

```
show interface { bridge port } spanning-tree
```

Alternatively, to display only specific information, execute the same command with the relevant option:

```
show interface { bridge port } spanning-tree [ state | role | oper-cost | rx-rst | tx-rst | designated-bridge-id | oper-edge ]
```

Example

The following displays the status and statistics of the Spanning Tree service for ethernet0/1:

```
localhost# show interface ethernet0/1 spanning-tree
spanning-tree
state                forwarding
role                 root
oper-cost             200000
rx-rst               318970
tx-rst                7
designated-bridge-id 28672/00:0A:DC:2D:BB:00
oper-edge             false
```

Example

The following displays only the state of the Spanning Tree service for ethernet0/1:

```
localhost# show interface ethernet0/1 spanning-tree state
state forwarding
```

Description

The following information can be displayed:

| Parameter | Description |
|----------------------|---|
| state | <p>The state of the bridge port.</p> <p>Possible values:</p> <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 | <p>The role of the bridge port.</p> <p>Possible values:</p> <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. |
| oper-cost | <p>The operational cost of the bridge port.</p> <p>A bridge port that transitions to STP will have its operational cost limited to 65535.</p> |
| rx-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 | <p>The designated bridge ID for the bridge port.</p> <p>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.</p> |
| oper-edge | <p>The operational edge state of a bridge port.</p> <p>Possible values:</p> <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, execute the following command in operational mode:

```
show switch spanning-tree mstp mst { MST ID }
```

Alternatively, to display only specific information, execute the same command with the relevant option:

```
show switch spanning-tree mstp mst { MST ID } [ bridge-status | bridge-id | root-id | root-port | root-cost | total-topology-changes ]
```

Example

The following displays the status and statistics for MST 2:

```
localhost# show switch spanning-tree mstp mst 2
spanning-tree
 mstp
  mst 2

    bridge-status designated-bridge
    bridge-id 32768/00:01:02:03:04:05
    root-id 32768/00:01:02:03:04:05
    root-port ethernet0/1
    root-cost 10000
    total-topology-changes 55
  exit

exit

exit
```

Example

The following displays only the bridge status for MST 2:

```
localhost# show switch spanning-tree mstp mst 2 bridge-status
spanning-tree
 mstp
  mst 2
    bridge-status designated-bridge
  exit
exit
exit
```

Description

The following information can be displayed:

| Parameter | Description |
|---------------|--|
| bridge-status | The bridge status of the MSTI. Possible values: <ul style="list-style-type: none"> unknown - The bridge status cannot be determined root-bridge - The MSTI is the root bridge designated-bridge - The MSTI is the designated bridge not-designated-for-any-lan - The MSTI is not designated for any LAN |
| bridge-id | The bridge ID of the MSTI. An MSTI's bridge ID is a combination of the bridge priority and the device's MAC address. A bridge ID is only assigned to an MSTI once it is mapped to a VLAN. |
| root-id | The root ID of the MSTI. An MSTI's root ID is a combination of the bridge priority and the device's MAC address. A root ID is only assigned to an MSTI once it is mapped to a VLAN. |
| root-port | The root port used by the MSTI. When the MSTI is the designated bridge, the root port is the port that provides connectivity towards the root bridge of the MSTP network. |

| Parameter | Description |
|------------------------|--|
| root-cost | The root path cost for the MSTI. The root path cost is the total cost of the path to the root bridge composed of the sum of the costs of each link in the path. 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 Internal Spanning Tree (IST) root bridge to the Common Spanning Tree (CST) root bridge. |
| total-topology-changes | The number of topology changes detected by the MSTI since STP statistics were last cleared. Each MSTI counts the number of topology changes by tracking link failures and signals from other bridges on the MSTP network. An excessively high count or rapidly increasing count signals network issues. |

10.1.7.5 Displaying the status of an MSTI per bridge port

To display the status of an MSTI assigned to a bridge port, execute the following command in operational mode:

```
show interface { bridge port } spanning-tree mst { MST ID }
```

Alternatively, to display only specific information, execute the same command with the relevant option:

```
show interface { bridge port } spanning-tree mst { MST ID } [ state | role  
| oper-cost | designated-bridge-id ]
```

Example

The following displays the status and statistics for MST 2 on ethernet0/1:

```
localhost# show interface ethernet0/1 spanning-tree mst 2 state
spanning-tree
mstp
mst 2
state forwarding
role designated
oper-cost 10000
designated-bridge-id 32768/00:01:02:03:04:05
exit

exit

exit
```

Example

The following displays only the state of MST 2 on ethernet0/1:

```
localhost# show interface ethernet0/1 spanning-tree mst 2 state
spanning-tree
  mstp
    mst 2
      state forwarding
    exit
  exit
exit
```

Description

The following information can be displayed:

| Parameter | Description |
|-----------|---|
| state | <p>The state of the MSTI.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <code>disabled</code> - STP is disabled on the port • <code>blocking</code> - The port is blocking traffic • <code>learning</code> - The port is learning MAC addresses to prevent flooding when it begins forwarding traffic • <code>forwarding</code> - The port is forwarding traffic • <code>linkdown</code> - STP is enabled on the port, but the link is down • <code>discarding</code> - 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"> • <code>designated</code> - The port is designated for (i.e. carries traffic towards the root for) the LAN to which it is connected. • <code>root</code> - The single port on the bridge, which provides connectivity towards the root bridge. • <code>backup</code> - The port is attached to a LAN that is serviced by another port on the bridge. It is not used, but is standing by. • <code>alternate</code> - The port is attached to a bridge that provides connectivity to the root bridge. It is not used, but is standing by. • <code>master</code> - 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). |

| Parameter | Description |
|----------------------|--|
| oper-cost | The operational cost of the MSTI. |
| designated-bridge-id | The MSTI designated bridge ID for the bridge port. 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. |

10.1.7.6 Clearing STP statistics

To clear all Spanning Tree statistics collected by the device, enter the following command in operational mode:

```
switch spanning-tree clear-statistics
```

When a confirmation message appears, enter "yes".

Example

```
localhost# switch spanning-tree clear-statistics
Are you sure you want to clear all spanning tree statistics?
[no,yes] yes
localhost#
```

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.

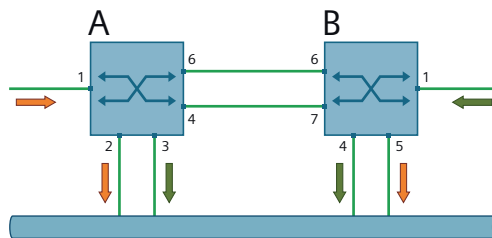


Figure 10-6 Example of a basic MSTP configuration

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 531)".
2. Create VLAN interfaces for the new VLANs.
For more information, refer to "Adding a VLAN interface (Page 290)".

10.1 Spanning Tree Protocol (STP)

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 535)".
4. Map VLAN 20 to bridge ports ethernet0/3 and ethernet0/4.
For more information, refer to "Configuring the port VLAN ID (Page 535)".
5. Assign the IP address `192.168.10.1` to the VLAN10 interface.
For more information, refer to "Configuring a static IPv4 address (Page 315)".
6. Assign the IP address `192.168.20.1` to the VLAN20 interface.
For more information, refer to "Configuring a static IPv4 address (Page 315)".
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 534)".
8. Set the Spanning Tree version to `mstp`.
For more information, refer to "Selecting the STP version (Page 352)".
9. Set the name of the MSTP region to `sinecos`.
For more information, refer to "Adding the region name (Page 372)".
10. Set the region revision level for the MSTP region to `1`.
For more information, refer to "Configuring the region revision level (Page 373)".
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 375)".

Configuration of Device B

To configure device B, do the following:

1. Create VLANs 10 and 20.
For more information, refer to "Adding or modifying a static VLAN (Page 531)".
2. Create VLAN interfaces for the new VLANs.
For more information, refer to "Adding a VLAN interface (Page 290)".
3. Map VLAN 10 to bridge ports ethernet0/5 and ethernet0/6.
For more information, refer to "Configuring the port VLAN ID (Page 535)".
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 535)".
5. Assign the IP address `192.168.10.2` to the VLAN10 interface.
For more information, refer to "Configuring a static IPv4 address (Page 315)".
6. Assign the IP address `192.168.20.2` to the VLAN20 interface.
For more information, refer to "Configuring a static IPv4 address (Page 315)".
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 534)".
8. Set the Spanning Tree version to `mstp`.
For more information, refer to "Selecting the STP version (Page 352)".
9. Set the name of the MSTP region to `sinecos`.
For more information, refer to "Adding the region name (Page 372)".

10. Set the region revision level for the MSTP region to 1.
For more information, refer to "Configuring the region revision level (Page 373)".
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 375)".

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:

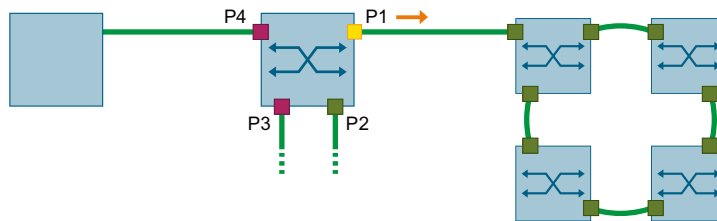


Figure 10-7 Port modes of Loop Detection

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.

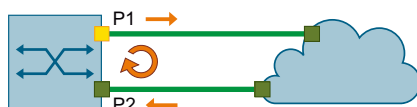


Figure 10-8 Local network loop

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.

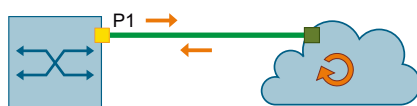


Figure 10-9 Remote network loop

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 Loop Detection

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. Ensure that the configuration of your device meets the configuration requirements for sending PDUs.
For more information, refer to "Requirements for sending PDUs (Page 393)".
2. 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 394)".
3. [Optional] Configure the interval at which a bridge port sends PDUs.
For more information, refer to "Configuring the send interval (Page 395)".
4. [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 396)".
5. [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 397)".
6. [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 398)".
7. [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 399)".
8. Enable taking into account the VLAN configuration of a bridge port.
For more information, refer to "Enabling VLAN mode (Page 401)".
9. Enable Loop Detection.
For more information, refer to "Enabling Loop Detection (Page 401)".
10. [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 402)".

10.2.2.1 Requirements for sending PDUs

Successful configuration of loop detection depends on the settings of other functions.

You can display and check the current configuration with the commands in the following table. The links lead to additional information and to the commands with which you can adapt the configuration according to the requirements for sending mode.

Before you configure sending mode for a bridge port, check the following settings and change the configuration if necessary:

| Instruction | Command |
|--|---|
| <p>Make sure that STP is disabled for the ports for which you wish to configure sending mode.</p> <p>Compatible configuration: <code>disabled</code></p> <p>For more information on the status of STP for a bridge port, refer to "Displaying the status of STP per bridge port (Page 380)".</p> <p>For more information on configuring STP for a port, refer to "Enabling STP for a bridge port (Page 358)".</p> | <pre>show interface { bridge port } spanning-tree state</pre> |
| <p>Make sure that MRP is disabled globally.</p> <p>Compatible configuration: <code>no enabled</code></p> <p>For more information, refer to "Enabling MRP globally (Page 428)".</p> | <pre>show running-config switch mrp enabled</pre> |
| <p>Make sure the ports for which you wish to configure sending mode are not DLR ports.</p> <p>For more information on configuring DLR ports, refer to "Selecting the DLR ports (Page 411)".</p> | <pre>show ethernetip device-level-ring ring-port1</pre> <pre>show ethernetip device-level-ring ring-port2</pre> |

Example

This example checks whether sending mode can be configured for the `ethernet0/1` bridge port.

```
localhost# show interface ethernet0/1 spanning-tree state
state disabled
localhost# show running-config switch mrp enabled
switch
  mrp
    no enabled
  exit

exit

localhost# show ethernetip device-level-ring ring-port1
ring-port1          ethernet0/6
ring-port1-status   up
localhost# show ethernetip device-level-ring ring-port2
ring-port2          ethernet0/7
ring-port2-status   up
```

10.2.2.2 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 390)".

To configure how a bridge port processes PDUs for the detection of network loops, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | For the desired bridge port, configure whether it sends and forwards PDUs for the detection of network loops. Options include: <ul style="list-style-type: none"> <code>blocking</code> - The bridge port sends no PDUs and does not forward PDUs. <code>forwarding</code> - The bridge port only forwards PDUs. <code>sending</code> - The bridge port sends PDUs and forwards PDUs. Default: <code>forwarding</code> | <code>interface { bridge port } loop-detection tx-state [blocking forwarding sending]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } loop-detection tx-state</code> |

Example

In this example, it is configured for `ethernet0/1` that it sends and forwards PDUs.

```
localhost# show interface ethernet0/1 spanning-tree state
state disabled
localhost# show switch mrp ring-id 1 ring-port1-oper
ring-port1-oper ethernet0/3
localhost# show switch mrp ring-id 1 ring-port2-oper
ring-port1-oper ethernet0/4
localhost# show ethernetip device-level-ring ring-port1
ring-port1          ethernet0/6
ring-port1-status   up
localhost# show ethernetip device-level-ring ring-port2
ring-port2          ethernet0/7
ring-port2-status   up
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 loop-detection tx-state
sending
localhost(config-interface-ethernet0/1-loop-detection)# commit
Commit complete.
localhost(config-interface-ethernet0/1-loop-detection)# end
localhost# show running-config interface ethernet0/1 loop-detection
tx-state
interface ethernet0/1
```

```

loop detection
  tx-state sending
exit

exit

```

10.2.2.3 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 applied only when a bridge port sends and forwards PDUs (`sending` parameter). For more information, refer to "Configuring bridge ports for the detection of network loops (Page 394)".

To configure the send interval for PDUs, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the transmit interval for PDUs. Conditions: <ul style="list-style-type: none"> Formatted as <code>nYnMnDnhnmns</code>, where <code>n</code> is a user-defined number Minimum 0.5 seconds (<code>0.5s</code>) Maximum 5 seconds (<code>5s</code>) Default: <code>1s</code> (1 second) | <code>interface { bridge port } loop-detection tx-interval { 0.5s - 5s }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } loop-detection tx-interval</code> |

Example

In this example, a send interval of 1.5 seconds is configured for `ethernet0/1`.

```

localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 loop-detection tx-interval
1.5s
localhost(config-interface-ethernet0/1-loop-detection)# commit
Commit complete.
localhost(config-interface-ethernet0/1-loop-detection)# end
localhost# show running-config interface ethernet0/1 loop-detection
tx-interval
interface ethernet0/1
  loop detection
    tx-interval 1.5s
exit

exit

```

10.2.2.4 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.

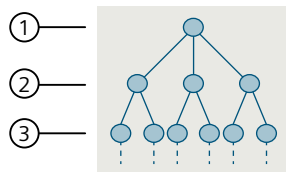


Figure 10-10 Tree topology

To define the limit for the detection of a local network loop, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define the number of received PDUs after which the function detects a local network loop. Default: 2 | <code>interface { bridge port } loop-detection detect-threshold { 1 - 500 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } loop-detection detect-threshold</code> |

Example

In this example, it is configured for `ethernet0/1` that it detects a local network loop as soon as it receives a PDU that it sent itself.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 loop-detection detect-threshold 1
localhost(config-interface-ethernet0/1-loop-detection)# commit
Commit complete.
localhost(config-interface-ethernet0/1-loop-detection)# end
localhost# show running-config interface ethernet0/1 loop-detection
detect-threshold
interface ethernet0/1
  loop detection
    detect-threshold 1
  exit
exit
```

10.2.2.5 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 on the bridge port at which a local network loop was detected, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Configure the effects of a local network loop on the desired bridge port.</p> <p>Options include:</p> <ul style="list-style-type: none"> <code>disable-if</code> - As soon as the function detects a local network loop, it disables the bridge port. The network loop is interrupted. <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 402)". 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 399)". <code>no-reaction</code> - A local network loop has no effects on the bridge port. <p>Default: <code>disable-if</code></p> | <pre>interface { bridge port } loop- detection reaction-local [disable-if no-reaction]</pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <pre>show running-config interface { bridge port } loop-detection reaction-local</pre> |

Example

In this example, it is configured for `ethernet0/1` that a local network loop has no effects on the bridge port.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 loop-detection reaction-
local no-reaction
localhost(config-interface-ethernet0/1-loop-detection)# commit
Commit complete.
localhost(config-interface-ethernet0/1-loop-detection)# end
```

```
localhost# show running-config interface ethernet0/1 loop-detection
reaction-local
interface ethernet0/1
  loop detection
    reaction-local no-reaction
  exit
exit
```

10.2.2.6 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 on the bridge port at which a remote network loop was detected, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Configure the effects of a remote network loop on the desired bridge port.</p> <p>Options include:</p> <ul style="list-style-type: none"> <code>disable-if</code> - 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>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 402)". 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 399)". <ul style="list-style-type: none"> <code>no-reaction</code> - A remote network loop has no effects on the bridge port. <p>Default: <code>disable-if</code></p> | <pre>interface { bridge port } loop- detection reaction-remote [disable-if no-reaction]</pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <pre>show running-config interface { bridge port } loop-detection reaction-remote</pre> |

Example

In this example, it is configured for ethernet0/1 that a remote network loop has no effects on the bridge port.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 loop-detection reaction-
remote no-reaction
localhost(config-interface-ethernet0/1-loop-detection)# commit
Commit complete.
localhost(config-interface-ethernet0/1-loop-detection)# end
localhost# show running-config interface ethernet0/1 loop-detection
reaction-remote
interface ethernet0/1
  loop detection
  reaction-remote no-reaction
exit

exit
```

10.2.2.7 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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Make sure the desired bridge port is configured in such a way that it is disabled in the case of a local and a remote network loop (disable-if). For more information, refer to "Configuring the reaction to local network loops (Page 397)" and "Configuring the reaction to remote network loops (Page 398)". | show running-config interface { bridge port } loop-detection details |
| 2 | Enter configuration mode. | config |

| Step | Instruction | Command |
|------|---|--|
| 3 | <p>Configure the duration for which the desired bridge port is disabled after a network loop has been detected. The bridge port is enabled again after the timer has elapsed.</p> <p>Conditions:</p> <ul style="list-style-type: none"> Formatted as <code>nYnMnDnHnmns</code>, where <code>n</code> is a user-defined number Minimum 0 seconds (<code>0s</code>) Maximum 86400 seconds (<code>86400s</code>) <p>Default: <code>0s</code> (0 seconds)</p> <p>When the value <code>0s</code> 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 402)".</p> | <pre>interface { bridge port } loop- detection reaction-timeout { 0s - 86400s }</pre> |
| 4 | Commit the change. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <pre>show running-config interface { bridge port } loop-detection reaction-timeout</pre> |

Example

In this example, it is configured for `ethernet0/1` that it remains disabled for 7200 seconds after a network loop has been detected. The bridge port is enabled again after the 7200 seconds have elapsed.

```
localhost# show running-config interface ethernet0/1 loop-detection
| details
interface ethernet0/1
  loop-detection
  .
  .
  .
  reaction-local    disable-if
  reaction-remote  disable-if
exit

exit

localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/1 loop-detection reaction-
timeout 7200s
localhost(config-interface-ethernet0/1-loop-detection)# commit
Commit complete.
localhost(config-interface-ethernet0/1-loop-detection)# end
localhost# show running-config interface ethernet0/1 loop-detection
reaction-timeout
interface ethernet0/1
```



```

loop detection
  reaction-timeout 2h
exit

exit

```

10.2.2.8 Enabling VLAN mode

Enable VLAN mode to take into account the VLAN configuration of bridge ports 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, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable VLAN mode for all bridge ports of the Loop Detection. | <code>switch loop-detection vlan-enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch loop-detection vlan-enabled</code> |

Example

In this example, VLAN mode is enabled for ethernet0/1.

```

localhost# config
Entering configuration mode terminal
localhost(config)# switch loop-detection vlan-enabled
localhost(config-switch-loop-detection)# commit
Commit complete.
localhost(config-switch-loop-detection)# end
localhost# show running-config switch loop-detection vlan-enabled
switch
  loop detection
    vlan-enabled
exit

exit

```

10.2.2.9 Enabling Loop Detection

By default, Loop Detection is disabled for all bridge ports.

To enable Loop Detection, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the detection of network loops for all bridge ports. | <code>switch loop-detection enabled</code> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch loop-detection enabled |

Example

In this example, Loop Detection is enabled for ethernet0/1.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch loop-detection enabled
localhost(config-switch-loop-detection)# commit
Commit complete.
localhost(config-switch-loop-detection)# end
localhost# show running-config switch loop-detection enabled
switch
  loop detection
    enabled
  exit
exit
```

10.2.2.10 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 manually reset a bridge port, execute the following command in operational mode:

```
interface { bridge port } loop-detection reset
```

Example

```
localhost# show interface ethernet0/1 loop-detection
loop-detection
  oper-state detected-remote-loop
localhost# interface ethernet0/1 loop-detection reset
localhost# show interface ethernet0/1 loop-detection
loop-detection
  oper-state active
localhost#
```

10.2.3 Monitoring the Loop Detection

This section describes how you can monitor the status of the Loop Detection.

10.2.3.1 Showing the status of Loop Detection

To display the status of Loop Detection, execute the following command in operational mode:

```
show interface { bridge port } loop-detection
```

Example

```
localhost# show interface ethernet0/1 loop-detection
loop-detection
  oper-state detected-local-loop
  ingress-if ethernet0/2
  ingress-vid 1
exit
```

Description

The following information is shown:

| Parameter | Description |
|-------------|---|
| oper-state | Shows the operating status of Loop Detection. Possible values: <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-if | 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-vid | 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

DLP 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.

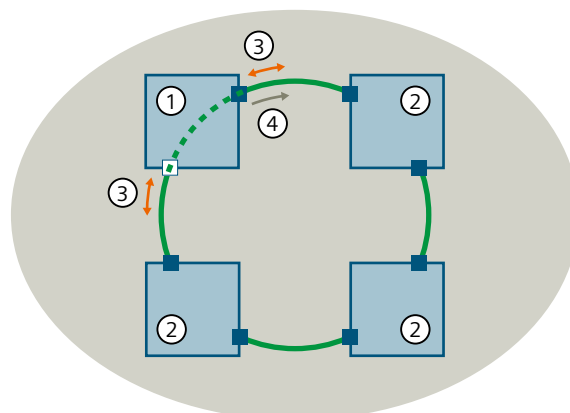
10.3.1.4 DLR network

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.



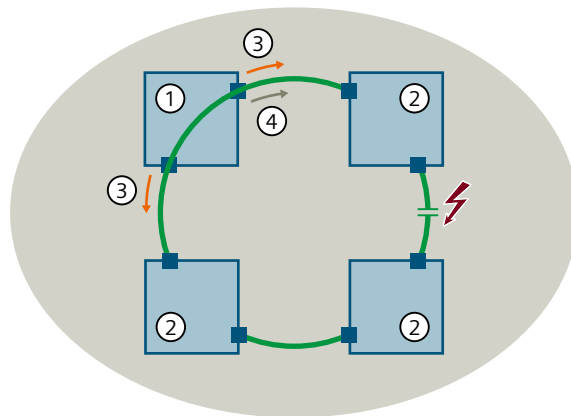
- ① Active ring supervisor
- ② Ring nodes
- ③ Beacon frames
- ④ Announce frames

Figure 10-11 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 nodes
- ③ Beacon frames
- ④ Announce frames

Figure 10-12 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 472)".
2. Add a static VLAN for DLR.
For more information, refer to "Adding or modifying a static VLAN (Page 531)".
3. Select the DLR VLAN.
For more information, refer to "Selecting the DLR VLAN (Page 409)".
4. Make sure that the configuration of your device meets the configuration requirements for DLR ports.
For more information, refer to "Checking requirements for DLR ports (Page 409)".
5. Select the DLR ports.
For more information, refer to "Selecting the DLR ports (Page 411)".
6. Enable DLR.
For more information, refer to "Enabling DLR (Page 412)".

10.3.2.1 Selecting the DLR VLAN

To select the VLAN in which DLR frames are sent, do the following:

| Step | Instruction | Command |
|------|--|---|
| 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 531)". | <code>show switch vlan { VLAN ID }</code> |
| 2 | Enter configuration mode. | <code>config</code> |
| 3 | Select the VLAN for DLR. | <code>ethernetip device-level-ring vid { VLAN ID }</code> |
| 4 | Commit the change. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config ethernetip device-level-ring vid</code> |

Example

In this example, the VLAN with the ID 10 is selected as DLR VLAN.

```
localhost# show switch vlan 10
vlan 10
  name DLR
localhost# config
Entering configuration mode terminal
localhost(config)# ethernetip device-level-ring vid 10
localhost(config-ethernetip-device-level-ring)# commit
Commit complete.
localhost(config-ethernetip-device-level-ring)# end
localhost# show running-config ethernetip device-level-ring vid
ethernetip
  device-level-ring
    vid 10
  exit

exit
```

10.3.2.2 Checking requirements for DLR ports

The configuration of the DLR ports depends on the settings of other functions.

You can display and check the current configuration with the commands in the following table. The links lead to additional information and to the commands with which you can adapt the configuration according to the requirements for DLR ports.

Before you select the DLR ports, check the following settings and change the configuration if necessary:

| Instruction | Command |
|--|---|
| <p>Make sure that both ports that you wish to use as DLR ports are configured as trunk ports.</p> <p>For more information on configuring port membership, refer to "Selecting the port membership type (Page 534)".</p> | <pre>show interface { bridge port } vlan type</pre> |
| <p>[Optional] Make sure that the ports that you wish to use as DLR ports are tagged members in the DLR VLAN.</p> <p>This configuration is only necessary if the DLR VLAN corresponds to the native VLAN of the DLR ring ports.</p> <p>For more information, refer to "Enabling PVID tagging on egress traffic (Page 537)".</p> | <pre>show switch vlan { VLAN ID } untagged-ports</pre> |
| <p>Make sure that STP is disabled for the ports that you wish to use as DLR ports.</p> <p>Compatible configuration: <code>disabled</code></p> <p>For more information on the status of STP for a bridge port, refer to "Displaying the status of STP per bridge port (Page 380)".</p> <p>For more information on configuring STP for a port, refer to "Enabling STP for a bridge port (Page 358)".</p> | <pre>show interface { bridge port } spanning-tree state</pre> |
| <p>Make sure that MRP is disabled globally.</p> <p>Compatible configuration: <code>no enabled</code></p> <p>For more information, refer to "Enabling MRP globally (Page 428)".</p> | <pre>show running-config switch mrp enabled</pre> |
| <p>Make sure that the ports that you wish to use as DLR ports forward PDUs for loop detection, at most.</p> <p>Compatible configurations:</p> <ul style="list-style-type: none"> <code>forwarding</code> <code>blocking</code> <p>For more information on the port modes of loop detection, refer to "Configuring bridge ports for the detection of network loops (Page 394)".</p> | <pre>show running-config interface { bridge port } loop-detection tx- state</pre> |

Example

The requirements for successful configuration of the DLR ports are checked in this example. The `ethernet0/6` and `ethernet0/7` bridge ports are to be configured as DLR ports.

```
localhost# show interface ethernet0/6 vlan type
vlan type trunk
localhost# show interface ethernet0/7 vlan type
vlan type trunk
localhost# show switch vlan 10 untagged-ports
untagged-ports [ ethernet0/1 ethernet0/3 ethernet0/4
ethernet0/5 ethernet0/8 ]
localhost# show interface ethernet0/6 spanning-tree state
state disabled
```

```

localhost# show interface ethernet0/7 spanning-tree state
state disabled
localhost# show running-config switch mrp enabled
switch
  mrp
    no enabled
  exit

exit

localhost# show running-config interface ethernet0/6 loop-detection
tx-state

interface ethernet0/6
  loop-detection
    tx-state forwarding
  exit

exit

localhost# show running-config interface ethernet0/7 loop-detection
tx-state

interface ethernet0/7
  loop-detection
    tx-state forwarding
  exit

exit

```

10.3.2.3 Selecting the DLR ports

To select the DLR ports, do the following:

| Step | Instruction | Command |
|------|-----------------------------|--|
| 1 | Enter configuration mode. | config |
| 2 | Select the first DLR port. | ethernetip device-level-ring ring-port1 { bridge port } |
| 3 | Select the second DLR port. | ring-port2 { bridge port } |
| 4 | Commit the changes. | commit |
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config ethernetip device-level-ring ring-port1 show running-config ethernetip device-level-ring ring-port2 |

Example

In this example, ethernet0/6 and ethernet0/7 are selected as DLR ports.

```

localhost# config
Entering configuration mode terminal

```

10.3 Device Level Ring

```

localhost(config)# ethernetip device-level-ring ring-port1
ethernet0/6
localhost(config-ethernetip-device-level-ring)# ring-port2
ethernet0/7
localhost(config-ethernetip-device-level-ring)# commit
Commit complete.
localhost(config-ethernetip-device-level-ring)# end
localhost# show running-config ethernetip device-level-ring ring-
port1
ethernetip
  device-level-ring
    ring-port1 ethernet0/6
  exit

exit
localhost# show running-config ethernetip device-level-ring ring-
port2
ethernetip
  device-level-ring
    ring-port2 ethernet0/7
  exit

exit

```

10.3.2.4 Enabling DLR

DLR is disabled by default.

To enable DLR, do the following:

| Step | Instruction | Command |
|------|---------------------------|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable DLR. | ethernetip device-level-ring enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config ethernetip device-level-ring enabled |

Example

In this example, DLR is enabled.

```

localhost# config
Entering configuration mode terminal
localhost(config)# ethernetip device-level-ring enabled
localhost(config-ethernetip-device-level-ring)# commit
Commit complete.
localhost(config-ethernetip-device-level-ring)# end
localhost# show running-config ethernetip device-level-ring enabled
ethernetip
  device-level-ring
    enabled

```

```
exit
exit
```

10.3.3 Monitoring DLR

To monitor the DLR network, execute the following command in operational mode:
show ethernetip device-level-ring

Example

```
localhost# show ethernetip device-level-ring
device-level-ring
supervisor-ip-address 192.0.2.2
supervisor-mac-address 10:00:00:00:00:FF
ring-topology         ring
ring-state            fault
node-state            normal
network-status        normal
ring-port1            ethernet0/6
ring-port1-status     up
ring-port2            ethernet0/7
ring-port2-status     up
```

Description

The following information is shown:

| 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. |
| 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) <code>idle</code> still or again. ring - The ring topology means that a ring node is in the status (Node State) <code>normal</code> or <code>fault</code>, 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. |

| Parameter | Description |
|--------------------------------|--|
| <code>node-state</code> | Shows the internal status of an Announce-based ring node (SINEC OS device). Possible values include: <ul style="list-style-type: none"> <code>idle</code> - The initial status of the device. The device changes to the <code>idle</code> status if it does not receive any Announce frames. <code>fault</code> - The device has the status <code>fault</code> if a fault has been detected in the network. <code>normal</code> - The device has the status <code>normal</code> if communication with all network nodes is possible. |
| <code>network-status</code> | Shows the current status of the DLR network. Possible values include: <ul style="list-style-type: none"> <code>normal</code> - Communication is possible between all network nodes. <code>ring fault</code> - A fault was detected in the network. |
| <code>ring-port1</code> | Shows the first DLR port. |
| <code>ring-port1-status</code> | Shows the current status of the first DLR port. Possible values include: <ul style="list-style-type: none"> <code>up</code> - The interface is enabled. <code>down</code> - The interface is disabled. |
| <code>ring-port2</code> | Shows the second DLR port. |
| <code>ring-port2-status</code> | Shows the current status of the second DLR port. Possible values include: <ul style="list-style-type: none"> <code>up</code> - The interface is enabled. <code>down</code> - 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:

- [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 534)".
- Disable STP for the ports that you wish to use as DLR ports.
For more information, refer to "Enabling STP for a bridge port (Page 358)".

3. Configure EtherNet/IP.
For more information, refer to "Configuring EtherNet/IP (Page 471)".
4. Select the DLR ports.
For more information, refer to "Selecting the DLR ports (Page 411)".
5. Configure the same native VLAN for both DLR ports.
For more information, refer to "Configuring the port VLAN ID (Page 535)".
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 533)".
7. Enable DLR.
For more information, refer to "Enabling DLR (Page 412)".
8. Ensure that **no** DLR VLAN is configured.
For more information, refer to "Selecting the DLR VLAN (Page 409)".

Example

In this example, ethernet0/6 and ethernet0/7 are selected as DLR ports. VLAN 7 is configured as native VLAN of the DLR ports.

```
localhost# show interface ethernet0/6 vlan type
vlan type access
localhost# show interface ethernet0/7 vlan type
vlan type access
localhost# config
Entering configuration mode terminal
localhost(config)# no interface ethernet0/6 spanning-tree enabled
localhost(config)# no interface ethernet0/7 spanning-tree enabled
localhost(config)# ethernetip enabled
localhost(config-ethernetip)# device-level-ring ring-port1
ethernet0/6
localhost(config-ethernetip-device-level-ring)# ring-port2
ethernet0/7
localhost(config-ethernetip-device-level-ring)# top
localhost(config)# interface ethernet0/6 vlan pvid 7
localhost(config-interface-ethernet0/6-vlan)# top
localhost(config)# interface ethernet0/7 vlan pvid 7
localhost(config-interface-ethernet0/7-vlan)# top
localhost(config)# switch vlan 7 vlan-0-tunnel
localhost(config)# ethernetip device-level-ring enabled
localhost(config-ethernetip-device-level-ring)# commit
Commit complete.
localhost(config-ethernetip-device-level-ring)# end
localhost# show running-config ethernetip device-level-ring vid
% No entries found.
```

10.4 Media Redundancy Protocol

The Media Redundancy Protocol (MRP) is a vendor-neutral redundancy protocol standardized according to IEC 62439-2 which ensures loop-free communication and the reconfiguration of a network in the event of interferences.

The Layer 2 method is a component of PROFINET and integrated in all PROFINET-capable field, control and network components.

10.4.1 Useful Information on MRP

MRP is designed in such a way that it reacts deterministically to the failure of a single transmission link or a single network node, managed by a defined manager.

An MRP-compliant network has a ring topology with multiple network nodes. The two ends of a line topology are connected via a network node to form a ring.

Each ring device is integrated in the ring via two Ethernet ports and is thus connected to two different neighboring nodes. To prevent network loops, a ring device (the manager) blocks one of its ring ports.

In a ring topology with MRP, exactly one ring device is manager. All other ring devices are clients.

10.4.1.1 MRP roles

In a ring topology with MRP, each ring device has one of the following roles:

- **Media Redundancy Manager (MRM)**

An MRM has the following tasks:

- Manages an MRP ring
- Regularly sends test frames to both ring ports
- Sends topology change frames to both ring ports in the event of a fault/restore
- Constantly monitors the status of the MRP ring
- Detects errors in the MRP ring
- Collects diagnostics information about the MRP ring

- **Media Redundancy Client (MRC)**

An MRC has the following tasks:

- Forwards test frames to its ring ports
- Processes topology change frames
- Learns the new network topology in the event of a fault/restore
- Sends link change frames to the MRM in the event of status changes on a local ring port (link up or link down)

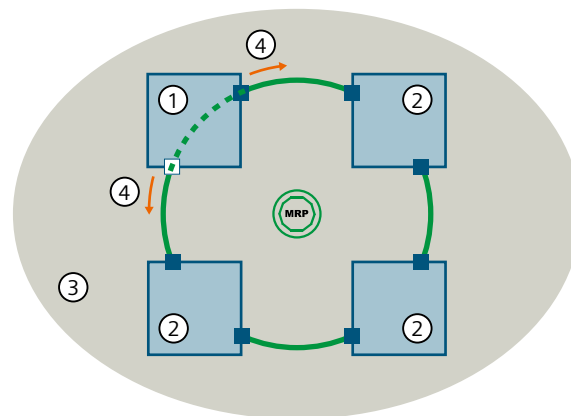
10.4.1.2 MRP network

MRP distinguishes between the following states:

- **Normal state**

An MRP ring is in normal state when the MRM has blocked data traffic on one of its ring ports, except for MRP-specific frames. This converts the physical ring structure on the logical layer for normal data traffic back into a line structure and avoids network loops.

In this state, the MRM sends test frames (also over the blocked ring port) to monitor the status of the MRP ring. All other ring devices forward the test frames. The test frames run through the ring in both directions until they arrive at the other ring port of the MRM. As long as the MRM receives its sent test frames again, all communication paths in the MRP ring are intact.



- ① MRM
- ② MRCs
- ③ Redundancy domain
- ④ Test frames
- Active port
- Blocked port

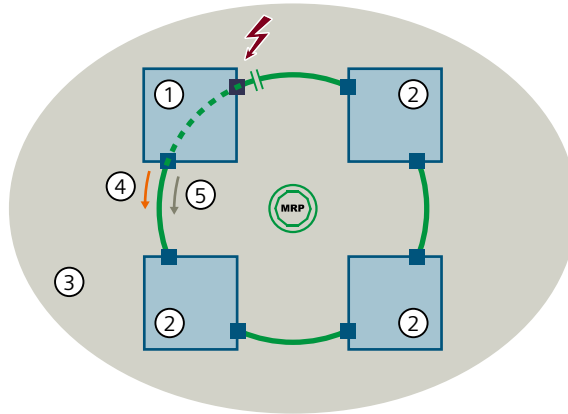
Figure 10-13 MRP ring in normal state

- **Error state**

If the transmission link in the ring is interrupted, for example, due to a break in the ring cable or the failure of a station, the test frames no longer arrive at the MRM. The MRM thus detects an error in the ring.

A distinction is made as to where in the MRP ring the transmission link is interrupted.

- Interruption on the ring port of the MRM
 If the interruption directly affects the active ring port of the MRM, this port goes to Link down status. The MRM enables its blocked ring port and thus the alternative communication path. The MRM informs the MRCs about the topology change. The MRCs learn the new communication path.



- ① MRM
- ② MRCs
- ③ Redundancy domain
- ④ Test frames
- ⑤ Topology change frames
- Active port
- Port in Link down status

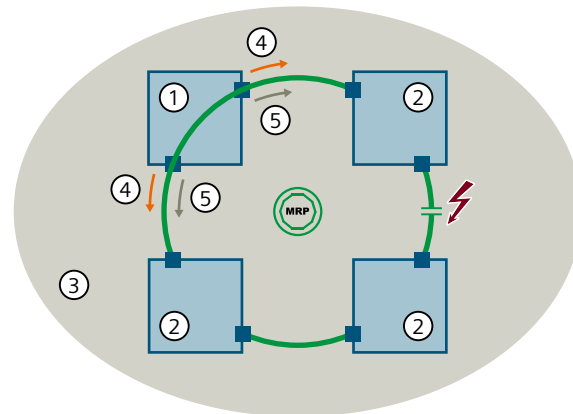
Figure 10-14 MRP ring in error state - Interruption on the ring port of the MRM

The MRP ring is in error state but unrestricted communication with the MRM is possible again as soon as the reconfiguration is complete.

If the interruption has been resolved, the ring port of the MRM enabled by the reconfiguration remains active. The MRM blocks data traffic on its other ring port.

| Ports | Before the reconfiguration | In error state | After the reconfiguration |
|-------------|-----------------------------------|----------------|---------------------------|
| Ring port 1 | Data traffic blocked | Is enabled | Remains active |
| Ring port 2 | Actively involved in data traffic | Link down | Data traffic is blocked |

- Interruption at another point in the MRP ring
If the MRP ring is interrupted at another point, the MRM enables its blocked ring port. Both ring ports are actively involved in data traffic and enable the alternative communication path. The MRM informs the MRCs about the topology change. The MRCs learn the new communication path.



- ① MRM
- ② MRCs
- ③ Redundancy domain
- ④ Test frames
- ⑤ Topology change frames
- Active port

Figure 10-15 MRP ring in error state - Interruption at another point in the MRP ring

The MRP ring is in error state but unrestricted communication between all ring devices is possible again as soon as the reconfiguration is complete.

If the interruption has been resolved, the MRM blocks the ring port that was enabled by the reconfiguration again. The MRM informs the MRCs about the topology change. The MRCs use the original paths to the other ring devices again.

| Ports | Before the reconfiguration | In error state | After the reconfiguration |
|-------------|-----------------------------------|----------------|-------------------------------|
| Ring port 1 | Data traffic blocked | Is enabled | Data traffic is blocked again |
| Ring port 2 | Actively involved in data traffic | Remains active | Remains active |

10.4.1.3 Media Redundancy Automanager

Media Redundancy Automanager (MRA) is an administrative, temporary role that can be configured for a ring device. It is not an operative role like MRM or MRC.

Each ring device for which MRA is configured must be either MRM or MRC in operational mode. The operative role that an MRA takes on is decided by a manager selection process.

A priority value is assigned to each MRA. The priority value in combination with the MAC address provides a unique priority. The lower the priority value, the higher the priority of the MRA in the manager selection process. If MRAs have the same priority value, the MAC

address is the decisive factor. The lower the MAC address, the higher the priority of the MRA in the manager selection process.

Note

The priority value cannot be configured with SINEC OS. All SINEC OS MRAs have the same priority value. In a manager selection process with exclusively SINEC OS MRAs, the MRA with the lowest MAC address always becomes the MRM.

The manager selection process runs as follows:

- After system startup, all ring devices with the MRA role start the manager selection process.
- Each MRA sends test frames via its two ring ports. The test frames contain their own priority value and the MAC address.
- For each received test frame, an MRA compares the priority of the neighboring MRA with its own priority.
- If its own priority is higher than the priority of a neighboring MRA, an MRA sends a rejecting response frame (MRP_TestMgrNAck) with the MAC address of the neighboring MRA.
- An MRA that receives a rejecting response frame with its own MAC address proceeds as follows:
 - It changes to the MRC role.
 - It saves the priority value and the MAC address of the MRA with the higher priority.
 - It informs the other ring devices about its role change and shares the information of the MRA with the higher priority (MRP_TestPropagate).
The other MRAs with the Client role update their saved information so that they all have the same MRA with the highest priority saved as manager in the end.
- The MRA with the highest priority becomes the MRM and manages the MRP ring.

The following circumstances affect the manager selection process:

- If the selected MRM fails or is removed from the ring, the manager selection process starts again.
In coordination with other MRAs, the MRA can switch from its initial role MRA to the role MRM or MRC and back.
- If an additional MRA is added to an existing ring topology in which an MRM has already been selected, the selected MRM and the new MRA exchange test frames and determine among themselves the MRM.

10.4.1.4 Ring ports

The ring ports need to be members of the same VLAN as the TIA interface.

10.4.1.5 Redundancy domain

A redundancy domain corresponds to an MRP ring and is represented by a unique ID.

All devices connected within a ring topology must be members of the same redundancy domain and have the same ID.

If a device is a member of multiple MRP rings, the MRP frames are delimited via the different redundancy domains. At least two unique ring ports must be defined per redundancy domain for a ring device.

10.4.1.6 Reconfiguration time

The time between a ring interruption and restoration of a functional linear topology is known as the reconfiguration time.

The reconfiguration time in an MRP ring with 50 ring devices is 200 ms.

The following factors can affect the reconfiguration time:

- The specific topology
- The devices used
- The number of devices
- The network load

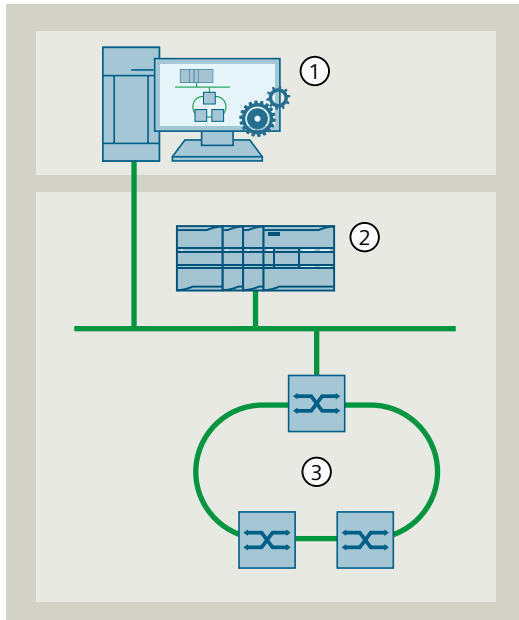
10.4.1.7 Installation guide

The following installation guidelines apply to an MRP ring:

- MRP is enabled for all ring devices
Because MRP is vendor-neutral, you can use devices from different manufacturers within an MRP ring.
Devices not capable of MRP can be connected to the ring using a device with MRP capability.
- Exactly one ring device is the MRM
The following configuration options exist:
 - The MRM role is configured for exactly one ring device. No other ring device can have the MRM role.
 - The MRA role is configured for one or more ring devices. The ring devices with the MRA role negotiate among themselves which one will take on the role of MRM.
- All other ring devices are MRCs
- Two ring ports are configured for all ring devices
- The ring ports of the ring devices have the same settings
- All ring devices are connected to each other via their ring ports
- All ring devices are members of the same redundancy domain

10.4.1.8 MRP configuration via a PROFINET controller

You can configure MRP not only directly on the devices, but also in a configuration tool (e.g. TIA Portal). If you create an MRP configuration in a configuration tool, it is loaded into the connected devices via a PROFINET controller.



- ① Configuration tool
- ② PROFINET controller
- ③ MRP ring with SINEC OS devices

Figure 10-16 MRP configuration via a PROFINET controller

To load an MRP configuration to a device via a PROFINET controller, follow these steps:

1. Create an MRP configuration in a configuration tool.
2. Prepare the SINEC OS device.

If the loaded MRP configuration violates a configuration rule of SINEC OS, the device rejects the configuration.

 - Ensure that the device has a PROFINET device name.
You configure the PROFINET device name. for example, with SINEC PNI.
 - Ensure that DCP is enabled with read and write access rights (read-write option).
For more information, refer to "Configuring the access rights of DCP (Page 452)".
 - Make sure that the configuration of your device meets the configuration requirements for MRP.
For more information, refer to "Checking MRP requirements (Page 423)".
3. Load the MRP configuration into the device via the PROFINET controller.

10.4.2 Configuring MRP

Note

If there is a connection to a PROFINET controller, you cannot change the MRP configuration.

Note

If you use MRP, ensure that the device is operated in a protected network area.

To configure MRP, do the following:

1. Make sure that the configuration of your device meets the configuration requirements for MRP.
For more information, refer to "Checking MRP requirements (Page 423)".
 2. Configure an MRP instance.
For more information, refer to "Configuring an MRP instance (Page 426)".
-

Note

Only one MRP instance is supported in the current firmware version.

3. Enable MRP globally.
For more information, refer to "Enabling MRP globally (Page 428)".

As soon as an MRP instance is configured, you can perform the following optional steps to change the existing values:

- Change the redundancy domain.
For more information, refer to "Changing the redundancy domain (Page 428)".
- Change the MRP role.
For more information, refer to "Changing the MRP role (Page 430)".
- Change the ring ports.
You can only configure 100 Mbps and 1 Gbps copper ports as ring ports.
For more information, refer to "Changing ring ports (Page 431)".

| |
|---|
| NOTICE |
| Configuration hazard - risk of data traffic floods |
| If you switch your network configuration from MRP to STP, make sure that you disable MRP fully and commit the changes before configuring STP. |

10.4.2.1 Checking MRP requirements

The successful configuration of MRP depends on the settings of other functions.

You can display and check the current configuration with the commands in the following table. The links lead to additional information and to the commands with which you can adapt the configuration according to the MRP requirements.

Before you configure MRP, check the following settings and change the configuration if necessary:

| Instruction | Command |
|--|---|
| <p>Make sure that the ports that you wish to use as ring ports are tagged members in the same VLAN as the TIA interface.</p> <p>For more information on the TIA interface, refer to "Monitoring the TIA interface (Page 466)".</p> <p>For more information on the VLAN ID of a port, refer to "Configuring the port VLAN ID (Page 535)".</p> | <pre>show running-config profinet tia- interface show interface { bridge port } vlan pvid</pre> |
| <p>Make sure that STP is disabled globally.</p> <p>Compatible configuration: <code>no enabled</code></p> <p>For more information, refer to "Enabling STP (Page 351)".</p> | <pre>show running-config switch spanning- tree enabled</pre> |
| <p>Make sure that DLR is disabled globally.</p> <p>Compatible configuration: <code>no enabled</code></p> <p>For more information, refer to "Enabling DLR (Page 412)".</p> | <pre>show running-config ethernetip device-level-ring enabled</pre> |
| <p>Make sure that loop detection is disabled globally.</p> <p>Compatible configuration: <code>no enabled</code></p> <p>For more information, refer to "Enabling Loop Detection (Page 401)".</p> | <pre>show running-config switch loop- detection enabled</pre> |
| <p>Make sure that port security is disabled for the ports that you wish to use as ring ports.</p> <p>For more information on configuring port security, refer to "Enabling port security (Page 254)".</p> | <pre>show running-config interface { bridge port } port-security</pre> |
| <p>Make sure that the ports that you wish to use as ring ports are not configured as destination for mirrored data traffic.</p> <p>For more information on mirroring data traffic, refer to "Configuring a mirroring destination (Page 679)".</p> | <pre>show running-config switch traffic- mirroring session { Session } destination</pre> |
| <p>Make sure that the ports that you wish to use as ring ports do not only accept tagged VLAN ingress frames.</p> <p>Compatible configurations:</p> <ul style="list-style-type: none"> • <code>admit-all-frames</code> • <code>admit-only-untagged-and-priority-tagged</code> <p>For more information on accepted frame types, refer to "Selecting the frame types accepted (Page 535)".</p> | <pre>show interface { bridge port } vlan acceptable-frame</pre> |
| <p>Make sure that GVRP is disabled.</p> <p>For more information on GVRP, refer to "Enabling GVRP (Page 532)".</p> | <pre>show switch device-config</pre> |
| <p>Make sure that GMRP is disabled.</p> <p>For more information on GMRP, refer to "Enabling GMRP (Page 596)".</p> | |

Example

The requirements for successful MRP configuration are checked in this example. The ethernet0/3 and ethernet0/4 bridge ports are to be configured as ring ports.

```
localhost# show running-config profinet tia-interface
profinet
  tia-interface vlan1
exit
```

```
localhost# show interface ethernet0/3 vlan pvid
vlan pvid 1
localhost# show interface ethernet0/4 vlan pvid
vlan pvid 1
```

```
localhost# show running-config switch spanning-tree enabled
switch
  spanning-tree
  no enabled
exit
```

```
exit
```

```
localhost# show running-config ethernetip device-level-ring enabled
ethernetip
  device-level-ring
  no enabled
exit
```

```
exit
```

```
localhost# show running-config switch loop-detection enabled
switch
  loop-detection
  no enabled
exit
```

```
exit
```

```
localhost# show running-config interface ethernet0/3 port-
security enabled
interface ethernet0/3
  port-security
  no enabled
exit
```

```
exit
```

```
localhost# show running-config interface ethernet0/4 port-
security enabled
interface ethernet0/4
  port-security
  no enabled
```

```

exit

exit

localhost# show running-config switch traffic-mirroring session 1
destination
switch
  traffic-mirroring
    session 1
      destination port ethernet0/1
    exit
  exit

exit

exit

localhost# show interface ethernet0/3 vlan acceptable-frame
vlan acceptable-frame admit-all-frames
localhost# show interface ethernet0/4 vlan acceptable-frame
vlan acceptable-frame admit-all-frames
localhost# show switch device-config
General vlan device configuration
  GVRP status                disabled
  GMRP status                disabled
  .
  .
  .
localhost#

```

10.4.2.2 Configuring an MRP instance

To configure an MRP instance, follow these steps:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Create an MRP instance. | <code>switch mrp ring-id { 1 }</code> |
| 3 | Define the redundancy domain. Options include: <ul style="list-style-type: none"> • <code>default-mrpdomain</code> • <code>mrpdomain-1</code> • <code>mrpdomain-2</code> • <code>mrpdomain-3</code> • <code>mrpdomain-4</code> • <code>Domain name</code> - User-defined name for the redundancy domain. <ul style="list-style-type: none"> – Condition: Must be between 0 and 240 characters long | <code>domain-name [default-mrpdomain mrpdomain-1 mrpdomain-2 mrpdomain-3 mrpdomain-4 { Domain name }]</code> |

| Step | Instruction | Command |
|------|--|--|
| 4 | Configure the MRP role. Options include: <ul style="list-style-type: none"> • <code>disabled</code> - No MRP role is assigned to the device. The device is not a participant in the MRP ring. • <code>mrp-auto-manager</code> - The ring device negotiates its MRP role automatically. In operational mode of an MRP ring, the ring device is either MRM or MRC. • <code>mrp-manager</code> - The role of the ring device is set permanently to MRM. • <code>mrp-client</code> - The role of the ring device is set permanently to MRC. | <code>mode [disabled mrp-auto-manager mrp-manager mrp-client]</code> |
| 5 | Select the first ring port. With ring ports, the maximum transmission unit (MTU) cannot be changed. | <code>ring-port1 { bridge port }</code> |
| 6 | Select the second ring port. With ring ports, the maximum transmission unit (MTU) cannot be changed. | <code>ring-port2 { bridge port }</code> |
| 7 | Commit the change. | <code>commit</code> |
| 8 | Exit configuration mode. | <code>end</code> |
| 9 | Verify the configuration. | <code>show running-config switch mrp ring-id</code> |

Example

An MRP instance is created in this example.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch mrp ring-id 1
localhost(config-ring-id-1)# domain-name default-mrpdomain
localhost(config-ring-id-1)# mode mrp-auto-manager
localhost(config-ring-id-1)# ring-port1 ethernet0/3
localhost(config-ring-id-1)# ring-port2 ethernet0/4
localhost(config-ring-id-1)# commit
Commit complete.
localhost(config-ring-id-1)# end
localhost# show running-config switch mrp ring-id
% The following list contains 1 entry.
switch
  mrp
    ring-id 1
    mode          mrp-auto-manager
    ring-port1    ethernet0/3
    ring-port2    ethernet0/4
    domain-name   default-mrpdomain
  exit
exit
```

```
exit
```

10.4.2.3 Enabling MRP globally

MRP is disabled by default.

To enable MRP globally, do the following:

| Step | Instruction | Command |
|------|---------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable MRP. | <code>switch mrp enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch mrp enabled</code> |

Example

MRP is enabled in this example.

```
localhost# show switch device-config
General vlan device configuration
  GVRP status                disabled
  GMRP status                disabled
  .
  .
  .
localhost# config
Entering configuration mode terminal
localhost(config)# switch mrp enabled
localhost(config-switch-mrp)# commit
Commit complete.
localhost(config-switch-mrp)# end
localhost# show running-config switch mrp enabled
switch
  mrp
  enabled
exit

exit
```

See also

Enabling GVRP (Page 532)

Enabling GMRP (Page 596)

10.4.2.4 Changing the redundancy domain

All devices connected within a ring topology must be members of the same redundancy domain.

Set the same redundancy domain for all ring devices that belong to the same MRP ring. Set different redundancy domains for different MRP rings.

To change a redundancy domain, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Change the redundancy domain. Options include: <ul style="list-style-type: none"> • <code>default-mrpdomain</code> • <code>mrpdomain-1</code> • <code>mrpdomain-2</code> • <code>mrpdomain-3</code> • <code>mrpdomain-4</code> • Domain name-User-defined name for the redundancy domain. <ul style="list-style-type: none"> – Condition: Must be between 0 and 240 characters long | <code>switch mrp ring-id { 1 } domain-name [default-mrpdomain mrpdomain-1 mrpdomain-2 mrpdomain-3 mrpdomain-4 { Domain name }]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch mrp ring-id { 1 } domain-name</code> |

Example

In this example, the redundancy domain `mrpdomain-1` is defined for a ring device.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch mrp ring-id 1 domain-name mrpdomain-1
localhost(config-ring-id-1)# commit
Commit complete.
localhost(config-ring-id-1)# end
localhost# show running-config switch mrp ring-id 1 domain-name
switch
  mrp
    ring-id
      domain-name mrpdomain-1
    exit
  exit
exit
```

10.4.2.5 Changing the MRP role

To change the MRP role of a device, follow the steps below:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Change the MRP role. Options include: <ul style="list-style-type: none"> <code>disabled</code> - No MRP role is assigned to the device. The device is not a participant in the MRP ring. <code>mrp-auto-manager</code> - The ring device negotiates its MRP role automatically. In operational mode of an MRP ring, the ring device is either MRM or MRC. <code>mrp-manager</code> - The role of the ring device is set permanently to MRM. <code>mrp-client</code> - The role of the ring device is set permanently to MRC. | <code>switch mrp ring-id { 1 } mode [disabled mrp-auto-manager mrp-manager mrp-client]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch mrp ring-id { 1 } mode</code> |

Example

In this example, the MRP role Client is defined for a ring device.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch mrp ring-id 1 mode mrp-client
localhost(config-ring-id-1)# commit
Commit complete.
localhost(config-ring-id-1)# end
localhost# show running-config switch mrp ring-id 1 mode
switch
  mrp
    ring-id 1
      mode mrp-client
    exit
  exit
exit
```

10.4.2.6 Changing ring ports

| |
|--|
| NOTICE |
| Restrictions <ul style="list-style-type: none"> • The ring ports need to be members of the same VLAN as the TIA interface. • You can only configure 100 Mbps and 1 Gbps copper ports as ring ports. |

To change the ring ports, follow the steps below:

| Step | Instruction | Command |
|------|--|---|
| 1 | Check the MRP requirements for ring ports. For more information, refer to "Checking MRP requirements (Page 423)". | - |
| 2 | Enter configuration mode. | config |
| 3 | Select the first ring port. | switch mrp ring-id { 1 } ring-port1 { bridge port } |
| 4 | Select the second ring port. | ring-port2 { bridge port } |
| 5 | Commit the changes. | commit |
| 6 | Exit configuration mode. | end |
| 7 | Verify the configuration. | show running-config switch mrp ring-id { 1 } |

Example

In this example, ethernet1/1 and ethernet1/2 are selected as ring ports.

```
localhost# show running-config profinet tia-interface
profinet
  tia-interface vlan1
exit

localhost# show interface ethernet1/1 vlan pvid
vlan pvid 1
localhost# show interface ethernet1/2 vlan pvid
vlan pvid 1
localhost# show interface ethernet1/1 spanning-tree state
state disabled
localhost# show interface ethernet1/2 spanning-tree state
state disabled
localhost# show running-config ethernetip device-level-ring ring-
port1
% No entries found.
localhost# show running-config ethernetip device-level-ring ring-
port2
% No entries found.
localhost# show running-config interface ethernet1/1 loop-detection
tx-state

interface ethernet1/1
  loop-detection
```

```
    tx-state forwarding
  exit

exit

localhost# show running-config interface ethernet1/2 loop-detection
tx-state

interface ethernet1/2
  loop-detection
    tx-state forwarding
  exit

exit

localhost# show running-config interface ethernet1/1 port-
security enabled
interface ethernet1/1
  port-security
    no enabled
  exit

exit

localhost# show running-config interface ethernet1/2 port-
security enabled
interface ethernet1/2
  port-security
    no enabled
  exit

exit

localhost# show running-config switch traffic-mirroring session 1
destination
switch
  traffic-mirroring
    session 1
      destination port ethernet0/1
    exit

  exit

exit

localhost# show interface ethernet1/1 vlan acceptable-frame
vlan acceptable-frame admit-all-frames
localhost# show interface ethernet1/2 vlan acceptable-frame
vlan acceptable-frame admit-all-frames
localhost# config
Entering configuration mode terminal
localhost(config)# switch mrp ring-id 1 ring-port1 ethernet1/1
```



```
localhost(config-ring-id-1)# ring-port2 ethernet1/2
localhost(config-ring-id-1)# commit
Commit complete.
localhost(config-ring-id-1)# end
localhost# show running-config switch mrp ring-id 1
switch
  mrp
    ring-id 1
    .
    .
    ring-port1 ethernet1/1
    ring-port2 ethernet1/2
    .
    .
  exit

exit

exit
```

10.4.3 Monitoring MRP

The various methods for monitoring MRP rings are described in this section.

10.4.3.1 Showing the operative MRP role

The configured MRP role of a device and its operative role in an MRP ring can be different. If the MRA role is configured for a device, it can take on the operative role MRM or MRC in operational mode.

To show which operative role a device has in an MRP ring, execute the following command in operational mode:

```
show switch mrp ring-id { 1 } operational-mode
```

Example

```
localhost# show switch mrp ring-id 1 operational-mode
operational-mode mrp-client
```

Description

The following information is shown:

| Parameter | Description |
|------------------|--|
| operational-mode | Shows the operative role of a device in an MRP ring. Possible values: <ul style="list-style-type: none"> • <code>disabled</code> - No MRP role is assigned to the device. The device is not a participant in the MRP ring. • <code>mrp-auto-manager</code> - The MRA role is configured for the ring device and it has taken on the operative role MRM in operational mode. • <code>mrp-manager</code> - The configured and operative role of the ring device is MRM. • <code>mrp-client</code> - The operative role of the ring device is MRC. Either the MRC role or the MRA role is configured for the ring device and it has taken on the operative role MRC in operational mode. • <code>--</code> - The MRA role is configured for the ring device and it has not yet taken on any operative role in operational mode. |

10.4.3.2 Showing the operative ring ports

To display the operative ring ports, execute one of the following commands in operational mode:

```
show switch mrp ring-id { 1 } ring-port1-oper
show switch mrp ring-id { 1 } ring-port2-oper
```

Example

```
localhost# show switch mrp ring-id 1 ring-port1-oper
ring-port1-oper ethernet0/3
```

10.4.3.3 Showing the status of the ring ports

To display the status of the ring ports, execute one of the following commands in operational mode:

```
show switch mrp ring-id { 1 } ring-port1-state
show switch mrp ring-id { 1 } ring-port2-state
```

Example

```
localhost# show switch mrp ring-id 1 ring-port1-state
ring-port1-state forwarding
```

Description

The following information is shown:

| Parameter | Description |
|--------------------------------------|---|
| ring-port1-state ring-port2-state | <p>Shows the status of the ring ports.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <code>disabled</code> - The port is disabled. • <code>blocked</code> - Data traffic on the ring port is blocked with the following exceptions: <ul style="list-style-type: none"> – Test frames from MRM – Topology change frames from MRM – Link change frames from an MRC – Frames from other protocols passing explicitly blocked ports – Frames required for the manager selection process (MRP_TestMgrNAck, MRP_TestPropagate) • <code>forwarding</code> - The ring port forwards data traffic without restriction. • <code>not-connected</code> - The ring port does not have a link. • <code>--</code> - MRP is disabled. |

10.4.3.4 Showing the delay of test frames

The delay time specifies how long test frames take to pass through the MRP ring, measured since the last restart.

To display the maximum delay of test frames in milliseconds, execute the following command in operational mode:

```
show switch mrp ring-id { 1 } maximum-delay
```

Example

```
localhost# show switch mrp ring-id 1 maximum-delay
maximum-delay 0
```

10.4.3.5 Showing the status of the MRM

This information is only available for ring devices with the operative role MRM.

To display the status of the MRM, execute the following command in operational mode:

```
show switch mrp ring-id { 1 } ring-manager-status
```

Example

```
localhost# show switch mrp ring-id 1 ring-manager-status
ring-manager-status passive
```

Description

The following information is shown:

| Parameter | Description |
|---------------------|---|
| ring-manager-status | Shows the current status of the MRM. Possible values: <ul style="list-style-type: none"> • <code>passive</code> - The MRM has blocked data traffic on one of its ring ports. The MRP ring is in normal state. • <code>active</code> - The MRM has detected an error in the MRP ring or at one of its ring ports. The MRP ring is in error state. |

10.4.3.6 Showing the number of status changes

This information is only available for ring devices with the operative role MRM.

The MRM saves the number of status changes from passive (MRP ring in normal state) to active (MRP ring in error state) since the last restart.

To show the number of status changes from passive to active since the last restart, execute the following command in operational mode:

```
show switch mrp ring-id { 1 } changes-to-active
```

Example

```
localhost# show switch mrp ring-id 1 changes-to-active
changes-to-active 3
```

10.5 Passive Listening

Passive Listening allows a redundant coupling between (R)STP networks and MRP ring topologies. The protocol is a proprietary Siemens solution.

10.5.1 Understanding Passive Listening

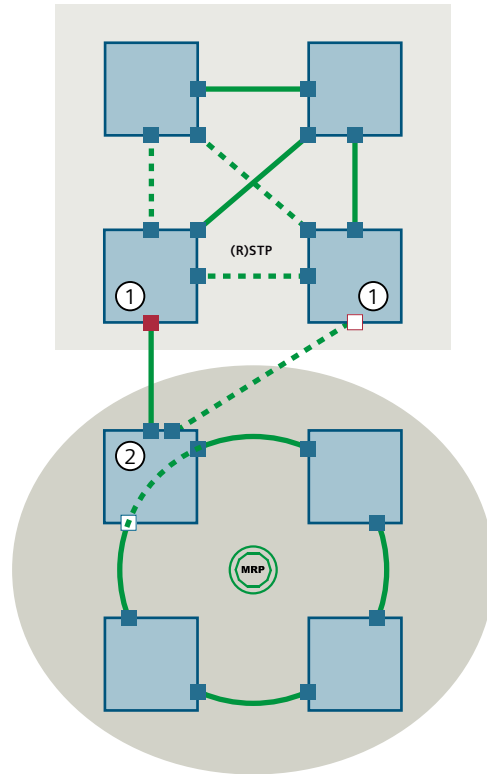
The connection of an office network that operates with an interconnected topology and RSTP to the ring topology of an automation network is a key component of communication in machine and plant construction. This means that process and manufacturing data is not only available at the field level, but is also seamlessly transferred to cross-department IT systems. Service personnel have access to controllers and field devices at all times.

To meet the requirements, a stable, flexible and redundant data network must be implemented. This is achieved by designing the communication networks with redundant physical connection paths between the network nodes. Special redundancy protocols ensure a loop-free network topology and the detection of communication interruptions.

In the redundant coupling of network segments that are managed with different redundancy protocols, circling frames and data traffic failure occur without further measures.

10.5.1.1 Simple coupling without Passive Listening

Without further measures, (R)STP networks can only be connected to MRP-based ring structures via a coupling device.



- ① Coupling devices that belong to the (R)STP network
- ② Coupling device that belongs to the MRP ring
- (R)STP port in Forwarding status
- (R)STP port in Block status

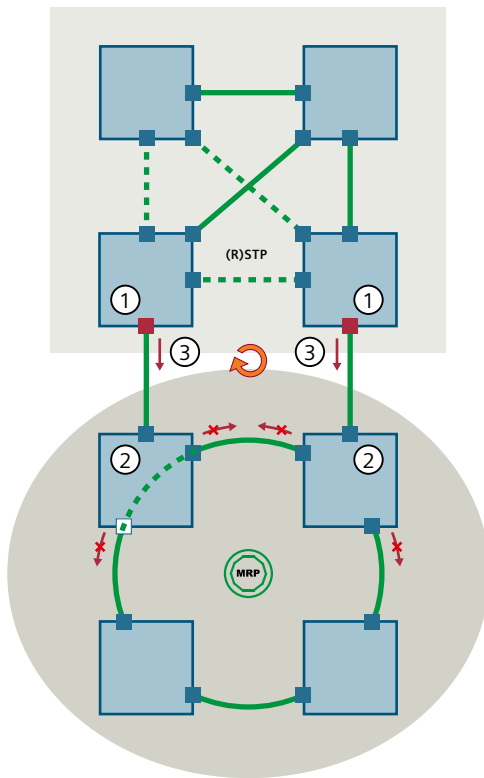
Figure 10-17 Simple coupling of an (R)STP network to an MRP ring

10.5.1.2 Redundant coupling with Passive Listening

If you couple an (R)STP network to an MRP ring via two different coupling devices and do not use a suitable protocol, a loop occurs in the network.

Redundant coupling without Passive Listening

Bridge ports for which (R)STP is not enabled reject (R)STP BPDUs. Because the (R)STP BPDUs are not forwarded in the MRP ring, the two coupling devices that belong to the (R)STP network ① do not recognize the additional connection between them. The coupling ports of the two devices receive the **Edge** role and switch to the **Forwarding** status. The data traffic is sent to the MRP ring via both coupling ports and circles.

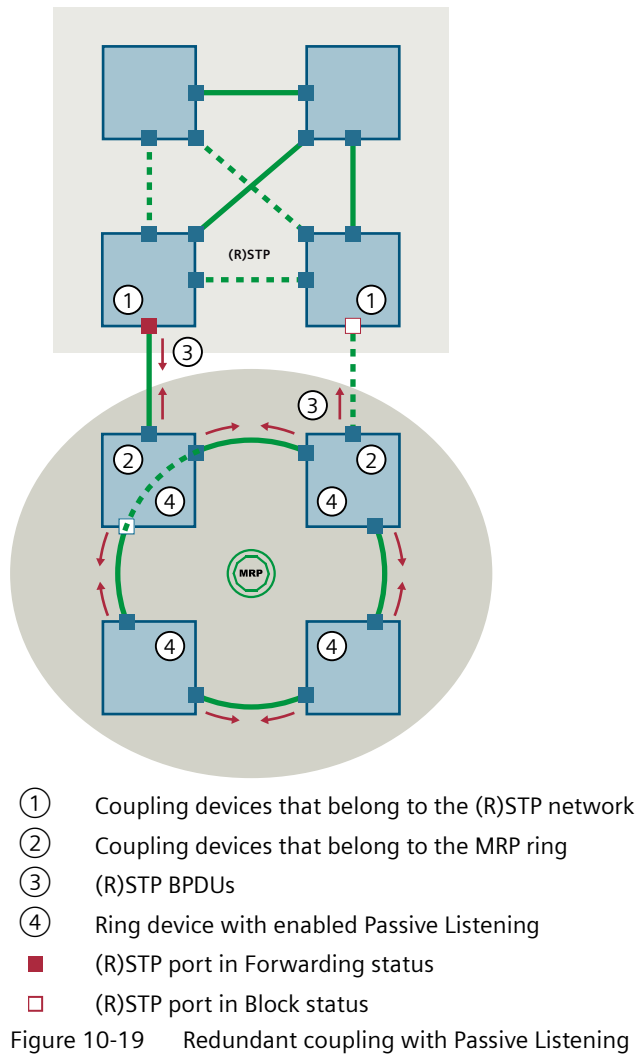


- ① Coupling devices that belong to the (R)STP network
- ② Coupling devices that belong to the MRP ring
- ③ (R)STP BPDUs
- (R)STP port in Forwarding status

Figure 10-18 Redundant coupling without Passive Listening

Redundant coupling with Passive Listening

If Passive Listening is enabled for all ring devices, the BPDUs from an RSTP network are forwarded in the MRP ring and get back to the (R)STP network. The two coupling devices in the (R)STP network ① detect the additional connection between them and resolve the loop by disabling a connection. One coupling port remains in the **Forwarding** status, the other switches to the **Block** status. From the perspective of the (R)STP network, the MRP ring is a point-to-point connection.



10.5.1.3 Topology changes

By default, ring devices would only learn new (R)STP communication paths if they update their MAC address table automatically after expiration of the aging time. To reduce the switchover time, ring devices with enabled Passive Listening behave in the following way:

- Ring devices with active Passive Listening react to (R)STP BPDUs that contain topology changes.
If a ring device receive a topology change message (TCN), it reduces its aging time temporarily so that it can update its MAC address table faster and learn the changed topology.
- Ring devices with enabled Passive Listening monitor the received (R)STP BPDUs for their source MAC address and labeling as query from the (R)STP proposal/agreeing process.
If a ring participant receives three consecutive (R)STP BPDUs from the same source, it marks this source as active sender. Only one source can be the active sender at any one time. If three consecutive (R)STP BPDUs contain a deviating source MAC address and labeling as query, the ring device updates its MAC address.
Alternatively, you can enable the Enhanced Passive Listening Compatibility function on the coupling ports of the (R)STP coupling devices. For more information on Enhanced Passive Listening Compatibility, refer to "Enhanced Passive Listening Compatibility (EPLC) (Page 339)".

10.5.2 Configuring passive listening

To configure passive listening, do the following:

1. Enable passive listening.
For more information, refer to "Activating passive listening (Page 440)".
2. [Optional] Enable VLAN-specific forwarding of (R)STP-BPDUs.
For more information, refer to "Activating VLAN-specific forwarding of BPDUs (Page 441)".
3. [Optional] Block forwarding of (R)STP-BPDUs to a bridge port.
For more information, refer to "Blocking forwarding of (R)STP-BPDUs (Page 442)".

10.5.2.1 Activating passive listening

Passive listening is disabled by default.

To enable passive listening globally, do the following:

| Step | Instruction | Command |
|------|---------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Disable STP globally. | <code>no switch spanning-tree enabled</code> |
| 3 | Enable passive listening. | <code>switch passive-listening enabled</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config switch passive-listening enabled</code> |

Example

Passive listening is enabled in this example.

```
localhost# config
Entering configuration mode terminal
localhost(config)# no switch spanning-tree enabled
localhost(config)# switch passive-listening enabled
localhost(config-passive-listening)# commit
Commit complete.
localhost(config-passive-listening)# end
localhost# show running-config switch passive-listening enabled
switch
  passive-listening
    enabled
  exit
exit
```

10.5.2.2 Activating VLAN-specific forwarding of BPDUs

By default, (R)STP-BPDUs are flooded to all bridge ports of a device, independent of the VLAN configuration.

This option allows you to enable a device to take into account the VLAN membership of the port on which an (R)STP BPDU is received. If a device receives an (R)STP-BPDU at a port with the PVID 7, it only forwards the (R)STP-BPDUs to the ports that are also members of the VLAN 7.

To forward (R)STP-BPDUs in a VLAN-specific manner, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable VLAN-specific forwarding of (R)STP-BPDUs. | switch passive-listening bpdu-flood-vlan |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch passive-listening bpdu-flood-vlan |

Example

In this example, the VLAN-specific forwarding of (R)STP-BPDUs is enabled.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch passive-listening bpdu-flood-vlan
localhost(config-passive-listening)# commit
Commit complete.
localhost(config-passive-listening)# end
localhost# show running-config switch passive-listening bpdu-flood-vlan
switch
  passive-listening
    bpdu-flood-vlan
```

```
exit
```

```
exit
```

10.5.2.3 Blocking forwarding of (R)STP-BPDUs

By default, (R)STP-BPDUs are flooded to all bridge ports of a device.

When you enable this option for a bridge port, received (R)STP-BPDUs are not forwarded to this bridge port.

To block forwarding of (R)STP-BPDUs to a bridge port, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Block forwarding of (R)STP-BPDUs to a bridge port. | <code>interface { bridge port } passive-listening bpdu-flood-block</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } passive-listening bpdu-flood-block</code> |

Example

In this example, the forwarding of (R)STP-BPDUs to the `ethernet0/10` bridge port is blocked.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/10 passive-listening bpdu-
flood-block
localhost(config-passive-listening)# commit
Commit complete.
localhost(config-passive-listening)# end
localhost# show running-config interface ethernet0/10 passive-
listening bpdu-flood-block
interface ethernet0/10
  passive-listening
  bpdu-flood-block
exit

exit
```

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 Understanding LLDP

The Link Layer Discovery Protocol (LLDP) is a protocol for automatic network detection defined in the IEEE standard (IEEE 802.1AB). LLDP enables devices in a local network to detect their neighboring devices and exchange information on properties and configuration with them.

Multicasts are periodically sent via LLDP; this is one-way transfer. Sent data packets are not committed with a receive packet. Sending and receiving take place independently of one another.

LLDP can contribute towards simplifying troubleshooting in complex networks. Network management systems (NMS) use LLDP to obtain and monitor detailed information on the topology of a network.

NOTICE

Security risk - Risk of unauthorized access and/or misuse

By definition, LLDP is not secure. Where possible, disable LLDP on devices that are connected to external networks. Siemens recommends the use of LLDP only in secure environments operated within a security environment.

Note

LLDP is implemented in such a way that only information about a single device can be saved per bridge port. If multiple items of LLDP information are received via a bridge port, the information about the neighboring device will change constantly on this bridge port.

11.1.1.1 TLV Format

LLDP data is composed of a series of attributes that are coded in **Type Length Value (TLV)** format.

11.1 LLDP

Attributes in TLV format are composed as follows:

- Type
Type of the attribute
For more information on attribute types, refer to "LLDPDUs (Page 444)".
- Length
Transmission length of the attribute
- Value
Value of the attribute

11.1.1.2 LLDPDUs

LLDP data is transmitted as Protocol Data Units (LLDPDUs). Each LLDPDU consists of a sequence of attributes in TLV format. An LLDPDU always begins with the mandatory attributes Chassis ID, Port ID and TTL. The mandatory attributes can be followed by any number of optional attributes. Every LLDPDU always ends with the End of LLDPDU TLV.

Mandatory attributes

An LLDPDU consists of at least the following attributes:

- Chassis ID TLV (Type 1)
The MAC address of the sending device, which is unique within the network
- Port ID TLV (Type 2)
The port number of the sending device.
- Time To Live TLV (Type 3)
The "Time To Live" (TTL) value specifies how long information is valid.
- End of LLDPDU TLV (Type 0)
Each LLDPDU must be concluded with this attribute.

Clear identification of the connection point in the topology is possible via these attributes. This information therefore counts as a minimum requirement for the detection of the topology with LLDP.

Optional attributes

An LLDPDU can contain the following attributes, for example:

- Port Description TLV (Type 4)
User-defined description of the port, supplementing the Port ID
This type can contain the value of "ifDescr" (RFC 2863).
- System Name TLV (Type 5)
User-defined description of the system name, supplementing the Chassis ID
This type can contain the value of "sysName" (RFC 3418).
- System Description TLV (Type 6)
User-defined description of the system, supplementing the Chassis ID
This type can contain the value of "sysDescr" (RFC 3148).

- **System Capabilities TLV (Type 7)**
The device category/characteristic of the device, e.g. router, bridge, telephone, WLAN access point or other end device
- **Management Address TLV (Type 8)**
The management address(es) via which the device can be reached

11.1.1.3 Send and receive module

An LLDP agent runs on devices that support LLDP. LLDP agent operation is usually implemented in the form of two modules:

- **LLDP transmit module**
In the activated state, the LLDP transmit module regularly sends information on the local device. This includes information on properties, configuration, networking and identification. If the transmit module is disabled, it no longer transmits LLDPDUs. After the last LLDPDU at the receiver end has expired, the neighboring devices clear the information associated with the local device from their databases.
- **LLDP receive module**
In the activated state, the LLDP receive module receives information about neighboring devices and saves this locally in its database, the Management Information Base (MIB). The saved LLDP data is accessible via SNMP. When new or updated information is received, the receive module initiates a timer for the lease time specified by the TTL TLV in the received LLDPDU. When this lease time expires and the LLDPDU has not been received again, the connection is deleted from the local LLDP-MIB. The saved connection is also deleted when the receive module receives an LLDPDU with a TTL TLV of 0.

11.1.2 Configuring LLDP

To configure LLDP, do the following:

1. Make sure that LLDPDUs can be sent and received from a bridge port.
For more information, refer to "Configuring the sending and receiving of LLDPDUs for a bridge port (Page 446)".
2. [Optional] Configure the TTL that a device supplies in outgoing LLDPDUs.
For more information, refer to "Defining the TTL in outgoing LLDPDUs (Page 446)".
3. [Optional] Configure the interval at which LLDPDUs are sent.
For more information, refer to "Defining the send interval for LLDPDUs (Page 447)".
4. [Optional] Configure the delay of LLDPDUs during initialization of LLDP on a bridge port.
For more information, refer to "Defining the delay of LLDPDUs during initialization of LLDP on a bridge port (Page 448)".
5. [Optional] Configure the delay of LLDPDUs after a configuration change.
For more information, refer to "Defining the transmission delay of the LLDPDU after a configuration change (Page 449)".

11.1.2.1 Configuring the sending and receiving of LLDPDUs for a bridge port

To configure how LLDPDUs are sent or received for a bridge port, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure how LLDPDUs are sent or received for a bridge port. Options include: <ul style="list-style-type: none"> <code>disabled</code> - LLDPDUs are neither sent nor received on the bridge port. <code>rxOnly</code> - LLDPDUs are received but not sent on the bridge port. <code>txAndRx</code> - LLDPDUs are sent and received on the bridge port. <code>txOnly</code> - LLDPDUs are sent but not received on the bridge port. Default: <code>txAndRx</code> | <code>interface { bridge port } lldp admin-status [disabled rxOnly txAndRx txOnly]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } lldp admin-status</code> |

Example

In this example, it is configured for `ethernet0/3` that it only receives LLDPDUs.

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/3 lldp admin-status rxOnly
localhost(config-interface-ethernet0/3-lldp)# commit
Commit complete.
localhost(config-interface-ethernet0/3-lldp)# end
localhost# show running-config interface ethernet0/3 lldp admin-
status
interface ethernet0/3
  lldp
    admin-status rxOnly
  exit
exit
```

11.1.2.2 Defining the TTL in outgoing LLDPDUs

The lease time (TTL) defines the time for which a neighboring device saves the LLDP information before deleting it. The value for the lease time is calculated from the send interval `tx-interval` and a multiplier.

To define the TTL included, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the multiplier. Default: 4 | <code>lldp hold { 2 - 10 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config lldp hold</code> |

Example

In this example, a multiplier of 6 is configured.

```
localhost# config
Entering configuration mode terminal
localhost(config)# lldp hold 6
localhost(config-lldp)# commit
Commit complete.
localhost(config-lldp)# end
localhost# show running-config lldp hold
lldp
  hold 6
exit
```

11.1.2.3 Defining the send interval for LLDPDUs

To configure the send interval for LLDPDUs, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the interval in seconds at which the LLDP agent sends LLDPDUs to all bridge ports. Default: 5 | <code>lldp tx-interval { 5 - 32768 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config lldp tx-interval</code> |

Example

In this example, a send interval of 50 seconds is configured.

```
localhost# config
Entering configuration mode terminal
localhost(config)# lldp tx-interval 50
localhost(config-lldp)# commit
Commit complete.
localhost(config-lldp)# end
localhost# show running-config lldp tx-interval
lldp
  tx-interval 50
```

```
exit
```

11.1.2.4 Defining the delay of LLDPDUs during initialization of LLDP on a bridge port

If sending and/or receiving LLDPDUs has been enabled again for a bridge port with the LLDP status `disabled`, the LLDP agent suppresses the transmission of LLDPDUs for the configured period. LLDP remains disabled on the relevant bridge port for this period.

To configure the delay in the event of re-initialization of LLDP for all bridge ports, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the time in seconds for which the LLDP agent waits before it sends LLDPDUs even though LLDP is activated. Default: 1 | <code>lldp reinit-delay { 1 - 10 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config lldp reinit-delay</code> |

Example

In this example, a delay of 2 seconds is configured.

```
localhost# config
Entering configuration mode terminal
localhost(config)# lldp reinit-delay 2
localhost(config-lldp)# commit
Commit complete.
localhost(config-lldp)# end
localhost# show running-config lldp reinit-delay
lldp
  reinit-delay 2
exit
```


11.1.2.5 Defining the transmission delay of the LLDPDU after a configuration change

To configure the transmission delay of LLDPDUs after a configuration change, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Configure the minimum time in seconds between two LLDPDUs when the device configuration has changed.</p> <p>The value of the transmission delay on a configuration change <code>tx-delay</code> should be no more than a quarter of the send interval for LLDPDUs <code>tx-interval</code>.</p> <p>Default: 1</p> <p>Example</p> <ul style="list-style-type: none"> <code>tx-interval 50 s</code> <code>tx-delay 10 s</code> <p>The LLDP agent sends an LLDPDU (<code>tx-interval</code>) every 50 seconds.</p> <p>If the configuration is changed 5 seconds after the last LLDPDU, the LLDP agent waits 5 seconds before sending the next LLDPDU.</p> <p>If the configuration is changed 15 seconds after the last LLDPDU, the 10 seconds of the transmission delay (<code>tx-delay</code>) are already exceeded and the LLDP agent immediately sends the next LLDPDU.</p> | <code>lldp tx-delay { 1 - 8192 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config lldp tx-delay</code> |

Example

In this example, a transmit delay of 10 seconds is configured.

```
localhost# config
Entering configuration mode terminal
localhost(config)# lldp tx-delay 10
localhost(config-lldp)# commit
Commit complete.
localhost(config-lldp)# end
localhost# show running-config lldp tx-delay
lldp
  tx-delay 10
exit
```

11.1.3 Monitoring LLDP

This section describes how you can view LLDP information of your own device and of the connected neighboring devices.

11.1.3.1 Displaying the LLDP information of the device that is transmitted to neighbor devices

To display the LLDP information for the device that is transmitted to neighboring devices, execute the following command in operating mode:

```
show lldp local-system-data
```

Example

```
localhost# show lldp local-system-data
LLDP local-system-data
  Local System Name           localhost
  Local System Description     Siemens, SIMATIC NET, SCALANCE ..,
                               6GK5 .., HW: Version x, FW: Version Vx, ..
  Local Device ID             10:00:00:00:00:00
  Local Chassis ID Subtype     macAddress
  Capabilities Enabled         bridge
```

Description

The following information is shown:

| Parameter | Description |
|--------------------------|---|
| Local System Name | System name of the device |
| Local System Description | Description of the device with the following information: <ul style="list-style-type: none"> • Manufacturer • System • Device name • Article number • Hardware version • Firmware version • Serial number |
| Local Device ID | Device ID The ID corresponds to the PROFINET device name. If no PROFINET device name is assigned, the MAC address of the device is shown. |
| Local Chassis ID Subtype | Data type with which the device ID is specified Possible values: <ul style="list-style-type: none"> • <code>macAddress</code> - The MAC address of the device is used as device ID. • <code>local</code> - A PROFINET device name was assigned. The PROFINET device name is used as device ID. |
| Capabilities Enabled | Properties that the device supports |

11.1.3.2 Monitoring the LLDP information of neighbor devices

To monitor LLDP information from neighboring devices, execute the following command in operational mode:

```
show lldp neighbors
```

Example

```
localhost# show lldp neighbors | notab
LLDP neighbor
  Remote Index                1
  Remote Device ID            10:00:00:00:00:FF
  Remote Time Mark            0
  Local Port ID                1
  Local Interface              ethernet0/1
  Remote System Name          SCALANCE
  Remote Capabilities Enabled  bridge,router
  Remote Hold Time             20s
  Remote Port ID               port-004-00004
```

Description

If neighboring devices that support LLDP are connected, the following information is displayed:

| Parameter | Description |
|-----------------------------|--|
| Remote Index | Ascending index in the table |
| Remote Device ID | Device ID of the connected device The ID corresponds to the PROFINET device name. If no PROFINET device name is assigned, the MAC address of the device is shown. |
| Remote Time Mark | System operating time in hundredths of a second at which the neighboring device was added |
| Local Port ID | Number of the physical port at which the information about the connected device was received |
| Local Interface | Name of the bridge port at which the information about the connected device was received |
| Remote System Name | System name of the connected device |
| Remote Capabilities Enabled | Properties of the connected device Possible values: <ul style="list-style-type: none"> • Bridge • Router • Station • DOCSIS Cable Device (cable modem) • WLAN Access Point • Repeater • Telephone • Other |
| Remote Hold Time | Time period formatted as nYnMnDnHnMnS for which LLDP information of the connected device is stored before the device deletes it |
| 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 452)".
2. Configure whether DCP frames can be sent from a bridge port.
For more information, refer to "Configuring the forwarding of DCP frames for a bridge port (Page 456)".

11.2.2.1 Configuring the access rights of DCP

NOTICE

Security hazard - Risk of unauthorized access and/or misuse

By definition, DCP is not secure. 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. 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.

To prevent unauthorized access and/or misuse, configure write-protected access rights for DCP (`read-only`).

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

If you use the device in PROFINET operation with the DCP option `read-only`, there is a risk of connection losses.

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.

To set the IP address retentively so that it is retained after a cold or warm restart, you have the following options:

- 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:

| Step | Instruction | Command |
|------|---------------------------|---------------------|
| 1 | Enter configuration mode. | <code>config</code> |

| Step | Instruction | Command |
|------|---|---|
| 2 | <p>Configure the access rights of DCP.</p> <p>Options include:</p> <ul style="list-style-type: none"> • <code>off</code> - DCP is disabled. Device parameters can neither be read nor modified. The device cannot be operated as a PROFINET device with this setting. • <code>read-only</code> - DCP is activated. 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>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> <ul style="list-style-type: none"> • <code>read-write</code> - DCP is activated. Device parameters can be both read and modified. IP parameters and/or the PROFINET device name can be changed or reset. • <code>setup</code> - The access rights of DCP depend on the status of the device. <p>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 <code>read-write</code> 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.</p> <p>In secure operating state, the device parameters can be read but cannot be modi-</p> | <pre>profinet dcp-mode [off read-only read-write setup]</pre> |

| Step | Instruction | Command |
|------|---|--|
| | <p>fed. The access rights of DCP correspond to the <code>read-only</code> option from this time.</p> <p>Default: <code>setup</code></p> | |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config profinet dcp-mode</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# profinet dcp-mode read-only
localhost(config-profinet)# commit
Commit complete.
localhost(config-profinet)# end
localhost# show running-config profinet dcp-mode
profinet
  dcp-mode read-only
exit
```

11.2.2.2 Configuring the forwarding of DCP frames for a bridge port

Receiving of DCP frames cannot be disabled. You can configure whether a bridge port forwards DCP frames.

DCP frames are forwarded and received on all bridge ports by default.

To configure whether a bridge port forwards DCP frames, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure whether a bridge port forwards DCP frames. | <code>interface { bridge port } profinet dcp-forwarding</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } profinet dcp- forwarding</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# interface ethernet0/3 profinet dcp-forwarding
localhost(config-interface-ethernet0/3-profinet)# commit
Commit complete.
localhost(config-interface-ethernet0/3-profinet)# end
localhost# show running-config interface ethernet0/3 profinet dcp-
forwarding
interface ethernet0/3
  profinet
```



```
dcp-forwarding
exit

exit
```

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

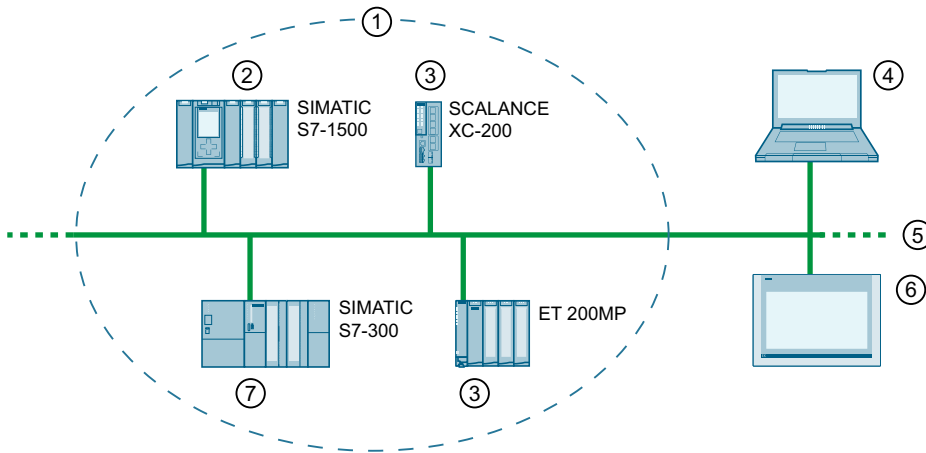
11.3 PROFINET

- 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.

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 461)".
2. [Optional] Configure the behavior in case of a PROFINET error.
For more information, refer to section "Configuring the behavior in case of a PROFINET error (Page 463)".
3. Enable PROFINET.
For more information, refer to section "Configuring PROFINET runtime mode (Page 463)".
4. [Optional] Save the GSD file.
For more information, refer to section "Saving the GSD file on a remote server (Page 464)".

Note

Although the `name-of-station` is displayed in configuration mode, you cannot change the PROFINET device name in the CLI. You configure the PROFINET device name with SINEC PNI, for example.

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 becomes active directly.

NOTICE

Configuration hazard - risk of frame loss

When you change the TIA interface, loss of sent and received PROFINET frames can occur for a short time.

To configure the TIA Interface, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the TIA interface. Default: <code>vlan1</code> | <code>profinet tia-interface { IP interface }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config profinet tia- interface</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# profinet tia-interface vlan4
localhost(config-profinet)# commit
Commit complete.
localhost(config-profinet)# end
localhost# show running-config profinet tia-interface
profinet
  tia-interface vlan4
exit
```

11.3.2.2 Configuring the behavior in case of a PROFINET error

To configure the behavior of a PROFINET device in case of a PROFINET error, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the behavior of a PROFINET device in case of a PROFINET fault. Options include: <ul style="list-style-type: none"> <code>latent</code> - The device ignores PROFINET faults. <code>evident</code> - The device signals a PROFINET fault when there is no connection to a PROFINET controller. <p>Even if the <code>latent</code> option is configured, the device automatically enables the <code>evident</code> option when the device had set up a connection to a PROFINET controller once before. When the connection to the PROFINET controller no longer exists, the <code>evident</code> option remains set. Default: <code>latent</code></p> | <code>profinet fault-mode [latent evident]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config profinet fault-mode</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# profinet fault-mode evident
localhost(config-profinet)# commit
Commit complete.
localhost(config-profinet)# end
localhost# show running-config profinet fault-mode
profinet
  fault-mode evident
exit
```

11.3.2.3 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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the PROFINET runtime mode. Options include: <ul style="list-style-type: none"> <code>off</code> - Only DCP and LLDP are enabled. <code>on</code> - PROFINET is enabled. Default: <code>on</code> | <code>profinet admin-status [off on]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | To enable the PROFINET runtime mode, restart the device. | <code>system restart</code> |
| 6 | Respond to the security prompt. To cancel the restart, answer the security prompt with <code>no</code> . | <code>yes</code> |
| 7 | Call up the CLI and log in. For more information, refer to "Calling the CLI (Page 111)" and "Logging in to a configured device (Page 115)". | - |
| 8 | Verify the configuration. | <code>show profinet oper-status</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# profinet admin-status off
localhost(config-profinet)# commit
Commit complete.
localhost(config-profinet)# end
localhost# system restart
Are you sure you want to reboot the device? [no,yes] yes
.
.
.
login as: admin
admin@192.168.16.15's password: *****

Welcome to the SINEC OS Command Line Interface
Copyright (c) 2019 Siemens AG

admin connected from 192.168.16.1 using ssh on localhost
localhost# show profinet oper-status
oper-status off
```

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.

Note

Name change in the GSD file

The names of some devices were modified in the GSD file that is supplied with SINEC OS version 2.4. If an older GSD file is already used in a configuration tool, this can lead to confusion.

If you use the GSD file in a configuration tool, we strongly recommend that you delete all older GSD files from SINEC OS devices.

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Save the GSD file. For more information on the URL, see "Specifying a URL (Page 67)". | <code>system data-model gsdml save target { URL }</code> |
| 2 | Respond to the security prompt. To cancel the saving, answer the security prompt with <code>no</code> . | <code>yes</code> |

Example

```

In this example, the GSD file is saved to a file with the name gsdml.zip on a TFTP server.
localhost# system data-model gsdml save target tftp://
192.168.200.10/gsdml.zip
Are you sure you want to save GSDML file? [no,yes] yes
Transferring file... done
localhost#

```

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 current PROFINET runtime mode, execute the following command in operational mode:

```
show profinet oper-status
```

11.3 PROFINET

Example

```
localhost# show profinet oper-status
oper-status off
```

Description

The following information is shown:

| Parameter | Description |
|-------------|---|
| oper-status | Displays the PROFINET runtime mode. Possible values: <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 monitor the connection to a PROFINET controller, execute the following command in operational mode:

```
show profinet oper-in-data-exchange
```

Example

```
localhost# show profinet oper-in-data-exchange
oper-in-data-exchange offline
```

Description

The following information is shown:

| Parameter | Description |
|-----------------------|--|
| oper-in-data-exchange | Shows whether there is a connection to a PROFINET controller. Possible values: <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

To display the TIA interface, execute the following command in operational mode:

```
show running-config profinet tia-interface
```

Example

In this example, the TIA interface is displayed.

```
localhost# show running-config profinet tia-interface
profinet
  tia-interface vlan1
exit
```

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, execute the following command in operational mode:

```
show profinet im
```

Example

```
localhost# show profinet im
im manufacturer-id      42
im order-id            "6GK5 332-0GA01-2AC2"
im serial-number       VPM5001664
im hardware-revision   1
im software-revision   V02.00.00
im revision-counter    0
im revision-date       "1970-01-01 00:00"
im function-tag        Function
im location-tag        Location
im date                "2020-11-01 09:00"
im descriptor          Comment
```

Description

The following information is shown:

| 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. |
| 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. |

11.4 EtherNet/IP

| Parameter | Description |
|------------|--|
| 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 current PROFINET device name, execute the following command in operational mode:

```
show running-config profinet name-of-station
```

Example

```
localhost# show running-config profinet name-of-station
profinet
 name-of-station switch-vpm6002848
exit
```

Description

The following information is shown:

| 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. |

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

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 471)".
2. Enable EtherNet/IP.
For more information, refer to section "Enabling EtherNet/IP (Page 472)".
3. [Optional] Save the EDS file.
For more information, refer to section "Saving the EDS file on a remote server (Page 472)".
4. [Optional] Configure DLR.
For more information, refer to section "Device Level Ring (Page 403)".

11.4.2.1 Configuring the management interface

All EtherNet/IP functions of the device are available over the management interface.

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the management interface. Default: <code>vlan1</code> | <code>ethernetip management-interface { IP interface }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config ethernetip management-interface</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# ethernetip management-interface vlan4
localhost(config-etherenetip)# commit
Commit complete.
localhost(config-etherenetip)# end
```

11.4 EtherNet/IP

```
localhost# show running-config ethernetip management-interface
ethernetip
  management-interface vlan4
exit
```

11.4.2.2 Enabling EtherNet/IP

EtherNet/IP is disabled by default.

To enable EtherNet/IP, do the following:

| Step | Instruction | Command |
|------|---------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable EtherNet/IP. | <code>ethernetip enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config ethernetip</code> |

Example

EtherNet/IP is enabled in this example.

```
localhost# config
Entering configuration mode terminal
localhost(config)# ethernetip enabled
localhost(config-ethernetip)# commit
Commit complete.
localhost(config-ethernetip)# end
localhost# show running-config ethernetip
ethernetip
  enabled
exit
```

11.4.2.3 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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Save the EDS file. For more information on the URL, see "Specifying a URL (Page 67)". | <code>system data-model eds save target { URL }</code> |
| 2 | Respond to the security prompt. To cancel the saving, answer the security prompt with <code>no</code> . | <code>yes</code> |

Example

In this example, the EDS file is saved to a file with the name `eds.zip` on a TFTP server.

```
localhost# system data-model eds save target tftp://192.168.200.10/eds.zip
Are you sure you want to save EDS file? [no,yes] yes
Transferring file... done
localhost#
```

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, execute the following command in operational mode:

```
show interface ipv4 arp
```

Alternatively, to display the ARP table for a specific interface, execute the following command in operational mode:

```
show interface { bridge port } ipv4 arp
```

Example

The following displays a summary for all VLAN interfaces.

```
localhost# show interface ipv4 arp
NAME      IP                PHYS ADDRESS      ORIGIN  AGE    TYPE  STATE
-----
vlan1    192.168.11.25    08:00:27:0a:ed:ac  dynamic 19s   arpa  delay
vlan2    192.168.10.242  00:0a:dc:2b:5a:c3  dynamic 2m5s  arpa  stale
```

Example

The following displays a summary for a specific VLAN interface.

```
localhost# show interface vlan1 ipv4 arp
IP                PHYS ADDRESS      ORIGIN  AGE    TYPE  STATE
-----
192.168.10.25    08:00:27:0a:ed:ac  dynamic 19s   arpa  reachable
```

Description

The following information is displayed for each VLAN interface:

| Parameter | Description |
|--------------|---|
| NAME | The name of the VLAN interface. |
| IP | The IP address of the neighboring node. |
| PHYS 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 69)". |

| Parameter | Description |
|-----------|---|
| TYPE | The encapsulation method used for ARP messages. Possible values include: <ul style="list-style-type: none"> <code>arpa</code> - 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"> <code>reachable</code> - 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. <code>stale</code> - The neighbor is considered unreachable. Reachability will be reassessed the next time traffic is sent to the neighbor. <code>delay</code> - ARP is preparing to probe the neighbor to determine if it is reachable. After 5 seconds, the state will change to <code>probe</code>. <code>probe</code> - 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 <code>reachable</code>. |

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.

11.6.1 Understanding SNMP

SNMP is a UDP/IP-based, open protocol for the monitoring, control and administration of networks. SNMP was developed to simplify management functions and allow a transparent exchange of data between different network components.

Tasks of SNMP

- Monitoring of network components
- Diagnostics of network components
- Error detection and error notification
- Remote configuration of network components

11.6.1.1 SNMP versions

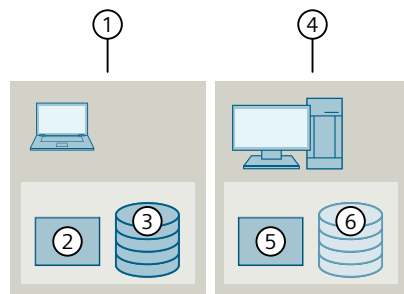
SINEC OS supports the following versions of SNMP:

- **SNMPv1**
SNMPv1 offers basic SNMP message types with which data of network components can be requested or changed.
SNMPv1 has few security mechanisms. Each user in the network can access and change data using the relevant community string.
- **SNMPv2c**
Like SNMPv1, SNMPv2c also has few security mechanisms. Each user in the network can access and change data using the relevant community string.
As compared to SNMPv1, SNMPv2c supports the following additional functions:
 - With the GetBulk command, several data records can be requested at once.
 - Extended error messages that differentiate between different error types. In SNMPv1, there is only one error message for all error types.
- **SNMPv3**
As compared to the previous versions SNMPv1 and SNMPv2c, the security concept of SNMPv3 was expanded by the following mechanisms:
 - Timeliness
Ensures messages are processed within a defined time and thereby protects against delayed or repeated messages.
 - User authentication
Ensures only messages from permitted sources are evaluated.
Ensures messages are not damaged or changed.
 - Encryption of the data traffic
Ensures packets cannot be read by unauthorized parties. This is achieved by appending a character string calculated from the user name and password.

11.6.1.2 SNMP components

SNMP controls communication between the following components:

- **Network component with SNMP agent**
A network component that supports SNMP needs an SNMP agent and a Management Information Base (MIB). The SNMP agent runs directly on the device. The SNMP agent manages the data records of the network component in a MIB and communicates with SNMP managers.
- **SNMP manager**
An SNMP manager is a central management station that manages network components. SNMP managers must know the structure of the MIB and thus the position of the data to be able to request or change the data records of a network component.
For more information on MIBs, refer to "Management information base (Page 477)".
If an SNMP manager is configured properly, it can also receive notifications from SNMP agents.



- ① Network component
- ② SNMP agent
- ③ On the network component, the configuration data is saved in the MIB.
- ④ SNMP manager
- ⑤ Recipient of notifications
- ⑥ The SNMP manager must know the structure of the MIB to be able to request data.

Figure 11-2 SNMP components

11.6.1.3 Engine ID

Every SNMP device has a unique SNMP engine ID. The device generates the engine ID based on its MAC address.

An SNMP manager must know the engine ID of a monitored network component. If an SNMP manager does not know the engine ID of a device, it sends an empty **Get** request and the SNMP agent responds with its engine ID.

11.6.1.4 Management information base

A management information base (MIB) represents the database of a network component in a hierarchical, object-oriented form. The data is also referred to as MIB objects. Each MIB object is identified by a unique Object Identifier (OID).

On a network component, the MIB is managed by the SNMP agent.

The following types of MIBs exist:

- **Standard MIBs**
Standard MIBs are defined in RFCs and other standards.
- **Private MIBs**
Private MIBs are provided by the manufacturer if component-specific, non-standardized data is necessary for network monitoring.
In terms of content and organization, private MIBs are based on the structure of standard MIBs. They can therefore be integrated in the overall SNMP model.

Either the SNMP manager knows the description of a MIB (when it is a standard MIB) or the description must be stored by an administrator, for example, in the case of private MIBs. The MIB files of the device can be downloaded with SINEC OS. For more information, refer to (<https://support.industry.siemens.com/cs/de/en/view/109797643>).

11.6.1.5 Requests and notifications

SNMP managers and SNMP agents can communicate by means of SNMP requests (Polling) and SNMP notifications:

- **Polling**

The SNMP manager requests the parameters of an SNMP agent to be monitored at regular time intervals. The SNMP agent responds with the relevant information.

Advantages

- Due to the regular requests, an SNMP manager is notified when an SNMP agent is no longer available.
- The regularly polled values give an overview of the development of a parameter. A slow deterioration can be detected at an early stage.

Disadvantages

- If an event occurs between two requests, the SNMP manager does not receive the information until its next request.

- **Notifications**

When certain events occur, the SNMP agent assumes the active role and sends an unsolicited notification to an SNMP manager.

Advantages

- Any errors that occur are immediately reported to the SNMP manager.

Disadvantages

- The supported notifications are not confirmed by the recipient, so it is not certain whether an SNMP manager has received the information.
- A flood of notifications increases network load and can, for example, make the problems indicated by the notifications worse.

The two methods can be combined for optimal monitoring by SNMP.

11.6.1.6 SNMP communication

The SNMP communication takes place between SNMP manager ① and SNMP agent ②.

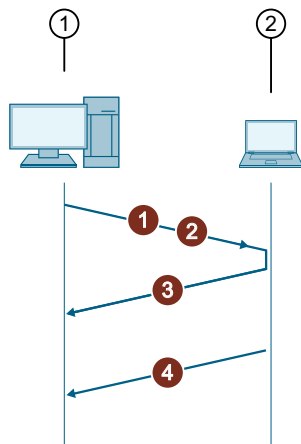


Figure 11-3 SNMP communication

SNMP is familiar with the following types of messages.

| | SNMP message type | Meaning | Available as of |
|---|-------------------|---|-----------------|
| 1 | Get | Is sent by the SNMP manager to an SNMP agent to request its data record. | v1 |
| | GetNext | GetNext is an extension of the Get query the requests the value of the next OID in the MIB. GetNext is used to request data from tables, to request a tag that cannot be addressed directly or to run through the structure of the MIB. | v1 |
| | GetBulk | With GetBulk, an SNMP manager requests multiple data records with only one message. This request is comparable with multiple consecutive GetNext messages. With GetBulk requests, the protocol requirements for sending large blocks of information are reduced. | v2c |
| 2 | Set | With Set, an SNMP manager changes the data records of a managed network component. | v1 |
| 3 | Response | With Response, an SNMP agent answers Get and Set messages of an SNMP manager. The SNMP agent reacts to a Get request with a Response message that contains either the requested data or an error message. The SNMP agent reacts to a Set request with a Response message that contains either a confirmation or an error message. | v1 |
| 4 | Trap | A notification (Trap) is triggered by a special event. This may be the occurrence of an error, for example. In this case, an SNMP agent immediately sends a message to the SNMP manager unprompted. Without notifications, the SNMP manager would only learn of the event with the next request. Notifications are not confirmed by the SNMP manager. | v1 |

11.6.1.7 SNMP ports

The following ports are required for SNMP communication:

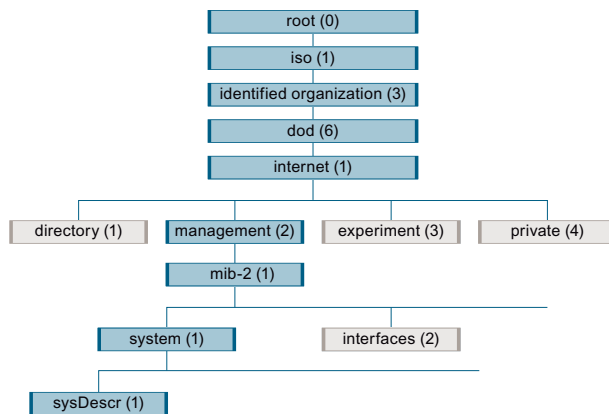
- **Port for receiving SNMP requests**
If SNMP is enabled, SNMP managers and SNMP agents communicate on port 161 by default. You can change the port number.
- **Port for receiving SNMP notifications**
Port 162 is used for receiving event-related notifications by default. You can change the port number separately for each SNMP target.

11.6.1.8 Object identifier

An Object Identifier (OID) describes the path through the hierarchical MIB to the relevant MIB object or sub-tree. The OID is represented as a string of numbers or an ASCII character string. By means of OIDs, SNMP objects are defined with a unique address, a name and information about the type, access rights, and a description.

Example

The OID 1.3.6.1.2.1.1.1 is the path to the sysDescr object.

**11.6.1.9 sysName MIB object**

The sysName MIB object corresponds to the device name. It uses the same data source as the host name. The two elements only differ in their default setting and after reset or deletion. If a specific value is configured for one of the two elements, both elements contain the same value.

The sysName MIB object is empty by default (empty string).

Conditions:

- Must be between 0 and 255 characters long

For more information on host names, refer to "Changing the host name (Page 116)".

11.6.1.10 Authentication and access rights

Depending on the SNMP version, there are different procedures for authentication with SNMP requests:

- Community strings with SNMPv1 and SNMPv2c
- SNMP user (User-Based Security Model, USM) with SNMPv3

The management of access rights by means of SNMP groups and SNMP views is handled for all SNMP versions using the View-Based Access Control Model (VACM).

11.6.1.11 SNMP communities with SNMPv1 and SNMPv2c

SNMP communities are configured for authentication with SNMPv1 and SNMPv2c. The name of an SNMP community is known as the community string.

A community string is transmitted unencrypted together with an SNMP request and serves as a password for authentication. If the community string is correct, the SNMP agent responds and sends the requested data. If the community string is not correct, the SNMP agent discards the query.

To limit unauthorized access, you can configure the following optional parameters for an SNMP community:

- **Context**
The context is transmitted with an SNMP request together with the community string. By default, an empty string is stored for the context. You can define the rights assignment for an SNMP community using a specific context.
- **IP address or IP range**
Using an SNMP target, you can define allowed IP addresses to an SNMP community and thereby only allow SNMP messages from specific IP addresses. Depending on the defined prefix length, frames are only accepted when the SNMP manager is located in a specific subnet. This helps control the SNMP managers from which specific community strings are accepted.

11.6.1.12 User-based Security Model (USM) with SNMPv3

SNMP users are configured for authentication with SNMPv3. The User-Based Security Model (USM) manages SNMP users with the relevant security levels:

- **No authentication, no privacy**
An SNMP request is valid without the use of specific security levels. Specification of the user name is sufficient for authentication. Data is transferred unencrypted.
- **Authentication, no privacy**
An SNMP request is only valid with the relevant authentication password. Data is transferred unencrypted.
- **Authentication and privacy**
An SNMP request is only valid with the relevant authentication and encryption password. Data is transferred encrypted.

With SNMPv3 communication, the message type defines who performs authentication:

- For SNMP messages demanding a response (e.g. Get and Set), the recipient checks the transmitted information.
- With SNMP notifications, the sender checks the transmitted information.

11.6.1.13 Passwords and localized keys

To enable a high level of security, USM uses an algorithm that transforms authentication and encryption passwords into localized keys (Localized Key).

A localized key is derived from the password of a user and the SNMP engine ID of a device. If a user uses the same password multiple times, they have different localized keys for each SNMP device due to the unique SNMP engine IDs.

For more information, see RFC 2574 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) (<https://tools.ietf.org/html/rfc2574>).

The authentication and encryption passwords are not saved in the device. The localized keys are saved in the MIB and in the configuration database (CDB). If you configure a password for a user, you cannot output the password again. You can only view the localized key with a `show` command.

11.6.1.14 View-based Access Control Model (VACM) for assigning access rights

The View-based Access Control Model (VACM) assigns access rights to SNMP groups. The following members can be linked with an SNMP group:

- SNMPv1/v2c communities
- SNMPv3 users

SNMP access rights can be assigned in various levels via the following parameters of a group:

- **Security model**

Define the security settings the sender can use when generating a message. The security model relates to the SNMP version used:

- v1
- v2c
- usm

Specification of the security model enables the SNMP communication to be restricted to specific SNMP versions.

If multiple SNMP versions are configured, an SNMP agent can assign different access rights to a message depending on the SNMP version used. For example, an SNMP agent can grant write access to an MIB object if the SNMP version is `usm` and read access only if the SNMP version is `v1`.

- **Security level**

The security level defines which security information is required for an SNMP request:

- `no-auth-no-priv` - No passwords need to be entered.
- `auth-no-priv` - The password for authentication must be provided with an SNMP request.
- `auth-priv` - The passwords for authentication and encryption must be provided with an SNMP request.

- **Context**

An SNMP agent can assign different access rights depending on the context. The context provided by the sender of an SNMP request must correspond to the configured context of the group in order for the associated access rights to be valid.

- **Type of access**

A distinction is made between the following types of access:

- Read (Get)
- Write (Set)
- Notifications (Trap)

- **SNMP View**

SNMP views can be individual values or complete paths of the MIB which are permitted to view or change an SNMP request with corresponding access rights. After successful authentication, the sender of an SNMP request only receives access to the data for which they have access rights according to the SNMP view.

11.6.1.15 Processing of an SNMP request

With an SNMP request, an SNMP agent receives at least the following information:

- **Community string (v1/v2c)**
SNMP managers must know the configured community strings.
- **User name (v3)**
SNMP managers must know the configured user names.
- **Security model**
SNMP managers must know the configured SNMP versions.
- **Security level**
SNMP managers must know the configured passwords for the authentication and encryption.
- **Context**
SNMP managers must know the configured contexts.

If the SNMP manager has more than one value stored for a parameter, the SNMP manager decides which value to provide. For example, an SNMP manager knows two community strings: one for read requests and one for write requests. For read requests, the SNMP manager uses the community string for read access. Correspondingly, for write requests, it uses the community string for write access.

An SNMP request is processed as follows:

1. The SNMP agent determines the security name using the community string. With SNMPv3, the user name corresponds to the security name.
2. Using the security name and the SNMP version, the SNMP agent finds the relevant group. The combination of security name and SNMP version must be uniquely assigned to a group.
3. The SNMP agent takes the access rights from the configuration of the group depending on the SNMP version, the security level and the context. The access rights define which SNMP view is released through which access type.

Example

The SNMP agent receives a request with the community string `Sinec`. Using the community string (`text-name`), the SNMP agent can determine the security name of the SNMP community: `Sinec-Sec`.

```
localhost# show running-config system management-services snmp
community
system
management-services
snmp
community Sinec-Community
text-name      Sinec
security-name  Sinec-Sec
exit

exit

exit

exit
```

The SNMP community is linked with the SNMP group `ReadWrite`.

```
localhost# show running-config system management-services snmp vacm
group ReadWrite
system
management-services
snmp
vacm
group ReadWrite
member Sinec-Sec
security-model [ v1 v2c ]
exit

access "" v1 no-auth-no-priv
read-view restricted
exit

access "" v2c no-auth-no-priv
write-view restricted
exit

exit

exit

exit

exit

exit
```

The corresponding access rights are assigned depending on the SNMP version used.

With an SNMPv1 request, read access `read-view` to the view `restricted` is given.

With an SNMPv2c request, write access `write-view` to the view `restricted` is given.

11.6.2 Configuring SNMP

To configure SNMP, do the following:

1. Configure the SNMP agent.
For more information, refer to "Configuring the SNMP agent (Page 485)".
2. If you are using SNMPv1/v2c, configure an SNMP community.
For more information, refer to "Configuring an SNMP community (Page 490)".
3. If you are using SNMPv3, configure an SNMP user.
For more information, refer to "Configuring an SNMP user (Page 494)".
4. Configure the assignment of access rights for an SNMP community or SNMP user.
For more information, refer to "Configuring SNMP access rights (Page 500)".

5. Configure an SNMP target.
For more information, refer to "Configuring an SNMP target (Page 506)".
6. Configure SNMP notifications.
For more information, refer to "Configuring an SNMP notification (Page 512)".

11.6.3 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 485)".
2. [Optional] Configure a server endpoint for SNMP.
For more information, refer to "Configuring a server endpoint for SNMP (Page 487)".
3. Enable a server endpoint for SNMP.
For more information, refer to "Enabling a server endpoint for SNMP (Page 488)".
4. Make sure the SNMP agent is enabled.
For more information, refer to "Enabling the SNMP agent (Page 489)".

11.6.3.1 Configuring the SNMP versions the SNMP agent supports

By default, the SNMP agent supports all SNMP versions.

To configure the SNMP version, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define the SNMP versions the SNMP agent supports. You can enable multiple SNMP versions in one command or disable them with the <code>no</code> form of the command. Default: <code>v1</code> , <code>v2c</code> and <code>v3</code> | <code>system management-services snmp version [v1 v2c v3]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services snmp version</code> |

Example

In this example, SNMPv1 is disabled for the SNMP agent. The SNMP agent does not support SNMP requests via `v1`.

```
localhost# config
Entering configuration mode terminal
localhost(config)# no system management-services snmp version v1
localhost(config)# commit
Commit complete.
localhost(config)# end
```

11.6 SNMP

```
localhost# show running-config system management-services snmp
version
system
management-services
  snmp
    version v2c
    version v3
  exit

exit

exit
```

Example

In this example, SNMPv1 and SNMPv2c are disabled for the SNMP agent. The SNMP agent only supports SNMP requests via v3.

```
localhost# config
Entering configuration mode terminal
localhost(config)# no system management-services snmp version v1 v2c
localhost(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config system management-services snmp
version
system
management-services
  snmp
    version v3
  exit

exit

exit
```

11.6.3.2 Configuring a server endpoint for SNMP

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

| NOTICE |
|---|
| <p>Configuration hazard - risk of connection loss</p> <p>If the device is assigned its IP address dynamically via DHCP, note the following:</p> <p>If the IP address that the device receives via DHCP does not match the IP address that you configured for the SNMP server endpoint, the device cannot be reached via the SNMP server endpoint.</p> <p>You have the following options to prevent connection loss:</p> <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.

To configure a server endpoint, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the local IP address and the port for a server endpoint. Default IP address: 0.0.0.0 The default IP address allows client requests on all local addresses. Default port: 161 | <code>system management-services snmp endpoint default udp ipv4 { IP address } port [161, 4096 - 12344, 12347 - 34963, 34965 - 49151]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services snmp endpoint default</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp endpoint default
udp port 10161 ipv4 192.168.1.1
localhost(config-udp)# commit
Commit complete.
```

11.6 SNMP

```

localhost(config-udp)# end
localhost# show running-config system management-services snmp
endpoint default
system
management-services
snmp
endpoint default
enabled
udp
port 10161
ipv4 192.168.1.1
exit

exit

exit

exit

exit

```

11.6.3.3 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:

| Step | Instruction | Command |
|------|--------------------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the server endpoint for SNMP. | <code>system management-services snmp endpoint default enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services snmp endpoint default enabled</code> |

Example

```

localhost# config
localhost(config)# system management-services snmp endpoint default
enabled
localhost(config-snmp-endpoint-default)# commit
Commit complete.
localhost(config-snmp-endpoint-default)# end
localhost# show running-config system management-services snmp
endpoint default enabled
system
management-services
snmp
endpoint default

```



```

        enabled
    exit

    exit

    exit

    exit

```

11.6.3.4 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:

| Step | Instruction | Command |
|------|---------------------------|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable the SNMP agent. | system management-services snmp enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system management-services snmp enabled |

Example

```

localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp enabled
localhost(config-system-management-services-snmp)# commit
Commit complete.
localhost(config-system-management-services-snmp)# end
localhost# show running-config system management-services snmp
enabled
system
  management-services
    snmp
      enabled
    exit

  exit

exit

```

11.6.4 Configuring an SNMP community

NOTICE

Security hazard - Risk of unauthorized access and/or misuse

The preset community strings are adopted from the SNMP standard and do not provide any protection. To prevent unauthorized access and/or misuse, change the preset community strings to specific values.

To configure an SNMP community, do the following:

1. Define an SNMP community.
For more information, refer to "Defining an SNMP community (Page 490)".
2. [Optional] Define the context which limits an SNMP community access to MIB data.
For more information, refer to "Defining the context in which an SNMP community can access MIB data (Page 492)".
3. [Optional] Link an SNMP community with an SNMP target.
For more information, refer to "Linking an SNMP community with an SNMP target (Page 493)".

11.6.4.1 Defining an SNMP community

By default, the following SNMP communities are configured:

| Community index | Community name (community string) | Security name | Context |
|-----------------|-----------------------------------|---------------|--------------|
| private | private | write | empty string |
| public | public | read | empty string |
| trap | public | trap | empty string |

To configure an SNMP community, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define an SNMP index. Condition: <ul style="list-style-type: none"> • Must be between 1 and 32 characters long | <code>system management-services snmp community { Index }</code> |

| Step | Instruction | Command |
|------|---|--|
| 3 | <p>Assign a name for the SNMP community.</p> <p>The community name corresponds to the community string that a user specifies in an SNMP request via SNMPv1 and v2c.</p> <p>Options include:</p> <ul style="list-style-type: none"> • <code>text-name</code> - The community name as string. • <code>binary-name</code> - The community name in hexadecimal representation with colons as separator. <p>Example: The value "0x123456ABCD" is configured/displayed as follows: 12:34:56:AB:CD.</p> <p>Use this option when the community name contains characters that cannot be displayed.</p> <p>Condition:</p> <ul style="list-style-type: none"> • Must be between 1 and 256 characters long | <pre>[text-name binary-name] { Name }</pre> |
| 4 | <p>Assign a security name for the SNMP community. A community is linked with a group via the security name.</p> <p>Condition:</p> <ul style="list-style-type: none"> • Must be between 1 and 32 characters long | <pre>security-name { Name }</pre> |
| 5 | Commit the changes. | <pre>commit</pre> |
| 6 | Exit configuration mode. | <pre>end</pre> |
| 7 | Verify the configuration. | <pre>show running-config system management-services snmp community { Index }</pre> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp community
v2cTrapIndex
localhost(config-snmp-community-v2cTrapIndex)# text-name publicv2c
localhost(config-snmp-community-v2cTrapIndex)# security-name v2c-Sec
localhost(config-snmp-community-v2cTrapIndex)# commit
Commit complete.
localhost(config-snmp-community-v2cTrapIndex)# end
localhost# show running-config system management-services snmp
community v2cTrapIndex
system
management-services
snmp
community v2cTrapIndex
text-name publicv2c
security-name v2c-Sec
exit
```

```

exit

exit

exit

```

11.6.4.2 Defining the context in which an SNMP community can access MIB data

The context is used together with a group to restrict access to specific areas of the MIB.

By default, an empty string is defined for the context of an SNMP community.

To define the context of an SNMP community, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define the context for an SNMP community. Condition: <ul style="list-style-type: none"> Must be between 0 and 32 characters long | <code>system management-services snmp community { Index } context { Name }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services snmp community { Index } context</code> |

Example

```

localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp community
v2cTrapIndex context public1
localhost(config-snmp-community-v2cTrapIndex)# commit
Commit complete.
localhost(config-snmp-community-v2cTrapIndex)# end
localhost# show running-config system management-services snmp
community v2cTrapIndex context
system
management-services
snmp
community v2cTrapIndex
context public1
exit

exit

exit

exit

```

11.6.4.3 Linking an SNMP community with an SNMP target

An IP address or an IP range is defined in an SNMP target by configuring a prefix length. By linking an SNMP community with an SNMP target, the IP address or the IP range from which SNMP requests to the SNMP agent are permitted, is stored for the corresponding community string. For SNMP requests with the corresponding community string, the SNMP agent checks whether the request comes from the stored permitted IP address or the IP range. If the information matches, the request is processed.

Note

If you want to link an SNMP community with an SNMP target, make sure that at least one SNMP target is defined and the prefix length is defined. For more information on SNMP targets, refer to "Configuring an SNMP target (Page 506)".

To assign an SNMP community with an SNMP target, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Link an SNMP community with an SNMP target. Only valid tags are shown with automatic completion (tab key). A tag is considered valid if the prefix length is defined for the SNMP target entry which uses the tag. | system management-services snmp community { Index } target-tag { Tag } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system management-services snmp community { Index } target-tag |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp community
v2cTrapIndex target-tag v2cTrapTag
localhost(config-snmp-community-v2cTrapIndex)# commit
Commit complete.
localhost(config-snmp-community-v2cTrapIndex)# end
localhost# show running-config system management-services snmp
community v2cTrapIndex target-tag
system
management-services
snmp
community v2cTrapIndex
target-tag v2cTrapTag
exit

exit

exit

exit
```

11.6.5 Configuring an SNMP user

To configure an SNMP user, do the following:

1. Define an SNMP user.
For more information, refer to "Creating an SNMP user (Page 494)".
2. [Optional] Define an authentication password for an SNMP user or specify a localized key.
For more information, refer to "Defining an authentication password for an SNMP user (Page 495)" or "Specifying a localized key for the authentication (Page 496)".
3. [Optional] Define an encryption password for an SNMP user or specify a localized key.
Make sure an authentication password is defined. You cannot only configure the encryption.
For more information, refer to "Defining an encryption password for an SNMP user (Page 497)" or "Specifying a localized key for the encryption (Page 499)".

11.6.5.1 Creating an SNMP user

By default, no SNMP user is configured.

To create an SNMP user, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Create an SNMP user. Condition: <ul style="list-style-type: none"> • Must be between 1 and 32 characters long | <code>system management-services snmp usm local user { Name }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services snmp usm local user { Name }</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp usm local user
User3
localhost(config-user-User3)# commit
Commit complete.
localhost(config-user-User3)# end
localhost# show running-config system management-services snmp usm
local user User3
system
management-services
snmp
usm
local user User3
exit

exit
```

```

exit

exit

exit

```

11.6.5.2 Defining an authentication password for an SNMP user

When you configure an authentication password for an SNMP user, you can configure the corresponding security level for the SNMP user.

SINEC OS supports MD5 or SHA algorithms as authentication method.

A localized key is derived from the entered authentication password and the engine ID of the device.

To configure an authentication password for an SNMP user, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select an algorithm and assign a password for the authentication of an SNMP user. To enter the password encrypted and not in plain text, press Enter after <code>password</code> . This will put you in Wizard mode. | <code>system management-services snmp usm local user { Name } auth [md5 sha] password</code> |
| 3 | Enter the password. Condition: <ul style="list-style-type: none"> Must be between 8 and 255 characters long | <code>{ Password }</code> |
| 4 | Confirm the password. To enter the password encrypted and not in plain text, press Enter after <code>password-confirm</code> . This will put you in Wizard mode. | <code>auth [md5 sha] password- confirm</code> |
| 5 | Enter the password again. | <code>{ Password }</code> |
| 6 | Commit the changes. | <code>commit</code> |
| 7 | Exit configuration mode. | <code>end</code> |
| 8 | Verify the configuration. The localized key is displayed instead of the configured password. | <code>show running-config system management-services snmp usm local user { Name } auth</code> |

Example

```

localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp usm local user
User3 auth md5 password
(<string, min: 8 chars, max: 255 chars>): *****
localhost(config-user-User3)# auth md5 password-confirm
(<string, min: 8 chars, max: 255 chars>): *****
localhost(config-user-User3)# commit
Commit complete.
localhost(config-user-User3)# end

```

11.6 SNMP

```

localhost# show running-config system management-services snmp usm
local user Userv3 auth
system
management-services
snmp
usm
local user Userv3
auth md5 localized-key "$8$tk2ukDr53pMp+..."
exit

exit

exit

exit

exit

```

11.6.5.3 Specifying a localized key for the authentication

To specify a localized key for the authentication for an SNMP user, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Select an algorithm and specify the localized key of an SNMP user for the authentication. You can enter the localized key as follows:</p> <ul style="list-style-type: none"> In hexadecimal representation with colon as separator. Example: 12:34:56:AB:CD As encrypted string beginning with \$8\$. Example: \$8\$tk2ukDr53pMp+... <p>Condition for a hexadecimal representation:</p> <ul style="list-style-type: none"> Must be between 1 and 128 characters long In the hexadecimal representation, 1 character means a two-digit value. Example: 12 <p>Condition for an encrypted string:</p> <ul style="list-style-type: none"> Must be between 1 and 1024 characters long | <pre> system management-services snmp usm local user { Name } priv [aes des] localized-key { Localized key } </pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <pre> show running-config system management-services snmp usm local user { Name } priv </pre> |

Example

```
localhost# config
```



```

Entering configuration mode terminal
localhost(config)# system management-services snmp usm local user
User3 priv aes localized-key 12:34:56:AB:...
localhost(config-user-User3)# commit
Commit complete.
localhost(config-user-User3)# end
localhost# show running-config system management-services snmp usm
local user User3 auth
system
management-services
snmp
usm
local user User3
priv aes localized-key $8$GKqcMw5xhRZ7X...
exit

exit

exit

exit

```

11.6.5.4 Defining an encryption password for an SNMP user

When you configure an encryption password for an SNMP user, you can configure the corresponding security level for the SNMP user.

SINEC OS supports encryption using DES or AES algorithms.

A localized key is derived from the entered encryption password and the engine ID of the device.

To configure an encryption password for an SNMP user, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Select an algorithm and assign a password for the encryption of an SNMP user. To enter the password encrypted and not in plain text, press Enter after password. This will put you in Wizard mode. | system management-services snmp usm local user { Name } priv [aes des] password |
| 3 | Enter the password. Condition: <ul style="list-style-type: none"> Must be between 8 and 255 characters long | { Password } |
| 4 | Confirm the password. To enter the password encrypted and not in plain text, press Enter after password-confirm. This will put you in Wizard mode. | priv [aes des] password- confirm |
| 5 | Enter the password again. | { Password } |

| Step | Instruction | Command |
|------|---|--|
| 6 | Commit the changes. | commit |
| 7 | Exit configuration mode. | end |
| 8 | Verify the configuration. The localized key is displayed instead of the configured password. | show running-config system management-services snmp usm local user { Name } priv |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp usm local user
User3 priv des password
(<string, min: 8 chars, max: 255 chars>): *****
localhost(config-user-User3)# priv des password-confirm
(<string, min: 8 chars, max: 255 chars>): *****
localhost(config-user-User3)# commit
Commit complete.
localhost(config-user-User3)# end
localhost# show running-config system management-services snmp usm
local user User3 priv
system
management-services
snmp
usm
local user User3
priv des localized-key "$8$GYSdllNlnQ2..."
exit

exit

exit

exit

exit
```

11.6.5.5 Specifying a localized key for the encryption

To specify a localized key for the encryption for an SNMP user, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Select an algorithm and specify the localized key of an SNMP user for the encryption.</p> <p>You can enter the localized key as follows:</p> <ul style="list-style-type: none"> In hexadecimal representation with colon as separator. Example: 12:34:56:AB:CD As encrypted string beginning with \$8\$. Example: \$8\$tk2ukDr53pMp+... <p>Condition for a hexadecimal representation:</p> <ul style="list-style-type: none"> Must be between 1 and 128 characters long In the hexadecimal representation, 1 character means a two-digit value. Example: 12 <p>Condition for an encrypted string:</p> <ul style="list-style-type: none"> Must be between 1 and 1024 characters long | <pre>system management-services snmp usm local user { Name } auth [md5 sha] localized-key { Localized key }</pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <pre>show running-config system management-services snmp usm local user { Name } auth</pre> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp usm local user
User3 auth md5 localized-key $8$tk2ukDr53pMp+...
localhost(config-user-User3)# commit
Commit complete.
localhost(config-user-User3)# end
localhost# show running-config system management-services snmp usm
local user User3 auth
system
management-services
snmp
usm
local user User3
auth md5 localized-key "$8$tk2ukDr53pMp+..."
exit

exit

exit
```

```
exit
```

```
exit
```

11.6.6 Configuring SNMP access rights

To configure SNMP access rights using the View-based Access Control Model (VACM), do the following:

1. Define an SNMP view.
For more information, refer to "Defining an SNMP view (Page 500)".
2. Configure an SNMP group with access rights to MIB areas.
For more information, refer to "Defining an SNMP group with access rights to MIB areas (views) (Page 502)".
3. Link an SNMPv1/v2c community or an SNMPv3 user with an SNMP group via the security name.
For more information, refer to "Assigning a security name with an SNMP group (Page 504)".

11.6.6.1 Defining an SNMP view

An SNMP view defines which parts of the MIB are accessible.

By default, the following SNMP views are configured:

| View name | View type | OID |
|------------|-----------|---|
| iso | include | 1.* |
| restricted | include | 1.* 1.3.6.1.6.3.18.1.1.1.*.112.117.98.108.105.99 |
| | exclude | 1.3.6.1.6.3.18.1 |

Note

An SNMP view of the type `include` cannot contain the same OIDs that are already contained in an SNMP view of the type `exclude`.

To configure an SNMP view, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define an SNMP view name. Condition: <ul style="list-style-type: none"> • Must be between 1 and 32 characters long | <code>system management-services snmp vacm view { Name }</code> |

| Step | Instruction | Command |
|------|--|---|
| 3 | <p>Define which parts of the MIB are accessible with this view and which are excluded from access.</p> <p>Options include:</p> <ul style="list-style-type: none"> <code>exclude</code> - Use this parameter to exclude the following part of the MIB from access. <code>include</code> - Use this parameter to make the following part of the MIB accessible. <p>Enter the MIB areas as a chain of numbers (OID):</p> <ul style="list-style-type: none"> Each number defines a specific sub-tree. Replace a number of the OID with * (wild-card) to define a group of sub-trees. | <code>[exclude include] { OID }</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config system management-services snmp vacm view { Name }</code> |

Example

In this example, access to an MIB object is made possible.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp vacm view
readview
localhost(config-view-readview)# include 1.3.6.1.2.1.1.5
localhost(config-view-readview)# commit
Commit complete.
localhost(config-view-readview)# end
localhost# show running-config system management-services snmp vacm
view readview
system
management-services
snmp
vacm
view readview
include [ 1.3.6.1.2.1.1.5 ]
exit

exit

exit

exit
```

In this example, access to an MIB object is excluded.

11.6 SNMP

```

localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp vacm view
writeview
localhost(config-view-writeview)# exclude 1.3.6.1.2.1.1.4
localhost(config-view-writeview)# commit
Commit complete.
localhost(config-view-writeview)# end
localhost# show running-config system management-services snmp vacm
view writeview
system
management-services
snmp
vacm
view writeview
exclude [ 1.3.6.1.2.1.1.4 ]
exit

exit

exit

exit

exit

```

11.6.6.2 Defining an SNMP group with access rights to MIB areas (views)

An SNMP group defines which information a member of the group needs to provide in an SNMP request to access a part of the MIB (view).

By default, the following SNMP groups are configured:

| Group name | Context | Security model | Security level | Type of access | View | Member |
|------------|--------------|----------------|-----------------|--------------------------|------------|--------|
| read | empty string | v1 | no-auth-no-priv | read-view | restricted | read |
| | empty string | v2c | no-auth-no-priv | read-view | restricted | read |
| trap | empty string | v1 | no-auth-no-priv | notify-view | restricted | trap |
| | empty string | v2c | no-auth-no-priv | notify-view | restricted | trap |
| write | empty string | v1 | no-auth-no-priv | read-view, write-view | iso | write |
| | empty string | v2c | no-auth-no-priv | read-view, write-view | iso | write |

To configure an SNMP group with access rights to parts of the MIB, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define a new group. Condition: <ul style="list-style-type: none"> Must be between 1 and 32 characters long | <code>system management-services snmp vacm group { Name }</code> |

| Step | Instruction | Command |
|------|--|--|
| 3 | <p>Define the access rights of an SNMP group. The access rights are composed of the context, the security model and the security level.</p> <p>Define the context in which the access rights are valid.</p> <p>Possible options for the security model:</p> <ul style="list-style-type: none"> • <code>any</code> - The access rights are independent of the security model. • <code>usm</code> - The access rights apply only to members with the security model <code>usm</code>. • <code>v1</code> - The access rights apply only to members with the security model <code>v1</code>. • <code>v2c</code> - The access rights apply only to members with the security model <code>v2c</code>. <p>Possible options for the security level:</p> <ul style="list-style-type: none"> • <code>auth-no-priv</code> - The password for authentication must be provided with an SNMP request. • <code>auth-priv</code> - The passwords for authentication and encryption must be provided with an SNMP request. • <code>no-auth-no-priv</code> - No passwords need to be entered. | <pre>access { context } [any usm v1 v2c] [auth-no-priv auth- priv no-auth-no-priv]</pre> |
| | <p>Define the type of access of the group to a part of the MIB (view).</p> <p>Options include:</p> <ul style="list-style-type: none"> • <code>notify-view</code> - Notifications can be sent for the specified view. • <code>read-view</code> - Group members are granted read access to the specified view. • <code>write-view</code> - Group members are granted write access to the specified view. | <pre>[notify-view read-view write- view] { Name }</pre> |
| | <p>[Optional] Define how precisely the transmitted context needs to match the configured context.</p> <p>Options include:</p> <ul style="list-style-type: none"> • <code>exact</code> - The context transmitted by the SNMP manager needs to match the configured context exactly. • <code>prefix</code> - It is sufficient if the context transmitted by the SNMP manager partially matches the configured context. The transmitted context must be a prefix of the configured context. <p>Default: <code>exact</code></p> | <pre>context-match [exact prefix]</pre> |
| 4 | Commit the changes. | <code>commit</code> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config system management-services snmp vacm group { Name } |

Example

In this example, the SNMP group **GroupWv3** is linked with the context **public1**. The group has write access to the **writeview** view. The view grants access to the MIB object 1.3.6.1.2.1.1.5.

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp vacm group
GroupWv3
localhost(config-group-GroupWv3)# access public1 usm auth-priv
localhost(config-access-public1/usm/auth-priv)# write-view writeview
localhost(config-access-public1/usm/auth-priv)# commit
Commit complete.
localhost(config-access-public1/usm/auth-priv)# end
localhost# show running-config system management-services snmp vacm
group GroupWv3
system
management-services
snmp
vacm
group GroupWv3
access public1 usm auth-priv
write-view writeview
exit

exit

exit

exit

exit

exit
```

11.6.6.3 Assigning a security name with an SNMP group

SNMPv1/v2c communities or SNMPv3 users are linked with SNMP views via an SNMP group. Make sure at least one SNMP community or one SNMP user is configured.

By default, the following communities are linked with the preconfigured SNMP groups:

| Group name | Community | Security model |
|------------|-----------|----------------|
| read | read | v1, v2c |
| trap | trap | v1, v2c |
| write | write | v1, v2c |

To link a security name with a group, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Link a security name with a group. With SNMPv3 users, the security name corresponds to the user name. | <code>system management-services snmp vacm group { Name } member { Security name }</code> |
| 3 | Define the security model via which the user can have access. Options include: <ul style="list-style-type: none"> <code>usm</code> - The user is assigned to the group when the user sends SNMPv3 requests to the agent. <code>v1</code> - The user is assigned to the group when the user sends SNMPv1 requests to the agent. <code>v2c</code> - The user is assigned to the group when the user sends SNMPv2c requests to the agent. | <code>security-model [usm v1 v2c]</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config system management-services snmp vacm group { Name } member</code> |

Example

In this example, the SNMP group `GroupWv3` is linked with the SNMP user `UserV3`.

The access rights of the group have already been defined. For more information, refer to "Defining an SNMP group with access rights to MIB areas (views) (Page 502)".

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp vacm group
GroupWv3 member UserV3
localhost(config-member-UserV3)# security-model usm
localhost(config-member-UserV3)# commit
Commit complete.
localhost(config-member-UserV3)# end
localhost# show running-config system management-services snmp vacm
group GroupWv3 member
system
management-services
snmp
```

11.6 SNMP

```

vacm
  group GroupWv3
    member Userv3
      security-model [ usm ]
    exit
  exit
exit
exit
exit
exit
exit
exit

```

11.6.7 Configuring an SNMP target

To configure an SNMP target, do the following:

1. Make sure at least one SNMP community or one SNMP user is defined.
For more information, refer to "Configuring an SNMP community (Page 490)" and "Configuring an SNMP user (Page 494)".
2. Define a parameter set for SNMP targets.
For more information, refer to "Configuring parameters for SNMPv1/v2c targets (Page 506)" and "Configuring parameters for SNMPv3 targets (Page 508)".
3. Define an SNMP target.
For more information, refer to "Defining an SNMP target (Page 509)".
4. [Optional] Change the port on which the SNMP agent sends notifications for an SNMP target.
For more information, refer to "Changing the port for receiving SNMP notifications (Page 511)".

11.6.7.1 Configuring parameters for SNMPv1/v2c targets

SNMP target parameters are used to define an SNMP target more precisely. You can use an SNMP target parameter for one or multiple SNMP targets.

The following entry is configured by default:

| SNMP target parameters | Security model | Security name |
|------------------------|----------------|---------------|
| SNMPv1Param | v1 | trap |

To configure parameters for SNMPv1 and SNMPv2c targets, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define a name for the SNMP target parameters. Condition: <ul style="list-style-type: none"> • Must be between 1 and 255 characters long | <code>system management-services snmp target-params { Name }</code> |
| 3 | Define the security model and specify the security name of the SNMP community to be used for sending notifications. Options include: <ul style="list-style-type: none"> • <code>v1</code> - Sending notifications is possible only via SNMPv1. • <code>v2c</code> - Sending notifications is possible only via SNMPv2c. | <code>[v1 v2c] security-name { Name }</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config system management-services snmp target-params { Name }</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp target-params
SNMPv2cParam
localhost(config-snmp-target-params-SNMPv2cParam)# v2c security-
name trap
localhost(config-snmp-target-params-SNMPv2cParam)# commit
Commit complete.
localhost(config-snmp-target-params-SNMPv2cParam)# end
localhost# show running-config system management-services snmp
target-params SNMPv2cParam
system
 management-services
  snmp
    target-params SNMPv2cParam
      v2c security-name trap
    exit
  exit
exit
exit
exit
```

11.6.7.2 Configuring parameters for SNMPv3 targets

SNMP target parameters are used to define an SNMP target more precisely. You can use SNMP target parameters for one or multiple SNMP targets.

To configure parameters for SNMPv3 targets, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define a name for the SNMP target parameters. Condition: <ul style="list-style-type: none"> • Must be between 1 and 255 characters long | <code>system management-services snmp target-params { Name }</code> |
| 3 | Define the security model and specify the user name of the SNMP user to be used for sending notifications. When sending notifications, the SNMP agent needs to authenticate itself with the recipient of the notifications (target). Define the security level with which an SNMP agent needs to log in to be able to send notifications. Options include: <ul style="list-style-type: none"> • <code>auth-no-priv</code> - The password for authentication must be provided with a notification. • <code>auth-priv</code> - The passwords for authentication and encryption must be provided with a notification. • <code>no-auth-no-priv</code> - No passwords need to be entered. The passwords for authentication and encryption are defined during configuration of the SNMP user. | <code>usm user-name { Name } security-level [auth-no-priv auth-priv no-auth-no-priv]</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config system management-services snmp target-params { Name }</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp target-params
SNMPv3Param
localhost(config-snmp-target-params-SNMPv3Param) # usm user-name
UserV3 security-level auth-priv
localhost(config-snmp-target-params-SNMPv3Param) # commit
Commit complete.
localhost(config-snmp-target-params-SNMPv3Param) # end
```

```

localhost# show running-config system management-services snmp
target-params SNMPv3Param
system
management-services
snmp
target-params SNMPv3Param
usm user-name Userv3
usm security-level auth-priv
exit

exit

exit

exit

```

11.6.7.3 Defining an SNMP target

An SNMP target describes the recipient of an SNMP message as well as additional parameters.

The IP address of the recipient for notification is configured via the SNMP target.

When you use an SNMP target to limit the number of SNMP managers that can access an SNMP agent with a community string, you must define the prefix length.

When an SNMP agent receives an SNMP message with a known community string with which an SNMP target is linked, the agent checks whether the IP address of the sender matches a configured IP address. Only if the IP address is configured in the linked SNMP target does the sender get access.

The following entry is configured by default:

| SNMP target | IP address | Port | Target tag | SNMP target parameters |
|--------------|------------|------|------------|------------------------|
| SIMATICNET01 | 127.0.0.1 | 162 | SIMATICNET | SNMPv1Param |

To configure an SNMP target, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define an SNMP target. Condition: <ul style="list-style-type: none"> Must be between 1 and 32 characters long | <code>system management-services snmp target { Name }</code> |
| 3 | Define the IP address and the prefix length of the target. If you do not specify a prefix length, the device uses the value 32 for outgoing messages. The prefix length is currently only used by the community-based security model to filter incoming SNMP messages. | <code>udp ipv4 { IP address } prefix- length { 0 - 32 }</code> |

| Step | Instruction | Command |
|------|---|---|
| 4 | Define a tag to select SNMP targets. Use the tag to link the SNMP target with an SNMP community or an SNMP notification. Condition: <ul style="list-style-type: none"> Must be between 1 and 255 characters long | tag { Tag } |
| 5 | Assign an existing target parameter to the SNMP target. | target-params { Name } |
| 6 | Commit the changes. | commit |
| 7 | Exit configuration mode. | end |
| 8 | Verify the configuration. | show running-config system management-services snmp target { Name } |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp target v2cTrap
localhost(config-snmp-target-v2cTrap)# udp ipv4 192.0.2.2 prefix-
length 32
localhost(config-snmp-target-v2cTrap)# tag v2cTrapTag
localhost(config-snmp-target-v2cTrap)# target-params SNMPv2cParam
localhost(config-snmp-target-v2cTrap)# commit
Commit complete.
localhost(config-snmp-target-v2cTrap)# end
localhost# show running-config system management-services snmp
target v2cTrap
system
management-services
snmp
target v2cTrap
udp ipv4 192.0.2.2
udp prefix-length 32
tag          [ v2cTrapTag ]
target-params SNMPv2cParam
exit

exit

exit

exit
```

11.6.7.4 Changing the port for receiving SNMP notifications

To change the port which the SNMP agent sends SNMP notifications to, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Change the SNMP port for notifications for an SNMP target. Default: 162 | <code>system management-services snmp target { Name } udp port { 1 - 65535 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system management-services snmp target { Name } udp port</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp target v2cTrap
udp port 10162
localhost(config-snmp-target-v2cTrap)# commit
Commit complete.
localhost(config-snmp-target-v2cTrap)# end
localhost# show running-config system management-services snmp
target v2cTrap udp port
system
management-services
snmp
target v2cTrap
udp port 10162
exit

exit

exit

exit
```

11.6.8 Configuring an SNMP notification

A notification can be sent for the following events:

- **Cold or warm restart**
 - After a device restart that was triggered by pulling and plugging the power supply
 - After a device restart that was triggered by running the corresponding CLI command or via the Web UI
- **Link up or link down**
 - If a connection to another device is established or interrupted
 - If an interface (logical or physical) is enabled or disabled
- **SNMP authentication failure**

If, for example, an SNMP manager attempts to access an SNMP agent with the incorrect access authorization using SNMP requests

To configure an SNMP notification, do the following:

1. Make sure that at least one SNMP target is defined.
For more information, refer to "Configuring an SNMP target (Page 506)".
2. Define an SNMP notification.
For more information, refer to "Configuring an SNMP notification (Page 512)".
3. [Optional] Enable SNMP notifications for link-up and link-down events for bridge ports.
By default, link-up and link-down notifications are disabled at all bridge ports.
For more information, refer to "Enabling link up/down traps (Page 287)".
4. [Optional] Enable SNMP notifications for link-up and link-down events for VLAN interfaces.
By default, link-up and link-down notifications are disabled at all VLAN interfaces.
For more information, refer to "Enabling link up/down traps (Page 292)".
5. [Optional] Enable SNMP notifications for selected alarms.
For more information, refer to "Enabling an event to trigger an SNMP trap (Page 655)".

11.6.8.1 Configuring an SNMP notification

By default, the SNMP notification `SNMPv1Traps` is configured with the following settings:

```
tag SIMATICNET
```

To configure an SNMP notification, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure an SNMP notification. Condition: <ul style="list-style-type: none"> • Must be between 1 and 32 characters long | <code>system management-services snmp notify { Name }</code> |
| 3 | Specify an existing target tag for the SNMP notification. | <code>tag { Tag }</code> |
| 4 | Commit the changes. | <code>commit</code> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config system management-services snmp notify { Name } |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system management-services snmp notify
SNMPv2cTraps
localhost(config-snmp-notify-SNMPv2cTraps)# tag v2cTrapTag
localhost(config-snmp-notify-SNMPv2cTraps)# commit
Commit complete.
localhost(config-snmp-notify-SNMPv2cTraps)# end
localhost# show running-config system management-services snmp
notify SNMPv2cTraps
system
management-services
snmp
notify SNMPv2cTrap
tag v2cTrapTag
exit

exit

exit

exit
```

11.6.9 Monitoring SNMP

This section describes the various ways in which you can monitor SNMP.

11.6.9.1 Displaying the engine ID

To show the engine ID of the device, execute the following command in operational mode:

```
show system management-services snmp engine-id
```

Example

```
localhost# show system management-services snmp engine-id
engine-id 80:00:10:e9:03:20:87:56:8c:94:09
```


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 516)"

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 516)".
2. Select the type of frames to limit. For more information, refer to "Selecting the type of frames to limit (Page 518)".
3. Select the rate of control. For more information, refer to "Selecting the rate limit (Page 519)".
4. Enable rate limiting. For more information, refer to "Enabling rate limiting (Page 520)".

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, execute the following command in operational mode:

```
show interface { bridge port } ethernet rate-control [ ingress | egress ] capabilities
```

Example

The following displays the egress capabilities for `ethernet0/1`.

```
localhost# show interface ethernet0/1 ethernet rate-control egress capabilities
```

```
rate-control egress capabilities traffic-type-capability all
rate-control egress capabilities rate-type-capability kbps
rate-control egress capabilities kbps-rate-min 64
rate-control egress capabilities kbps-rate-max 256000
```

Example

The following displays the ingress capabilities for ethernet0/1.

```
localhost# show interface ethernet0/1 ethernet rate-control ingress
capabilities

rate-control ingress capabilities traffic-type-capability
all,broadcast,multicast,unknown-unicast,mcast-and-unknown-ucast,bcast-and-
unknown
ucast,bcast-and-mcast,bcast-and-mcast-and-unknown-ucast
rate-control ingress capabilities rate-type-capability kbps
rate-control ingress capabilities kbps-rate-min 64
rate-control ingress capabilities kbps-rate-max 256000
```

Description

| Parameter | Description |
|-------------------------|--|
| traffic-type-capability | The type of traffic supported by the bridge port on ingress/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 |
| rate-type-capability | The data transfer speed for ingress/egress rate limits. Default: kbps |
| kbps-rate-min | The minimum ingress/egress rate in kilobits-per-second (kbps). |
| kbps-rate-max | The maximum ingress/egress rate in kilobits-per-second (kbps). |

12.1 Rate limiting

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:

| Step | Instruction | Command |
|------|---|---|
| 1 | <p>[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).</p> <p>For example, if the traffic type capability for an interface is <code>all</code> for egress traffic, the rate cannot be limited on egress based on the traffic type.</p> <p>For more information, refer to "Determining interface capabilities (Page 516)".</p> | <pre>show interface { bridge port } ethernet rate-control [ingress egress] capabilities traffic- type-capability</pre> |
| 2 | Enter configuration mode. | <code>config</code> |
| 3 | <p>For the selected bridge port and traffic direction, select the type of traffic that should be rate limited.</p> <p>Options include:</p> <ul style="list-style-type: none"> <code>all</code> - Rate limiting is applied to all traffic <code>broadcast</code> - Rate limiting is applied to only broadcast traffic <code>unknown-unicast</code> - Rate limiting is applied to only unknown unicast traffic <p>Default: <code>all</code></p> <p>Note the following options are available as well, but are not supported in this release:</p> <ul style="list-style-type: none"> <code>bcast-and-mcast</code> - Rate limiting is applied to both broadcast and multicast traffic <code>bcast-and-mcast-and-unknown-ucast</code> - Rate limiting is applied to broadcast, multicast, and unknown unicast traffic <code>bcast-and-unknown-ucast</code> - Rate limiting is applied to both broadcast and unknown unicast traffic <code>mcast-and-unknown-ucast</code> - Rate limiting is applied to both multicast and unknown unicast traffic <code>multicast</code> - Rate limiting is applied to only multicast and unknown multicast traffic <code>unicast</code> - Rate limiting is applied to only unicast and unknown unicast traffic <code>unknown-multicast</code> - Rate limiting is applied to only unknown multicast traffic | <pre>interface { bridge port } ethernet rate-control [ingress egress] traffic-type [all bcast-and-mcast bcast-and- mcast-and-unknown-ucast bcast- and-unknown-ucast broadcast mcast-and-unknown-ucast multicast unicast unknown- multicast unknown-unicast]</pre> |
| 4 | Commit the change. | <code>commit</code> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config interface { bridge port } ethernet rate-control [ingress egress] traffic-type |

Example

The following applies rate limiting to only broadcast traffic forwarded on ethernet0/1.

```
localhost# config
localhost(config)# interface ethernet0/1 ethernet rate-control ingress
traffic-type broadcast
localhost(config-inteface-ethernet0/1)# commit
Commit complete.
localhost(config-inteface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 ethernet rate-control
ingress traffic-type
interface ethernet0/1
 ethernet
  rate-control ingress traffic-type broadcast
exit

exit
```

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | [Optional] Check the capabilities of the selected bridge port to determine the speed range supported by the port in the chosen direction. 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 516)". | show interface { bridge port } ethernet rate-control [ingress egress] capabilities kbps-rate-min show interface { bridge port } ethernet rate-control [ingress egress] capabilities kbps-rate-max |
| 2 | Enter configuration mode. | config |
| 3 | Select the rate of control in kilobits-per-second (kbps) for the selected bridge port and traffic direction. The rate can be set separately for egress and ingress traffic. Default: 0 | interface { bridge port } ethernet rate-control [ingress egress] rate { Limit } |
| 4 | Commit the change. | commit |
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config interface { bridge port } ethernet rate-control [ingress egress] rate |

12.1 Rate limiting

Example

The following limits the ingress traffic rate on ethernet0/1 to 1000 kbps.

```
localhost# config
localhost(config)# interface ethernet0/1 ethernet rate-control ingress rate
1000
localhost(config-inteface-ethernet0/1)# commit
Commit complete.
localhost(config-inteface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 ethernet rate-control
ingress rate
interface ethernet0/1
    ethernet
        rate-control ingress rate 1000
    exit

exit
```

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.

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable rate limiting for the selected bridge port and traffic direction. | interface { bridge port } ethernet rate-control [ingress egress] enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } ethernet rate- control |

Example

In this example, rate limiting is enabled on ingress traffic for ethernet0/1.

```
localhost# config
localhost(config)# interface ethernet0/1 ethernet rate-control ingress
enabled
localhost(config-inteface-ethernet0/1)# commit
Commit complete.
localhost(config-inteface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 ethernet rate-control
interface ethernet0/1
  ethernet
    rate-control ingress enabled
  exit
exit
```

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

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 519)".
2. Enable rate limiting for the egress traffic on ethernet0/1.
For more information, refer to "Enabling rate limiting (Page 520)".

12.2 VLANs

This section describes the configuration and successful deployment of VLANs on Layer 2 networks to virtually bridge different LAN segments together.

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 542)".

The following illustrates how traffic emanating from different LAN segments can be logically grouped into VLANs.

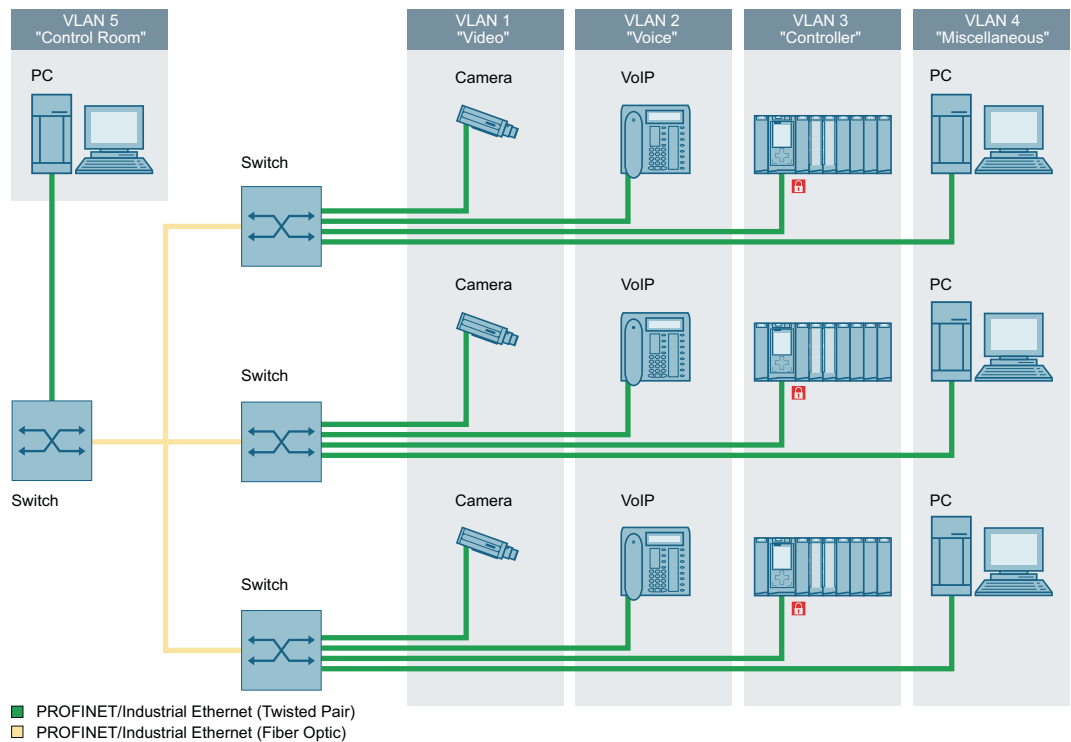


Figure 12-2 Separation of traffic using multiple VLANs

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 529)".

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 534)".

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 535)".

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 538)".

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.

GVRP PDUs

To use GVRP, GVRP needs to be enabled on one or more interfaces. These interfaces will then broadcast Protocol Data Units (PDUs). GVRP PDUs advertise all the VLANs known to the device (configured statically or learned dynamically through GVRP) to the rest of the network.

When a GVRP-enabled device receives a GVRP PDU advertising a set of VLANs, all trunk interfaces become members of those advertised VLANs. The device then begins advertising those VLANs through all the GVRP-enabled interfaces (other than the interface on which the VLANs were learned).

For information about how to enable GVRP, refer to "Enabling GVRP (Page 532)".

Declare vs. Declare and Register

To improve network security, GVRP-enabled interfaces may be configured to only advertise (declare) the VLANs configured for the device. Those interfaces are not permitted to learn (register) about new VLANs.

For information about how to set the GVRP mode for a switch interface, refer to "Selecting the GVRP mode (Page 536)".

A Sample GVRP Topology

In the following example, a core switch is connected to three edge switches. The edge switches are further connected to other hosts.

GVRP is enabled on all devices and hosts outside the topology are configured to advertise their VLANs to the edge switches. The edge switches then learn the advertised VLANs and advertise them to the core switch.

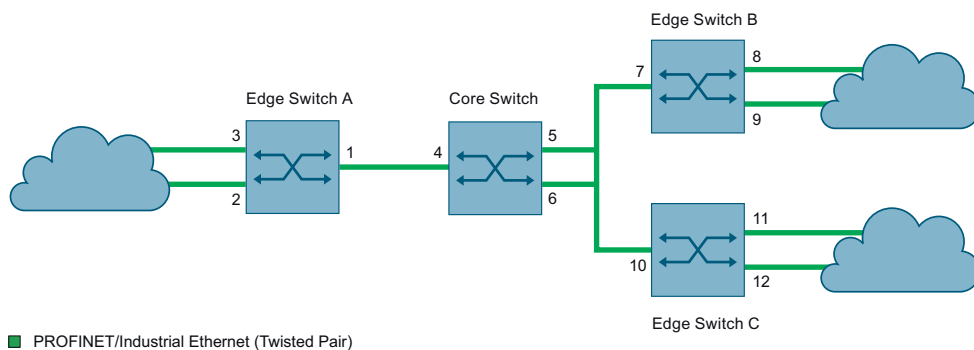


Figure 12-5 A Sample GVRP Application

This configuration does not require static VLANs be configured for the core and edge switches. All VLANs are advertised and learned automatically through GVRP.

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

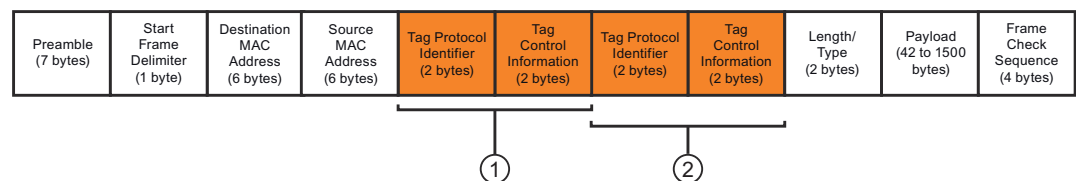
Enable ingress filtering when using forbidden VLAN lists. Forbidden VLAN lists only prevent bridge port's from joining specific VLANs. They do not prevent a frame associated with a VLAN on the list from being forwarded to another port that is a member of that VLAN.

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 12-6 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.
For more information, refer to "Adding or modifying a static VLAN (Page 531)" or "Enabling GVRP (Page 532)".

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 289)".
3. [Optional] Enable VLAN-0-Tunnel mode.
For more information, refer to "Enabling VLAN-0-Tunnel mode (Page 533)".
4. Configure the VLAN settings for one or more bridge ports.
For more information, refer to "Configuring VLAN settings for bridge ports (Page 534)".

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 315)".

| Step | Instruction | Command |
|------|--|---------------------------------------|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enter a new VLAN ID or an existing ID to modify a VLAN. The CLI is now in VLAN configuration mode. | <code>switch vlan { 1 - 4094 }</code> |
| 3 | [Optional] Enter a name for the VLAN. Conditions: <ul style="list-style-type: none"> • Can 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. | <code>name { name }</code> |
| 4 | Commit the changes. | <code>commit</code> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config switch vlan { 1 - 4094 } |

Example

The following assigns the name subst10 to VLAN 10.

```
localhost# config
localhost(config)# switch vlan 10
localhost(config-vlan-10)# name subst10
localhost(config-vlan-10)# commit
Commit complete.
localhost(config-vlan-10)# end
localhost# show running-config switch vlan 10
switch
  vlan 10
    name subst10
  exit
exit
```

12.2.2.2 Enabling GVRP

By default, the GVRP service is disabled globally. It must first be enabled before individual bridge ports can use GVRP to distribute their VLAN configuration information to other devices on the network.

To enable the GVRP service globally, do the following:

| Step | Instruction | Command |
|------|---------------------------|---------------------------|
| 1 | Enter configuration mode. | config |
| 2 | Enable the GVRP service. | switch gvrp |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show switch device-config |

Once enabled, the GVRP mode can be configured for one or more bridge ports. For more information, refer to "Selecting the GVRP mode (Page 536)".

Example

```
localhost# config
localhost(config)# switch gvrp
localhost(config-gvrp)# commit
Commit complete.
localhost(config-gvrp)# end
localhost# show switch device-config
General vlan device configuration
  GVRP status                               enabled
  Traffic classes weighting                 strict
  Max supported vlan                        255
```

12.2.2.3 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 529)".

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable VLAN-0-Tunnel mode for the selected VLAN. | <code>switch vlan { 1 - 4094 } vlan-0-tunnel</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch vlan { 1 - 4094 }</code> |

Example

The following enables VLAN-0-Tunnel mode for VLAN 10.

```
localhost# config
localhost(config)# switch vlan 10 vlan-0-tunnel
localhost(config-vlan-10)# commit
Commit complete.
localhost(config-vlan-10)# end
localhost# show running-config switch vlan 10
switch
  vlan 10
    name          vlan10
    vlan-0-tunnel
    msti          2
  exit
exit
```

12.2.3 Configuring VLAN settings for bridge ports

To configure the VLAN settings for a bridge port, do the following:

1. Configure the bridge port as an access or trunk interface.
For more information, refer to "Selecting the port membership type (Page 534)".
2. [Optional] Configure 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 535)".
3. [Optional] If GVRP is enabled, select the GVRP mode for the bridge port.
For more information, refer to "Selecting the GVRP mode (Page 536)".
4. [Optional] Enable PVID tagging for traffic egressing the bridge port.
For more information, refer to "Enabling PVID tagging on egress traffic (Page 537)".
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 535)".
 - To filter frames based on their VID, enable ingress filtering.
For more information, refer to "Enabling ingress filtering (Page 538)".
6. [Optional] For trunk-type bridge ports only, define the forbidden VLANs list.
For more information, refer to "Restricting VLAN membership (Page 539)".

12.2.3.1 Selecting the port membership type

To select the port membership type for a bridge port, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | 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. | <code>interface { bridge port } vlan trunk gvrp-mode disable</code> <code>no interface { bridge port } vlan trunk forbidden-vlans</code> |
| 3 | Select the port membership type for the selected bridge port. Options include: <ul style="list-style-type: none"> • <code>access</code> - The bridge port only carries traffic on the native VLAN • <code>trunk</code> - The bridge port carries traffic for all VLANs Default: <code>access</code> | <code>interface { bridge port } vlan type [access trunk]</code> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show interface { bridge port } vlan type</code> |

Example

The following converts ethernet0/1 to a trunk port.

```
localhost# config
localhost(config)# interface ethernet0/1 vlan type trunk
localhost(config-vlan)# commit
Commit complete.
localhost(config-vlan)# end
localhost# show interface ethernet0/1 vlan type
vlan type trunk
```

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Configure the port VLAN ID for the selected interface. | interface { bridge port } vlan pvid { 1 - 4094 } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show interface { bridge port } vlan pvid |

Example

The following sets the port VLAN ID for ethernet0/1 to 10.

```
localhost# config
localhost(config)# interface ethernet0/1 vlan pvid 10
localhost(config-vlan)# commit
Commit complete.
localhost(config-vlan)# end
localhost# show interface ethernet0/1 vlan pvid
vlan pvid 10
```

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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select the frame type accepted by the selected bridge port. Options include: <ul style="list-style-type: none"> • <code>admit-all-frames</code> - Both tagged and untagged ingress frames are accepted • <code>admit-only-untagged-and-priority-tagged</code> - Only untagged ingress frames or frames that have a priority tag are accepted • <code>admit-only-VLAN-tagged-frames</code> - Only VLAN ingress tagged frames are accepted Default: <code>admit-all-frames</code> | <code>interface { bridge port } vlan acceptable-frame [admit-all-frames admit-only-VLAN-tagged-frames admit-only-untagged-and-priority-tagged]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show interface { bridge port } vlan acceptable-frame</code> |

Example

The following sets `ethernet0/1` to only accept VLAN tagged frames.

```
localhost# config
localhost(config)# interface ethernet0/1 vlan acceptable-frame admit-only-
VLAN-tagged-frames
localhost(config-vlan)# commit
Commit complete.
localhost(config-vlan)# end
localhost# show interface ethernet0/1 vlan acceptable-frame
vlan acceptable-frame admit-only-VLAN-tagged-frames
```

12.2.3.4 Selecting the GVRP mode

GVRP can be set to a different mode for individual bridge ports.

To select the GVRP mode for a bridge port, do the following:

Note

The GVRP mode only applies when GVRP is enabled globally. For more information, refer to "Enabling GVRP (Page 532)".

Note

The selected bridge port must be defined as a trunk.

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select the GVRP mode for the selected bridge port. Options include: <ul style="list-style-type: none"> <code>disabled</code> - GVRP is disabled on the bridge port <code>declare-only</code> - All VLANs (configured or learned) are declared, but new VLANs are not registered <code>declare-and-register</code> - All VLANs are declared and new VLANs are registered dynamically Default: <code>disabled</code> | <code>interface { bridge port } vlan trunk gvrp-mode [disable declare-only declare-and-register]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show interface { bridge port } vlan gvrp-mode</code> |

Example

The following sets the GVRP mode for ethernet0/1 to `declare-and-register`.

```
localhost# config
localhost(config)# interface ethernet0/1 vlan trunk gvrp-mode declare-and-register
localhost(config-vlan)# commit
Commit complete.
localhost(config-vlan)# end
localhost# show interface ethernet0/1 vlan gvrp-mode
vlan-gvrp-mode declare-and-register
```

12.2.3.5 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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable PVID tagging for the selected bridge port. | <code>interface { bridge port } vlan pvid-egress-tag</code> |

12.2 VLANs

| Step | Instruction | Command |
|------|---------------------------|--|
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show interface { bridge port } vlan pvid-egress-tag |

Example

The following enables PVID tagging for ethernet0/1.

```
localhost# config
localhost(config)# interface ethernet0/1 vlan pvid-egress-tag
localhost(config-vlan)# commit
Commit complete.
localhost(config-vlan)# end
localhost# show ethernet0/1 vlan pvid-egress-tag
vlan pvid-egress-tag
```

12.2.3.6 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.

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable ingress filtering for the selected bridge port. | interface { bridge port } vlan ingress-filtering |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show interface { bridge port } vlan ingress-filtering |

Example

The following enables ingress filtering for ethernet0/1.

```
localhost# config
localhost(config)# interface ethernet0/1 vlan ingress-filtering
localhost(config-vlan)# commit
Commit complete.
localhost(config-vlan)# end
localhost# show interface ethernet0/1 vlan ingress-filtering
vlan ingress-filtering
```

12.2.3.7 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 538)".

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Specify which VLAN(s) the selected bridge port is restricted from joining. Multiple VLANs can be expressed as a comma-separated list, a range, or a combination of both. | <code>interface { bridge port } vlan trunk forbidden-vlans { 1 - 4094 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show interface { bridge port } vlan forbidden-vlans</code> |

Example

The following defines the list of forbidden VLANs for `ethernet0/1`.

```
localhost# config
localhost(config)# interface ethernet0/1 vlan trunk forbidden-vlans
10,12,14,16-20
localhost(config-vlan)# commit
Commit complete.
localhost(config-vlan)# end
localhost# show interface ethernet0/1 vlan forbidden-vlans
vlan forbidden-vlans 10,12,14,16-20
```

12.2.4 Monitoring VLANs

This section describes the various methods for monitoring the status of static and dynamically-learned VLANs.

12.2.4.1 Displaying dynamically-learned VLANs

Various commands can be executed in operational mode to display information about dynamically-learned VLANs.

| Command | Description |
|--|---|
| <code>show switch dynamic-vlan</code> | Displays all dynamically-learned VLANs. |
| <code>show switch dynamic-vlan egress-ports</code> | Displays the egress ports associated with each dynamically-learned VLAN. |
| <code>show switch dynamic-vlan untagged-ports</code> | Displays the untagged ports associated with each dynamically-learned VLAN. |
| <code>show switch dynamic-vlan { VLAN ID }</code> | Displays the egress and untagged ports associated with a specific dynamically-learned VLAN. |
| <code>show switch dynamic-vlan { VLAN ID } egress-ports</code> | Displays the egress ports associated with a specific dynamically-learned VLAN. |
| <code>show switch dynamic-vlan { VLAN ID } untagged-ports</code> | Displays the untagged ports associated with a specific dynamically-learned VLAN. |

Example

The following displays which VLANs were dynamically learned:

```
localhost# show switch dynamic-vlan
Dynamic-vlan 10
  Untagged ports      -
  Egress ports        [ ethernet0/1 ethernet0/2 ethernet0/3
ethernet0/4 ethernet0/5 ethernet0/6 ethernet0/7 ethernet0/8 ]
Dynamic-vlan 11
  Untagged ports      -
  Egress ports        [ ethernet0/1 ethernet0/2 ethernet0/3
ethernet0/4 ethernet0/5 ethernet0/6 ethernet0/7 ethernet0/8 ]
```

Example

The following displays only the egress ports associated with dynamically-learned VLANs:

```
localhost# show switch dynamic-vlan egress-ports
Dynamic-vlan 10
  Egress ports        [ ethernet0/1 ethernet0/2 ethernet0/3
ethernet0/4 ethernet0/5 ethernet0/6 ethernet0/7 ethernet0/8 ]
Dynamic-vlan 11
  Egress ports        [ ethernet0/1 ethernet0/2 ethernet0/3
ethernet1/4 ethernet0/5 ethernet0/6 ethernet0/7 ethernet0/8 ]
```

Example

The following displays the untagged ports associated with all dynamically-learned VLANs:

```
localhost# show switch dynamic-vlan untagged-ports
UNTAGGED
```

```

VID   PORTS
-----
10    -
11    -

```

Example

The following displays the untagged and egress ports associated with a specific dynamically-learned VLAN:

```

localhost# show switch dynamic-vlan 11
Dynamic-vlan 11
  Untagged ports      -
  Egress ports       [ ethernet0/1 ethernet0/2 ethernet0/3
ethernet0/4 ethernet0/5 ethernet0/6 ethernet0/7
ethernet0/8 ]

```

Example

The following displays the egress ports associated with a specific dynamically-learned VLAN:

```

localhost# show switch dynamic-vlan 11 egress-ports
  Egress ports       [ ethernet0/1 ethernet0/2 ethernet0/3
ethernet0/4 ethernet0/5 ethernet0/6 ethernet0/7 ethernet0/8 ]

```

Example

The following displays the untagged ports associated with a specific dynamically-learned VLAN:

```

localhost# show switch dynamic-vlan 11 untagged-ports
  Untagged ports      -

```

12.2.4.2 Displaying untagged ports for static VLANs

To display the untagged ports associated with a static VLAN, execute the following command in operational mode:

```
show switch vlan { VLAN ID } untagged-ports
```

Example

```

localhost# show switch vlan 1 untagged-ports
untagged-ports [ ethernet0/1 ethernet0/2 ethernet0/3 ethernet0/4
ethernet0/5 ethernet0/6 ethernet0/7 ethernet0/8 ]

```

12.2.4.3 Displaying egress ports for static VLANs

To display the egress ports associated with a static VLAN, execute the following command in operational mode:

```
show switch vlan { VLAN ID } egress-ports
```

Example

```

localhost# show switch vlan 1 egress-ports
egress-ports [ ethernet0/1 ethernet0/2 ethernet0/3 ethernet0/4
ethernet0/5 ethernet0/6 ethernet0/7 ethernet0/8 ]

```

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 544)".

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 548)" and/or "Mapping a DSCP tag to a traffic class (Page 549)".

12.3.1.4 Prioritization of ingress frames

The following details how ingress frames are prioritized and forwarded:

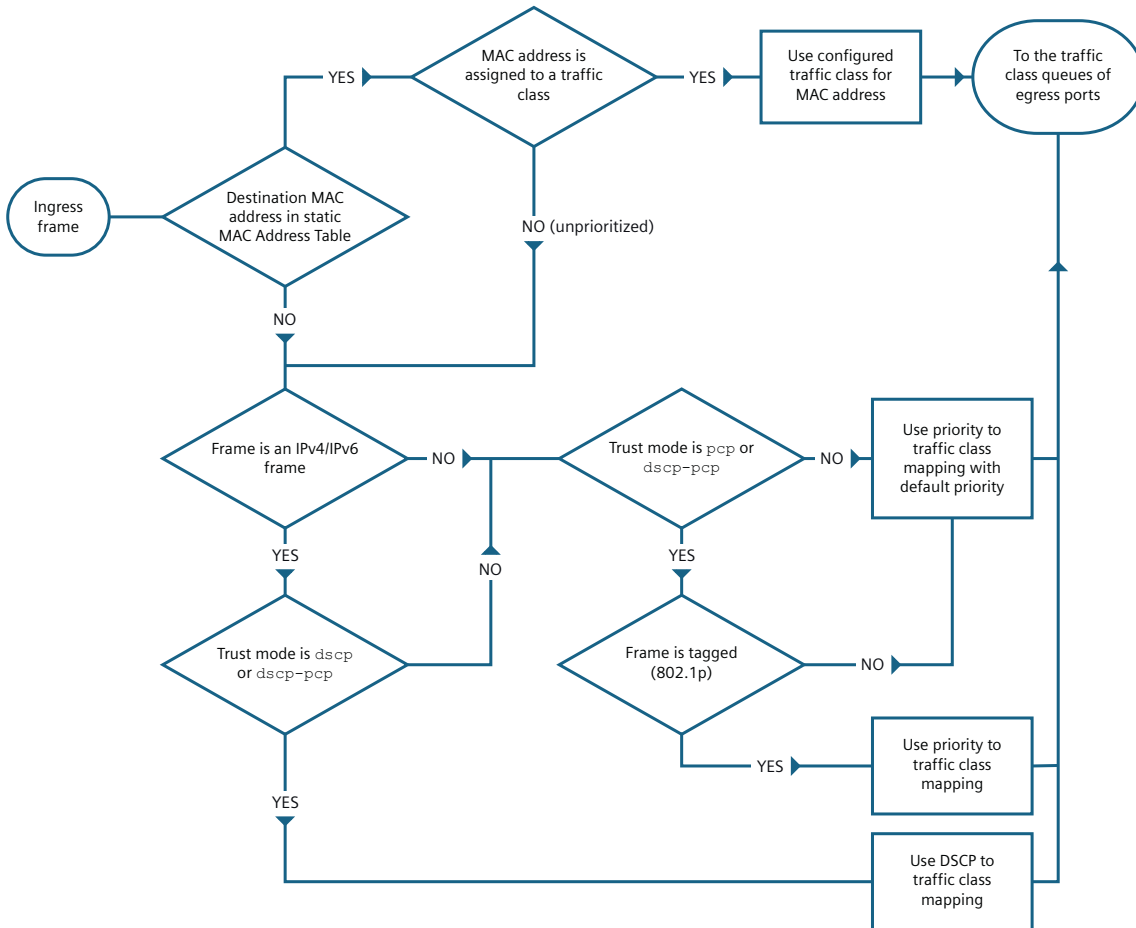


Figure 12-7 Ingress frame prioritization

12.3.1.5 Priority regeneration

The following details how the priority assigned to an ingress frame is regenerated on egress:

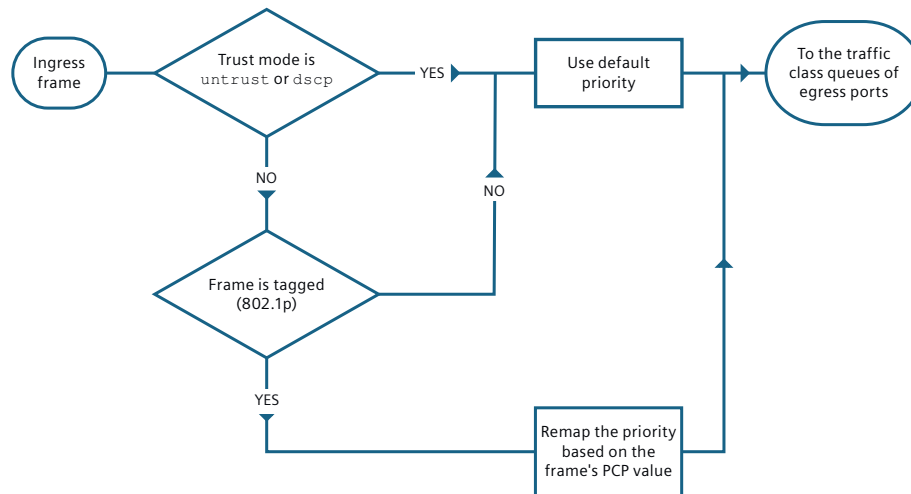


Figure 12-8 Priority regeneration

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 547)".
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 548)"
 - For Layer 3 frames, refer to "Mapping a DSCP tag to a traffic class (Page 549)"

3. If the bridge port is an ingress interface, set the trust mode.
For more information, refer to "Configuring trust mode (Page 550)".
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 552)".

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 set the default priority for a bridge port, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the default priority for the selected bridge port. Default: 0 | <code>interface { bridge port } traffic-classes default-priority { 0 - 7 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } traffic-classes default-priority</code> |

Example

The following changes the default priority for `ethernet0/1` to 4.

```
localhost# config
localhost(config)# interface ethernet0/1 traffic-classes default-priority 4
localhost(config-vlan)# commit
Commit complete.
localhost(config-vlan)# end
localhost# show running-config interface ethernet0/1 traffic-classes
default-priority
interface ethernet0/1
  traffic-classes
    default-priority 4
  exit
exit
```

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 544)".

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Configure the selected bridge port to assign a specific traffic class to frames that have a specific priority tag at ingress. <ul style="list-style-type: none"> ingress-priority - The PCP value at ingress traffic-class - The queue in which to map the frame | interface { bridge port } traffic-classes priority-tc-map ingress-priority { 0 - 7 } traffic-class { 0 - 7 } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } traffic-classes priority-tc-map ingress- priority { 0 - 7 } |

Example

The following configures ethernet0/1 to assign any frame it receives whose priority tag is 2 to traffic class 3.

```
localhost# config
localhost(config)# interface ethernet0/1 traffic-classes priority-tc-map
ingress-priority 2 traffic-class 3
localhost(config-available-traffic-class-3)# commit
Commit complete.
localhost(config-available-traffic-class-3)# end
localhost# show running-config interface ethernet0/1 traffic-classes
priority-tc-map ingress-priority 2
interface ethernet0/1
  traffic-classes priority-tc-map ingress-priority 2
  traffic-class 3
exit

exit
```

```

localhost# show running-config interface ethernet0/1 traffic-classes
priority-tc-map | tab
          TRAFFIC
PRIORITY CLASS
-----
0         1
1         0
2       3
3         3
4         4
5         5
6         6
7         7

exit

```

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 544)".

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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the bridge port to assign a specific traffic class to frames that have a specific DSCP value at ingress. <ul style="list-style-type: none"> <code>dscp-tc-map</code> - The DSCP value at ingress <code>traffic-class</code> - The queue in which to map the frame | <code>interface { bridge port } traffic-classes dscp-tc-map { 0 - 63 } traffic-class { 0 - 7 }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } traffic-classes dscp-tc-map { 0 - 63 }</code> |

12.3 Traffic classes

Example

The following configures ethernet0/1 to assign frames it receives that have a DSCP value of 2 to traffic class 3.

```
localhost# config
localhost(config)# interface ethernet0/1 traffic-classes dscp-tc-map 2
traffic-class 3
localhost(config-dscp-tc-map-2)# commit
Commit complete.
localhost(config-dscp-tc-map-2)# end
localhost# show running-config interface ethernet0/1 traffic-classes dscp-
tc-map 2
interface ethernet0/1
  traffic-classes dscp-to-map 2
    traffic-class 3
  exit

exit
```

```
localhost# show running-config interface ethernet0/1 traffic-classes dscp-
tc-map | tab
      TRAFFIC
DSCP  CLASS
-----
0     1
1     1
2     3
3     1
4     1
.
.
.
exit
```

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.

- **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 trust mode for an ingress bridge port, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure trust mode for the selected bridge port. Options include: <ul style="list-style-type: none"> • <code>untrust</code> - Ingress frames are prioritized based on the interface's default priority. PCP and DSCP values (if present) are ignored. • <code>pcp</code> - 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. • <code>dscp</code> - 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. • <code>dscp-pcp</code> - 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. Default: <code>pcp</code> | <pre>interface { bridge port } traffic-classes trust-mode [untrust pcp dscp dscp- pcp]</pre> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <pre>show running-config interface { bridge port } traffic-classes trust-mode</pre> |

Example

The following sets the trust mode for ethernet0/1 to dscp-pcp.

```
localhost# config
localhost(config)# interface ethernet0/1 traffic-classes trust-mode dscp-
pcp
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 traffic-classes trust-
mode
interface ethernet0/1
  traffic-classes trust-mode dscp-pcp
exit
```

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 bridge port to apply priority regeneration to select frames, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Configure the selected bridge port to assign a different priority tag to frames on egress. | interface { bridge port } traffic-classes priority- regeneration-map ingress- priority { 0 - 7 } egress- priority { 0 - 7 } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } traffic-classes priority-regeneration-map ingress-priority { 0 - 7 } or show running-config interface { bridge port } traffic-classes priority-regeneration-map |

Example

The following configures ethernet0/1 to assign egress priority 3 to frames that have an ingress priority of 2.

```
localhost# config
localhost(config)# interface ethernet0/1 traffic-classes priority-
regeneration-map ingress-priority 2 egress-priority 3
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 traffic-classes
priority-regeneration-map ingress-priority 2
interface ethernet0/1
  traffic-classes priority-regeneration-map ingress-priority 2 egress-
priority 3
exit
```

```
localhost# show running-config interface ethernet0/1 traffic-classes
priority-regeneration-map
interface ethernet0/1
  traffic-classes priority-regeneration-map ingress-priority 0 egress-
priority 0
  traffic-classes priority-regeneration-map ingress-priority 1 egress-
priority 1
  traffic-classes priority-regeneration-map ingress-priority 2 egress-
priority 3
  traffic-classes priority-regeneration-map ingress-priority 3 egress-
priority 3
  traffic-classes priority-regeneration-map ingress-priority 4 egress-
priority 4
  traffic-classes priority-regeneration-map ingress-priority 5 egress-
priority 5
  traffic-classes priority-regeneration-map ingress-priority 6 egress-
priority 6
  traffic-classes priority-regeneration-map ingress-priority 7 egress-
priority 7
```

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.

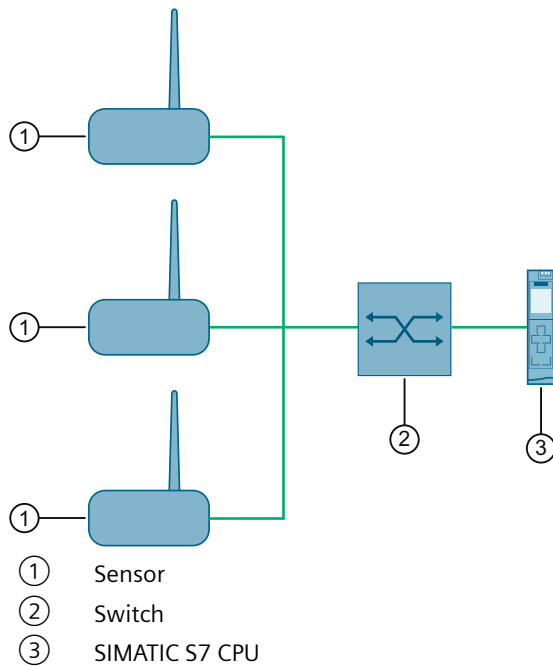


Figure 12-9 A basic traffic class topology

12.3.3.1 Prioritizing all frames

In this version of the scenario, all frames received by the device 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 547)".
2. For each bridge port connected to the sensors, set the trust mode to `untrust`.
For more information, refer to "Configuring trust mode (Page 550)".
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 |
|-----------------------|---|
| <code>pcp</code> | All frames are placed in the queue mapped to their PCP value. |
| <code>dscp</code> | All frames are placed in the queue mapped to their DSCP value. |
| <code>dscp-pcp</code> | 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 priority 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 550)".
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 interface's default priority to incoming frames

In SINEC OS, assign the interface 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 547)".
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 550)".
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 548)" and/or "Mapping a DSCP tag to a traffic class (Page 549)".
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 550)".
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 Manual time setting

This section describes how you configure the date and the system time manually.

13.1.1 Configuring the date and the system time manually

If possible, use a time service. Only configure the system time manually when no time source is available with which the device can synchronize.

After restarting the device, the date and the system time are once again reset to the default value.

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.

Once you have changed the time manually, you can enable the time service to set the time automatically.

To configure the date and the system time manually, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Configure the date and the system time. Options include: <ul style="list-style-type: none"> Date YYYY= Year MM= Month: 01 - 12 DD= Day: 01 - 31 Time HH= Hour: 00 - 23 MM= Minute: 00 - 59 SS= Seconds: 00 - 59 | <code>system clock set-current-datetime date { YYYY-MM-DD } time { HH:MM:SS }</code> |
| 2 | Respond to the security prompt. | <code>yes</code> |

Example

```
localhost# system clock set-current-datetime date 2019-03-25 time
10:00:00
Are you sure you want to change the system date and time settings?
[yes,no] yes
localhost# show system clock current-datetime
current-datetime "2019-03-25 10:00:46"
```

13.1.2 Showing the date and system time

To display information on date and system time, execute the following command in operating mode:

```
show system clock
```

Example

```
localhost# show system clock
clock
  timezone-name      Europe/Paris
  current-datetime   "2019-03-25 14:50:50"
  dst-active         false
```

Description

The following information is shown:

| Parameter | Description |
|-------------------------------|--|
| <code>timezone-name</code> | Shows which time zone is set. |
| <code>current-datetime</code> | Shows the set date and the system time. |
| <code>dst-active</code> | Shows whether the daylight saving time changeover is active (<code>true</code>) or not (<code>false</code>). |

13.2 Time change and daylight saving

Note

When you configure a time change after the system time has already been set, the displayed system time can change. To prevent this, start by configuring the time change.

If you do not configure a time change, the system time of the device corresponds to UTC. UTC is the time standard from which the time zones are derived. The displayed system time can take into account the number of hours by which the time at the location of the device differs.

As a result of the changeover to daylight saving or standard time, the system time for the local time zone is set correctly.

You have the following alternatives to configure a deviation from UTC:

- Configure the relevant time zone. The switch to daylight saving time takes place automatically according to the rules of the configured time zone.
For more information, refer to "Configuring the time zone (Page 559)".
- Configure the time change and switching to daylight saving time manually:
 - Configure the time change.
For more information, refer to "Configuring the time offset (Page 560)".
 - Configure a fixed date or a rule for switching to daylight saving time.
For more information, refer to "Configuring a date for switching to daylight saving time (Page 561)" and "Configuring a rule for switching to daylight saving time (Page 562)".
 - Configure the time change during daylight saving time.
For more information, refer to "Configuring the time offset during daylight saving time (Page 563)".

13.2.1 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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | [Optional] Show all available time zones. | <code>system clock timezone-name ?</code> |
| 3 | Configure the time zone. Default: UTC | <code>system clock timezone-name { time zone }</code> |
| 4 | Commit the change. | <code>commit</code> |

13.2 Time change and daylight saving

| Step | Instruction | Command |
|------|---------------------------|---|
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config system clock timezone-name |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system clock timezone-name Europe/Paris
localhost(config-system-clock)# commit
Commit complete.
localhost(config-system-clock)# end
localhost# show running-config system clock timezone-name
system
clock
    timezone-name Europe/Paris
exit

exit
```

13.2.2 Configuring the time offset

To configure the time offset, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Configure the deviation from the UTC time in minutes to determine the time zone. Example: The value -480 corresponds to the time zone "UTC-08:00". Default: 0 | system clock timezone-utc-offset { -1500 - 1500 } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system clock timezone-utc-offset |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system clock timezone-utc-offset -480
localhost(config-system-clock)# commit
Commit complete.
localhost(config-system-clock)# end
localhost# show running-config system clock timezone-utc-offset
system
clock
    timezone-utc-offset -480
exit
```



```
exit
```

13.2.3 Configuring a date for switching to daylight saving time

Define a date for switching to daylight saving time. This setting is suitable for regions in which the daylight saving time changeover is not governed by rules. As a result of the changeover to daylight saving or standard time, the system time for the local time zone is set correctly.

To configure a date for switching to daylight saving time, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the date for switching to daylight saving time. <ul style="list-style-type: none"> { Year } Format: YYYY YYYY= Year: 1970 ... 2037 { Start date }/{ End date } Format: MMDDHH:MM MM= Month: 01 ... 12 DD= Day: 01 ... 31 HH= Hour: 00 ... 23 MM= Minute: 00 ... 59 | <code>system clock summer-time date { year } start { start date } end { end date }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system clock summer-time date</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system clock summer-time date 2020 start
021002:00 end 100502:00
localhost(config-summer-time)# commit
Commit complete.
localhost(config-summer-time)# end
localhost# show running-config system clock summer-time date
system
clock
summer-time
date 2020 start 021002:00
date 2020 end 100502:00
exit

exit

exit
```

13.2.4 Configuring a rule for switching to daylight saving time

Define a rule for the daylight saving time changeover. This setting is suitable for regions in which the daylight saving time always begins or ends on a specific weekday. As a result of the changeover to daylight saving or standard time, the system time for the local time zone is set correctly.

To configure a rule for switching to daylight saving time, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the start time for a regular daylight saving time changeover. <ul style="list-style-type: none"> • {week} Range of values: 1 ... 5, last last is the last week of the month • {weekday} Range of values: 0 ... 6 0 is Sunday • {month} Range of values: 1 ... 12 1 is January • {time} Format: HH:MM HH= Hour: 00 ... 23 MM= Minute: 00 ... 59 | <pre>system clock summer-time recurring start { Week } { Weekday } { Month } { Time }</pre> |
| 3 | Configure the end time for a regular daylight saving time changeover. <ul style="list-style-type: none"> • {week} Range of values: 1 ... 5, last last is the last week of the month • {weekday} Range of values: 0 ... 6 0 is Sunday • {month} Range of values: 1 ... 12 1 is January • {time} Format: HH:MM HH= Hour: 00 ... 23 MM= Minute: 00 ... 59 | <pre>recurring end { Week } { Weekday } { Month } { Time }</pre> |
| 4 | Commit the changes. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <pre>show running-config system clock summer-time recurring</pre> |

Example

```
localhost# config
Entering configuration mode terminal
```

```

localhost(config)# system clock summer-time recurring start 3 6 3
02:00
localhost(config-summer-time)# recurring end 3 6 10 02:00
localhost(config-summer-time)# commit
Commit complete.
localhost(config-summer-time)# end
localhost# show running-config system clock summer-time recurring
system
clock
summer-time
recurring start 3 6 3 02:00
recurring end 3 6 10 02:00
exit

exit

exit

```

13.2.5 Configuring the time offset during daylight saving time

To configure the time offset during daylight saving time, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Configure the difference to UTC time during daylight saving time in minutes. Default: 60 | system clock summer-time offset { 1 - 1440 } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system clock summer-time offset |

Example

```

localhost# config
Entering configuration mode terminal
localhost(config)# system clock summer-time offset 120
localhost(config-summer-time)# commit
Commit complete.
localhost(config-summer-time)# end
localhost# show running-config system clock summer-time offset
system
clock
summer-time
offset 120
exit

exit

exit

```

13.3 NTP

This section describes the configuration of the Network Time Protocol (NTP).

13.3.1 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.

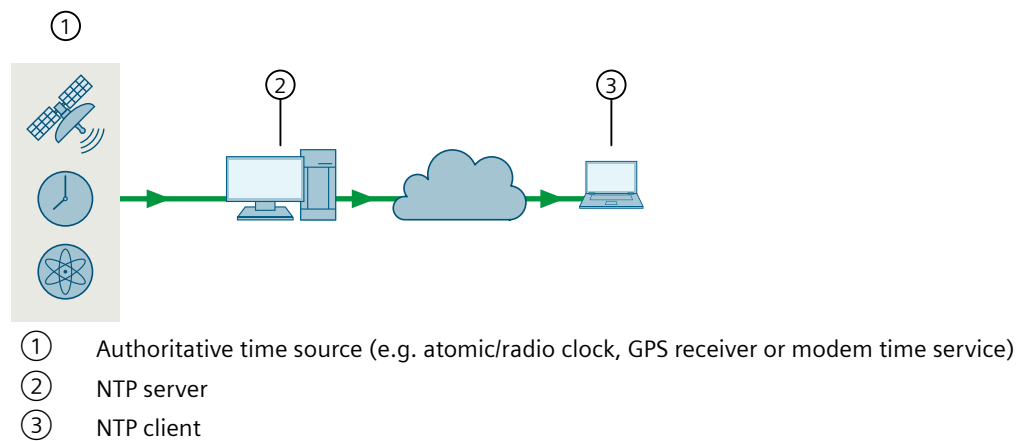


Figure 13-1 NTP

13.3.1.1 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.

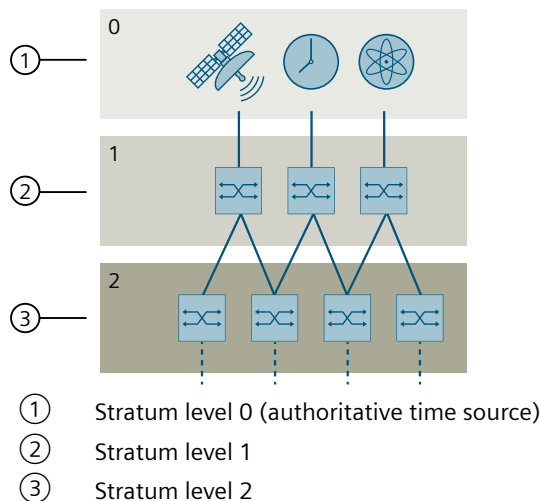


Figure 13-2 NTP stratum levels

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. Stratum level 16 is equivalent to unsynchronized.

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.

13.3.1.2 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

13.3 NTP

- NTP multicast server
- Local software clock

13.3.1.3 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.

13.3.1.4 NTP authentication

When NTP authentication is enabled, the device only synchronizes itself with a time source that has the same authentication key as the device itself. The device discards all packets for which authentication failed.

Key-based authentication therefore needs to be configured identically for both the server and the client.

By using authentication keys, you increase the security of the NTP communication. This ensures that time-of-day synchronization only takes place with trusted sources. Invalid time information is discarded.

For more information, refer to RFC 1305 (<https://www.rfc-editor.org/rfc/rfc1305>).

13.3.2 Configuring an NTP client

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. [Optional] To adjust the time offset of the system time from UTC, you have the following alternatives:
 - Configure the local time zone.
 - Configure the time offset and switching to daylight saving time.
 For more information, refer to "Time change and daylight saving (Page 559)".
2. Enable the NTP service.
For more information, refer to "Enabling the NTP service (Page 567)".
3. Configure an NTP server.
For more information, refer to "Configuring an NTP server (Page 568)".
4. [Optional] Enable an NTP server.
For more information, refer to "Enabling an NTP server (Page 569)".
5. [Optional] If a version other than NTP V4 is required, define the NTP version.
For more information, refer to "Changing the NTP version (Page 569)".
6. [Optional] Configure the values of the polling interval.
For more information, refer to "Configuring the NTP polling interval (Page 570)".
7. [Optional] To accelerate synchronization during the first connection establishment, enable iBurst.
For more information, refer to "Enabling iBurst (Page 572)".
8. [Optional] To improve the quality of the time-of-day synchronization, enable Burst.
For more information, refer to "Enabling Burst (Page 572)".

13.3.2.1 Enabling the NTP service

By default, NTP is disabled.

To enable NTP, do the following:

| Step | Instruction | Command |
|------|---------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable NTP. | <code>system time-sync ntp enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system time-sync ntp enabled</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system time-sync ntp enabled
localhost(config-ntp)# commit
Commit complete.
localhost(config-ntp)# end
localhost# show running-config system time-sync ntp enabled
system
  time-sync
```

13.3 NTP

```

ntp
  enabled
exit

exit

exit

```

13.3.2.2 Configuring an NTP server

By default, no NTP server is configured.

To define an NTP server, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enter the IP address of the NTP server. By default, a newly configured NTP server is automatically enabled. | <code>system time-sync ntp unicast-configuration ipv4 { IP address }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system time-sync ntp unicast-configuration</code> |

Example

```

localhost# config
Entering configuration mode terminal
localhost(config)# system time-sync ntp unicast-configuration ipv4
192.168.16.100
localhost(config-ipv4-192.168.16.100)# commit
Commit complete.
localhost(config-ipv4-192.168.16.100)# end
localhost# show running-config system time-sync ntp unicast-
configuration
system
  time-sync
    ntp
      unicast-configuration ipv4 192.168.16.100
      .
      .
      .
    exit
  exit

exit

exit

exit

```


13.3.2.3 Enabling an NTP server

By default, a newly configured NTP server is automatically enabled.

To enable an NTP server, do the following:

| Step | Instruction | Command |
|------|---------------------------|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable the NTP server. | system time-sync ntp unicast-configuration ipv4 { IP address } enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system time-sync ntp unicast-configuration ipv4 { IP address } enabled |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system time-sync ntp unicast-configuration ipv4
192.168.16.100 enabled
localhost(config-ipv4-192.168.16.100)# commit
Commit complete.
localhost(config-ipv4-192.168.16.100)# end
localhost# show running-config system time-sync ntp unicast-
configuration ipv4 192.168.16.100 enabled
system
  time-sync
    ntp
      unicast-configuration ipv4 192.168.16.100
      enabled
    exit
  exit
exit
exit
exit
```

13.3.2.4 Changing the NTP version

To change the NTP version, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Change the NTP version you are using. Only change the NTP version if a version other than version 4 is required. Default: 4 | system time-sync ntp unicast-configuration ipv4 { IP address } version { 1 - 4 } |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------|--|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system time-sync ntp unicast-configuration ipv4 { IP address } version |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system time-sync ntp unicast-configuration ipv4
192.168.16.100 version 3
localhost(config-ipv4-192.168.16.100)# commit
Commit complete.
localhost(config-ipv4-192.168.16.100)# end
localhost# show running-config system time-sync ntp unicast-
configuration ipv4 192.168.16.100 version
system
  time-sync
  ntp
    unicast-configuration ipv4 192.168.16.100
    version 3
  exit

exit

exit

exit
```

13.3.2.5 Configuring the NTP polling interval

To configure the polling interval for an NTP server, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Configure the minimum value of the query interval in seconds as power of 2. Default: 6 The value 6 corresponds to 2 ⁶ (64 seconds). | system time-sync ntp unicast-configuration ipv4 { IP address } minpoll { 4 - 17 } |
| 3 | Configure the maximum value of the query interval in seconds as power of 2. Default: 10 The value 10 corresponds to 2 ¹⁰ (1024 seconds). | maxpoll { 4 - 17 } |
| 4 | Commit the changes. | commit |

| Step | Instruction | Command |
|------|---------------------------|--|
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config system time-sync ntp unicast-configuration ipv4 {IP address} minpoll show running-config system time-sync ntp unicast-configuration ipv4 {IP address} maxpoll |

Example

```

localhost# config
Entering configuration mode terminal
localhost(config)# system time-sync ntp unicast-configuration ipv4
192.168.16.100 minpoll 8
localhost(config-ipv4-192.168.16.100)# maxpoll 12
localhost(config-ipv4-192.168.16.100)# commit
Commit complete.
localhost(config-ipv4-192.168.16.100)# end
localhost# show running-config system time-sync ntp unicast-
configuration ipv4 192.168.16.100 minpoll
system
  time-sync
    ntp
      unicast-configuration ipv4 192.168.16.100
        minpoll 8
    exit
  exit
exit

localhost# show running-config system time-sync ntp unicast-
configuration ipv4 192.168.16.100 maxpoll
system
  time-sync
    ntp
      unicast-configuration ipv4 192.168.16.100
        maxpoll 12
    exit
  exit
exit

localhost# show running-config system time-sync ntp unicast-
configuration ipv4 192.168.16.100 maxpoll
system
  time-sync
    ntp
      unicast-configuration ipv4 192.168.16.100
        maxpoll 12
    exit
  exit
exit

```

13.3.2.6 Enabling iBurst

iBurst (initial Burst) increases the number of frames from the default of one frame to eight 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:

| Step | Instruction | Command |
|------|----------------------------------|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable iBurst for an NTP server. | <code>system time-sync ntp unicast-configuration ipv4 { IP address } iburst</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system time-sync ntp unicast-configuration ipv4 { IP address } iburst</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system time-sync ntp unicast-configuration ipv4
192.168.16.100 iburst
localhost(config-ipv4-192.168.16.100)# commit
Commit complete.
localhost(config-ipv4-192.168.16.100)# end
localhost# show running-config system time-sync ntp unicast-
configuration ipv4 192.168.16.100 iburst
system
 time-sync
  ntp
    unicast-configuration ipv4 192.168.16.100
      iburst
    exit
  exit
exit
exit
exit
```

13.3.2.7 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:

| Step | Instruction | Command |
|------|---------------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable Burst for an NTP server. | <code>system time-sync ntp unicast-configuration ipv4 { IP address } burst</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system time-sync ntp unicast-configuration ipv4 { IP address } burst</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system time-sync ntp unicast-configuration ipv4
192.168.16.100 burst
localhost(config-ipv4-192.168.16.100)# commit
Commit complete.
localhost(config-ipv4-192.168.16.100)# end
localhost# show running-config system time-sync ntp unicast-
configuration ipv4 192.168.16.100 burst
system
  time-sync
    ntp
      unicast-configuration ipv4 192.168.16.100
        burst
      exit
    exit
  exit
exit
```

13.3.3 Configuring NTP authentication

To configure NTP authentication, follow these steps:

1. Configure an authentication key.
For more information, refer to "Configuring an authentication key (Page 574)".
2. Configure the device as NTP client.
For more information, refer to "Configuring an NTP client (Page 566)".
3. Link an authentication key with a NTP server.
For more information, refer to "Applying an authentication key (Page 575)".

13.3.3.1 Configuring an authentication key

To configure an authentication key, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure a unique number for the NTP authentication key. | <code>system time-sync ntp authentication key-id { 1 - 65534 }</code> |
| 3 | Configure the authentication method. Options include: <ul style="list-style-type: none"> • md5 • sha-1 • sha-256 | <code>algorithm [md5 sha-1 sha-256]</code> |
| 4 | Configure the symmetrical key for authentication. The permissible characters depend on the authentication method. Conditions for MD5: <ul style="list-style-type: none"> • Must be between 1 and 40 characters long • With 1 to 20 characters, the following ASCII characters are permitted: 0x21, 0x22 and 0x24 to 0x7E. • With 21 to 40 characters, the following ASCII characters are permitted: 0x30 bis 0x39, 0x41 to 0x5A and 0x61 to 0x7A Conditions for SHA-1 and SHA-256: <ul style="list-style-type: none"> • Must be exactly 40 characters long • The following ASCII characters are permitted: 0x30 bis 0x39, 0x41 to 0x5A and 0x61 to 0x7A | <code>key { key }</code> |
| 5 | Label the authentication key as trusted. | <code>trusted</code> |
| 6 | Commit the changes. | <code>commit</code> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 7 | Exit configuration mode. | end |
| 8 | Verify the configuration. | show running-config system time-sync ntp authentication key-id { Key ID } |

Example

In this example, a trusted authentication key with key ID 19 and the authentication procedure is sha-1 configured.

```
localhost# config
localhost(config)# system time-sync ntp authentication key-id 19
localhost(config-authentication-keys-19)# algorithm sha-1
localhost(config-authentication-keys-19)# key a96f4dbb14fb73...
localhost(config-authentication-keys-19)# trusted
localhost(config-authentication-keys-19)# commit
localhost(config-authentication-keys-19)# end
localhost# show running-config system time-sync ntp authentication
key-id 19
system
  time-sync
    ntp
      authentication
        key-id 19
          algorithm sha-1
          key a96f4dbb14fb73...
        exit
      exit
    exit
  exit
exit
```

13.3.3.2 Applying an authentication key

Before you can apply an authentication key, you need to configure an authentication key.

To link an authentication key with an NTP server, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Enter the number of the symmetrical authentication key for communication with an NTP time-of-day source. | system time-sync ntp unicast-configuration ipv4 { IP address } key-id { Key ID } |
| 3 | Commit the changes. | commit |

| Step | Instruction | Command |
|------|---------------------------|---|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system time-sync ntp unicast-configuration ipv4 { IP address } key-id |

Example

In this example, the NTP server with IP address 192.168.16.100 is linked with the authentication key with key ID 19.

```
localhost# config
localhost(config)# system time-sync ntp unicast-configuration ipv4
192.168.16.100 key-id 19
localhost(config-ipv4-192.168.16.100)# commit
localhost(config-ipv4-192.168.16.100)# end
localhost# show running-config system time-sync ntp unicast-
configuration ipv4 192.168.16.100 key-id
system
time-sync
ntp
unicast-configuration ipv4 192.168.16.100
key-id 19
exit

exit

exit

exit
```

13.3.4 Monitoring NTP

This section describes the various ways in which you can view the status of NTP and monitor NTP connections.

13.3.4.1 Displaying the NTP configuration

Execute the following command in operational mode to show the NTP configuration of the device:

```
show running-config system time-sync ntp | details
```

Example

```
localhost# show running-config system time-sync ntp | details
system
time-sync
ntp
enabled
authentication

key-id 19
```



```

    algorithm sha-1

    key a96f4dbb14fb73...

    trusted

    exit

exit

unicast-configuration ipv4 192.168.16.100
    key-id 19
    no burst
    iburst
    minpoll 8
    maxpoll 12
    version 4
    enabled
    exit

exit

exit

exit

```

Description

The following information is shown:

| Parameter | Description |
|-------------------------------|--|
| enabled | Shows whether NTP is enabled. |
| key-id | Shows the number of an NTP authentication key. |
| algorithm | Shows the authentication method. |
| key | Shows the symmetrical key for authentication. |
| trusted | Shows whether the authentication key is labeled trusted. |
| unicast-configuration ipv4 | Shows the IPv4 address of the NTP server. |
| key-id | Shows the number of the symmetrical authentication key linked to the NTP server. |
| burst | Shows whether Burst is enabled. |
| iburst | Shows whether iBurst is enabled. |
| minpoll | Shows the minimum value of the polling interval. |
| maxpoll | Shows the maximum value of the polling interval. |
| version | Shows the NTP version used. |
| enabled | Shows whether the NTP server is enabled. |

13.3.4.2 Showing the status of the NTP system time

To display the status of the NTP system time, execute the following command in operating mode:
`show system time-sync ntp clock-state`

Example

```
localhost# show system time-sync ntp clock-state
clock-state                synchronized
clock-stratum              2
clock-refid                192.168.2.5
associations-address       192.168.2.5
associations-local-mode    client
associations-isConfigured  true
actual-freq                1.857
clock-precision            18
clock-offset               -0.0212
root-delay                 1.0
root-dispersion            4.24
reference-time              2019-03-25T01:42:03+00:00
sync-state                  clock-synchronized
```

Description

The following information is shown:

| Parameter | Description |
|---------------------------|---|
| clock-state | Shows whether or not the device is synchronized with a time source via NTP. Possible values include: <ul style="list-style-type: none"> <code>synchronized</code> The device is synchronized with a time source via NTP. <code>unsynchronized</code> - The device is not synchronized. |
| clock-stratum | Stratum number of the device |
| clock-refid | NTP reference of the time source from which the device obtains its time information |
| associations-address | IP address of the time source from which the device obtains its time information |
| associations-local-mode | Role of the device with regard to its time source Possible values include: <ul style="list-style-type: none"> <code>client</code> - The device is a client of the time source specified under <code>associations-address</code>. |
| associations-isConfigured | Displays whether or not the time source is static or was learned. Possible values include: <ul style="list-style-type: none"> <code>true</code> - The time source was configured statically. <code>false</code> - The time source was learned dynamically. |
| actual-freq | Measured frequency of the internal hardware clock in Hertz |
| clock-precision | Precision of the internal software clock in seconds as power of 2 ($2^{(-n)}$). Example: The value 18 corresponds to $2^{(-18)}$ (0.000003815 seconds) |

| Parameter | Description |
|-----------------|--|
| clock-offset | Time difference in milliseconds between the system time and the reference time of the time source |
| root-delay | Round trip delay in milliseconds for a time query of the device to the relevant time source at the root of the hierarchical NTP network |
| root-dispersion | Maximum time difference in milliseconds between the system time of the device and the relevant time source at the root of the hierarchical NTP network |
| reference-time | System time at which the time of the device was last updated The value is 0 if no synchronization has yet taken place. |
| sync-state | Displays detailed information about the status of the synchronized system time. Possible values include: <ul style="list-style-type: none"> clock-synchronized The device is synchronized with a time source via NTP. The system time is set. freq - The system time is set; the frequency is not set. freq-set-by-cfg - The system time is set and the frequency is set through configuration. spike - The time difference in milliseconds between the system time of the device and the time source is greater than 128 ms (spike). clock-never-set - The system time was not set. |

13.3.4.3 Monitoring NTP connections

To monitor the NTP connections, execute the following command in operating mode:
`show system time-sync ntp associations`

Example

```
localhost# show system time-sync ntp associations
associations 192.0.2.12 client true
  stratum      11
  refid        LOCAL(0)
  reach        377
  unreachable  0
  poll         64
  offset       35279876224.835
  delay        0.59
  dispersion   7937.5
  receive-time 2019-03-25T010:30:00+00:00
  ntp-statistics packet-sent 0
  ntp-statistics packet-received 1
```

Description

The following information is shown:

| Parameter | Description |
|-----------------|--|
| stratum | Stratum number of the time source |
| refid | NTP reference of the time source from which the time source of the device obtains its time information |
| reach | <p>Reachability of the time source</p> <p>Shows the status of the last eight NTP packets as octal number. The binary display of the octal number shows whether or not a response packet was received from the time source. The bit value "1" indicates that a response was received. The bit value "0" indicates that no response was received.</p> <p>When the value 377 (binary 1111 1111) is displayed, the last eight NTP responses were received.</p> <p>When a response packet is lost, the missing packet is tracked over the next eight query intervals.</p> <p>Example:</p> <p>Time 0: reach 377 $\hat{=}$ 1111 1111 = The last eight responses were received.</p> <p>Time 1: reach 376 $\hat{=}$ 1111 1110 = The last response was not received.</p> <p>Time 2: reach 375 $\hat{=}$ 1111 1101 = The last response was received.</p> <p>Time 3: reach 373 $\hat{=}$ 1111 1011 = The last response was received.</p> <p>.</p> <p>.</p> <p>.</p> |
| unreach | Counts the unanswered queries to an NTP server. When the server can be reached again, the counter is automatically reset. |
| poll | Current query interval in seconds |
| offset | Time difference in milliseconds between the system time and the reference time of the time source |
| delay | Round trip delay in milliseconds for a time query of the device to the time source via the network |
| dispersion | Maximum time difference in milliseconds between the system time of the device and the time source |
| receive-time | <p>System time at which the time of the time source was last updated</p> <p>The value is 0 if no synchronization has yet taken place.</p> |
| packet-sent | Number of sent NTP packets |
| packet-received | Number of received NTP packets |

13.4 SIMATIC time

The SIMATIC method for time synchronization is a proprietary protocol by which the SIMATIC components can keep their times synchronized.

13.4.1 Understanding SIMATIC Time

The SIMATIC procedure is based on SNAP services and can only be used in the local Industrial Ethernet subnet. SNAP works with MAC addresses (ISO layer 2) and is not routable.

The SIMATIC method is mainly used in process automation on the plant bus in combination with ISO transport services and reaches an accuracy of +/- 10 ms.

For more information, refer to "Time synchronization - time synchronization in the automation environment (<https://support.industry.siemens.com/cs/ww/en/view/86535497>)".

For switches in the PROFINET fieldbus, synchronization via the SIMATIC method is recommended because the CPU supports this method as a time master. When the CPU is active as a SIMATIC time master in the fieldbus, you only need to enable the SIMATIC Time client for the switch.

13.4.2 Enabling the SIMATIC time client

The SIMATIC time client is disabled by default.

To enable the SIMATIC time client, do the following:

| Step | Instruction | Command |
|------|---------------------------------|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the SIMATIC time client. | <code>system time-sync simatic-time enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system time-sync simatic-time</code> |

Example

```
localhost# config
Entering configuration mode terminal
localhost(config)# system time-sync simatic-time enabled
localhost(config-system-time-sync)# commit
Commit complete.
localhost(config-system-time-sync)# end
localhost# show running-config system time-sync simatic-time
system
  time-sync
    simatic-time enabled
  exit
exit
```

13.5 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.

13.5.1 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

13.5.1.1 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 585)".

13.5.1.2 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.

13.5.1.3 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 |

13.5.1.4 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 |

13.5.1.5 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.

13.5.1.6 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 peer-to-peer 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. |

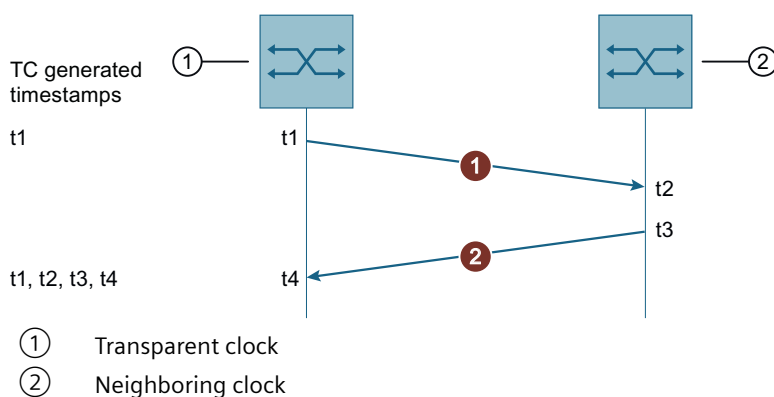


Figure 13-3 Transparent clock message exchange (one-step)

Once all required timestamps are collected, the peer-to-peer transparent clock calculates the peer mean path delay using the following formula:

$$Delay = [(t4 - t1) - (t3 - t2)] / 2$$

For information about determining the peer mean path delay for an individual bridge port, refer to "Displaying the peer mean path delay (Page 588)".

13.5.2 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 586)".
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 587)".
3. Make sure the PTP service is enabled globally.
For more information, refer to "Enabling PTP globally (Page 588)".

13.5.2.1 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:

| Step | Description | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define the domain number. Default: 0 | <code>system time-sync ptp domain-number [0-127 254]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system time-sync ptp domain-number</code> |

Example

```

localhost# config
localhost(config)# system time-sync ptp domain-number 1
localhost(config-ptp)# commit
Commit complete.
localhost(config-ptp)# end
localhost# show running-config system time-sync ptp domain-number
system
time-sync
  ptp
    domain-number 1
  exit
exit
exit

```

13.5.2.2 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:

| Step | Description | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable PTP for the selected bridge port. | interface { bridge port } ptp enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config interface { bridge port } ptp enabled |

Example

The following enables PTP for bridge port ethernet0/1.

```

localhost# config
localhost(config)# interface ethernet0/1 ptp enabled
localhost(config-interface-ethernet0/1-ptp)# commit
Commit complete.
localhost(config-interface-ethernet0/1-ptp)# end
localhost# show running-config interface ethernet0/1 ptp enabled
interface ethernet0/1
  ptp
    enabled
  exit
exit

```

13.5.2.3 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.

| Step | Description | Command |
|------|---------------------------|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable PTP. | <code>system time-sync ptp enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config ptp enabled</code> |

Example

```
localhost# config
localhost(config)# system time-sync ptp enabled
localhost(config-ptp)# commit
Commit complete.
localhost(config-ptp)# end
localhost# show running-config system time-sync ptp enabled
system
  time-sync
    ptp
      enabled
    exit
  exit
exit
```

13.5.3 Monitoring PTP

This section describes the various ways to look up information about the PTP service.

13.5.3.1 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 585)".

To display the peer mean path delay determined for each PTP-enabled bridge port, execute the following command in operational mode:

```
show interface ptp peer-mean-path-delay
```

To display the peer mean path delay determined for a specific PTP-enabled bridge port, execute the following command in operational mode:

```
show interface ethernet0/1 ptp peer-mean-path-delay
```

Example

The following displays the peer mean path delay for all PTP-enabled bridge ports:

```
localhost# show interface ptp peer-mean-path-delay
% The following list contains 35 entries.
interface ethernet0/1
  ptp
  peer-mean-path-delay 0
interface ethernet0/2
  ptp
  peer-mean-path-delay 0
interface ethernet0/3
  ptp
  peer-mean-path-delay 0
interface ethernet0/4
  ptp
  peer-mean-path-delay 707
interface ethernet0/5
  ptp
  peer-mean-path-delay 0
.
.
.
```

Example

The following displays the peer mean path delay for a specific bridge port:

```
localhost# show interface ethernet0/4 ptp
ptp
peer-mean-path-delay 761
```


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 591)".
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 592)".
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 593)".

Note

All static multicast groups are added to the multicast filtering database upon creation.
For more information, refer to "Multicast filtering database (Page 617)".

14.1.1.1 Adding a static multicast group

To add a static multicast group, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Add the static multicast group. All static multicast groups must be assigned to a specific VLAN and have a valid MAC address. | <code>switch multicast-filtering static { VLAN ID } { MAC address }</code> |
| 3 | Commit the change. | <code>commit</code> |

14.1 Static multicast groups

| Step | Instruction | Command |
|------|---------------------------|---|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch multicast-filtering static { VLAN ID } |

Example

The following adds a static multicast group to VLAN 1 with the MAC address 01:4E:15:00:00:01.

```
localhost# config
localhost(config)# switch multicast-filtering static 1 01:4E:15:00:00:01
localhost(config-static-1/01:4E:15:00:00:01)# commit
Commit complete.
localhost(config-static-1/01:4E:15:00:00:01)# end
localhost# show running-config switch multicast-filtering static 1
switch
  multicast-filtering
    static 1 01:4E:15:00:00:01
  exit
exit
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Select the traffic class for the selected static multicast group. Options include: <ul style="list-style-type: none"> 0 - 7 - A traffic class queue unprioritized - No traffic class queue is assigned Default: unprioritized | switch multicast-filtering static { VLAN ID } { MAC address } traffic-class [{ 0 - 7 } unprioritized] |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch multicast-filtering static { VLAN ID } { MAC address } traffic-class |

Example

```

localhost# config
localhost(config)# switch multicast-filtering static 1 01:4E:15:00:00:01
traffic-class 7
localhost(config-static-1/01:4E:15:00:00:01)# commit
Commit complete.
localhost(config-static-1/01:4E:15:00:00:01)# end
localhost# show running-config switch multicast-filtering static 1
01:4E:15:00:00:01 traffic-class
switch
multicast-filtering
static 1 01:4E:15:00:00:01
traffic-class 7
exit

exit

exit

```

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Assign an interface to the selected static multicast group. | switch multicast-filtering static { VLAN ID } { MAC address } forwarding-port-map { port } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch multicast-filtering static { VLAN ID } { MAC address } forwarding-port-map |

Example

```
localhost# config
localhost(config)# switch multicast-filtering static 1 01:4E:15:00:00:01
forwarding-port-map ethernet0/1
localhost(config-forwarding-port-map-ethernet0/1)# commit
Commit complete.
localhost(config-forwarding-port-map-ethernet0/1)# end
localhost# show running-config switch multicast-filtering static 1
01:4E:15:00:00:01 forwarding-port-map
switch
multicast-filtering
static 1 01:4E:15:00:00:01
forwarding-port-map ethernet0/1
exit

exit

exit
```

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 596)".
- 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 597)".
- [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 597)".
- [Optional] Enable topology change flooding.
For more information, refer to "Enabling topology change flooding (Page 598)".

14.2.2.1 Enabling GMRP

To enable GMRP for all bridge port interfaces, do the following:

Note

GMRP is disabled by default.

| Step | Instruction | Command |
|------|----------------------------------|---|
| 1 | Enter global configuration mode. | config |
| 2 | Enable GMRP globally. | switch multicast-filtering gmrp enabled |
| 3 | Commit the change. | commit |
| 4 | Exit global configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch multicast-filtering gmrp |

Example

```
localhost# config
localhost(config)# switch multicast-filtering gmrp enabled
localhost(config-gmrp)# commit
Commit complete.
localhost(config-gmrp)# end
localhost# show running-config switch multicast-filtering gmrp
switch
 multicast-filtering
  gmrp
    enabled
  exit
exit
```

```
exit
```

14.2.2.2 Selecting the GMRP mode per bridge port

A GMRP mode can be set for each interface, which determines how the interface processes GMRP **join** and **leave** messages.

To configure how a bridge port interface to process GMRP messages, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select the GMRP mode for the selected bridge port. Options include: <ul style="list-style-type: none"> <code>declare-and-register</code> - All multicast groups are declared and new groups are registered dynamically <code>declare-only</code> - All multicast groups (configured or learned) are declared, but new groups are not registered <code>disabled</code> - GMRP is disabled on the interface Default: <code>disabled</code> | <code>interface { bridge port } gmrp-mode [disabled declare-and-register declare-only]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit global configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config interface { bridge port } gmrp-mode</code> |

Example

The following sets the GMRP mode to `declare-only` for `ethernet0/1`.

```
localhost# config
localhost(config)# interface ethernet0/1 gmrp-mode declare-only
localhost(config-interface-ethernet0/1)# commit
Commit complete.
localhost(config-interface-ethernet0/1)# end
localhost# show running-config interface ethernet0/1 gmrp-mode
interface ethernet0/1
  gmrp-mode declare-only
exit
```

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 configure a delay before removing a host from a multicast group, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the time delay. Conditions: <ul style="list-style-type: none"> Formatted as <code>nYnMnDnhnmns</code>, where <code>n</code> is a user-defined number Minimum of 0.6 seconds (<code>0.6s</code>) Maximum of 5 minutes (<code>5m</code>) or 300 seconds (<code>300s</code>) Default: <code>4s</code> (4 seconds) | <code>switch multicast-filtering gmrp leave-timer [0.6s - 300s]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch multicast-filtering gmrp leave- timer</code> |

Example

The following sets the delay to 2 minutes and 3 seconds.

```
localhost# config
localhost(config)# switch multicast-filtering gmrp leave-timer 2m3s
localhost(config-gmrp)# commit
Commit complete.
localhost(config-gmrp)# end
localhost# show running-config switch multicast-filtering gmrp
leave-timer
switch
multicast-filtering
  gmrp
    leave-timer 2m3s
  exit
exit
exit
```

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Make sure RSTP is enabled, as this feature is dependent on topology change notices. For more information, refer to "Selecting the STP version (Page 352)". | - |
| 3 | Enable topology change flooding. | <code>switch multicast-filtering gmrp topology-change-flooding</code> |
| 4 | Commit the change. | <code>commit</code> |
| 5 | Exit configuration mode. | <code>end</code> |
| 6 | Verify the configuration. | <code>show running-config switch multicast-filtering gmrp topology-change-flooding</code> |

Example

```
localhost# config
localhost(config)# switch multicast-filtering gmrp topology-change-flooding
localhost(config-igmp-snooping)# commit
Commit complete.
localhost(config-igmp-snooping)# end
localhost# show running-config switch multicast-filtering igmp-snooping
topology-change-flooding
switch
  multicast-filtering
    igmp-snooping
      topology-change-flooding
    exit
  exit
exit
```

14.2.3 Configuration examples

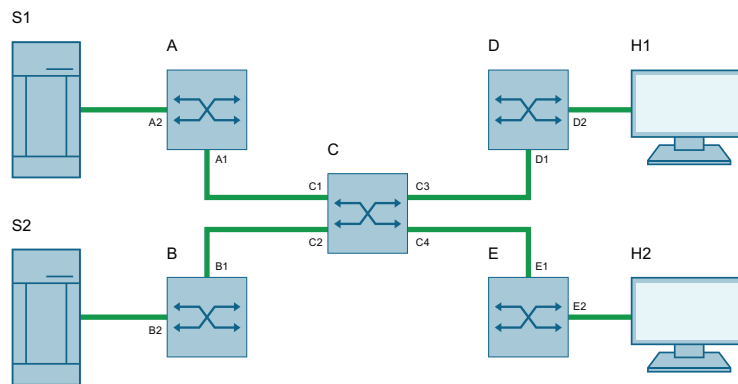
The following are examples of how to deploy GMRP.

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.



■ 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 603)".
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 604)".
3. Select the IGMP mode.
For more information, refer to "Selecting the IGMP mode (Page 605)".
4. Configure the IGMP query interval.
For more information, refer to "Configuring the IGMP query interval (Page 606)".
5. [Optional] Enable topology change flooding.
For more information, refer to "Enabling topology change flooding (Page 607)".
6. [Optional] Configure multicast router forwarding.
For more information, refer to "Configuring multicast router forwarding (Page 609)".
7. Enable IGMP snooping for one or more static VLANs.
For more information, refer to "Enabling IGMP snooping per VLAN (Page 608)".

14.3.2.1 Enabling IGMP snooping

To enable IGMP snooping, do the following:

Note

IGMP snooping is enabled by default.

| Step | Instruction | Command |
|------|---------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable IGMP snooping. | <code>switch multicast-filtering igmp-snooping enabled</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch multicast-filtering igmp-snooping</code> |

Example

```
localhost# config
localhost(config)# switch multicast-filtering igmp-snooping enabled
localhost(config-igmp-snooping)# commit
Commit complete.
localhost(config-igmp-snooping)# end
localhost# show running-config switch multicast-filtering igmp-snooping
switch
  multicast-filtering
    igmp-snooping
      enabled
      send-query
    exit
  exit
exit
```

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 change the version of IGMP, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select the IGMP version. Options include: <ul style="list-style-type: none"> • 2 - Changes the IGMP version to IGMPv2 • 3 - Changes the IGMP version to IGMPv3 Default: 2 | <code>switch multicast-filtering igmp-snooping version [2 3]</code> |
| 3 | Commit the change. | <code>commit</code> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch multicast-filtering igmp- snooping version |

Example

The following selects IGMPv2.

```
localhost# config
localhost(config)# switch multicast-filtering igmp-snooping version
2
localhost(config-igmp-snooping)# commit
Commit complete.
localhost(config-igmp-snooping)# end
localhost# show running-config switch multicast-filtering igmp-
snooping version
switch
  multicast-filtering
    igmp-snooping
      version 2
    exit
  exit
exit
```

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 601)".

To change the IGMP mode, do the following:

| Step | Instruction | Command |
|------|--------------------------------|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Select the IGMP snooping mode. | Active Mode <code>switch multicast-filtering igmp-snooping send-query</code> Passive Mode <code>no switch multicast-filtering igmp-snooping send-query</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch multicast-filtering igmp-snooping send-query</code> |

Example

The following enables active mode.

```
localhost# config
localhost(config)# switch multicast-filtering igmp-snooping send-query
localhost(config-igmp-snooping)# commit
Commit complete.
localhost(config-igmp-snooping)# end
localhost# show running-config switch multicast-filtering igmp-snooping
send-query
switch
  multicast-filtering
    igmp-snooping
      send-query
    exit
  exit
exit
```

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:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Configure the query interval. Conditions: <ul style="list-style-type: none"> Formatted as <code>nYnMnDnhnmns</code>, where <code>n</code> is a user-defined number Minimum of 10 seconds (<code>10s</code>) Maximum of 60 minutes (<code>60m</code>) or 3600 seconds (<code>3600s</code>) Default: <code>2m5s</code> (2 minutes, 5 seconds) | <code>switch multicast-filtering igmp-snooping query-interval [10s - 3600s]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch multicast-filtering igmp-snooping query-interval</code> |

Example

The following sets the IGMP query interval to 3 minutes and 20 seconds.

```
localhost# config
localhost(config)# switch multicast-filtering igmp-snooping query-
interval 3m20s
localhost(config-igmp-snooping)# commit
Commit complete.
localhost(config-igmp-snooping)# end
localhost# show running-config switch multicast-filtering igmp-
snooping query-interval
switch
  multicast-filtering
    igmp-snooping
      query-interval 3m20s
    exit
  exit
exit
```

14.3.2.5 Enabling topology change flooding

When STP topology changes occur or link changes occur without triggering a TCN, 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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Make sure RSTP is enabled, as this feature is dependent on topology change notices. For more information, refer to "Configuring STP globally (Page 350)". | - |
| 3 | Enable topology change flooding. | switch multicast-filtering igmp-snooping topology-change-flooding |
| 4 | Commit the change. | commit |
| 5 | Exit configuration mode. | end |
| 6 | Verify the configuration. | show running-config switch multicast-filtering igmp-snooping topology-change-flooding |

Example

```
localhost# config
localhost(config)# switch multicast-filtering igmp-snooping topology-
change-flooding
localhost(config-igmp-snooping)# commit
Commit complete.
localhost(config-igmp-snooping)# end
localhost# show running-config switch multicast-filtering igmp-snooping
topology-change-flooding
switch
  multicast-filtering
    igmp-snooping
      topology-change-flooding
    exit
  exit
exit
exit
```

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.

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable IGMP snooping for the selected static VLAN. | switch vlan { VLAN ID } igmp-snooping enabled |

| Step | Instruction | Command |
|------|---------------------------|--|
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch vlan { VLAN ID } igmp-snooping |

Example

```
localhost# config
localhost(config)# switch vlan 1 igmp-snooping enabled
localhost(config-switch-vlan-1)# commit
Commit complete.
localhost(config-switch-vlan-1)# end
localhost# show running-config switch vlan 1 igmp-snooping
switch
  vlan 1
    igmp-snooping enabled
  exit
exit
```

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 609)".
2. Configure one or more multicast router interfaces.
For more information, refer to "Configuring a multicast router interface (Page 610)".

14.3.3.1 Enabling multicast router forwarding

To enable multicast router forwarding, do the following:

Note

Multicast router forwarding is enabled by default.

| Step | Instruction | Command |
|------|-------------------------------------|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable multicast router forwarding. | switch multicast-filtering igmp-snooping mrouter-forwarding |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch multicast-filtering mrouter-forwarding |

Example

```

localhost# config
localhost(config)# switch multicast-filtering igmp-snooping mrouter-
forwarding
localhost(config-igmp-snooping)# commit
Commit complete.
localhost(config-igmp-snooping)# end
localhost# show running-config switch multicast-filtering igmp-
snooping mrouter-forwarding
switch
 multicast-filtering
  igmp-snooping
  mrouter-forwarding
  exit

exit

exit

```

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Configure the selected bridge port to be a static connection. Multiple static connections must be defined separately. | switch multicast-filtering igmp-snooping static-bridge-mrouter-interface { bridge port } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch multicast-filtering igmp-snooping static-bridge-mrouter-interface |

Example

The following configures ethernet0/1 and ethernet0/2 to be static connections to a multicast router.

```
localhost# config
localhost(config)# switch multicast-filtering igmp-snooping static-bridge-
mrouter-interface ethernet0/1
localhost(config)# switch multicast-filtering igmp-snooping static-bridge-
mrouter-interface ethernet0/2
localhost(config-igmp-snooping)# commit
Commit complete.
localhost(config-igmp-snooping)# end
localhost# show running-config switch multicast-filtering igmp-snooping
static-bridge-mrouter-interface
switch
  multicast-filtering
    igmp-snooping
      static-bridge-mrouter-interface [ ethernet0/1 ethernet0/2 ]
    exit
  exit
exit
```

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 number of learned multicast groups

To display the total number of multicast groups dynamically learned by IGMP Snooping, execute the following command in operational mode:

```
show switch multicast-filtering igmp-snooping entries-count
```

Example

```
localhost# show switch multicast-filtering igmp-snooping entries-
count
entries-count 3
```

14.3.4.2 Displaying the status of learned multicast groups

To display the status of multicast groups dynamically learned by IGMP Snooping, execute the following command in operational mode:

```
show switch multicast-filtering igmp-snooping group-summary
```

Example

```
localhost# show switch multicast-filtering igmp-snooping group-summary
igmp-snooping
group-summary ethernet0/6 1 225.0.2.2
  last-reporter 192.168.0.203
  mac-address   01-00-5E-00-02-02
  up-time       112
  joined-ports  [ ethernet0/6 ]
group-summary ethernet0/7 1 239.255.255.250
  last-reporter 192.168.0.1
  mac-address   01-00-5E-7F-FF-FA
  up-time       112
  joined-ports  [ ethernet0/7 ]
  mrouter-ports [ ethernet0/1 ]
```

Description

The following information is displayed for each multicast group:

| Parameter | Description |
|---|--|
| group-summary { Bridge port } { VLAN ID } { MAC address } | Displays the following: <ul style="list-style-type: none"> The bridge port on which the multicast group was learned The VLAN ID of the VLAN on which the multicast group operates 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. |
| mrouter-ports | A list of bridge ports that will forward multicast traffic to multicast routers. |

14.3.4.3 Displaying the destination MAC address of a learned multicast group

To display the destination MAC address of a multicast group learned dynamically by IGMP Snooping, execute the following command in operational mode:

```
show switch multicast-filtering igmp-snooping group-summary mac-address
```

Details can also be filtered based on bridge port, VLAN ID, and/or IPv4 address using the following command:

```
show switch multicast-filtering igmp-snooping group-summary { bridge pPort } { VLAN ID } { IPv4 address } mac-address
```

Example

The following displays the MAC addresses for all groups.

```
localhost# show switch multicast-filtering igmp-snooping group-summary mac-
address | tab
PORT          VID  ADDRESS          MAC ADDRESS
-----
ethernet0/6  1    225.0.2.2       01-00-5E-00-02-02
                2    225.0.3.3       01-00-5E-1C-70-46
ethernet0/7  1    239.255.255.250 01-00-5E-7F-FF-FA
```

Example

The following displays the MAC addresses for a specific bridge port.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 mac-address | tab
PORT          VID  ADDRESS          MAC ADDRESS
-----
ethernet0/6  1    225.0.2.2       01-00-5E-00-02-02
                2    225.0.3.3       01-00-5E-1C-70-46
```

Example

The following displays the MAC addresses for a specific bridge port and VLAN ID.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 mac-address | tab
PORT          VID  ADDRESS          MAC ADDRESS
-----
ethernet0/6  1    225.0.2.2       01-00-5E-00-02-02
```

Example

The following displays the MAC addresses for a specific bridge port, VLAN ID, and IPv4 address.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 225.0.2.2 mac-address
mac-address 01-00-5E-00-02-02
```

14.3.4.4 Displaying the last host to send a report to a learned multicast group

To determine the last host to send a report to a multicast group dynamically learned by IGMP Snooping, execute the following command in operational mode:

```
show switch multicast-filtering igmp-snooping group-summary last-reporter
```

Details can also be filtered based on bridge port, VLAN ID, and/or IPv4 address using the following command:

```
show switch multicast-filtering igmp-snooping group-summary { bridge port }
{ VLAN ID } { IPv4 address } last-reporter
```

Example

The following displays the last report for all bridge ports.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
last-reporter
PORT          VID  ADDRESS          LAST REPORTER
-----
ethernet0/6   1    225.0.2.2        192.168.0.203
               2    225.0.3.3        192.168.0.204
ethernet0/7   1    239.255.255.250  192.168.0.1
```

Example

The following displays the last reporter for a specific bridge port.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 last-reporter
PORT          VID  ADDRESS          LAST REPORTER
-----
ethernet0/6   1    225.0.2.2        192.168.0.203
               2    225.0.3.3        192.168.0.204
```

Example

The following displays the last reporter for a specific bridge port and VLAN ID.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 last-reporter
PORT          VID  ADDRESS          LAST REPORTER
-----
ethernet0/6   1    225.0.2.2        192.168.0.203
```

Example

The following displays the last reporter for a specific bridge port, VLAN ID, and IPv4 address.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 192.168.0.203 last-reporterlast-reporter 192.168.0.203
```

14.3.4.5 Displaying the interfaces that receive IGMP join messages for a learned multicast group

To display the interfaces that receive IGMP join messages for multicast groups dynamically learned by IGMP Snooping, execute the following command in operational mode:

```
show switch multicast-filtering igmp-snooping group-summary joined-ports
```

Details can also be filtered based on bridge port, VLAN ID, and/or IPv4 address using the following command:

```
show switch multicast-filtering igmp-snooping group-summary { bridge port }
{ VLAN ID } { IPv4 address } joined-ports
```

Example

The following displays the joined ports for all bridge ports.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
joined-ports
PORT          VID  ADDRESS          JOINED PORTS
-----
ethernet0/6   1    225.0.2.2        [ ethernet0/6 ]
                2    225.0.3.3        [ ethernet0/6 ]
ethernet0/7   1    239.255.255.250 [ ethernet0/7 ]
```

Example

The following displays the joined ports for a specific bridge port.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 joined-ports
PORT          VID  ADDRESS          JOINED PORTS
-----
ethernet0/6   1    225.0.2.2        [ ethernet0/6 ]
                2    225.0.3.3        [ ethernet0/6 ]
```

Example

The following displays the joined ports for a specific bridge port and VLAN ID.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 joined-ports
PORT          VID  ADDRESS          JOINED PORTS
-----
ethernet0/6   1    225.0.2.2        [ ethernet0/6 ]
```

Example

The following displays the joined ports for a specific bridge port, VLAN ID, and IPv4 address.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 225.0.2.2 joined-ports
joined-ports [ ethernet0/6 ]
```

14.3.4.6 Displaying the interfaces that forward multicast traffic to multicast routers for a learned multicast group

To display the interfaces that forward IGMP join messages for multicast groups dynamically learned by IGMP Snooping, execute the following command in operational mode:

```
show switch multicast-filtering igmp-snooping group-summary mrouter-ports
```

Details can also be filtered based on bridge port, VLAN ID, and/or IPv4 address using the following command:

```
show switch multicast-filtering igmp-snooping group-summary { bridge port }
{ VLAN ID } { IPv4 address } mrouter-ports
```

Example

The following displays the multicast router ports for all bridge ports.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
mrouter-ports
PORT          VID  ADDRESS          MROUTER PORTS
-----
ethernet0/6   1    225.0.2.2        [ ethernet0/1 ]
               2    225.0.3.3        [ ethernet0/1 ]
ethernet0/7   1    239.255.255.250 [ ethernet0/1 ]
```

Example

The following displays the multicast router ports for a specific bridge port.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 mrouter-ports
PORT          VID  ADDRESS          MROUTER PORTS
-----
ethernet0/6   1    225.0.2.2        [ ethernet0/1 ]
               2    225.0.3.3        [ ethernet0/1 ]
```

Example

The following displays the multicast router ports for a specific bridge port and VLAN ID.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 mrouter-ports
PORT          VID  ADDRESS          MROUTER PORTS
-----
ethernet0/6   1    225.0.2.2        [ ethernet0/1 ]
```

Example

The following displays the multicast router ports for a specific bridge port, VLAN ID, and IPv4 address.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 225.0.2.2 mrouter-ports
mrouter-ports [ ethernet0/1 ]
```

14.3.4.7 Displaying the uptime of a learned multicast group

To display the time that has elapsed since a multicast group was learned, execute the following command in operational mode:

```
show switch multicast-filtering igmp-snooping group-summary up-time
```

Details can also be filtered based on bridge port, VLAN ID, and/or IPv4 address using the following command:

```
show switch multicast-filtering igmp-snooping group-summary { bridge port }
{ VLAN ID } { IPv4 address } up-time
```


Example

The following displays the uptime for all bridge ports.

```
localhost# show switch multicast-filtering igmp-snooping group-summary up-time
                                UP
PORT          VID  ADDRESS          TIME
-----
ethernet0/6  1   225.0.2.2       88
              2   225.0.3.3       92
ethernet0/7  1   239.255.255.250 96
```

Example

The following displays the uptime for a specific bridge port.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 up-time
                                UP
PORT          VID  ADDRESS          TIME
-----
ethernet0/6  1   225.0.2.2       88
              2   225.0.3.3       92
```

Example

The following displays the uptime for a specific bridge port and VLAN ID.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 up-time
                                UP
PORT          VID  ADDRESS          TIME
-----
ethernet0/6  1   225.0.2.2       88
```

Example

The following displays the uptime for a select bridge port, VLAN ID, and IPv4 Address.

```
localhost# show switch multicast-filtering igmp-snooping group-summary
ethernet0/6 1 225.0.2.2 up-time
up-time 88
```

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.

14.4.1 Displaying multicast filtering database

To display the multicast filtering database, execute the following command in operational mode:

```
show switch multicast-filtering filtering-database
```

Example

```
localhost# show switch multicast-filtering filtering-database |
notab
filtering-database entry 1 01:4E:15:00:00:01
  traffic-class 1
  port-map ethernet0/1
    state statically-configured
  port-map ethernet0/2
    state statically-configured-dynamically learned
filtering-database entry 2 01:4E:15:00:00:02
  traffic-class 2
  port-map ethernet0/1
    state statically-configured
filtering-database entry 1 01:4E:15:00:00:03
  traffic-class unprioritized
  port-map ethernet0/1
    state dynamically-learned
3 entry in the list.
```

Note

A total count of MAC addresses is shown when the filtering database is displayed in a table format. The total count is not displayed when the `notab` customization is applied.

Description

The following information is displayed for each entry:

| Parameter | Description |
|---------------|---|
| VID | The VID of the VLAN on which the multicast group operates. |
| 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 |
| PORT | The outbound forwarding port(s) associated with the MAC address. |
| STATE | The current state of the forwarding port. Possible values include: <ul style="list-style-type: none"> statically-configured - The MAC address was added statically by a user dynamically-learned - The MAC address was learned dynamically by a bridge protocol statically-configured-dynamically-learned - The MAC address was learned dynamically and then added statically by a user |

14.4.2 Displaying the traffic class assigned to a multicast group entry

To display the traffic class assigned to a multicast MAC address entry, execute the following command:

```
switch multicast-filtering filtering database entry { database ID } { VLAN
ID } { MAC address } traffic-class
```

Example

```
localhost# show switch multicast-filtering filtering-database entry 1 1
01:4E:15:00:00:01 traffic-class
traffic-class 1
```

Description

The following information is displayed for the entry:

| Parameter | Description |
|---------------|--|
| traffic-class | The traffic class assigned to the entry. |

14.4.3 Displaying the forwarding port assigned to a multicast group entry

To display the forwarding ports assigned to a multicast MAC address entry, execute the following command:

```
switch multicast-filtering filtering database entry { VLAN ID } { MAC
Address } port-map
```

Example

```
localhost# show switch multicast-filtering filtering-database entry 1
01:4E:15:00:00:01 port-map | tab
PORT                STATE
-----
ethernet0/1         statically-configured
ethernet0/2         statically-configured-
                    dynamically learned
```

Description

The following information is displayed for each entry:

| Parameter | Description |
|-----------|--|
| PORT | The forwarding port. |
| STATE | Indicates how the forwarding port was added for the selected VLAN and MAC address. Possible values include: <ul style="list-style-type: none"> statically-configured - The forwarding port was added manually dynamically-learned - The forwarding port was learned dynamically statically-configured-dynamically learned - The forwarding port was added manually and learned dynamically |

14.4.4 Displaying the state of a forwarding port assigned to a multicast group entry

To display the state of a forwarding port, execute the following command:

```
switch multicast-filtering filtering database entry { VLAN ID }
{ MAC address } port-map { bridge port } state
```

Example

```
localhost# show switch multicast-filtering filtering-database entry
1 1 01:4E:15:00:00:01 port-map ethernet0/1 state
state          statically-configured
```

Description

The following information is displayed:

| Parameter | Description |
|-----------|--|
| state | Indicates how the forwarding port was added for the selected VLAN and MAC address. Possible values include: <ul style="list-style-type: none"> statically-configured - The forwarding port was added manually dynamically-learned - The forwarding port was learned dynamically statically-configured-dynamically learned - The forwarding port was added manually and learned dynamically |

Diagnostics

This chapter describes the diagnostic tools available, including related protocols. This includes alarms, logs, network utilities, traffic analysis, etc.

15.1 System status

This section describes how to monitor the system state, including uptime, last reboot, etc.

15.1.1 Displaying the system boot time

To display the date and time when the device was last rebooted, execute the following command in operational mode:

```
show system state boot-datetime
```

Example

```
localhost# show system state boot-datetime  
state boot-datetime "2021-01-01 00:08:00"
```

15.1.2 Displaying the system up time

To display the total time the system has been running since the device was last rebooted, execute the following command in operational mode:

```
show system state uptime
```

Example

```
localhost# show system state uptime  
state uptime 2D4h42m35s
```

15.2 Network utilities

SINEC OS is equipped with built-in programs for pinging hosts and tracking routes.

15.2.1 Ping

Ping is a diagnostic tool with which you can check whether a host on an IP network can be reached.

15.2.1.1 Understanding Ping

To check the availability of a host, Ping sends an **Echo-Request** via ICMP (Internet Control Message Protocol) to the IP address of the host and waits for its **Echo-Reply**.

With the response from the host, the time interval between sending a request and receiving a request is specified. This interval is referred to as Round Trip Delay (RTD) or Round Trip Time (RTT).

If the sender does not receive a response, this can be due to a number of reasons:

- The host cannot be reached.
Possible reasons are that the host is no longer connected to the network, is not assigned an IP address or is malfunctioning.
- The configuration of the host prevents a response.
The host may be configured in such a way that it ignores and discards ICMP packets and thus also pings. A host that does not respond to a ping can still be connected to the network and working correctly.
- The request is filtered out on its way to the host.
A firewall can be configured in such a way that ICMP packets and thus also pings may not go through the firewall. The ping does not arrive at the host.

If the host does not respond, the information Network unreachable or Host unreachable is returned by the responsible router.

15.2.1.2 Pinging an IP address or a host

NOTICE**Security risk - Danger of unauthorized access**

The CLI session is not ended while a ping request is active. This applies also if you have configured a timeout after which the CLI session is automatically terminated (`terminal idle-timeout`).

If you do not configure any parameters that stop a ping request, the ping request runs infinitely and the CLI session never ends.

Configure automatic ending of a ping request after a specific period of time (`deadline`) or number of retries (`attempts`) in order to prevent unauthorized access.

To ping an IP address or a host, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Specify the IP address or the FQDN of the host that you want to ping. <ul style="list-style-type: none"> IP address - IP address of the host that you want to ping. Hostname - FQDN of the host that you want to ping. | <code>ping { ip address hostname }</code> |
| 2 | Configure the number of repetitions for a ping request. The ping request is automatically terminated after the specified number. Default: Unlimited | <code>attempts { 1 - 10000 }</code> |
| 3 | Specify the duration in seconds that elapses before the device stops a ping request. The ping request is stopped independent of the configured number of retries in the "attempts" parameter. Default: Unlimited | <code>deadline { 1 - 1000 }</code> |
| 4 | Change size of the outbound packets in bytes for a ping request. Default: 56 | <code>size { 1 - 2080 }</code> |
| 5 | Specify the IP address to be used as the source for ping requests. Default: IP address of the outbound IP interface | <code>source { IP address }</code> |
| 6 | Configure the duration in seconds for which the device waits for the first response from the destination host. The "timeout" parameter is subordinate to the "attempts" parameter. When the device receives a response, it sends the number of ping requests defined in the "attempts" parameter and stops the request independent of the "timeout" parameter. If the device does not receive a response to the number of ping requests defined in the "attempts" parameter, it starts the timeout. The ping request is stopped after the timeout. If you configure a value > 300, change the value of the <code>terminal idle-timeout</code> parameter first. The parameter specifies the number of seconds before the current CLI session is automatically ended (default: 300). For more information, refer to "Configuring the local CLI environment (Page 102)". Default: 10 | <code>timeout { 1 - 1000 }</code> |
| 7 | If you have not configured the number of repetitions, you must stop the ping manually. Stop the ping request. | <code>[Strg] + [C]</code> |

Example

```
localhost# ping 192.168.16.177 attempts 3
PING 192.168.16.177 (192.168.16.177): 56 data bytes
64 bytes from 192.168.16.177: seq=0 ttl=64 time=2.442 ms
64 bytes from 192.168.16.177: seq=1 ttl=64 time=1.221 ms
64 bytes from 192.168.16.177: seq=2 ttl=64 time=1.409 ms
--- 192.168.16.177 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.221/1.690/2.442 ms
```

15.2.2 Traceroute

Traceroute is a diagnostic tool with which you can trace the path of an IP packet to its destination host hop by hop. For this purpose, Traceroute uses the TTL value (Time To Live) of the IP protocol. Traceroute sends IP packets to the IP address of the destination host multiple times. The IP packets contain different TTL values.

15.2.2.1 Understanding the trace route

Traceroute sends the first IP packets with a TTL value of 1. The router that receives the IP packet decreases the TTL value by 1 to the value 0 and discards the packet. It responds with the ICMP message "Time exceeded". The ICMP message contains the IP address of the relevant router and the round-trip delay time. Traceroute thus maps the first step (Hop) of the packet to the path through the network. If more than one router responds, all responses are recorded. If no router responds within a configurable period of time, this is noted with a *.

In each subsequent IP packet, Traceroute increases the TTL value by 1 to determine the next hop.

For example, the second IP packet has a TTL of 2. This IP packet gets to the next hop on the path to the destination host via the first router. The first router decreases the TTL by 1 when it receives the IP packets. The IP packet reaches the second router with a TTL of 1. The second router discards the IP packet and sends an ICMP message "Time exceeded" to the original host.

Traceroute sends IP packets until the target host responds or the maximum TTL value is reached.

Traceroute with UDP

This method uses UDP datagrams as IP packets. To prevent UDP datagrams from being forwarded, an "unlikely Port" is configured and an increase by 1 takes place for each subsequent packet. The advantage of traceroute with UDP is that the required packets can be sent with normal user rights.

When the destination host is reached, it replies with the message:

```
Destination Unreachable/Port Unreachable
```


15.2.2.2 Determining the data path to a host (Traceroute)

To determine the data path to a host, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Specify the IP address or the FQDN of the host whose path you want to determine. <ul style="list-style-type: none"> IP-Adresse - IP address of the host whose path you want to determine. Hostname - FQDN of the host whose path you want to determine. | <code>traceroute { IP address host name }</code> |
| 2 | [Optional] Change the maximum TTL value of the packets. Default: 30 | <code>maxttl { 1 - 255 }</code> |
| 3 | [Optional] Change the number of IP packets that are sent with each TTL value (hop). Default: 3 | <code>probes { 1 - 50 }</code> |
| 4 | [Optional] Specify the IP address given as the source in the packets. Default: IP address of the outbound IP interface | <code>source { IP address }</code> |
| 5 | [Optional] Specify the duration in seconds that elapses before the device stops a ping request. If you configure a value > 300, change the value of the <code>terminal idle-timeout</code> parameter first. The parameter specifies the number of seconds before the current CLI session is automatically ended (default: 300). For more information, refer to "Configuring the local CLI environment (Page 102)". Default: 3 | <code>timeout { 1 - 3600 }</code> |
| 6 | Close the application. | <code>[Strg] + [C]</code> |

Example

```
localhost# traceroute 192.168.16.177 maxttl 10
traceroute to 192.168.16.177 (192.168.16.177), 10 hops max, 38 byte
packets
 1 192.168.16.177 (192.168.16.177) 0.759 ms 0.590 ms 0.042 ms
```

15.3 System logging

SINEC OS records all alarms and select events in a syslog, or system log. The syslog is used by network administrators to identify events related to performance and security.

The syslog 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.

Note

For information about sending notifications via e-mail, refer to "SMTP (Page 663)".

For information about triggering SNMP traps, refer to "Enabling an event to trigger an SNMP trap (Page 655)".

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: nYnMnDnhnmns | 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. |
| 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.

15.3.1.6 Repudiation

Repudiation is the concept where a user performs an action and later denies taking such action. This could include changing the device configuration, deleting or importing a file, etc.

SINEC OS automatically logs each change made to the system state to establish a clear audit trail. This not only allows administrators to challenge repudiation, but to also identify potential attacks.

Action logs are assigned to the user who performed the action and are recorded in the syslog. Each log message is in the form of:

```
{ protocol }: Action: '{ action }' was executed by user { user } with role { role }
```

This feature is not configurable and cannot be disabled.

15.3.2 Configuring system logging

To configure system logging, do the following:

1. [Optional] Select your preferred format for timestamps applied to each entry in the syslog. For more information, refer to "Setting the timestamp format (Page 629)".
2. [Optional] Apply a filter to the logbook to control which events are displayed. For more information, refer to "Filtering the logbook (Page 629)".
3. [Optional] Configure SINEC OS to forward all or select events to one or more remote syslog servers. For more information, refer to "Configuring remote system logging (Page 631)".

15.3.2.1 Setting the timestamp format

To set the format of the timestamp applied to each syslog entry, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the timestamp format. Options include: <ul style="list-style-type: none"> • <code>isodate</code> - A format that adheres to the ISO 8601 date and time format. For example: 2021-03-13T15:58:00.123+01:00.123 • <code>fulldate</code> - A format that includes the year, month, day, and time. For example: 2006 Jun 13 15:58:00.123 • <code>date</code> - A format that includes only the month, day, and time. For example: Jun 13 15:58:00.123 Default: <code>isodate</code> | <code>system logging actions syslog-format timestamp-format [date fulldate isodate]</code> |
| 3 | Commit the changes. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system logging actions syslog-format</code> |

Example

```
localhost# config
localhost(config)# system logging actions syslog-format timestamp-format fulldate
localhost(config-system-logging)# commit
Commit complete.
localhost(config-system-logging)# end
localhost# show running-config system logging actions syslog-format
system
logging
actions syslog-format timestamp-format fulldate
exit

exit
```

15.3.2.2 Filtering the logbook

By default, the logbook displays all events listed in the syslog. However, the logbook can be configured to display event messages associated with specific severity-levels.

Note

Only one filter can be defined for the logbook at a time.

To set the logbook to display or hide specific events, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Choose which event messages are displayed in the logbook based on their associated severity. Options include: <ul style="list-style-type: none"> • <code>all</code> - Selects all events • <code>alert</code> - Selects alert-level events • <code>critical</code> - Selects critical-level events • <code>emergency</code> - Selects emergency-level events • <code>error</code> - Selects error-level events • <code>info</code> - Selects info-level events • <code>none</code> - No events are displayed • <code>notice</code> - Selects notice-level events • <code>warning</code> - Selects warning-level events Default: <code>info</code> | <code>system logging actions logbook severity [alert all critical emergency error info none notice warning]</code> |
| 3 | Choose whether only the selected event is displayed, or if the selected event and events with a higher severity level are displayed. Options include: <ul style="list-style-type: none"> • <code>equals</code> - Only event messages associated with the selected severity are selected • <code>equals-or-higher</code> - Event messages associated to the selected severity and higher are selected Default: <code>equals-or-higher</code> | <code>advanced-compare compare [equals equals-or-higher]</code> |
| 4 | [Optional] Choose whether or not the logbook displays event messages. Options include: <ul style="list-style-type: none"> • <code>log</code> - Event messages are displayed based on the filtering rule selected • <code>block</code> - No event messages are displayed Default: <code>log</code> | <code>advanced-compare action [log block]</code> |
| 5 | Commit the changes. | <code>commit</code> |
| 6 | Exit configuration mode. | <code>end</code> |
| 7 | Verify the configuration. | <code>show running-config system logging actions logbook severity</code> |

Example

Set the logbook to only display critical event messages. No other messages are displayed.

```
localhost# config
localhost(config)# system logging actions logbook severity critical
advanced-compare compare equals action log
```

```
localhost(config-system-logging)# commit
Commit complete.
localhost(config-system-logging)# end
localhost# show running-config system logging actions logbook
severity
system
  logging
    actions logbook severity critical
  exit
exit
```

15.3.3 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 631)".
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 634)".

15.3.3.1 Adding a remote syslog server profile

Up to five remote syslog server profiles can be configured. Each profile defines:

- The server's hostname or IP address
- The server's designated port
- Which logs are forwarded to the server
- TLS certificates and keys (if applicable)

To add a remote syslog server profile, do the following:

Note

For TLS server connections, a key-pair and certificate must be available in the keystore.

For information, refer to "Keys and certificates (Page 201)".

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Assign a name to the remote syslog server profile. | <code>system logging actions remote destination { name }</code> |

| Step | Instruction | Command |
|------|--|---|
| 3 | Select one or more filtering rules to control which logs are forwarded to the server. For more information, refer to "Defining a filtering rule for a remote syslog server (Page 634)". | facility-filter facility-list [all auth authpriv daemon kern mail messages syslog user] [alert all critical debug emergency error none notice warning] |
| 4 | Exit to the top level. | top |
| 5 | Configure the connection to the server, using the server's host name or IP address, as well as its designated port. The default port for remote system logging is 514 for UDP and 6514 for TLS. If UDP is selected, proceed to step 9. | system logging actions remote destination { name } [tls udp] [host { hostname } ipv4 { IP address }] port { port } |
| 6 | For TLS connections, select an asymmetric key and client certificate to use for authentication with the remote syslog server. | tls client-identity certificate keystore-reference asymmetric- key { key } certificate { certificate } |
| 7 | Exit to the top level. | top |
| 8 | For TLS connections, select a CA certificate. | system logging actions remote destination { name } tls server- authentication ca-certs truststore-reference { CA certificate } |
| 9 | Commit the changes. | commit |
| 10 | Exit configuration mode. | end |
| 11 | Verify the configuration. | show running-config system logging actions remote destination |

Example

The following defines a UDP connection to a remote syslog server (rlog) on port 514 that will only receive messages from the auth log with a severity of critical or higher.

```
localhost# config
localhost(config)# system logging actions remote destination rlog
localhost(config-destination-rlog)# facility-filter facility-list auth
critical
localhost(config-facility-list-auth/critical)# top
localhost(config)# system logging actions remote destination rlog udp ipv4
172.30.145.28 port 514
localhost(config-destination-rlog)# commit
Commit complete.
localhost(config-destination-rlog)# end
localhost# show running-config system logging actions remote destination
system
logging
actions remote destination rlog
udp ipv4 172.30.145.28
facility-filter facility-list auth critical
exit

exit

exit

exit
```

Example

The following defines a TLS connection to a remote syslog server (rlog) on port 6514 that will only receive messages from the auth log with a severity of critical or higher.

```
localhost# config
localhost(config)# system logging actions remote destination rlog
localhost(config-destination-rlog)# facility-filter facility-list auth
critical
localhost(config-facility-list-auth/critical)# top
localhost(config)# system logging actions remote destination rlog tls ipv4
172.30.145.28 port 6514
localhost(config-destination-rlog)# tls client-identity certificate
keystore-reference asymmetric-key AK1 certificate CN1
localhost(config-keystore-reference)# top
localhost(system)# system logging actions remote destination rlog tls
server-authentication ca-certs truststore-reference BN1
localhost(config-destination-rlog)# commit
Commit complete.
localhost(config-destination-rlog)# end
localhost# show running-config system logging actions remote destination
system
logging
actions remote destination rlog
tls ipv4 172.30.145.28
tls client-identity certificate keystore-reference
asymmetric-key AK1
certificate CN1
exit

tls server-authentication ca-certs truststore-reference BN1
facility-filter facility-list auth critical
exit

exit

exit

exit
```

15.3.3.2 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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | <p>Choose which event messages are selected based on their associated facility and severity.</p> <p>Options for facility include:</p> <ul style="list-style-type: none"> • <code>all</code> - All facilities • <code>auth</code> - Authentication- and authorization-related messages • <code>authpriv</code> - Non-system authorization-related messages • <code>daemon</code> - System daemon-related messages • <code>kern</code> - Kernel-related messages • <code>mail</code> - Mail related messages • <code>syslog</code> - Systemd-related messages • <code>user</code> - User-related messages <p>Options for severity include:</p> <ul style="list-style-type: none"> • <code>all</code> - Selects all events • <code>alert</code> - Selects alert-level events • <code>critical</code> - Selects critical-level events • <code>emergency</code> - Selects emergency-level events • <code>error</code> - Selects error-level events • <code>info</code> - Selects info-level events • <code>none</code> - No events are displayed • <code>notice</code> - Selects notice-level events • <code>warning</code> - Selects warning-level events | <pre>system logging actions remote destination { name } facility- filter facility-list [all auth authpriv daemon kern mail syslog user] [all alert critical emergency error info none notice warning]</pre> |

| Step | Instruction | Command |
|------|---|---|
| 3 | Choose whether only the selected event is forwarded, or if the selected event and events with a higher severity level are forwarded. Options include: <ul style="list-style-type: none"> • <code>equals</code> - Only event messages associated with the selected severity are forwarded • <code>equals-or-higher</code> - Event messages associated to the selected severity and higher are forwarded | <code>advanced-compare compare</code> <code>[equals equals-or-higher]</code> |
| 4 | [Optional] Choose whether or not the filtering rule is applied. Options include: <ul style="list-style-type: none"> • <code>log</code> - The rule is applied. • <code>block</code> - The rule is ignored. Use this option for troubleshooting purposes. Default: <code>log</code> | <code>advanced-compare action [log block]</code> |
| 5 | Commit the changes. | <code>commit</code> |
| 6 | Exit configuration mode. | <code>end</code> |
| 7 | Verify the configuration. | <code>show running-config system logging actions remote destination { name } facility-filter facility-list</code> |

Example

Forward only event messages belonging to the `syslog` facility that have a severity level of error or higher. Event messages with a severity level lower than error are not forwarded.

```
localhost# config
localhost(config)# system logging actions remote destination rsysl facility-
filter facility-list syslog error
localhost(config-facility-list-syslog/error)# advanced compare equals-or-
higher
localhost(config-facility-list-syslog/error)# commit
Complete complete.
localhost(config-facility-list-syslog/error)# end
localhost# show running-config system logging actions remote destination
rsysl facility-filter facility-list
system
logging
actions remote destination rsysl
facility-filter facility-list syslog error
exit
exit

exit

exit
```

15.3.4 Monitoring the system log

This section describes how to access the logbook and work with system log files.

15.3.4.1 Displaying the logbook

To display the logbook in the console, execute the following command in operational mode:

```
show system logging logbook
```

Note

If a filter is applied to the logbook, text for entries that do not match the filtering rule is hidden.

Example

```
localhost# show system logging logbook | notab
system logging logbook log-list
time      2021-01-03T02:49:15-00:00
host      localhost
uptime    5D16h24m42s
program   dmfd
severity  info
message   INFO: User 'admin' logged
system logging logbook log-list
time      2021-01-03T02:49:24-00:00
host      localhost
uptime    5D16h24m42s
program   dmfd
severity  info
message   INFO: User 'admin' logged in via cli from 192.168.11.200:65217
with ssh using local authentication
```

Description

For information about how system log entries are constructed, refer to "Structure of a syslog entry (Page 626)".

15.3.4.2 Clearing the logbook

To clear entries from the logbook, execute the following command in operational mode:

```
system logging logbook clear
```

All entries displayed previously in the logbook are removed. The logbook will collect new messages from this point forward as events occur.

Note

Clearing the logbook does not clear the system log.

Upon clearing the logbook, a new entry is automatically added indicating a specific user has cleared the logging buffer. For example:

```
TIME                HOST      UPTIME   PROGRAM SEVERITY
MESSAGE
2021-06-11T01:48:19+00:00 localhost 1h48m19s dmfd      notice
Console: User admin has cleared the logging buffer.
```

Example

```
localhost# show system logging logbook | notab
system logging logbook log-list
time      2021-01-03T02:49:15-00:00
host      localhost
uptime    182955
program   dmfd
severity  info
message   INFO: User 'admin' logged
system logging logbook log-list
time      2021-01-03T02:49:24-00:00
host      localhost
uptime    182964
program   dmfd
severity  info
message   INFO: User 'admin' logged in via cli from
192.168.11.200:65217 with ssh using local authentication
localhost# system logging logbook clear
localhost# show system logging logbook
% No entries found.
```

15.3.4.3 Clearing local system log files

The logbook is converted to a series of system log files when a user downloads the logbook from the device. When these files are present, SINEC OS updates them automatically with new log entries. If needed, however, you can also remove (clear) these files. They will be regenerated when you or another user downloads them from the device.

To clear the local system log files from the device, enter the following command in operational mode:

```
system logging files clear
```

15.3.4.4 Exporting the system log

In addition to forwarding select log entries to a remote system log server, the system log can be exported in its entirety to a local server.

All logs are saved in a single compressed ZIP file.

To export the complete system log, execute the following command in operational mode:

```
system service log-files save target { URL }
```

The URL must define the protocol (i.e. FTP, TFTP, SFTP, or HTTP), the IP address or hostname of the local server, the path to the destination folder, and the name of the file.

Note

For information about how to define a URL using one of the supported protocols, refer to "Specifying a URL (Page 67)".

Example

```
localhost# system service log-files save target http://192.168.20.10/
syslog.zip
```

15.3.5 Configuration examples

The following are examples of how to use the system log.

15.3.5.1 Filtering the logbook

In the following example, logbook is configured to only display events with the severity error. All other events are hidden.

```
localhost# config
localhost(config)# system logging actions logbook severity error
advanced-compare compare equals
localhost(config)# commit
Commit complete.
localhost(config)# end
```

Alternatively, the same rule can be modified to show all messages with severity error and higher. Events with severity warning or lower are hidden.

```
localhost# config
localhost(config)# system logging actions logbook severity error
advanced-compare compare equals-or-higher
localhost(config)# commit
Commit complete.
localhost(config)# end
```

15.3.5.2 Filtering messages forwarded to remote syslog servers

The following examples demonstrate how to control the forwarding of event messages to the remote syslog server(s).

Defining a range of event messages to forward

The following makes sure that all critical-level event messages and higher from the syslog and auth facilities are forwarded to **rsys1**.

```
localhost# config
```

```
localhost(config)# system logging actions remote destination rsysl
facility-filter facility-list syslog critical advanced-compare
compare equals-or-higher
localhost(config)# commit
Commit complete.
localhost(config)# end
```

Forwarding event messages with specific severities

The following builds on the previous example and adds specifically event messages with a severity of error.

```
localhost# config
localhost(config)# system logging actions remote destination rsysl
facility-filter facility-list syslog critical advanced-compare
compare equals-or-higher
localhost(config)# system logging actions remote destination rsysl
facility-filter facility-list syslog error advanced-compare compare
equals
localhost(config)# commit
Commit complete.
localhost(config)# end
```

Ignoring a rule using the block action

If you want to temporarily block messages captured by a rule set in the previous example to observe the results, set its action to block.

```
localhost# config
localhost(config)# system logging actions remote destination rsysl
facility-filter facility-list syslog critical advanced-compare
action block
localhost(config)# commit
Commit complete.
localhost(config)# end
```

Ignoring all messages from a specific facility

To prevent all messages from a specific facility from being forwarded, set the severity for the facility to `none`. Note this rule is negated if other rules are applied to the same facility.

```
localhost# config
localhost(config)# system logging actions remote destination rsysl
facility-filter facility-list syslog none
localhost(config)# commit
Commit complete.
localhost(config)# end
```

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 management 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 641)".

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 |

| Resource | Event ID | Default severity |
|-------------|---------------------------|------------------|
| 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 660)".

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 <i>None</i> 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 <i>None</i> 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 <i>None</i> 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 messages "{ 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 messages "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 "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 | Static message "Bouncing link detected or disappeared on a port." Dynamic message "Bouncing link [is was] detected [on port { port number }]." | 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 | Static message "BPDU Guard activated on a port." Dynamic message "Port { port number } BPDU Guard activated." | 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 | Static message "Inconsistent speed detected or disappeared on a port." Dynamic message "Inconsistent speed [is was] detected on port { port number }." | 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 | Static message "Monitoring device with configured IP can't be reached." 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." | The packet analyzer/sniffer (monitoring device to which mirrored traffic is sent) is unreachable. | If the packet analyzer/sniffer is on the same subnet (local), make sure the device is operational. If the packet analyzer/sniffer is on a different subnet (remote), verify the gateway configuration and/or make sure the device is operational. |
| Fast-link-detection-disabled | No | Warning | Static message "FLD disabled or enabled on a port." Dynamic message "Bouncing link [was] detected [on port { port number }] [, disabling FLD]." | 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 | Static message "Looped back BPDU received on a port." Dynamic message "Port { port number } received looped back BPDU." | A looped back BPDU is detected on the specified bridge port. This can happen when: <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. | Based on the possible reasons given, do the following: <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 | Static message "Unresolved speed detected or disappeared on a port." Dynamic message "[Was] [Unable unable] to obtain speed information from port { port number }." | Unable to determine the speed capabilities of the specified port. | Contact Siemens Customer Support. |
| Gmrp-cannot-learn-more-addresses | Yes | Alert | Static message <i>None</i> Dynamic message "GMRP cannot learn more addresses." | The maximum number of learned multicast groups has been reached. | Wait until learned groups no longer required by hosts are removed dynamically. |
| Gvvp-cannot-learn-more-vlans | Yes | Alert | Static message <i>None</i> Dynamic message "GVRP cannot learn more VLANs." | The device has reached the maximum number of supported VLANs. | Either remove static VLANs or wait for VLANs to be removed dynamically. |

| 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 Alarms

| Related event | Conditional | Severity | Alarm message | Description | Suggested resolution |
|---------------------|-------------|----------|---|--|---|
| Expired-certificate | No | Error | Static message "The TLS certificate is expired." Dynamic message "Certificate validation failed; subject='{ subject }', issuer='{ issuer }', error='certificate has expired', depth='{ depth }'" | The certificate for a TLS session has expired. | Replace the certificate used for the specified TLS session. |
| Invalid-certificate | No | Error | Static message "The TLS certificate is invalid." Dynamic message "Certificate validation failed; subject='{ subject }', issuer='{ issuer }', error='{ error details }', depth='{ depth }'" | The certificate for a TLS session is invalid. | Replace the certificate used for the specified TLS session. |

15.4.2 Configuring events

To configure individual events, do the following:

- [Optional] Enable the event to generate an alarm.
For more information, refer to "Enabling an event to generate an alarm (Page 652)".
- [Optional] Set the event severity.
For more information, refer to "Defining the severity for an event (Page 653)".
- [Optional] Enable the event to activate the signaling contact (if equipped).
For more information, refer to "Enabling an event to activate the signaling contact (Page 656)".
- [Optional] Enable the event to illuminate the Alarm LED.
For more information, refer to "Enabling an event to activate the alarm LED (Page 657)".
- [Optional] Enable the event to issue e-mail notifications to select recipients via SMTP.
For more information, refer to "Enabling an event to issue an e-mail notification (Page 654)".
- [Optional] Enable the event to trigger SNMP traps.
For more information, refer to "Enabling an event to trigger an SNMP trap (Page 655)".
- [Optional] Enable the event to clear automatically when the original condition is resolved.
For more information, refer to "Enabling alarms to clear automatically (Page 658)".
- [Optional] Enable the event.
For more information, refer to "Enabling an event (Page 659)".

15.4.2.1 Enabling an event to generate an alarm

Most events are associated with an alarm that is generated when the event occurs. The alarm message appears in the alarm list and/or system log.

An event's ability to generate an alarm is configurable.

Note

If attempting to enable alarms for an event that is not associated with an alarm, the following error message is generated in the system log:

```
This change is not allowed when event type is not alarm.
```

For more information about which events are associated with an alarm, refer to "Resources and events (Page 641)".

Note

Whether an alarm is enabled for an event or not, a **Cleared** event is logged in the system log when the event clears. For example:

```
1970-01-01T00:38:21+00:00 X-300-CSRpdefault 38m21s switch-mgmt info
Cleared event, resource:switch-mgmt, id:Mcast-cpu-filtering-table-
full, message:Can't filter more mcast streams from CPU
```

To enable an event to generate an alarm when the event occurs, do the following:

| Step | Instruction | Command |
|------|---------------------------------------|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable alarms for the selected event. | <code>system events event-config event { resource } { event ID } alarm</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system events event-config event { resource } { event ID } alarm</code> |

Example

The following enables alarms for the **Bouncing-link** event.

```
localhost# config
localhost(config)# system events event-config event switch-mgmt Bouncing-
link alarm
localhost(config-event-switch-mgmt/Bouncing-link)# commit
Commit complete.
localhost(config-event-switch-mgmt/Bouncing-link)# end
localhost# show running-config system events event-config event switch-mgmt
Bouncing-link alarm
system
  events
    event-config
      event switch-mgmt Bouncing-link
      alarm
    exit
  exit
exit
exit
```

15.4.2.2 Defining the severity for an event

To define the severity associated with an event, do the following:

Note

The severity of an event should only be changed if its default severity is *error*, *info*, *notice*, or *warning*. And it should only be changed to one of those severity levels. Do not, for instance, change *emergency* to *notice*, as high severity events will not be properly highlighted in the system log.

For information about the available severity levels, refer to "Severity levels (Page 641)".

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Define the severity level for the selected event. Options include: <ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • info | <code>system events event-config event { Resource } { Event ID } severity [emergency alert critical error warning notice info]</code> |
| 3 | Commit the change. | <code>commit</code> |

| Step | Instruction | Command |
|------|---------------------------|--|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system events event-config event { Resource } { Event ID } severity |

Example

The following changes the severity for the **Bouncing-link** event to alert.

```
localhost# config
localhost(config)# system events event-config event switch-mgmt
Bouncing-link severity alert
localhost(config-event-switch-mgmt/Bouncing-link)# commit
Commit complete.
localhost(config-event-switch-mgmt/Bouncing-link)# end
localhost# show running-config system events event-config event
switch-mgmt Bouncing-link severity
system
events
event-config
event switch-mgmt Bouncing-link
severity alert
exit

exit

exit

exit
```

15.4.2.3 Enabling an event to issue an e-mail notification

Events can be configured to send an e-mail notification to users when the event occurs. The e-mail includes identifying information about the device, a timestamp, and details about the event.

Note

E-mail notifications are sent via the Simple Mail Transfer Protocol (SMTP). SMTP must be enabled and configured for administrators to be alerted by e-mail when an event occurs.

For more information, refer to "SMTP (Page 663)".

To enable an event to send an e-mail notification when the event occurs, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable e-mail notifications for the selected event. | system events event-config event { Resource } { Event ID } email |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------|--|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system events event-config event { Resource } { Event ID } email |

Example

The following enables e-mail notifications for the **Bouncing-link** event.

```
localhost# config
localhost(config)# system events event-config event switch-mgmt
Bouncing-link email
localhost(config-event-switch-mgmt/Bouncing-link)# commit
Commit complete.
localhost(config-event-switch-mgmt/Bouncing-link)# end
localhost# show running-config system events event-config event
switch-mgmt Bouncing-link email
system
  events
    event-config
      event switch-mgmt Bouncing-link
      email
    exit
  exit
exit
exit
exit
```

15.4.2.4 Enabling an event to trigger an SNMP trap

To enable an event to trigger an SNMP trap, do the following:

Note

For an event to trigger an SNMP trap, SNMP must first be configured and enabled.

For more information, refer to "SNMP (Page 475)".

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable SNMP traps for the selected event. | system events event-config event { resource } { event ID } snmp- trap |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------|--|
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system events event-config event { resource } { event ID } snmp- trap |

Example

The following enables the **Bouncing-link** event to trigger an SNMP trap.

```
localhost# config
localhost(config)# system events event-config event switch-mgmt Bouncing-
link snmp-trap
localhost(config-event-switch-mgmt/Bouncing-link)# commit
Commit complete.
localhost(config-event-switch-mgmt/Bouncing-link)# end
localhost# show running-config system events event-config event switch-mgmt
Bouncing-link snmp-trap
system
  events
    event-config
      event switch-mgmt Bouncing-link
      snmp-trap
    exit
  exit
exit
exit
exit
```

15.4.2.5 Enabling an event to activate the signaling contact

The signaling contact on the device can be activated (open) automatically when the alarm is generated. This behavior is disabled by default for some events.

Note**Requirement**

Events must be configured to generate an alarm to also active the signaling contact.

For more information, refer to "Enabling an event to generate an alarm (Page 652)".

Note

By default, the signaling contact is activated by events that are set to open it when the event occurs. However, the signaling contact can be configured to ignore events and stay in an open or closed state at all times.

For more information about controlling the state of the signaling contact, refer to "Signaling contact (Page 146)".

To enable an event to activate the signaling contact, do the following:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the selected event to activate the signaling contact. | <code>system events event-config event { resource } { event ID } signaling-contact</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system events event-config event { resource } { event ID } signaling-contact</code> |

Example

The following enables the **Bouncing-link** event to activate the signaling contact when the event occurs.

```
localhost# config
localhost(config)# system events event-config event switch-mgmt Bouncing-link signaling-contact
localhost(config-event-switch-mgmt/Bouncing-link)# commit
Commit complete.
localhost(config-event-switch-mgmt/Bouncing-link)# end
localhost# show running-config system events event-config event switch-mgmt Bouncing-link signaling-contact
system
 events
  event-config
    event switch-mgmt Bouncing-link
      signaling-contact
    exit
  exit
exit
exit
```

15.4.2.6 Enabling an event to activate the alarm LED

Events can be configured to activate the Alarm LED on the device when the event occurs. This behavior is disabled by default for some events.

Note

Requirement

Events must be configured to generate an alarm to also activate the Alarm LED.

For more information, refer to "Enabling an event to generate an alarm (Page 652)".

To enable an event to activate the Alarm LED when the event occurs, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable the selected alarm to activate the Alarm LED on the device. | system events event-config event { resource } { event ID } led |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system events event-config event { resource } { event ID } led |

Example

The following enables the **Bouncing-link** event to activate the Alarm LED when the event occurs.

```
localhost# config
localhost(config)# system events event-config event switch-mgmt Bouncing-link led
localhost(config-event-switch-mgmt/Bouncing-link)# commit
Commit complete.
localhost(config-event-switch-mgmt/Bouncing-link)# end
localhost# show running-config system events event-config event switch-mgmt
Bouncing-link led
system
  events
    event-config
      event switch-mgmt Bouncing-link
        led
      exit
    exit
  exit
exit
```

15.4.2.7 Enabling alarms to clear automatically

To enable the alarm raised by an event to automatically clear once the underlying condition that caused the event is resolved and acknowledged, do the following:

Note

The auto-clear option can only be enabled for non-conditional alarms. Conditional alarms clear automatically, as long as the condition that triggered the event no longer exists.

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | config |
| 2 | Set the selected alarm to clear itself automatically. | system events event-config event { resource } { event ID } auto-clear |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system events event-config event { resource } { event ID } auto-clear |

Example

The following enables the alarm generated by the **Bouncing-link** event to automatically clear from the alarms list when the underlying condition is resolved and acknowledged.

```
localhost# config
localhost(config)# system events event-config event switch-mgmt Bouncing-link auto-clear
localhost(config-event-switch-mgmt/Bouncing-link)# commit
Commit complete.
localhost(config-event-switch-mgmt/Bouncing-link)# end
localhost# show running-config system events event-config event switch-mgmt Bouncing-link auto-clear
system
 events
  event-config
    event switch-mgmt Bouncing-link
      auto-clear
    exit
  exit
exit
exit
```

15.4.2.8 Enabling an event

To enable an event, do the following:

| Step | Instruction | Command |
|------|----------------------------|---|
| 1 | Enter configuration mode. | config |
| 2 | Enable the selected event. | system events event-config event { resource } { event } enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system events event-config event { resource } { event } enabled |

Example

The following enables the **Bouncing-link** event.

```
localhost# config
localhost(config)# system events event-config event switch-mgmt Bouncing-
link enabled
localhost(config-event-switch-mgmt/Bouncing-link)# commit
Commit complete.
localhost(config-event-switch-mgmt/Bouncing-link)# end
localhost# show running-config system events event-config event switch-mgmt
Bouncing-link enabled
system
  events
    event-config
      event switch-mgmt Bouncing-link
      enabled
    exit
  exit
exit
exit
exit
```

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, execute the following command in operational mode:

```
show system events alarm-list
```

Alarms can also be listed in reverse chronological order by executing the following command:

```
show system events alarm-time-order
```

Example

The following displays active alarms.

```
localhost# show system events alarm-list
alarm-list alarm device-mgmt Authentication-failure "A user failed
to login due to incorrect authentication credentials."
  event-number      2
  severity          warning
  date-time         "Fri Jun 11 22:52:59 2021"
  user-actions      clear-or-ack
  actuators-status none
alarm-list alarm switch-mgmt Linkdown/linkup "Link status changed
on a port"
  event-number      1
  severity          info
  date-time         "Fri Jun 11 22:36:12 2021"
```

```

user-actions      clear-or-ack
actuators-status none

```

Example

The following displays active alarms in reverse chronological order.

```

localhost# show system events alarm-time-order
alarm-time-order
date-time         "Fri Jun 11 22:52:59 2021"
resource          device-mgmt
event-id          Authentication-failure
message           "A user failed to login due to incorrect
authentication credentials."
event-number      2
severity          warning
user-actions      clear-or-ack
actuators-status none
alarm-time-order
date-time         "Fri Jun 11 22:36:12 2021"
resource          switch-mgmt
event-id          Linkdown/linkup
message           "Link status changed on a port"
event-number      1
severity          info
user-actions      clear-or-ack
actuators-status none

```

Example

The following is the result when there no alarms are active.

```

localhost# show system events alarm-list
% No entries found

```

Description

The following is displayed for each active alarm:

| Parameter | Description |
|--------------|---|
| 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. |
| date-time | The date and time at which the event occurred. |

| Parameter | Description |
|------------------|--|
| user-actions | 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.

Clearing/acknowledging all active alarms

To clear all active alarms, execute the following command in operational mode:

Note

Only non-conditional alarms can be cleared.

```
system events alarm-list clear-all
```

To acknowledge all active alarms, execute the following command in operational mode:

```
system events alarm-list acknowledge-all
```

Clearing/acknowledging select alarms

To clear a specific non-conditional alarm, execute the following command in operational mode:

```
system events alarm-list alarm { Resource } { Event ID }
{ Message } clear
```

To acknowledge a specific conditional alarm, execute the following command in operational mode:

```
system events alarm-list alarm { Resource } { Event ID }
{ Message } acknowledge
```

Example

The following clears the non-conditional **Bouncing-link** alarm.

```
localhost# system events alarm-list alarm switch-mgmt Bouncing-link
"Bouncing link detected or disappeared on a port" clear
```

Are you sure you want to clear the system alarm? [no,yes] yes

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, refer to "Enabling an event to issue an e-mail notification (Page 654)".

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:

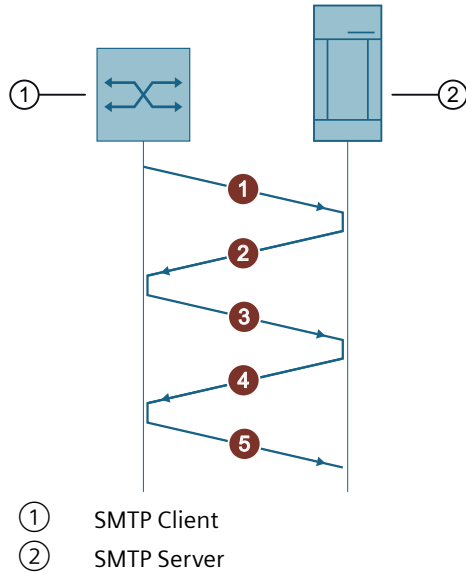


Figure 15-1 SMTP Communication Sequence

| 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 665)".
2. Configure the SMTP user account.
For more information, refer to "Configuring the SMTP account (Page 667)".
3. Configure the SMTP server settings.
For more information, refer to "Configuring the SMTP server (Page 669)".
4. Test the server connection.
For more information, refer to "Testing the SMTP server connection (Page 666)".
5. Enable SMTP.
For more information, refer to "Enabling SMTP (Page 666)".

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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Add an e-mail address to the recipients list. | <code>system smtp recipients { address }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system smtp recipients</code> |

Example

```
localhost# config
localhost(config)# system smtp recipients winston.smith@company.com
localhost(config)# commit
Commit complete.
localhost(config)# end
localhost# show running-config system smtp recipients
system
smtp
recipients [ winston.smith@company.com emmanuel.goldstein@company.com ]
exit

exit
```

15.5.2.2 Testing the SMTP server connection

To test the SMTP server connection, enter the following command in operational mode:

```
system smtp 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 667)".

| Step | Instruction | Command |
|------|---------------------------|----------------------------------|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Enable the SMTP service. | <code>system smtp enabled</code> |

| Step | Instruction | Command |
|------|---------------------------|---|
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system smtp enabled |

Example

```
localhost# config
localhost(config)# system smtp enabled
localhost(config-system-smtp)# commit
Commit complete.
localhost(config-system-smtp)# end
localhost# show running-config system smtp enabled
system
  smtp
    enabled
  exit

exit
```

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 667)".
2. [Optional] Add a description for the address.
For more information, refer to "Adding a description for the account (Page 668)".

15.5.3.1 Configuring the account e-mail address

To define the e-mail account from which SMTP sends all event messages, do the following:

| Step | Instruction | Command |
|------|---------------------------|--|
| 1 | Enter configuration mode. | config |
| 2 | Set the e-mail address. | system smtp account email-address { address } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system smtp account e-mail-address |

Example

```

localhost# config
localhost(config)# system smtp account email-address alerts@company.com
localhost(config-smtp-account)# commit
Commit complete.
localhost(config-smtp-account)# end
localhost# show running-config system smtp account email-address
system
  smtp
    account
      email-address alerts@company.com
    exit
  exit
exit
exit

```

15.5.3.2 Adding a description for the account

To give a description to the SMTP account, do the following:

| Step | Instruction | Command |
|------|---|--|
| 1 | Enter configuration mode. | config |
| 2 | Define a description for the SMTP account. If the string you enter includes spaces, it must either be wrapped in double-quotes ("") or you can press Enter after <code>description</code> to enter wizard mode. Condition: <ul style="list-style-type: none"> Must be between 1 and 128 characters long | system smtp account description { description } system smtp account description (<string, min: 1 chars, max: 128 chars>): { description } |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system smtp account description |

Example

```

localhost# config
localhost(config)# system smtp account description "System alerts"
localhost(config-smtp-account)# commit
Commit complete.
localhost(config-smtp-account)# end
localhost# show running-config system smtp account description
system
smtp
  account
  description "System alerts"
  exit

exit

exit

```

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 669)".
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 670)".
3. [Optional] Configure the SMTP client to authenticate itself with the SMTP server.
For more information, refer to "Configuring SMTP authentication (Page 671)".

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:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the hostname or IP address of the SMTP server. Condition: <ul style="list-style-type: none"> The hostname can be between 0 and 253 characters long | IPv4 Address <code>system smtp account server ipv4 { IP address }</code> Hostname <code>system smtp account server host { hostname }</code> |

| Step | Instruction | Command |
|------|--|---|
| 3 | Set the port on which the SMTP server receives messages. Default: 25 | port { 1 - 65535 } |
| 4 | [Optional] Set a description for the SMTP server. If the string you enter includes spaces, it must either be wrapped in double-quotes (") or you can press Enter after description to enter wizard mode. Condition: <ul style="list-style-type: none"> Must be between 1 and 128 characters long | description { description } description (<string, min: 1 chars, max: 128 chars>): { description } |
| 5 | Commit the changes. | commit |
| 6 | Exit configuration mode. | end |
| 7 | Verify the configuration. | show running-config system smtp account server |

Example

```
localhost# config
localhost(config)# system smtp account server ipv4 172.30.145.128
localhost(config-smtp-server)# port 1
localhost(config-smtp-server)# description "E-mail service"
localhost(config-smtp-server)# commit
Commit complete.
localhost(config-smtp-server)# end
localhost# show running-config system smtp account server
system
smtp
account
server
description "E-mail service"
address 172.30.145.128
port 1
exit

exit

exit
```

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 set how long the SMTP client will wait for a response from the SMTP server, do the following:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the time the SMTP client will wait for a response from the SMTP server. Conditions: <ul style="list-style-type: none"> Formatted as nYnMnDnhnmns, where n is a user-defined number Minimum of 1 second (1s) Maximum of 255 seconds (255s) Default: 30s (30 seconds) | <code>system smtp account server timeout [1s - 255s]</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config system smtp account server timeout</code> |

Example

```
localhost# config
localhost(config)# system smtp account server timeout 30s
localhost(config-smtp-server)# commit
Commit complete.
localhost(config-smtp-server)# end
localhost# show running-config system smtp account server timeout
system
smtp
  account
  server
  timeout 30s
  exit

exit

exit

exit
```

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 672)".
3. Enable SMTP authentication. For more information, refer to "Enabling SMTP authentication (Page 673)".

15.5.5.1 Configuring the SMTP user

To configure the SMTP user, do the following:

| Step | Instruction | Command |
|------|--|--|
| 1 | Enter configuration mode. | <code>config</code> |
| 2 | Set the username associated with the account on the SMTP server. If the username includes special characters, wrap it in double-quotes (") or press Enter to enter wizard mode. Conditions: <ul style="list-style-type: none"> • 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 (@) | <pre>system smtp account authentication username { user nName } system smtp account authentication username (<strng, min: 1 chars, max: 128 chars>): { user name }</pre> |
| 3 | Set the password associated with the username. The password is displayed in plain text when entered directly after the <code>password</code> parameter. To avoid this, press Enter to enter wizard mode. Condition: <ul style="list-style-type: none"> • Must be between 1 and 128 characters | <pre>password { password } password (<AES encyrpted string>): { password }</pre> |
| 4 | Confirm the password. | <pre>password-confirm { password } password-confirm (<AES encyrpted string>): { password }</pre> |
| 5 | Commit the changes. | <code>commit</code> |
| 6 | Exit configuration mode. | <code>end</code> |
| 7 | Verify the configuration. | <code>show running-config system smtp account authentication</code> |

Example

```

localhost# config
localhost(config)# system smtp account authentication username wsmith
localhost(config-smtp-auth)# password
(<AES encrypted string>): *****
localhost(config-smtp-auth)# password-confirm
(<AES encrypted string>): *****
localhost(config-smtp-auth)# commit
Commit complete.
localhost(config-smtp-auth)# end
localhost# show running-config system smtp account authentication
system
smtp
  account
  authentication
    enabled
    username wsmith
    password $8$k5UjF4TQFE0LUZpUTVsbuqayYkyfxx10QE/UFdKMyw8=
  exit

exit

exit

exit

```

15.5.5.2 Enabling SMTP authentication

To enable SMTP user authentication, do the following:

Note

SMTP user authentication is disabled by default.

| Step | Instruction | Command |
|------|-----------------------------|--|
| 1 | Enter configuration mode. | config |
| 2 | Enable SMTP authentication. | system smtp account authentication enabled |
| 3 | Commit the change. | commit |
| 4 | Exit configuration mode. | end |
| 5 | Verify the configuration. | show running-config system smtp account authentication enabled |

Example

```

localhost# config
localhost(config)# system smtp account authentication enabled
localhost(config-smtp-auth)# commit
Commit complete.
localhost(config-smtp-auth)# end

```

```
localhost# show running-config system smtp account authentication
enabled
system
smtp
account
authentication
enabled
exit

exit

exit

exit
```

15.5.6 Displaying the status of SMTP

To display the current status of the SMTP service, enter the following command in operational mode:

```
show system smtp status
```

This displays operational state of the service, selected e-mail recipients, the account information, and server settings.

Example

```
localhost# show system smtp status
status enabled true
status recipients "emmanuel.goldstein@company.com;
winston.smith@company.com"
status account email-address alerts@company.com
status account authentication-enabled true
status account server port 25
status account server timeout 30
```

15.5.7 Configuration examples

The following are examples of how to deploy SMTP.

15.5.7.1 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 on port 25.

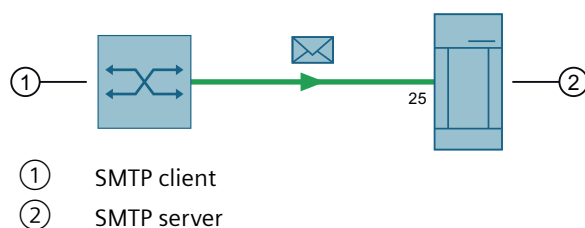


Figure 15-2 Sending e-mail notifications to an SMTP server

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 667)".
2. Set the SMTP server and port number.
For more information, refer to "Configuring the SMTP server profile (Page 669)".
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 670)".
4. Set the SMTP username known to the SMTP server.
For more information, refer to "Configuring the SMTP user (Page 672)".
5. Enable SMTP authentication.
For more information, refer to "Enabling SMTP authentication (Page 673)".
6. Set the e-mail recipients.
For more information, refer to "Adding e-mail recipients (Page 665)".
7. Enable the SMTP service.
For more information, refer to "Enabling SMTP (Page 666)".
8. Configure one or more alarms to send an e-mail notification via SMTP.
For more information, refer to "Enabling an event to issue an e-mail notification (Page 654)".
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, the mirrored traffic can be forwarded using Encapsulated Remote Traffic Mirroring (ERTM) to a connected device on which an installed packet analyzer/sniffer can be reached via an IP address. ERTM encapsulates mirrored traffic with MAC, IP, and GRE headers and routes it over a GRE tunnel on a Layer 3 network. The encapsulated traffic is forwarded to the analyzer in the same way as normal Layer 3 traffic, which decapsulates the traffic if necessary before analysis.

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.
- Network management frames generated by the device (e.g. RSTP, GVRP, etc.) cannot 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.
- Bridge ports designated as the mirroring destination do not support bi-directional traffic. All ingress traffic is dropped and the source MAC address is not learned.

15.6.1.4 Traffic mirroring and ARP

For long traffic mirroring sessions, it is recommended to configure the analyzer to ping the device periodically. This will prevent the analyzers IP address from being removed from the mirroring port's ARP table.

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 677)".
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 a mirroring destination (Page 679)".
3. Enable traffic mirroring.
For more information, refer to "Enabling traffic mirroring (Page 681)".

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:

| Step | Instruction | Command |
|------|--|---|
| 1 | Enter global configuration mode. | <code>config</code> |
| 2 | Select a traffic source. This can be either a bridge port or a VLAN. For bridge ports, the direction of traffic must be defined. Options include: <ul style="list-style-type: none"> <code>ingress</code> - Traffic received by the port is mirrored <code>egress</code> - Traffic forwarded by the port is mirrored <code>both</code> - Traffic received or forwarded by the port is mirrored Default: <code>both</code> | Bridge port <code>switch traffic-mirroring session { session } source ports { bridge port } direction [ingress egress both]</code> VLAN <code>switch traffic-mirroring session { session } source vlans { VLAN ID }</code> |
| 3 | Commit the change. | <code>commit</code> |
| 4 | Exit global configuration mode. | <code>end</code> |
| 5 | Verify the configuration. | <code>show running-config switch traffic-mirroring session { session } source</code> |

Example

The following configures session 1 to only mirror the traffic received by bridge port ethernet0/3.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch traffic-mirroring session 1 source ports
ethernet0/3
localhost(config-ports-ethernet0/3)# direction ingress
localhost(config-ports-ethernet0/3)# commit
Commit complete.
localhost(config-ports-ethernet0/3)# end
localhost# show running-config switch traffic-mirroring session 1 source
switch
  traffic mirroring
    session 1
      source port ethernet0/3
      direction ingress
    exit
  exit
exit
exit
```

Example

The following configures session 1 to additionally mirror any traffic belonging to VLAN 10.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch traffic-mirroring session 1 source vlans 10
localhost(config-ports-ethernet0/3)# commit
Commit complete.
localhost(config-ports-ethernet0/3)# end
localhost# show running-config switch traffic-mirroring session 1 source
switch
  traffic mirroring
    session 1
      source vlans [ 10 ]
      source port ethernet0/3
      direction ingress
    exit
  exit
exit
exit
exit
```

15.6.2.2 Configuring a mirroring destination

Mirrored traffic can be forwarded to a bridge port 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:

| Step | Instruction | Command |
|------|---|---|
| 1 | Enter global configuration mode. | config |
| 2 | Configure the destination. The destination can be either: <ul style="list-style-type: none"> A bridge port (either one connected to a traffic analyzer or one that leads to another Layer 2 device on the network that is connected to a traffic analyzer) The IP address of the packet analyzer/sniffer | Bridge port switch traffic-mirroring session { session } destination port { bridge port } IP address switch traffic-mirroring session { session } destination ertm-ip { IP address } |
| 3 | Commit the change. | commit |

| Step | Instruction | Command |
|------|---------------------------------|---|
| 4 | Exit global configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch traffic-mirroring session { Ssession } destination |

Example

The following configures session 1 to forward mirrored traffic on ethernet0/2.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch traffic-mirroring session 1 destination ports
ethernet0/2
localhost(config-ports-ethernet0/2)# commit
Commit complete.
localhost(config-ports-ethernet0/2)# end
localhost# show running-config switch traffic-mirroring session 1
destination
switch
  traffic mirroring
    session 1
      destination port ethernet0/2
    exit
  exit
exit
```

Example

The following configures session 1 to forward mirrored traffic to 172.30.141.141.

```
localhost# config
Entering configuration mode terminal
localhost(config)# switch traffic-mirroring session 1 destination ertm-ip
172.30.141.141
localhost(config-ports-ethernet0/2)# commit
Commit complete.
localhost(config-ports-ethernet0/2)# end
localhost# show running-config switch traffic-mirroring session 1
destination
switch
  traffic mirroring
    session 1
      destination ertm-ip 172.30.141.141
    exit
  exit
exit
```


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, any bridge port selected as a mirroring destination 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:

| Step | Instruction | Command |
|------|----------------------------------|--|
| 1 | Enter global configuration mode. | config |
| 2 | Enable traffic mirroring. | switch traffic-mirroring session 1 enabled |
| 3 | Commit the change. | commit |
| 4 | Exit global configuration mode. | end |
| 5 | Verify the configuration. | show running-config switch traffic-mirroring session 1 |

Example

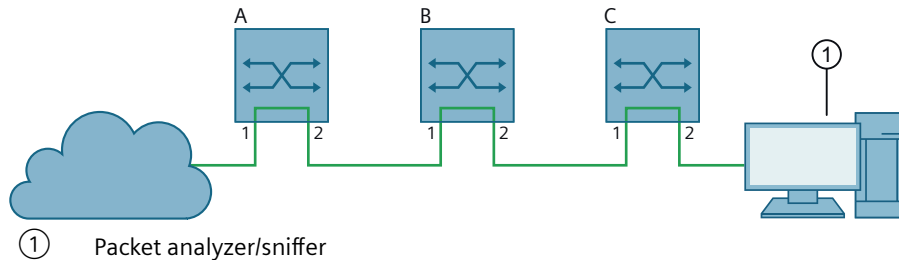
```
localhost# config
Entering configuration mode terminal
localhost(config)# switch traffic-mirroring session 1 enabled
localhost(config-session-1)# commit
Commit complete.
localhost(config-session-1)# end
localhost# show running-config switch traffic-mirroring session 1
switch
  traffic mirroring
    session 1
      destination port ethernet0/1
    exit
  exit
exit
```

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

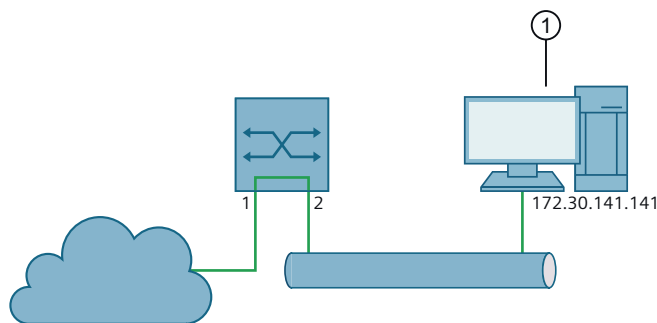
Figure 15-3 Traffic mirroring across a Layer 2 network

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 677)".
2. Set the destination to bridge port ethernet0/2.
For more information, refer to "Configuring a mirroring destination (Page 679)".
3. Enable traffic monitoring.
For more information, refer to "Enabling traffic mirroring (Page 681)".

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 677)".
2. Set the destination to IP address 172.30.141.141.
For more information, refer to "Configuring a mirroring destination (Page 679)".
3. Enable traffic monitoring.
For more information, refer to "Enabling traffic mirroring (Page 681)".

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.

| Step | Instruction | Command |
|------|---|---------|
| 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 | Log on to the device. For more information, refer to "Logging in (Page 112)". | - |

| Step | Instruction | Command |
|------|--|---|
| 4 | <p>Start the cable diagnostic test for the target bridge port.</p> <p>Alternatively, you can start the test for all bridge ports.</p> <p>Test results are displayed immediately once the test is complete.</p> <p>For more information about the test results, refer to "Displaying cable diagnostics results (Page 684)".</p> | <p>Single bridge port</p> <pre>interface { bridge port } cabletest start</pre> <p>All bridge ports</p> <pre>interface ethernet* cabletest start</pre> |
| 5 | <p>[Optional] Reset the bridge port.</p> <p>For more information, refer to "Resetting a bridge port (Page 294)".</p> | <pre>interface { bridge port } ethernet reset</pre> |

Example

The following runs a cable diagnostic test on bridge port ethernet0/3.

```
localhost# interface ethernet0/3 cabletest start
action-start-result cabletest state stopped
cabletest result passed
cabletest result-pair12 good
cabletest distance-pair12 2
cabletest result-pair36 short
cabletest distance-pair36 0
cabletest result-pair45 open
cabletest distance-pair45 05
cabletest result-pair78 good
cabletest distance-pair78 2
```

15.7.2 Displaying cable diagnostics results

Test results can be displayed for all bridge ports or a single bridge port. Only the results of the last cable diagnostic test are displayed for each bridge port.

Displaying test results for all bridge ports

To display the test results for all bridge ports, enter the following command in operational mode:

```
show interface ethernet* cabletest
```

For example:

```
localhost# show interface ethernet* cabletest
interface ethernet0/1
  cabletest state stopped
interface ethernet0/2
  cabletest state stopped
interface ethernet0/3
  cabletest state stopped
  cabletest result passed
  cabletest result-pair12 good
  cabletest distance-pair12 26
  cabletest result-pair36 short
  cabletest distance-pair36 17
  cabletest result-pair45 open
  cabletest distance-pair45 9
  cabletest result-pair78 good
  cabletest distance-pair78 27
interface ethernet0/4
  cabletest state stopped
  cabletest result passed
  cabletest result-pair12 good
  cabletest distance-pair12 0
  cabletest result-pair36 good
  cabletest distance-pair36 2
  cabletest result-pair45 good
  cabletest distance-pair45 2
  cabletest result-pair78 good
  cabletest distance-pair78 2
interface ethernet0/5
  cabletest state stopped
```

Displaying test results for a single bridge port

To display the test results for a single bridge port, enter the following command in operational mode:

```
show interface { bridge port } cabletest
```

For example:

```
localhost# show interface ethernet0/3 cabletest
cabletest state stopped
cabletest result passed
cabletest result-pair12 good
cabletest distance-pair12 26
cabletest result-pair36 short
cabletest distance-pair36 17
cabletest result-pair45 open
cabletest distance-pair45 9
cabletest result-pair78 good
cabletest distance-pair78 27
```

Interpreting the test results

The following information is displayed for each bridge port:

| Result | Description |
|--------------------------------|---|
| <code>state</code> | 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 |
| <code>result</code> | 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 |
| <code>result-pair [N]</code> | The cable test result for the wire pair, where <i>N</i> is either: <ul style="list-style-type: none"> 12 (pair 1/2) 36 (pair 3/6) 45 (pair 4/5) 78 (pair 7/8) Possible values include: <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 For FastEthernet bridge ports, a <code>good</code> result is required for <code>result-pair12</code> and <code>result-pair36</code> . For Gigabit Ethernet bridge ports, a <code>good</code> result is required for all wire pairs. |
| <code>distance-pair [N]</code> | The Distance-to-Fault (DTF) measurement for the wire pair, where <i>N</i> is either: <ul style="list-style-type: none"> 12 (pair 1/2) 36 (pair 3/6) 45 (pair 4/5) 78 (pair 7/8) The measurement is the distance in meters (m) from the device to the fault in the wire. |

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 (Page 26).

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 26)".
- 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 function (Page 148)".

16.2 The device switches off during system startup

You have inserted a CLP on which no firmware is saved into a device with no power and connected the device to the power supply again. During system startup, the device switches itself off independently. A configuration error has occurred and the configuration of the device is no longer usable.

16.3 The device changes the mode of a bridge port (use of DLR in connection with loop detection)

Solution

If the described scenario occurs, follow these steps:

1. Remove the CLP.
2. Restart the device.
You have the following options:
 - Connect the device to the power supply again.
The device starts and activates the backup firmware.
 - Reset the device to default settings with the button during 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 users
- 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. Make sure that the power supply to the device is switched off.
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.

16.3 The device changes the mode of a bridge port (use of DLR in connection with loop detection)

If you use Device Level Ring (DLR) in connection with Loop Detection and errors occur after the firmware version is changed or a configuration file is loaded, check the configuration.

16.4 The device cannot be reached via CLI and Web UI (loading a firmware file via TFTP)

Solution

As of firmware version 2.3, the following two configurations are not possible simultaneously on a bridge port:

- DLR port and DLR enabled
- Loop detection enabled and port mode **sending**

If the device detects such a configuration, it changes the port mode of loop detection to **forwarding** on the affected bridge port.

16.4 The device cannot be reached via CLI and Web UI (loading a firmware file via TFTP)

The device cannot be reached via CLI and Web UI.

Solution

You can restart the device with the button and load a firmware file into the device in rescue mode via TFTP.

While the device is starting, you can switch to rescue 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.

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.

16.6 Data traffic floods occur on conversion from MRP to Spanning Tree

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.

16.5 The device interrupts the transmission of a firmware file from a remote server.

When loading a firmware file from a remote server, the device interrupts the transmission of the file.

Example

The following lines are output in the CLI:

```
localhost# system firmware update source tftp://192.168.1.1/sinec-
os_V02.00.00.00.sfw
The backup firmware will be discarded and updated with the new
firmware. Are you sure you want to continue? [yes,no] yes
Preparing update... done
Transferring file... aborted.
Aborting update... done
Error: Failed to transfer file: Transferred a partial file.
```

Solution

While SINEC OS is downloading a firmware file from a remote server, there are pauses in the file transfer during which SINEC OS processes parts of the received firmware file in the background.

To prevent interruptions in the transmission of firmware files, you can set a timeout on the remote server.

If your remote server supports timeout configuration, set a value of at least two minutes.

16.6 Data traffic floods occur on conversion from MRP to Spanning Tree

After you have reconfigured a network from MRP to Spanning Tree, data traffic floods occur.

Example

The following example shows a possible scenario that can lead to data traffic floods:

1. You have configured MRP for multiple devices and connected the devices in a ring topology.
2. You have terminated a connection of the ring topology so that a line topology occurs.

3. You have disabled MRP and configured and enabled Spanning Tree on all devices.
4. You have connected the devices to a ring topology again.
5. You have detected data traffic floods.

Solution

You have the following options for avoiding data traffic floods, depending on your configuration tool.

Configuration via CLI, Web UI or NETCONF

If you configure the devices via CLI, Web UI or NETCONF, follow these steps:

1. Terminate a connection of the ring topology so that a line topology occurs.
2. Configure the individual devices one after the other.
3. Disable MRP for a device again.
4. Commit the change.
5. Enable Spanning Tree on the device again.
6. Commit the change.
7. When the steps have been performed for all devices in the network, connect the devices to a ring topology again.

Configuration via a configuration file

If you configure the devices via a configuration file, follow these steps:

1. Terminate a connection of the ring topology so that a line topology occurs.
2. Restart the devices.
3. When all devices in the network have restarted, connect the devices to a ring topology again.

