



Hardened Lite Managed Ethernet Switch SmartE Series

User Manual

All Rights Reserved

Dissemination or reproduction of this document, or its contents, is not authorized except where expressly permitted. Violators are liable for damages. All rights reserved, for the purposes of patent application or trademark registration.

Disclaimer of Liability

The information contained in this document is subject to change without notice. EtherWAN is not liable for any errors or omissions contained herein or for resulting damage in connection with the information provided in this manual.

All other trademarks are property of their respective owners.

Warranty

For details on the EtherWAN warranty replacement policy, please visit our web site at:

www.etherwan.com

Products Supported by this Manual:

SmartE Series Switches

Preface

Audience

This guide is designed for the person who installs, configures, deploys, and maintains the Ethernet network. This document assumes the reader has moderate hardware, computer, and Internet skills.

Document Revision Level

This section provides a history of the revision changes to this document.

Revision	Document Version	Date	Description
А	1	04/20/2021	First version of document.
A	2	08/10/2021	Added to page 41: "If the 'Large Tree Support' function is enabled, we recommend using the default parameters."
A	3	08/20/2021	Added information to Mode Table on page 8 and description on page 9.
А	4	09/02/2021	Deleted MRP commands

Document Conventions

This guide uses the following conventions to draw your attention to certain information.

Safety and Warnings

This guide uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
	Note	Notes emphasize or supplement important points of the main text.
	Тір	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Warning	Warnings indicate that failure to take a specified action could result in damage to the device, or could result in serious bodily injury.

Contents

Preface Document Conventions	2 3
Safety and Warnings	3
Contents	4
Introduction SmartE Series	7 7
Mode Setting Entering Mode Setting	8 8
BootP	9
Management Using the Web Interface Default IP Address	10 10
Login Process and Default Credentials	10
Layout of Web Management Interface	11
Information - Help & Documentation	12
Information – Device Status	13
Information – Local Diagnostic	14
Information – Alarm & Events	15
Information – Port Table	16
Information – MAC Address Table	17
Configuration – My Profile	17
Configuration – User Management	18
Configuration – System	21
Configuration – Quick Setup	25
Configuration – Network	27
Configuration – Service	29
Configuration – Port Configuration	32
Configuration – VLAN Configuration	35
Configuration – Multicast Filtering	39
Configuration – Network Redundancy	41
Configuration – Security	47
Configuration – DHCP Service	52

.56
.57
.58
.59
.60
.60
.61
.62
.63
.65
.65
.66
.69
.69
.69
.70
.70
.71
.71
.71
.73
.73
.76
.77
.78
.79
.80
.83
.83
.83
.84
.84

Services Commands	86
LLDP Services Commands	88
Port Features Commands	90
Port Mirroring Commands	92
VLAN Commands	93
Multicast Commands	96
RSTP Commands	
Port Channel Commands	102
Security Context Commands	104
DHCP Commands	105
Alarm Output Commands	109
QoS Commands	110
Trap Manager Commands	111
Contact Information	113

Introduction

SmartE Series

The SmartE series is a portfolio of hardened lite managed Ethernet switches. SmartE offers a key set of Layer 2 management features that are perfect for supporting network connectivity for edge applications even in extreme environments. With a wide range of models available in both Fast Ethernet and Gigabit Ethernet configurations, offering up to 16 Ethernet ports and 2 optional SFP ports for network expansion, the SmartE series provides a reliable and cost-effective network management solution for critical applications.

Before you install and use this product, please read this manual in detail.

Mode Setting

With mode setting, you can change the operating mode of the switch, without having access to one of the management interfaces.

Press the Mode button to enter mode setting, select the desired setting, and exit Mode setting. The four Mode LEDs indicate the setting that is currently selected, which will be applied when exiting mode setting.

The following setting options can be selected via Smart mode:

- Reset to factory default values
- Operate with a fixed IP address
- Reset the IP configuration
- Operate in unmanaged mode
- Exit mode selection without changes

Entering Mode Setting

At the bottom right of the front face there is a Mode button. To select an operating mode, power up the switch. When the LEDs of all ports go out, press the mode button for more than ten seconds. The four LEDs of ports 1 and 2 will flash, indicating that the device is ready for mode selection. The active state is then identified by the combination of the four flashing LEDs.

When the mode selection is started, the initial state is "Exit mode selection without changes." Select the desired mode by pressing the mode button.

Mode	Description	Link/Act LED of	Link Speed LED	Link/Act LED of	Link Speed LED
		Port 1	of Port 1	Port 2	of Port 2
Initial State	Exit mode selection without changes	On	Off	Off	Off
Mode 1	Reset to factory default values	Off	On	Off	Off
Mode 2	Operate with a fixed IP address	Off	On	On	Off
Mode 3	Reset the IP configuration	On	On	On	Off
Mode 4	Operate in unmanaged mode	Off	On	Off	On

To exit the selected mode, press and hold down the MODE button for at least five seconds. The selected operating mode will then be saved and activated as soon as you release the MODE button.

Mode descriptions:

Mode 1 – Reset to factory default values: When activated, all switch settings and configurations will be reset to factory defaults.

Mode 2 – Operate with a fixed IP address: This is the default setting for the switch. – DHCP server is activated to assign IP to connected PC, and device has a fixed IP: 192.168.0.254.

Mode 3 – Reset the IP configuration: Reset IP to default IP 192.168.1.10, subnet mask and default gateway to 0.0.0.0 only, but not reset stored configurations.

Mode 4 – Operate in unmanaged mode: The switch can be used without an IP address. The switch adopts the static IP address 0.0.0.0. The subnet mask and gateway are also 0.0.0.0. In this mode, web-based management can no longer be accessed, and the switch no longer sends BootP and DHCP requests.

The following main Layer 2 management features can be active in Unmanaged mode, but require a few configuration steps in the web GUI before setting the SmartE device to Unmanaged mode.

- Redundancy mechanisms (RSTP, LTS, FRD)
- Broadcast/multicast limiter
- IGMP snooping

NOTE: The device can only exit unmanaged mode by switching to a different mode or by resetting the switch to the factory default settings.

BootP

The device uses the BootP protocol for IP address assignment. Numerous BootP servers are available on the Internet. You can use any of these programs for address assignment.

Notes on BootP

During initial startup, the device sends BootP requests without interruption until it receives a valid IP address. As soon as the device receives a valid IP address, it stops sending further BootP requests.

After a restart, the device sends three BootP requests and will only then adopt the old IP address if there is no BootP response.

Management Using the Web Interface

The web interface allows for remote monitoring, configuration, and control of the switch through any standard web browser. All switch features that can be configured through the Command Line Interface can also be configured through the web interface.

Default IP Address

The switch's default IP address is 192.168.1.10. The management computer must be set up so that it is on the same network as the switch. For example, the IP address of the management computer can be set to 192.168.1.100 with a subnet mask of 255.255.255.0. DHCP is disabled by default.

Login Process and Default Credentials

Once a compatible IP address has been assigned to the management computer, the user is ready to log in to the switch. To log in, type the URL into the address field of the browser and hit return.

- The Default Login is root (case sensitive)
- There is no password by default
- Enter the login name and click the Login button

It is highly recommended that you change the default password when you first set up the switch. Use a secure password with adequate complexity.

Cookies must be enabled in the web browser in order to use web management.

Layout of Web Management Interface

The web management interface is divided into three sections:

- Information: General device information
- Configuration: Device configuration
- Diagnostics: Device-specific diagnostics

The contents of each section are as follows:

Information

- -Help & Documentation
- -Device Status
- -Local Diagnostic
- -Alarm & Events
- -Port Table
- -MAC Address Table

Configuration

- -My Profile
- -User Management
- -System
- -Quick Setup
- -Network
- -Service
- -Port Configuration
- -VLAN Configuration
- -Multicast Filtering
- -Network Redundancy
- -Security
- -DHCP Service
- -Local Events
- -Quality of Service

Diagnostics

-LLDP Topology -RSTP Diagnostic -Current VLANs -Current Multicast Groups -Port Mirroring -Trap Manager -Port Counter -Port Counter -Port Utilization -Snapshot -Syslog

Information - Help & Documentation

Here you will find useful information about using web-based management.

Help & Documentation
Help
The navigation tree is structured as follows:
Information
Here you will find information on the product and the current device status. You do not need to log-in to access the web
pages.
Configuration
Here you can configure the Device. For security reasons you must log-in with a password before you can access the
website.
The Outer Setup website includes all parameters for fact and easy configuration of a the device
Discretion of a the device.
Here you will find further information on diagnostics of the device.
Help There is a (?) after every parameter on the website. When you move the mouse pointer across you will get information on the parameter in a Fly Out window.

Information – Device Status

Here you will find general information about your device, such as the serial number, firmware version, or hardware version.

Device Status		
Vendor	:	EtherWAN Systems, Inc.
Address	:	New Taipei City 231
Phone	:	+886 (2) 6629 8986
Internet	:	www.etherwan.com
Family	:	EtherWAN SmartE
Туре	:	SG300-16
Order No	:	SG300-16
Serial No	:	2034998503
Firmware Version	:	2.94.01 BETA
Hardware Version	:	00
Logic Version	:	0x5
Bootloader Version	:	1.16
Hostname	:	SmartE
Device Name	:	SmartE
Description	:	
Physical Location	:	
Contact	:	
IP Address	:	192.168.1.10
Subnet Mask	:	255.255.255.0
Gateway	:	0.0.0.0
IP Address Assignment	:	Static
MAC Address	:	00:E0:B3:48:03:90

Information – Local Diagnostic

Here you will find a brief explanation of how to interpret the individual LEDs on the device.

Local Diagnostics	
Power Supply	
US1	: Supply Voltage 1 (green LED)
US2	: Supply Voltage 2 (green LED)
Alarm Output	
FAIL	: Alarm Output failed (red LED)
Ethernet	
PORT LED 1	: Link and Activity (green LED)
PORT LED 2	: Speed 10 Mbit/s (LED off)

Information – Alarm & Events

This page displays a list of alarms and events in a table. You can save event table entries, so that they are also retained after the device is restarted. The event table can be downloaded from the device in CSV format.

Alarm & Events					
Invalid	Cold start.				
Oct 28 2020 00:00:02	US 2 lost.				
Oct 28 2020 00:00:02	Alarm output 1 Failed.				
Oct 28 2020 00:00:03	Name of the device changed.				
Oct 28 2020 00:00:10	LLDP new neighbour on Port 16.				
Oct 28 2020 00:00:11	Link up on port 16.				
Oct 28 2020 00:12:58	Successful user login.				
Oct 28 2020 00:41:11	Successful user login.				
Oct 28 2020 00:52:04	Automatic user logout.				
Oct 28 2020 01:48:00	Successful user login.				
Oct 28 2020 01:51:12	Automatic user logout.				
Oct 28 2020 03:46:29	Successful user login.				
Oct 28 2020 03:53:04	Automatic user logout.				
Oct 28 2020 03:53:31	Successful user login.				
Oct 28 2020 04:00:04	Automatic user logout.				
Oct 28 2020 04:01:27	Successful user login.				
Oct 28 2020 04:08:04	Automatic user logout.				
Oct 28 2020 04:08:35	Successful user login.				
00120202004.00.00					
Syste	System Uptime (?) 7h:8m:40s				
Current system time (?) 2020/10/28 07:05:45 (Not synced)					
Event Count (?) Loaded 29 events					
Event Table as CSV File (?) Read from device					
Clear Event Table (?) Clear					

A maximum of 3000 entries can be stored in the event table. The oldest entries are then overwritten. If there is a large number of entries, it may take several seconds to load the Event Table.

Information – Port Table

This page displays a list of the current states of the individual ports.

Port Table			
Advanced Tables			
	(?) Port Redundancy Tab	ble	
Physical Ports			
Interface/Port	Туре	Status	Mode
1	TX 10/100/1000	enable	Not connected
<u>2</u>	TX 10/100/1000	enable	Not connected
<u>3</u>	TX 10/100/1000	enable	Not connected
<u>4</u>	TX 10/100/1000	enable	Not connected
<u>5</u>	TX 10/100/1000	enable	Not connected
<u>6</u>	TX 10/100/1000	enable	Not connected
<u>7</u>	TX 10/100/1000	enable	Not connected
<u>8</u>	TX 10/100/1000	enable	Not connected
<u>9</u>	TX 10/100/1000	enable	Not connected
<u>10</u>	TX 10/100/1000	enable	Not connected
<u>11</u>	TX 10/100/1000	enable	Not connected
<u>12</u>	TX 10/100/1000	enable	Not connected
<u>13</u>	TX 10/100/1000	enable	Not connected
<u>14</u>	TX 10/100/1000	enable	Not connected
<u>15</u>	TX 10/100/1000	enable	Not connected
<u>16</u>	TX 10/100/1000	enable	1000 MBit/s FD

Clicking on the "Port Redundancy Table" button opens a table containing information about the individual ports and their redundancy mechanism assignment.

Interface/Port: Clicking on a port number in the "Interface/Port" column opens the "Port Configuration" page for the selected port.

Type: The "Type" column indicates whether it is a copper port (e.g., TX 10/100) or a fiberglass port (e.g., FX 100).

Status: The "Status" column shows whether the port is activated or deactivated.

Mode: The "Mode" column indicates the current connection status of the ports.

- Not connected: No active link at the port.

- 100 Mbps FD (or comparable status): Displays the transmission speed and duplex mode if there is an active link.

- Far-End Fault: Provides information about a fault on a fiber of a bi-directional fiberglass connection (e.g., due to a defective fiberglass cable). If the device at the other end also supports Far-End Fault, it detects a communication failure on its own receiver connection and sends a Far-End Fault signal pattern to the peer.

Information – MAC Address Table

On this page, you will find a list of the current devices in the network. You can download the list from the device in CSV format.

MAC Address Table					
No.	VLAN	MAC-Address	Port		
1	1	F8:75:A4:8B:07:7D	16		
	MAC Table as CSV File (?) Clear MAC Table (?)	Read from device			

Configuration – My Profile

This page allows for the changing of the password of the root account, and the setting of an SNMPv3 password. The minimum SNMPv3 password length is eight characters.

My Profile		_	_	
Username (?)	root			
User Password (?)	•••			
Retype Password (?)	•••			
SNMPv3 Password				
Individual SNMPv3 Password (?)				
		Apply	Revert	Apply&Save

Configuration – User Management

Create and manage user accounts for the web-based management of the switch here. You can assign permissions to users via user roles.

User Management	_		-	_	_	
Create/Edit User (?)	Create	~				
User Status (?)	Enable	~				
Username (?)						
User Role (?)	Read-only	~				
User Password (?)	•••					
Retype Password (?)	•••					
User account locking (?)	Disable	~				
Login Attempts Limit (?)	5					
Access Lock Time (?)	1					
Custom User Roles						
Custom User Roles Webpage (?)	Custom User Roles					
		-	_			
				Apply	Revert	Apply&Save

Create/Edit User: Select the user account that you wish to edit or delete. Select "Create" to create a new user account.

Delete button: Click here to delete the selected user account. The "root" account cannot be deleted.

User Status: Activate or deactivate the selected user account. When a user account is deactivated, access to the device is blocked, even if the correct login parameters are entered.

User Name: Configure the user name. Once the user account is created, you will not be able to change the user name.

User Role: Assign a role to the selected account that defines the user rights. The following roles can be selected:

 Read-only: The user has read access to the device and therefore access to the web pages in the information and diagnostics areas. Furthermore, the user has permission to change their own access password.

- Expert: An expert user account has extensive read and write access to the device and can therefore modify a good portion of the configuration parameters. However, this excludes "User

Management".

- Admin: An admin user has unrestricted read and write access to the device.

User Password / Retype Password: Here, you can configure the password for the selected user account. For a new user account, this password is also used for initial access to the device. Passwords must be between eight and 64 characters long.

User account locking: This function can be used to lock out a user for a certain period of time if they have repeatedly attempted to log in using the wrong password. It is not possible to access the device during this time, even if the correct access data is entered.

Login Attempts Limit: When the 'User account locking" function is enabled, configure here the number of failed login attempts after which the user account is locked.

Access Lock Time: When the "User account locking" function is enabled, set the time (in minutes) for which a user account is locked if the "Login Attempts Limit" is exceeded.

Custom User Roles: Clicking the Custom User Roles link opens a new page on which user roles can be created and edited. Create a new custom role by selecting "Create," or edit a role by selecting an existing role name. Role names can be up to 32 characters long. Once a role name is assigned, it cannot be edited. Use the check boxes in the table below to assign read-write or read-only rights to for the various permission groups.

Create/Edit Custom Role (?) Create	\checkmark			
Rolename (?)				
Permission Groups	Read-Write	Re	ad-Only	
System Configuration (?)				
Device Identification (?)				
User Management (?)				
Network (?)				
User Interface Configuration (?)				
Automation Protocols (?)				
Device Discovery (?)				
L2 and L3 Communication (?)				
Device Redundancy (?)				
Time Synchronization (?)				
DHCP Services (?)				
Physical Ports (?)				
RMON and port statistics (?)				
Port Mirroring (?)				
Port Security (?)				
Device Logging and Alarming (?)				
Snapshot (?)				
		Apply	Revert	Apply

Configuration – System

Reboot Device	
Reboot Device (?) Reboot
Firmware Update	
Firmware Update ((?) <u>Update Firmware</u>
Configuration Handling	
Status of Current Configuration (?) Configuration saved
Perform Configuration Action	(?)
Advanced Configuration ((?) Further configuration handling options
Secure UIs ((?) <u>Security Context</u>
Device Identification	
Device Name (?) SmartE
Device Description (?)
Physical Location ((?)
Device Contact	(?)
	Apply Revert Apply&Save

Reboot Device: Clicking on the "Reboot" button restarts the device. All unsaved parameters will be lost.

Firmware Update: Clicking on the "Update Firmware" link opens a new window in which the parameters for the firmware update must be entered.

Firmware Update					
Update method (?)	HTTP	~			
TFTP Server IP Address (?)	0.0.0.0				
Remote Firmware Filename (?)				Browse	
Automatic Reboot After Write (?)	Reboot	~			
Update Status (?)	No Update				
			[Apply	Revert

To update the firmware via HTTP:

Browse: Clicking on the "Browse" button allows you to select the desired file on your PC.

Automatic Reboot After Write: Here, specify whether a reboot should be performed after the firmware update.

Click "Apply" to start the firmware update.

If you perform a firmware update without rebooting immediately, "Update Status" displays the message "Firmware Update successful", which informs you that the firmware has been transferred to the device and will be activated on the next reboot.

To update the firmware via TFTP, select "TFTP" as the update method. Enter the IP address of the computer on which the TFTP server is active, and the filename. Click "Apply" to start the update.

Firmware Update		
Update method (TFTP v	
TFTP Server IP Address (192.168.1.100	
Remote Firmware Filename (MVetherWan_v3_00.bin	
Automatic Reboot After Write (Reboot ~	
Update Status (No Update	
		Apply Revert

Configuration Handling items

Status of Current Configuration: Shows the status of the active configuration.

Perform Configuration Action: Select an action from the dropdown menu:

- Factory Default: Resets the device configuration to the delivery state.
- Save Configuration: Saves the active device configuration to Flash memory.

- Reload Configuration: Loads the configuration file from Flash memory and applies it. The device is then restarted.

Advanced Configuration: Clicking on the "Further configuration handling options" link opens a "File Transfer" window (see below). On that screen, enter the parameters for transferring a configuration file from the device to the PC (download) or from the PC to the device (upload).

File Transfer	_	_	
Transfer method (?) HTTP ~			
File type (?) Configuration ~			
Update Status (?) No transfer started			
Start Transfer (?) Write to Device			
HTTP Read (?) <u>config.cfg</u>			
Configuration Name (?) SmartE Configuration			
(Apply	Revert	Apply&Save

Transfer Method: Select the transmission protocol you would like to use to transfer the file.

File Type: Select the file type to be transferred. It can be either a configuration file, a security context or a snapshot file.

Configuration Name: Enter the name under which you want to save the configuration on the PC. Any change to the configuration name only takes effect when you click on the "Apply & Save" button.

Update Status: Shows the current transfer status.

Start Transfer: Click on the "Write to device" button to select the file on your PC that is to be transferred to the switch.

HTTP Read: Click on the "config.cfg" link to download the active configuration directly to the connected PC. If transferring a snapshot file, click on the "snapshot.tar.gz" link to download the current snapshot file directly to your PC.

If transferring files via TFTP, enter the IP address of the computer on which the TFTP server is active, and the remote filename. Then select "Read from device" or "Write to device" in the **Direction** field. Click on the "Start" button to start the transfer of the file.

Secure UIs: Clicking on the "Security Context" link opens the "Security Context" screen.

Security Context	
Create new context (?) Generate	
Current state (?) valid	
	_
Root CA (?) <u>cacert.cer</u> Advanced Configuration (?) <u>File transfer</u>	

Create new context: Clicking on the "Generate" button creates all the necessary keys and certificates for operation with HTTPS and SSH.

Current state: Shows the status of the current availability of the security context.

Root CA: Clicking on the "cacert.cer" link loads the Root CA certificate for installation in the browser.

Advanced Configuration: Clicking on the "File transfer" link opens the "Advanced Configuration" window for file transfer with file type set to "Security Context".

Device Identification items

Information entered in this section is displayed on the "Device Status" page.

Device Name: Enter the device name.

Device Description: Enter a device description. It may be up to 255 characters long.

Physical Location: Here, you can provide the location of the device, such as the building in which it is installed.

Device Contact: Here, you can enter a contact address.

Configuration – Quick Setup

Basic settings can be quickly configured in the Quick Setup area.

	Profile	(?)	Universal				
	IP Address Assignment	(?)	STATIC ~]			
1	IP Address	(?)	192.168.1.10				
	Network Mask	(?)	255.255.255.0				
	Default Gateway	(?)	0.0.0.0				
	Device Name	(?)	SmartE				
	Device Description	(?)					
	Physical Location	(?)					
	Device Contact	(?)					
	LLDP Mode	(?)	Enable ~				
		(?)	LLDP Topology				
					Apply	Revert	Apply&Save

Automation Profile: Only one profile is available for this model – Universal. In Universal mode, BootP is activated for IP address assignment.

IP Address Assignment: Select the type of IP address assignment from the dropdown menu. The options are:

- STATIC: Static IP address
- BOOTP: Assignment via the Bootstrap protocol
- DHCP: Assignment via a DHCP server

IP Address: Set the desired IP address.

Network Mask: Set the desired subnet mask here.

Default Gateway: Set the desired default gateway here.

Device Name: Enter the device name of the switch.

Device Description: Enter a description for the device, up to 255 characters in length.

Physical Location: Enter a location for the device.

Device Contact: Here, you can enter the name of a contact person for the device.

LLDP Mode: Enable or disable LLDP.

- Disable: LLDP is deactivated
- Enable: LLDP is activated
- Send only: Received LLDP BPDUs are ignored
- Receive only: No LLDP BPDUs are sent

The "LLDP Topology" link opens the corresponding page. This can also be accessed via the menu item of the same name.

Configuration – Network

Configure basic network settings on this page.

Network		_	_		_	_	_
IP Address Assignment	(?)	STATIC	~				
IP Address	(?)	192.168.1.10					
Network Mask	(?)	255.255.255.0					
Default Gateway	(?)	0.0.00					
DNS Server 1	(?)	0.0.0.0					
DNS Server 2	(?)	0.0.0.0					
Management VLAN	(?)	1	~				
DHCP Configuration	(?)	DHCP Services					
Topology Based IP Assignment					_	_	
Assignment port	(?)	Choose-Port	~				
Assignment state	(?)	Feature disabled	on this o	device	9		
Hostname Configuration							
Name resolution	(?)	Enable	~				
Hostname	(?)	SmartE					
ACD Configuration		_					
ACD Mode	(?)	None	~				
ACD Status Information	(?)	See ACD status	on Devic	e stat	us page		
					Apply	Revert	Apply&Save

IP Address Assignment: Select the type of IP address assignment.

- STATIC: Static IP address
- BOOTP: Assignment via the Bootstrap protocol
- DHCP: Assignment via a DHCP server

For static IP addressing, complet the following fields:

- IP Address: Set the desired IP address.
- Network Mask: Set the desired subnet mask.
- Default Gateway: Set the desired default gateway.

DNS Server 1: Enter the IP address of the primary DNS server.

DNS Server 2: Enter the IP address of the secondary DNS server.

Management VLAN: Set the VLAN in which the web-based management can be accessed (default is "1").

DHCP Configuration: Click the "DHCP Services" link to navigate to the DHCP Services page.

Topology Based IP Assignment allows for the assigning of blocks of IP addresses from an IP pool for different topological areas.

Assignment port: Select the desired port from the dropdown menu. A device connected to the selected port requests incremented IP at DHCP server. Choosing a port disables the Accept Bootp feature of the DHCP server settings.

Assignment state: Displays if the topology based IP assignment feature on this device is disabled, acting as root or acting as client.

Hostname Configuration items

Name resolution: Here, you can enable and disable DNS name resolution via mDNS and LLMNR. When the function is activated, you can also access the device via the host name (e.g., http://smarte.local).

Hostname: Configure the DNS host name of the device here. The host name must be between two and 63 characters long. Alphanumeric characters and dashes are permitted. A host name must not start with a dash.

ACD (Address Conflict Detection) Configuration items

ACD Mode: Here, you can enable and disable the "Address Conflict Detection" function.

ACD Status Information: Clicking on the link opens the "Device Status" page.

Configuration – Service

Service												
Web Server (?)	HTTP			~							
Confidential Web Server view (?)	Enable			~							
SNMP Agent (?)	SNMP v	2		~							
SNMPv2 read community (?)	public										
CLI Service (?)	Telnet			~							
CLI Network Scripting UI (?)	Enable			~							
Smart mode (?)	Enable			~							
Persistent Event Logging (?)	Disable			~							
Login expire time (?)	1200										
LLDP Configuration												
LLDP Mode (?)	Enable			~							
LLDP Transmit Interval (?)	5										
LLDP Transmission (?)	1 2	3	4	5	6	7	8				
		9 10	11	12	13	14	15	16				
LLDP Reception (2)	1 2	3	 ✓ 4 	 ✓ 	✓	7	✓				
	.,			2								
		9 10		12	I3 ✓	14						
LLDP Topology (?)	Link to L	_DP T	opolog	<u>jy we</u>	bpage	<u>e</u>					
System Time												
Current system time (?)	2020/12/	18 04:	07:20	(Not	synce	ed)					
Network time protocol (?)	None			~							
Manual system time set (?)	click to s	et tim	е								
Synchronization Status (?)	Not Sync	hroniz	zed								
Last SNTP synchronization (?)	Not Sync	hroniz	red								
			_		A	pply		Re	vert	A	pply&	Save

Web Server: Here, you can enable and disable the web server function and also select the mode (HTTP/HTTPS).

Confidential Web Server View: If this view is activated, no web pages in web-based management can be accessed without logging in first – this also applies to the web pages in the information area.

SNMP Agent: Enable and disable the SNMP server function and select the mode (SNMP v2, SNMP v3).

CLI Service:

- Disable: The entry of CLI commands is deactivated.
- Telnet: The entry of CLI commands via Telnet is activated.
- SSH: The entry of CLI commands via Secure Shell (SSH) is activated.

CLI Network Scripting UI:

- Disable: The transmission of CLI commands via the network is deactivated.
- Enable: The transmission of CLI commands via the network is activated.

Smart mode: Here, you can enable and disable the Mode button

Persistent Event Logging: Here, you can enable and disable the persistent storage of events. Persistent storage means that events are not deleted when the device is restarted.

Login expire time: Configure the duration until automatic logout (30 ... 3600 seconds, default is 1200 seconds). Entering 0 deactivates automatic logout.

LLDP Configuration items

LLDP Mode:

- Disable: LLDP is disabled
- Enable: LLDP is enabled
- Send only: Only LLDP BPDUs are sent.
- Receive only: Only LLDP BPDUs are received.

LLDP Transmit Interval: Set the interval at which LLDP telegrams are to be sent. The value must be between 5 and 32,786 seconds (default is 5 s).

LLDP Transmission: Enable and disable the forwarding of LLDP telegrams for specific ports.

LLDP Reception: Enable and disable the ignoring of LLDP telegrams for specific ports.

LLDP Topology: Clicking on the "Link to LLDP Topology webpage" link opens the page for "<u>LLDP</u> <u>Topology</u>".

System Time items

Current system time: Displays the current system time. "Not synced" means that the system time has either been configured manually or it is not synchronized with an (S)NTP server.

Network time protocol: Activates synchronization via a web server.

Manual system time set: Manual setting of the system time if no SNTP server is available.

Synchronization Status: Displays the current status of synchronization with the SNTP server.

Last SNTP synchronization: Displays the time of the last synchronization.

Configuration – Port Configuration

Individual Port Configuration					
Port (?	?)	port-1 🗸			
Status (?	?)	Enable ~			
Name (?	?)	Port 1			
Туре (?	?)	TX 10/100/1000			
Link (?	?)	Not connected			
Negotiation Mode (?	?)	Auto			
Speed (?	?)	0 MBit/s			
Duplex (?	?)	Undefined			
Mode (?	?)	Auto 🗸			
Link Monitoring (?	?)	Disable ~			
Default Priority (?	?)	0 ~]		
Jumbo Frames (?	?)	Disable 🗸			
MTU (?	?)	1536			
Flow Control (?	?)	Disable 🗸			
CRC Surveillance					
Received Pkts (?	?)	0			
CRC Errors (?	?)	0			
CRC Proportion Peak (ppm) (?	?)	0			
CRC Port Status (?	?)	Ok			
Critical Threshold (ppm) (?	?)	40000			
Warning Threshold (ppm) (?	?)	20000			
Clear CRC Peak and CRC Status (?	?)	Clear Check to clear a	all	ports	
Port Counter Overview (?	?)	Monitor all ports simultar	ni	<u>ously</u>	
Advanced Port Configuration					
Port Configuration Table (?	?)	Configure all ports simul	lta	iniously	
	_				
Port Mirroring (?	?)	Configure Port Mirroring			
VLAN Port Configuration (?	?)	Configure Port settings f	for	r a VLAN	
Link Aggregation (?	?)	Configure Link Aggregat	tio	n	
Port Based Security (?	?)	Configure Port Based Se	ec	<u>curity</u>	
		Apply		Revert	Apply&Save

Port Configuration items

Port: Select the port that you want to configure individually.

Status: The port can be activated/deactivated here.

Name: You can assign a name to the port.

Type: Describes the physical properties of the port.

Link: Shows the current link status of the port.

Negotiation Mode: Shows the current auto negotiation status.

Speed: Displays the current transmission speed at which the port is operating.

Duplex: Displays the transmission mode of the port.

Mode: The port can be set to a fixed speed and transmission mode here, and fast startup can also be set.

Link Monitoring: Specify whether the link behavior is to be monitored at the selected port.

Default Priority: Set the priority for incoming data packets to this port.

Jumbo Frames: Enable/disable the support of jumbo frames (>1518 bytes). The MTU size is set to 9600 bytes following activation.

U The Jumbo Frames" function is only available on SG300 Gigabit models.

MTU: Here, you can set the maximum transmission unit (MTU). Packet sizes between 1522 bytes and 9600 bytes are accepted.

Flow Control: Flow control for the selected port can be enabled and disabled here.

CRC Surveillance items

Received Pkts: Shows the number of packets received at the selected port since the last reboot or counter reset.

CRC Errors: Shows the number of CRC errors at the selected port since the last reboot or counter reset.

CRC Proportion Peak (ppm): Shows the highest proportion of CRC errors that occurred in a 30second interval, relative to the total number of packets received in this interval since the last reboot or counter reset. CRC Port Status: Shows the status of the current port.

Critical Threshold (ppm): Here, you can enter the threshold value at which the CRC Port Status switches to Critical (1000 ppm - 1,000,000 ppm are acceptable).

Warning Threshold (ppm): Shows the threshold value in ppm at which the CRC Port Status switches to Warning (50% of Critical Threshold).

Clear CRC Peak and CRC Status: Clicking the "Clear" button resets the CRC Peak and CRC Status.

Port Counter Overview: Clicking on the "Monitor all ports simultaneously" link takes you to the "<u>Port</u> <u>Counter</u>" page.

Advanced Port Configuration items

Port Configuration Table: Clicking on the "Configure all ports simultaneously" link takes you to the "<u>Port Configuration Table</u>" page. There, you can set the status, mode, link monitoring, jumbo frames, and flow control for all ports.

Port Mirroring: Clicking on the "Configure Port Mirroring" button takes you to the <u>port mirroring</u> <u>configuration</u> page.

VLAN Port Configuration: Clicking on the "Configure Port Settings for a VLAN" button takes you to the "<u>VLAN Port Configuration</u>" page.

Link Aggregation: Clicking on the "Configure Link Aggregation" button takes you to the "<u>Link Aggregation</u>" page.

Port Based Security: Clicking on the "Configure Port Based Security" button takes you to the "<u>Port</u> <u>Based Security</u>" page.

Port Configuration Table

Port Configuration Table											
Interface/Port	Status		Mode		Linkmonitor	Jumbo Frames		MTU [byte]	Flo	Flow Control	
1	Enable	~	Auto	~	Enable 🗸	Disable	~	1536	Disa	able	~
2	Enable	~	Auto	~	Enable 🗸	Disable	~	1536	Disa	able	~
3	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
4	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
5	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
6	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
7	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
8	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
9	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
10	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
11	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
12	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
13	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
14	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
15	Enable	~	Auto	~	Disable 🗸	Disable	~	1536	Disa	able	~
16	Enable	~	Auto	~	Disable ~	Disable	~	1536 Disab		able	~
							Арр	ly Reve	ert	Apply&S	Save

Configuration – VLAN Configuration

VLAN Configuration		_	_	_	_	
VLAN Mode (?)	Tagged	~				
Static VLANs			_	_	_	
Static VLAN Configuration Webpages (?)	Static VLAN Cor	nfiguration				
	VLAN Port Confi	iguration				
	VLAN Port Confi	iguration Table				
VLAN Diagnostic						
VLAN Diagnostic Webpages (?)	Current VLANs					
			Apply	Ā	Revert	Apply&Save

VLAN Mode:

- Transparent: In "Transparent" mode, the switch processes the incoming data packets as described in the "Frame switching" section. Neither the structure nor the contents of the data packets are changed. The information about VLAN assignment from a tag that may be contained in the data packet is ignored.

- Tagged: In "Tagged" mode, the switch forwards the data packets based on the VLAN assignment.

Static VLANs

Static VLAN Configuration Webpages:

Clicking on the "Static VLAN Configuration" link takes you to the "Static VLAN Configuration" web page (see below). Up to 32 static VLANs can be set up here.

Clicking on the "VLAN Port Configuration" link takes you to the "VLAN Port configuration" web page.

Clicking on the "VLAN Port Configuration Table" link takes you to the VLAN port configuration table.

VLAN Diagnostic Webpages:

Clicking on the "Current VLANs" link opens the "Current VLANs" page as a pop-up.

Static VLAN Configuration

Static VLAN Configuration												
List of Static VLANs (?)	1 - V	LAN	1									
VLAN ID (?)	1											
VLAN Name (?)	VLAN	V 1										
VLAN Memberships (?)	1	2	3	4	5	6	7	8				
	U	U 10	U 11	U 12	U 13	U 1/	U 15	U 16				
	Ű	U	U	U	U	U	U	U				
(?)	Dele	ete										
	_	-	_			_					_	_
				App	ly		Reve	ert	Apply&	Save		

List of Static VLANs: All VLANs created up to this point are displayed here.

VLAN ID: Set the VLAN ID you wish to assign to the new VLAN. The value must be between 2 and 4094.

VLAN Name: Specify the VLAN name you wish to create.
VLAN Memberships: Specify which ports are to be located in the VLAN.

- T: Tagged port
- U: Untagged port
- -: Not a member of the VLAN

Use the "Delete" button to delete the VLAN selected in the list. VLAN 1 cannot be deleted.

VLAN Port configuration

VLAN Port configuration	
Port Number (?) port-1	~
Default VLAN ID (?) 1	\checkmark
Default Priority (?) 0	~
Ingress Filter (?) disable	~
	Apply Revert Apply&Save

Port Number: Select the port for which you want to change the VLAN settings.

Default VLAN ID: Select the VLAN ID that is to be assigned to the port.

Default Priority: Set the VLAN priority for the selected port.

Ingress Filter: Specify whether the ingress filter should be activated.

VLAN Port Configuration Table

VLAN Port Configuration	Table		
Port	Default VLAN	Default Priority	Ingress Filter
1	1 🗸	0 ~	disable 🗸
2	1 ~	0 ~	disable 🗸
3	1 ~	0 ~	disable 🗸
4	1 ~	0 ~	disable 🗸
5	1 ~	0 ~	disable 🗸
6	1 ~	0 ~	disable 🗸
7	1 🗸	0 ~	disable 🗸
8	1 ~	0 ~	disable 🗸
9	1 🗸	0 ~	disable 🗸
10	1 ~	0 ~	disable 🗸
11	1 🗸	0 ~	disable 🗸
12	1 🗸	0 🗸	disable 🗸
13	1 🗸	0 ~	disable 🗸
14	1 🗸	0 ~	disable 🗸
15	1 🗸	0 🗸	disable 🗸
16	1 ~	0 ~	disable 🗸
		Apply	Revert Apply&Save

Current VLANs

This page lists the current VLANs, their type, and the ports for each VLAN, which are either "Tagged" or "Untagged".

Current VLANs					
VLAN ID	Туре	Untagged Member	Tagged Member		
1	Static / Management	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16			
2	Static				

Configuration – Multicast Filtering

Multicast Filtering
IGMP
IGMP Snooping (?) disable
Snoop Aging Time (?) 300
IGMP Query Version (?) disable
Query Interval (?) 125
Current Querier (?) No Query device available
IGMP Extensions
Extension FUQ (?) enable
Extension BUQ (?) enable
Auto Query Ports (?) enable
(?) Clear AQP
Static Query Ports (?) 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 9 10 11 12 13 14 15 16 (?) Current multicast groups Image: Comparison of the set of
Apply Revert Apply&Save

IGMP Snooping: - disable: The "IGMP Snooping" function is disabled.

- enable: The "IGMP Snooping" function is enabled.

Snoop Aging Time: Set the snoop aging time. This is the time period during which membership reports are expected from the querier. If no membership reports are received during this time, the associated ports are deleted from the multicast groups. The value must be between 30 and 3600 (default is 300).

IGMP Query Version: Here, you can set the IGMP query version which the switch should use to send the queries. The switches support IGMP query versions v1 and v2. For EtherNet/IP applications, it is recommended that you activate version v2.

Query Interval: Here, you can set the interval at which the switch should send the queries.

Current Querier: Displays the IP address of the current querier in the network.

The IGMP querier function can only be used if the device has an IP address. Use of multicast filtering in Unmanaged mode is therefore limited to IGMP snooping.

Clicking on the "Current multicast groups" link opens the "<u>Current Multicast Groups</u>" page as a popup.

Extensions FUQ (Forward Unknown to Querier): Specify whether a multicast group should be created for unknown multicast packets, which forwards the packets in the direction of the querier.

Extension BUQ (Block Unknown at Querier): Specify whether unknown multicast packets should be blocked at the querier.

Auto Query Ports: Specify whether automatic selection of additional query ports is activated. Ports are automatically integrated in every multicast group. In the case of redundancy switch-over, the multicast packets are not blocked because the ports required are already members of the multicast group.

Clear AQP: Button for deleting the ports that are automatically assigned to the groups.

Static Query Ports: Select the ports that are static query ports.

D The device can manage up to 50 dynamic multicast groups.

Click the **Current Multicast Groups** link to open a window that displays the current multicast groups:

Current Multicast Groups							
VLAN ID	Multicast Address	Port Member					
1	01:00:5e:00:01:81	56					
1	01:00:5e:40:0e:c1	56					
1	01:00:5e:40:0f:00	56					
1	01:00:5e:7f.ff.fa	6, 56					

Configuration – Network Redundancy

Network Redundancy	
Spanning-Tree Configuration	
RSTP Mode (?)	802.1D V
Large Tree Support (?)	Disable ~
Fast Ring Detection (?)	Disable v
Bridge Priority (?)	32768
Bridge Hello Time (?)	2
Bridge Forward Delay (?)	15
Bridge Max Age (?)	20
(?)	RSTP Port Configuration
(?)	RSTP Port Configuration Table
(?)	RSTP Diagnostic
Link Aggregation	
Link Aggregation (?)	Configure Link Aggregation
	Apply Revert Apply&Save

Spanning-Tree Configuration Items

RSTP Mode: - Disable: The RSTP function is not activated

- 802.1D: The RSTP function is activated globally and working in accordance with standard IEEE802.1D-2004

The functions below are only available if "802.1D" is activated.

Large Tree Support: This option makes the ring topology suitable for 28 switches along the relevant path if RSTP is used. The Large Tree Support option could provide an RSTP ring topology with up to 57 devices. If the "Large Tree Support" function is enabled, it is recommended to use the default parameters.

Fast Ring Detection: This function speeds up switch-over to a redundant path in the event of an error and enables easy diagnostics. RSTP Fast Ring Detection assigns an ID to each ring. This ID is

communicated to every switch in the respective ring. One switch can belong to several different rings at the same time.

Bridge Priority: The bridge and backup root can be specified via "Bridge Priority". Only multiples of 4096 are permitted. The value will be rounded automatically to the next multiple of 4096. When you click on "Apply&Save", the initialization mechanism is started (default is 32,768).

Bridge Hello Time: Specifies the time interval within which the root bridge regularly reports to the other switches via BPDU.

Bridge Forward Delay: The value indicates how long the switches are to wait for the port state in STP mode to change from "Discarding" to "Listening" and from "Listening" to "Learning" (2 x Forward Delay).

Bridge Max Age: The parameter is set by the root switch and used by all switches in the ring. The parameter is sent to ensure that each switch in the network has a constant value, which is used as the basis for testing the age of the saved configuration.

Clicking on the "RSTP Port Configuration" button takes you to the "RSTP Port Configuration" pop-up (see below).

Clicking on the "RSTP Port Configuration Table" button takes you to the "<u>RSTP Port Configuration</u> <u>Table</u>" pop-up.

Clicking on the "RSTP Diagnostics" button opens the "<u>RSTP Diagnostics</u>" page as a pop-up.

RSTP Port Configuration

RSTP Port Configuration	
Select Port (?	port-1 v
RSTP Enable (?	enable v
Admin Path Cost (?) 0
Operating Path Cost (?) 0
Auto Edge (?) enable 🗸
Admin Edge (?	Non-Edge 🗸
Operating Edge (?) Non-Edge
Priority (?) 128
Forward Transitions (?) 0
Designated Root (?) 8000.00:E0:B3:48:03:90
Designated Bridge (?) 8000.00:E0:B3:48:03:90
Designated Port ID (?) 8001
Designated Cost (?) 0
Protocol Version (?) RSTP
(?	Force RSTP
	Apply Revert Apply&Save

Select Port: Select the port for which you want to change the RSTP settings.

RSTP Enable: - Enable: RSTP is activated for the port

- Disable: RSTP is deactivated for the port

Admin Path Cost: Displays the path costs set for this port. A path cost equal to "0" activates cost calculation according to the transmission speed (10 Mbps = 2,000,000; 100 Mbps = 200,000).

Operating Path Cost: Displays the path costs used for this port.

Auto Edge: Specify whether to automatically switch from non-edge port to edge port after a link up.

Admin Edge: Specify whether this port is to be operated as an edge port (default setting), if possible.

Operating Edge: Shows whether this port is operated as an edge port or a non-edge port.

Priority: Shows the priority set for this port (default is 128).

Forward Transitions: Indicates the number of times the port has switched from the "Discarding" state to the "Forwarding" state.

Designated Root: Shows the root bridge for this spanning tree.

Designated Bridge: Indicates the switch from which the port receives the best BPDUs.

Designated Port ID: Indicates the port via which the BPDUs are sent from the designated bridge. The value is based on the port priority (2 digits) and the port number.

Designated Cost: Shows the path costs of this segment to the root switch.

Protocol Version: Shows the protocol version.

Force RSTP: Clicking on the "Force RSTP" button activates RSTP for the port as long as it has been operated in STP mode beforehand.

RSTP Port Configuration Table

RSTP Port Configuration Table					
Port	RSTP Enab	ole	Admin	Edge	Admin Cost
1	enable	~	Non-Edge	~	0
2	enable	~	Non-Edge	~	0
3	enable	~	Non-Edge	~	0
4	enable	~	Non-Edge	~	0
5	enable	~	Non-Edge	~	0
6	enable	~	Non-Edge	~	0
7	enable	~	Non-Edge	~	0
8	enable	~	Non-Edge	~	0
9	enable	~	Non-Edge	~	0
10	enable	~	Non-Edge	~	0
11	enable	~	Non-Edge	~	0
12	enable	~	Non-Edge	~	0
13	enable	~	Non-Edge	~	0
14	enable	~	Non-Edge	~	0
15	enable	~	Non-Edge	~	0
16	enable	~	Non-Edge	~	0
			[Apply	Revert Apply&Save

Port: Shows the ports for which RSTP is available.

RSTP Enable: Activate or deactivate RSTP for each port individually.

Admin Edge: Specify whether this port is to be operated as an edge port (default setting), if possible.

Admin Cost: Displays the path costs set for this port. A path cost equal to "0" activates cost calculation according to the transmission speed (10 Mbps = 2,000,000; 100 Mbps = 200,000).

Link Aggregation

Clicking on the "Link Aggregation" link takes you to the configuration page for link aggregation:

Link Aggregation						
Available Trunks Trunk ID Trunk Nam	9	Admin	Status	Configure	Delete	
Create New Trunk						
Name of New True	nk (?)					
Create New Tru	nk (?) Create					
			Apply	Revert	pply&Save	

Name of New Trunk: Enter a name for a new trunk.

Create New Trunk: Click on the "Create" button to create a new empty trunk.

Configure: Clicking on the "Configure" link in the table containing all the created trunks opens the configuration page for the respective trunk.

Configure Trunk					
Trunk Number (?	port-52		~		
Admin Mode (?	Enable		~		
Spanning-Tree Mode (?	Enable		~		
Trunk Name (?	Test trunk				
Mode (?	Lacp Activ	/	~		
Member-Ports (?	1 2	3 4	5 6	7 8	
	9 10	11 12	13 14	15 16	
		Appl	У	Revert	Apply&Save

Trunk Number: Select the trunk to be configured by entering its ID.

Admin Mode: Enable or disable a trunk.

Spanning-Tree Mode: Here, select whether the RSTP protocol is to be enabled for this trunk.

Trunk Name: Here, you can change the name of the trunk.

Mode: Here, you can specify how ports are to be added to the trunk.

- If you select "Static", the ports are immediately added to the trunk.
- When "LACP Active/Passive" is selected, the two members of a link aggregation first exchange information via LACPDUs:
- With "Active", this is regardless of whether the peer also has LACP.
- With "Passive", this only occurs after LACPDUs have been received by the peer.

Member-Ports: Select up to four ports that are to belong to the trunk.

Configuration – Security

Security		_	_	
UI Security				
Secure UIs (?)	Security Context			
Port Based Security				
Port Security Status (?)	Disable 🗸			
Port Based Configuration (?)	Configure Port Based Security			
Clear Illegal Counter (?)	Clear			
Global Radius Authentication Server C	onfiguration	_	_	
Radius Server (?)	0.0.0.0			
Radius Server Port (?)	1812			
Radius Shared Secret (?)	••••••	□ Sh	ow cleartext sec	cret
Dot1x Authenticator (?)				
Port Authentication Table (?)	Dot1x Port Configuration Table			
Port Authentication (?)	Dot1x Port Configuration			
		Apply	Revert	Apply&Save

UI Security Items

Secure UIs: Clicking on the "Security Context" link opens the pop-up of the same name.

Port Based Security Items

Port Security Status: Here, you can globally enable and disable port-based security.

Port Based Configuration: Clicking on the "Configure Port Based Security" link takes you to the configuration page for port-based security (see below).

Clear Illegal Counter: Clicking on the "Clear" button sets the illegal access counter for all of the ports to zero.

Global Radius Authentication Server Configuration Items

Radius Server: Here, you can set the IP address of the RADIUS authentication server.

Radius Server Port: Here, you can set the UDP port of the RADIUS server (default is 1812).

Radius Shared Secret: Here, you can set the shared secret required for encrypted communication with the RADIUS authentication server. The shared secret must not exceed 128 characters.

Dot1x Authenticator: Here, you can specify whether the device should be an 802.1x authenticator or not.



One end device can be authenticated via 802.1x per port.

Port Authentication Table: Clicking on the "Dot1x Port Configuration Table" link takes you to the table-based configuration page for RADIUS authentication.

Port Authentication: Clicking on the "Dot1x Port Configuration" link takes you to the port-based configuration page for RADIUS authentication.

Port Based Security

Port Based Secu	rity			
	Port (?) port-1	~		
	Name (?) Port 1			
	Security Mode (?) None	~		
Last M	AC Address Learnt (?) 00:00:00:	:00:00:00 - 0	~	
Illeg	al Address Counter (?) 0			
Allowed MAC Ad	dresses			
Index	Description	MAC Address	VLAN ID	
Add new entry				
1	Address 1	00:a0:45:09:c3:f5	0	*
			Apply	vert Apply&Save

Port: Select the port for which the security settings should be made.

Name: Displays the name of the selected port.

Security Mode: Here, set what happens if a MAC address that is not permitted is detected by the device.

- None: No security settings for this port.

- Trap: If a MAC address that is not permitted is detected at the port, a trap is sent to the defined SNMP trap server. The packets are not blocked.

- Block: If a MAC address that is not permitted is detected at the port, all packets are blocked at the port and a trap is sent to the defined SNMP trap server. The packets at this port remain blocked until a permitted MAC address is detected.

Last MAC Address Learnt: Displays the MAC address of the last connected device. By clicking on the green checkmark, this MAC address can be added to the list of permitted MAC addresses.

Illegal Address Counter: Displays the number of times a port has been accessed illegally. Each initial access by a MAC address is counted. Repeated access by known MAC addresses are counted twice if a different MAC address has accessed the port in the meantime.

Allowed MAC Addresses Items

Up to 50 MAC addresses are permitted per port. Each MAC address can only be permitted at one port. MAC addresses that are permitted at one port also cannot be dynamically learned at other ports. The web-based management or network cannot be accessed via a MAC address that is permitted at another port.

Index: Displays the index of the permitted MAC addresses.

Description: Here, you can provide a description for a permitted MAC address.

MAC Address: Enter a MAC address for which you want to allow access. Alternatively, you can select the green checkmark to the right of the "Last MAC Address Learned" field to use the last MAC address that was learned.

VLAN ID: Enter the VLAN where the device with the permitted MAC address is located.

Clicking on the red "X" to the right of this column deletes the permitted MAC address for this port.

Dot1x Port Configuration Table Page

Dot1x Port Configuration Table		
Interface/Port	Mode	Status
1	Force Authenticate 🗸	Initialize
2	Force Authenticate 🗸	Initialize
3	Force Authenticate 🗸	Initialize
4	Force Authenticate 🗸	Initialize
5	Force Authenticate 🗸	Initialize
6	Force Authenticate 🗸	Initialize
7	Force Authenticate 🗸	Initialize
8	Force Authenticate 🗸	Initialize
9	Force Authenticate 🗸	Initialize
10	Force Authenticate 🗸	Initialize
11	Force Authenticate 🗸	Initialize
12	Force Authenticate 🗸	Initialize
13	Force Authenticate 🗸	Initialize
14	Force Authenticate 🗸	Initialize
15	Force Authenticate 🗸	Initialize
16	Force Authenticate 🗸	Initialize
		Apply Revert Apply&Save

Interface/Port: Displays the port number.

Mode: Here, you can set the authentication mode for the port.

- Auto: Devices connected to the port are authenticated via 802.1x. 802.1x (Dot1x

Authenticator) must be activated for this.

- Force Authenticate: All of the devices connected to the port are authenticated.
- Force Unauthenticate: None of the devices connected to the port are authenticated.

Status: Displays the authentication status of the port

Dot1x Port Configuration Page

x Port Configuration					_		
Por	t (?)	port-1	~				
Authentication Mode	e (?)	Force Authenticate	~				
Authentication Status	s (?)	Initialize					
Re-Authentication Mode	e (?)	Disable	~				
Re-Authentication Period (secs) (?)	3600					
EAPOL Frames Received	1 (?)	0					
Last EAPOL Frame Source	; (?)	00:00:00:00:00:00					
	_						
					Apply	Apply Revert	Apply Revert Apply

Port: Here, select the port for which you wish to carry out RADIUS configuration.

Authentication Mode: Here, you can set the authentication mode for the port.

- Auto: Devices connected to the port are authenticated via 802.1x. 802.1x (Dot1x
- Authenticator) must be activated for this.
- Force Authenticate: All of the devices connected to the port are authenticated.
- Force Unauthenticate: None of the devices connected to the port are authenticated.

Authentication Status: Displays the authentication status of the port

Re-Authentication Mode: Here, you can specify whether a client should be re-authenticated at a regular interval.

Re-Authentication Period (secs): Set the interval at which a client should be re-authenticated (1 ... 65,535 seconds).

EAPOL Frames Received: Displays the received EAPOL packets.

Last EAPOL Frame Source: Displays the last MAC address from which an EAPOL packet was received at the port.

Configuration – DHCP Service

DHCP Service	
DHCP Network Service (?)	Server ~
Running State (?)	Inactive
Pool Start Address (?)	0.0.0.0
Pool Size (?)	32
Network Mask (?)	0.0.0.0
Router IP (?)	0.0.0.0
DNS IP (?)	0.0.0.0
Lease Time (s) (?)	3600
Accept Bootp (?)	enable 🗸
DHCP Port-based Service (?)	Port-based DHCP Configuration
Leases	
(?)	Current DHCP leases
(?)	DHCP static leases
	Apply Revert Apply&Save

DHCP Network Service: Select the DHCP service you wish to use.

- None: No DHCP service will be used on the switch.

- Relay Agent: The DHCP relay agent (DHCP option 82) is enabled.

- Server: The switch will be used as the DHCP server. This can only be activated if the IP Address Assignment mode is set to "STATIC".

When "Relay Agent" is selected as the DHCP network service, the following fields become available:

Option 82: Here, select the address that should be used as the remote ID.

- IP: Uses the IP address of the switch as the remote ID.

- MAC: Uses the MAC address of the switch as the remote ID.

Server IP Address: Here, set the IP address of the DHCP server in your network.

Port Mode: Here, select the ports for which the DHCP relay agent should be activated.

When "Server" is selected as the DHCP network service, the following fields become available:

Running State: Shows the current status of the DHCP server. The status is "Inactive" if some setting options are incorrect.

Pool Start Address: Set the first IP address of the DHCP server address pool.

Pool Size: Set the number of IP addresses in the DHCP server address pool. Please note that the number of IP addresses must match the configured subnet.

Network Mask: Set the subnet mask that is assigned to the DHCP clients.

Router IP: Here, set the router/default gateway IP address that is assigned to the DHCP clients.

DNS IP: Here, set the DNS IP address that is assigned to the DHCP clients.

Lease Time (s): Here, you can set the time that the DHCP server leases an IP address to a client before it has to report to the server again. The value must be between 300 and 2,592,000 seconds; "0" is interpreted as an infinite time (default is 3600).

Accept Bootp: Here, you can specify whether the switch acting as the DHCP server accepts BootP requests. If this function is activated, an IP address with an infinite lease time is assigned to the requesting DHCP clients.

DHCP Port-based Service: Clicking on the "Port-based DHCP Configuration" link opens the "Port-based DHCP Configuration" window (See below).

Leases

Clicking on the "Current DHCP leases" link opens the "<u>Current DHCP leases</u>" window where the IP addresses that are currently assigned are displayed

Clicking on the "DHCP static leases" link opens the "<u>DHCP Static Leases</u>" window for configuring static IP address assignments.

Port-based DHCP Configuration

DHCP Port Local Service		_	_	
Select Port (?)	port-1 🗸			
Local Service enable (?)	disable 🗸			
Local IP (?)	0.0.0.0			
Netmask (?)	0.0.0.0			
Router (?)	0.0.0.0			
DNS (?)	0.0.0.0			
Clear Port Local Service (?)	Clear			
		Apply	Revert	Apply&Save

Select Port: Select the port for which you wish to carry out port-based DHCP server configuration.

Local Service enable: Here, activate the port-based DHCP server function for the selected port.

Local IP: Enter the IP address that is assigned to the client at the selected port.

Netmask: Here, enter the subnet mask that is assigned to the client at the selected port.

Router: Here, enter the gateway address that is assigned to the client at the selected port.

DNS: Here, enter the DNS address that is assigned to the client at the selected port.

Current DHCP Leases

Current DHCP leases						
Leased IP	Client ID	System Uptime	Local Port	State		
192.168.1.50	00:a4:45:70:d9:34			static		
	Lease count (?) 1					
	(?) Rele	ease				

Leased IP: Displays the assigned IP addresses.

Client ID: Displays the MAC address of the client to which the IP address is assigned.

System Uptime: Displays the time that has elapsed since the IP address was assigned to the client.

Local Port: Displays the port to which the client is connected.

State: Displays the status of the client.

Lease count: Displays the number of assigned IP addresses.

Release: Clicking on the "Release" button releases unused entries again.

DHCP Static Leases

DHCP Static	Leases		
Lease list No	IP address	Client address	Delete
1	192.168.1.50	00:a4:45:70:d9:34	*
Create new s	static entry		
	IP address (?)		
	Client address (?)		
	(?) Create		
	Clear static table (?) Clear		

Lease list Items

IP address: Displays the static IP address that is assigned.

Client address: Displays the MAC address of the client.

Delete: Clicking on the red "X" in the "Delete" column deletes the entry.

Create new static entry items

IP address: Enter the static IP address that you wish to assign.

Client address: Enter the MAC address to which you wish to assign a static IP address.

Create: Click on the "Create" button to perform the static assignment.

Clear static table: Click on the "Clear" button to delete all the static DHCP leases.

Configuration – Local Events

Local Events						
Alarm Output 1						
Alarm Output Enal	ble (?) Enable	~				
Alarm Output State (?) Failed						
Event	Alarm Output 1		Ac	dvanced		
Power Supply Lost	o					
Monitored Link Down			<u>P</u> (orts [+/-]		
			Apply	Revert	Apply&Save	

Alarm output 1

Here, you can activate the digital alarm output or signal contact and read the current status (if a red "o" is present, this event has occurred).

Events

Specify the conditions under which the digital alarm output or signal contact should report an error.

Power Supply lost: An error message is generated if supply voltage PWR1 or PWR2 is lost.

Monitored link down: Under "Advanced", select the ports to which link down behavior should be reported.

Configuration – Quality of Service

Quality of Service	
Traffic Prioritization	
Quality of Service Profile (?	') Universal 🗸
Port Priority (?	Configure Port priority for multiple ports at once
Broadcast Limiter	
Broadcast (?	') disable 🗸
Broadcast Threshold (?) 1024
Multicast (?) disable 🗸
Multicast Threshold (?) 1024
Unknown Unicast (?) disable 🗸
Unicast Threshold (?) 1024
If you are not firm with handling the	dimension packet per seconds the following link will help you. \underline{Help}
Flow Control	
Port Configuration (?) Configure Flow control per port
Port Configuration Table (?	Configure Flow control for multiple ports at once
	Apply Revert Apply&Save

Traffic Prioritization

The switch has eight priority queues into which incoming data traffic is sorted according to specific criteria. These queues are processed in descending order of priority. High-priority data traffic is therefore always forwarded first.

Quality of Service Profile: Select the profile for prioritizing data traffic.

- Universal: This profile is the factory setting on standard versions. Class of Service (VLAN tag priority) is activated for data prioritization.

- EtherNet/IP: In this profile, prioritization via DSCP values is activated in addition to Class of Service. This means that preferential treatment is given to EtherNet/IP data traffic. Only control packets of redundancy protocols (such as RSTP) are given even higher priority.

Port Priority: Clicking on the link takes you directly to the configuration page for the default priority. Incoming data traffic on the device that does not have a priority tag is marked according to the setting

and is assigned to a priority queue. To activate these settings, the VLAN mode of the device must also be set to "Tagged".

Broadcast Limiter items

Broadcast: Activate or deactivate the broadcast limiter.

Broadcast Threshold: Set the threshold value in frames per second for the broadcast limiter. The value entered is rounded down to the next valid value.

Multicast: Activate or deactivate the multicast limiter.

Multicast Threshold: Set the threshold value in frames per second for the multicast limiter. The value entered is rounded down to the next valid value.

Unknown Unicast: Here, you can activate or deactivate the limiter for unknown unicasts. Unicasts of a MAC address that have been learned by the switch are not affected.

Unicast Threshold: Here, set the threshold value in frames per second for the limiter of unknown unicasts. The value entered is rounded down to the next valid value.

Flow Control items

Port Configuration: Clicking on the "Configure Flow Control per port" link opens the "Port Configuration" page, which contains the configuration options for flow control.

Port Configuration Table: Clicking on the "Configure Flow control for multiple ports at once" link opens the "<u>Port Configuration Table</u>" page where flow control can be configured for all ports.

Diagnostics – LLDP Topology

LLDP Topology						
Local Port	Chassis ID	IP Address	Remote Port			
16	F8:75:A4:8B:07:7D		F8:75:A4:8B:07:7D			

Local Port: Contains the port number of the local switch that is used to connect a neighbor to this switch.

Chassis ID: MAC address of the connected neighboring device.

IP Address: Management IP address for the neighbor.

Remote Port: Port number of the neighboring switch that is used to connect the neighbor to the local switch.

Diagnostics –	RSTP	Diagnostic
----------------------	-------------	------------

RSTP Diagnostic	
Designated Root (?)	This device is the Root
Root Port (?)	0
Root Cost (?)	0
Topology Changes (?)	0
Last Topology Change (?)	0s ago
Hello Time (?)	2
Forward Delay (?)	15
Max Age (?)	20
(?)	Redundancy Port Table

Designated Root: Shows the root bridge for this spanning tree.

Root Port: Displays the port to which the root is connected. If the root is not directly connected, it shows the direction of the root.

Root Cost: Displays the total path costs for the root.

Topology Changes: Displays the number of topology changes.

Last Topology Change: Displays when the last topology changes took place.

Hello Time: Shows the hello time set at the root.

Forward Delay: Shows the forward delay set at the root.

Max Age: Shows the maximum age time set at the root.

Clicking on the "Redundancy Port Table" button opens a table containing information about the individual ports and their redundancy mechanism assignment:

Redundancy Port Table						
Further Redundancy State Information						
	(?) RSTP Port Config	uration				
Physical Ports						
Port	Protocol	Blocking State	Protocol Role			
1	RSTP	Disabled	Disabled			
2	RSTP	Disabled	Disabled			
3	RSTP	Disabled	Disabled			
4	RSTP	Disabled	Disabled			
5	RSTP	Disabled	Disabled			
6	RSTP	Disabled	Disabled			
7	RSTP	Disabled	Disabled			
8	RSTP	Disabled	Disabled			

Diagnostics – Current VLANs

Refer to Configuration - VLAN Configuration - Current VLANs

Diagnostics – Current Multicast Groups

Refer to Configuration - Multicast Filtering - Current Multicast Groups

Diagnostics – Port Mirroring

The port mirroring function allows you to mirror the incoming and outgoing data traffic of individual ports to one port where it can be analyzed using a connected diagnostic device or tool.

Port Mirroring										
Global Status (?)	Disable			~						
Destination Port (?)	port-1			~						
Mirrored Ports (Ingress) (?)	1 2 9 10 52	3 11	4 12	5 13	6 14	7 15	8 16			
Mirrored Ports (Egress) (?)	1 2 9 10 52	3 11 	4 12	5 13	6 14	7 15	8 16			
		A	Apply		F	Revert	:	Apply	&Save	

Global Status:

- Enable: Port mirroring is activated globally
- Disable: Port mirroring is deactivated globally

Destination Port: Select the port to which the diagnostic device or tool is connected.

Mirrored Ports (Ingress): Specify the ports from which the incoming data traffic should be mirrored.

Mirrored Ports (Egress): Specify the ports from which the outgoing data traffic should be mirrored.

Diagnostics – Trap Manager

Trap Manager			
	Trap Mode (?) Disable	~	
	Trap Server (?)	*	
	Add Trap Server (?)	Add	
Te:	st Trap Connection (?) Send Trap		_
Index	Trap Name	Mode	_
1	Cold Start		
2	Warm Start		
3	3 User Password Changed 🗸		
4	4 Authentication Failure		
5	Firmware Configuration		
6	Power Source Changed		
7	RSTP Link Failure		
8	RSTP New Root		
9	RSTP Topology Change		
10	Link Down		
11	Link Up		
10	Port Socurity Violation	-	
		Apply Revert Ap	ply&Save

Trap Mode: - Enable: The sending of SNMP traps is enabled

- Disable: The sending of SNMP traps is disabled

Trap Server: All trap servers that are to receive SNMP traps from this device are displayed here.

Add Trap Server: Enter the IP address or DNS name of a trap server and click on "Apply&Save" to create this trap server.

Test Trap Connection: Click on the "Send Trap" button to test the connection to the trap server.

The table lists the SNMP traps that the device can send. Select the actions for which SNMP traps should be sent by clicking the corresponding check boxes.

Diagnostics – Port Counter

This page provides an overview of the port statistics for the device. Four views provide an overview of the general, sent and received packets, errors, and collisions on the individual ports.

Port Counter	_	_	_	_	
Overview	ransmit Receiv	ve Surveillance			
Port Counter Ove	erview				
Interface/Port	Received Packets	Transmitted Packets	CRC Errors	Drop Events	Collisions
1	0	0	0	0	0
2	0	0	0	0	0
<u>3</u>	0	0	0	0	0
<u>4</u>	0	0	0	0	0
<u>5</u>	0	0	0	0	0
<u>6</u>	0	0	0	0	0
Z	0	0	0	0	0
<u>8</u>	0	0	0	0	0
<u>9</u>	0	0	0	0	0
<u>10</u>	0	0	0	0	0
<u>11</u>	0	0	0	0	0
<u>12</u>	0	0	0	0	0
<u>13</u>	0	0	0	0	0
<u>14</u>	0	0	0	0	0
<u>15</u>	0	0	0	0	0
<u>16</u>	13706	26471	0	0	0
Clear s	statistics of all ports (?) Clear			

Interface/Port: Clicking on one of the port numbers in the "Interface/Port" column takes you to the <u>Port Details</u> page. Here, you can view detailed statistics about the sent and received data packets for every port. In addition, the current and maximum port utilization is displayed as a percentage.

Clear statistics of all ports: Clicking on the "Clear" button resets all of the port counters in the Overview, Transmit, and Receive views to zero.

In Surveillance view, click the button to reset the CRC Proportion Peak and CRC Status of all ports.

Port Configuration: Clicking on the "Configure Ports" link opens the "Port Configuration" page.

Port Details Page

Port Counter Details	
Port Counter Overview	
Port Counter Overview (?)	Monitor all ports simultaniously
Port (?)	port-16 V
Name (?)	Port 16
Utilization Details	
Tx Utilization (%) (?)	0
Rx Utilization (%) (?)	0
Rx max Utilization (%) (?)	0
Received Port Details	44005
Hackels (Rx) (?)	12004
Multicest (Rx) (?)	13004
Breadcast (Rx) (?)	520
G4 Octate (Dv) (2)	7000
64 Octets (RX) (?)	
128 To 255 Octets (Rx) (?)	945
256 To 511 Octets (Rx) (?)	6
512 To 1023 Octets (Rx) (?)	5450
1024 To 1518 Octets (Rx) (?)	11
Fragments (?)	0
Undersize (?)	0
Oversize (?)	0
CRC errors (?)	0
Jabbers (?)	0
Drop Events (?)	0
Transmission Port Details	
Packets (Tx) (?)	28962
Unicast (Tx) (?)	13769
Multicast (Tx) (?)	15193
Broadcast (Tx) (?)	0
Clear Port Statistics (?)	Clear

Port Counter Overview: Clicking on the "Monitor all ports simultaneously" link takes you back to the "Port Counter" overview page.

Clear Port Statistics: Clicking on the "Clear" button resets all of the counters for the currently displayed port to zero.

Diagnostics – Port Utilization

Here you will find an overview of the percentage port utilization for this device. For a detailed overview, click on the graph of an individual port.



Diagnostics – Snapshot

You can use the snapshot function to capture and download all parameters relevant to the runtime (e.g., configuration, events, etc.) and provide them to a service technician.

Snapshot	
Take snapshot (?) Snapshot	
Current snapshot state (?) Not present	
Timestamp of last snapshot (?) No snapshot file present	
Download of snapshot file (?) <u>File transfer</u>	

Take snapshot: Click the "Snapshot" button to take a snapshot.

Current snapshot state: Indicates whether the snapshot is available, is currently being generated or does not exist.

Timestamp of last snapshot: Displays the time at which the last snapshot was generated.

Download of snapshot file: Clicking on the "File transfer" link opens the window for manual file download.

Diagnostics – Syslog

The Syslog function enables messages or events to be transmitted to one or more servers via UDP. In the event that two Syslog servers have been configured, the switch sends all messages/events to both servers.

Syslog		_	_	_	
	Activate syslog (?) 🗌 Enable				
	Syslog server 1 (?) 0.0.0.0				
	Syslog server 1 port (?) 514				
	Syslog server 2 (?) 0.0.0.0				
	Syslog server 2 port (?) 514				
S	Syslog test message (?) Send message				
Index	Message group			Status	3
1	Connectivity				
2	Diagnosis			~	
3	Automation protocol			~	
4	System information			~	
5	Redundancy			~	
6	Security			~	
			Apply	Revert	Apply&Save

Activate syslog: Activate or deactivate the Syslog function here.

Syslog server 1: Set the IP address or DNS name of the first Syslog server here.

Syslog server 1 port: Set the UDP port of the first Syslog server here (default: 514).

Syslog server 2: Set the IP address or DNS name of the second Syslog server here.

Syslog server 2 port: Set the UDP port of the second Syslog server here (default: 514)

Syslog test message: Click on the "Send message" button to test the connection to the Syslog server. With Syslog, message reception is not confirmed by the server. Therefore the connection status can only be checked on the server, and not in the web-based management of the switch.

Status: Use the check boxes in the "Status" column to select the categories whose events are to be sent to the Syslog server.

The table below provides an overview of the specific events in the respective categories.

	IP conflict detected
	TFTP connection failed
	ACDconflict detected IP
	LLDP new neighbor on port
	LLDP neighbor information changed on port
Connectivity	Link monitor alarm raises on port
	IP address changed on interface
	Port Link up/down
	SFP module plugged on Port
	ACD device has no IP
	MTU size changed
	CRC status and peak on port reset
	CRC status on port changed to ok
Diagnosis	CRC status on port changed to critical
	CRC thresholds on port changed by user
	Alarm output failed
	CRC status on port changed to warning

	System time synchronized
	Pluggable memory removed
	Update firmware successful
	Configuration saved/loaded on/from pluggable memory
	Update failed
	Configuration difference detected
	Configuration saved/loaded successfully
	Configuration parameter changed
	Smart Mode entered
	Smart Mode button enabled/disabled
	Error in configuration file
System information	Pluggable memory cleared
	New interface created
	Power supply lost
	Name of the device changed
	Parameter has been changed by the user
	FW image not valid
	Update processing
	Write to flash memory
	Wrong update image
	IGMP Snooping mode changed
	IGMP Snooping aging time changed
	Syslog test message
	Start FW update
	Write FW image into flash
	RSTP ring detected
Redundancy	RSTP topology changed
	RSTP root changed
	RSTP ring failed

CLI (Command Line Interface)

Using the Command Line Interface (CLI)

The CLI is a text-based tool that can be used to configure the switch. The CLI is accessed by means of a connection via Telnet (factory default) or SSH. A third-party program such as PuTTY can also be used for connection.

Connect to the IP address of the switch and enter the username (default is **root**) and password (default is blank). The switch model/SKU number will be displayed.

🚽 Telnet 192.168.1.10	
(SG300-16) User: root Password: **********	
SG300-16 ************************************	

Basic Principles of CLI Commands

In this manual, **CLI command names** are in bold. *CLI parameters* are in italics and must be replaced by appropriate values (e.g., names or numbers). If a command has several parameters, the order of these must be strictly observed.

The parameters of a command may be mandatory, optional or a selection of values (see Command Syntax table below).

Command Syntax Symbols

The following symbols are used to describe the values and arguments for command entries in the CLI.

<angle brackets=""></angle>	Variable or value that must be specified.
[square brackets]	Optional parameters or arguments.
optionA optionB	Vertical bar. Separates multiple exclusive items in a list of options.
{braces}	Denotes the mandatory selection of a value from a given list of values
[{}] Braces within square brackets	Denotes a selection within an optional parameter

Command Syntax

A command consists of one or more terms which can be followed by one or more parameters. These parameters can be mandatory or optional values.

Some commands, e.g., **show network** or **clear config**, do not require parameters. Other commands, e.g., **network parms**, require values to be specified after the command name. The parameters must be entered in the specified order, whereby optional parameters always follow mandatory parameters.

The following example illustrates the syntax using the **network parms** command:

network parms <ipaddr> <netmask> [gateway]

network parms is the command name. <ipaddr> and <netmask> are parameters and represent mandatory values, which must be specified after entering the command name. [gateway] is an optional parameter, which means that a value does not have to be specified.

The following examples illustrate the *correct* syntax for entering the **network parms** command:

network parms 192.168.10.42 255.255.255.0

network parms 192.168.10.42 255.255.255.0 192.168.10.0

The following examples illustrate *incorrect* syntax for entering the network parms command:

network parms 192.168.10.42 - missing mandatory parameter

network parms 255.255.255.0 - missing mandatory parameter

network parms 255.255.255.0 192.168.10.42 - incorrect parameter sequence

Using the CLI Help

Entering a question mark (?) in the command prompt displays a list of all the commands currently available together with a brief description. Typing a question mark (?) after each entry displays all the available command names or parameters from that point on.

Auto Completion of Commands

The auto completion command is an additional way of writing a command, provided enough letters have already been entered to clearly identify the command name. As soon as enough letters have been entered, press space or TAB to automatically complete the words.

Using the CLI Network Scripting UI

The CLI network scripting UI enables CLI commands from scripts to be loaded into the device via the network. This means that the device can be configured and diagnosed using a URL via a PC or from a controller. Each command that is entered is confirmed by the device, either with OK (config commands) or by outputting the device data (show commands).

The command entry must follow a specific syntax:

http://ipaddress/php/command.php?usr=username&pwd=password&cmd=cli_command_1 | cli_command_2 |

The following examples illustrate the correct syntax for entering commands via the CLI network scripting UI:

Example: changing the device name

http://192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=device-identity name SmartE

Image: Contract of the second state of the second state

Example: displaying the network parameters and changing the user password

http://192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=show network | users passwd private2

🗲 🞯 192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=show network users passwd private2
OK IP Assignment : bootp IP Address : 192.168.10.42 Network Mask : 255.255.255.0 Default Gateway : 0.0.0.0 Management VLAN : 1 ACD Mode : None ERROR
CLI Commands

General Commands

Command		Value range	Default
reload			
Description Restart the device			
Example	reload		

Command		Value range	Default
logout			
Description Exit the CLI session (unsaved changes will be lost).			
Example	logout		

Command		Value range	Default
help			
Description Open the CLI help			
Example	help		

Command		Value range	Default	
quit				
Description	scription Exit the CLI session (unsaved changes will be lost).			
Example	quit			

Command		Value range	Default	
show tech-support				
Description				
Example	show tech-support			

Command		Value range	Default	
clear config				
Description Reset configuration to factory default.				
Example	clear config			

Command		Value range	Default
write <config< th=""><td>guration-name></td><td>Max. 256 chars</td><td></td></config<>	guration-name>	Max. 256 chars	
Description Save the device configuration.			
Example	write prodconfig		

Command		Value range	Default
show configuration-status			
Displays the following items: Configuration Name Configuration Status (modified, save Configuration Source		ed, not saved, etc)	
Example	show configuration-status		

Command	Value range	Default		
users create {username} {password} {repeat-	Password 8 – 64 characters			
password}				
Description Create a new user				
Example users create kautsky password123	users create kautsky password123 password123			

Command		Value range	Default	
users delete {username}				
Description Delete a user				
Example	users delete kautsky			

Command		Value range	Default	
users passwd <username> <old-password></old-password></username>		New password (8 - 64 chars)		
<new-password> <repeat-new-password></repeat-new-password></new-password>				
Description Change a user password				
Example users passwd admin?	oldpass Switc	h123 Switch123		

Command		Value range	Default
users roles create <rolename></rolename>			
Description Create a new rolename			
Example	users roles create testrole		

Command		Value range	Default
users roles delete <rolename></rolename>			
Description Delete a rolename			
Example	users roles delete testrole		

Command		Value range	Default
users role <username> {admin expert read-</username>			
only}			
Description Set user role.			
Example	Users role gandalf admin		

Command		Value range	Default
users status <username> {enable disable}</username>			
Description Enable or disable a user account. A disabled user cannot login to the device anymore.			
Example	users status noobuser enable		

Command		Value range	Default
users lock-status <username> {enable </username>			
disable}			
Description	Enable or disable the mode that a user access to the device is denied if the configured number		
Description	of consecutive invalid login attempts has been reached.		
Example	users lock-status newuser1 disable		

Command		Value range	Default
users lock-limit <username> <lock-limit></lock-limit></username>		(1 – 100)	
Description Set user lock limit			
Example	users lock-limit userbob 5		

Command		Value range	Default
users lock-timeout <username> <value></value></username>		1-1440 minutes	
Description Set user lock timeout			
Example	users lock-timeout userbob 5		

Command	Value range	Default	
users roles add-group-ro {rolename} {system ident user network ui automation discovery I2I3 redundancy timesynch dhcp port-cfg rmon port-mirr port-sec routing logging}			
Description Add permission group to role with read-only capabilities			
Example users roles add-group-ro testgroup	o ui		

Command	Value range	Default		
users roles add-group-rw {rolename} {system ident user network ui automation discovery I2I3 redundancy timesynch dhcp port-cfg rmon port-mirr port-sec routing logging}				
Description Add permission group to role with read-write capabilities				
Example users roles add-group-rw testgroup	o ui			

Command		Value range	Default
users roles i	remove-group <rolename></rolename>		
<permissiongroup></permissiongroup>			
Description Remove permission group from role			
Example	users roles remove-group testrole c	liscovery	

CRC Surveillance Commands

Command		Value range	Default
show surveillance crc port-no <port></port>			
Description Displays the CRC information of the selected port.			
Example	show surveillance crc port-no 5		

Command		Value range	Default
show surveillance crc all			
Description Shows the CRC information of all ports.			
Example	show surveillance crc all		

Command		Value range	Default
show port-info port-no <port></port>			
Description Displays port information of the selected port, including the CRC status.			
Example	show port-info port-no 5		

Command		Value range	Default
show snmp-	trap		
Description	Description Shows all SNMP traps, including the CRC trap (ok / warning / critical).		
Example			

Command		Value range	Default
clear crc-surveillance port-no <port></port>			
Description Sets the CRC error counter of the selected port to 0 and the CRC error status to OK.		is to OK.	
Example	clear crc-surveillance port-no 5		

Command		Value range	Default
clear crc-surveillance all			
Description	Description Sets the CRC error counter of all ports to 0 and the CRC error status to OK		
Example			

Command		Value range	Default	
port <port> crc-threshold <threshold></threshold></port>		1000 ppm to 1000000 ppm	40000	
Description Sets the CRC threshold for the selected port				
Example	port 5 crc-threshold 50000			

Port Security Commands

Command		Value range	Default	
port-security	v status {enable disable}		disable	
Description Enable or disable port security				
Example	port-security status enable			

Command		Value range	Default
port-security	/ port <port-no> status <status></status></port-no>	{none trap block}	
Description Set port security mode for a specific port none: no security function trap: send trap when a new device/new MAC address is detected block: block everything except the exceptions entered (whitelist)			
Example	port-security port 1 status trap		

Command		Value range	Default
port-security <vlan></vlan>	port <port-no> add-mac <mac></mac></port-no>	MAC: (xx:xx:xx:xx:xx)	
Create new filter entry Description An entry consists of MAC and VLAN. Always use "VLAN 1" for WLAN. Note: the command "port-security port 10 configure" can be used to add a description.		escription.	
Example	port-security port 10 add-mac 00:A0:45:DD:5E:8C 1		

Command		Value range	Default	
port-security <mac> <vl< th=""><th>/ port <port-no> remove-mac AN></port-no></th><th>MAC: (xx:xx:xx:xx:xx) VLAN: for WLAN: 1</th><th></th></vl<></mac>	/ port <port-no> remove-mac AN></port-no>	MAC: (xx:xx:xx:xx:xx) VLAN: for WLAN: 1		
Description	Description Remove filter entry. The entry is specified via MAC and VLAN.			
Example	port-security port 10 remove-mac 00:a0:45:dd:5e:8c 1			

Command		Value range	Default
port-security <vlan> des</vlan>	<pre>v port <port-no> configure <mac> scription <description></description></mac></port-no></pre>	description: (15 characters)	
Description Add or edit description for filter entry. The entry is specified via MAC and VLAN.			
Example	port-security port 10 configure 00:a0:45:dd:5e:8c 1 description "Testdesc1"		

Command		Value range	Default
show port-se	ecurity port <port-no></port-no>	Port: (1 all)	
Show port security port security settings for the port: Show all current security settings for the port: Security mode Description Last MAC Address Learned Illegal Address Counter Allowed MAC Address table with columns (description, MAC-address, VLAN ID)		I ID)	
Example	show port-security port 1		

Command		Value range	Default	
show port-security global				
Description Shows the global port security settings				
Example	show port-security global			

Command		Value range	Default
port-security	/ clear-illegal-cntr		
Description	Clear port security illegal counters.		
Example	port-security clear-illegal-cntr		

Radius Commands

Command		Value range	Default	
users radius	auth-server_Id <id> name</id>			
Description Configure the name of the authentication server				
Example users radius auth-server_ld 1 name testname				

Command		Value range	Default
users radius	auth-server_Id <id> shared-secret</id>		
Description	Shared secret (password) for login	to Radius server	
Example	users radius auth-server_Id 1 share	ed-secret "MySecret"	

Command		Value range	Default	
users radius	auth-server_Id <id> udp-port</id>			
Description Radius server port				
Example	users radius auth-server_Id 1 udp-p	oort 8888		

Command	Value range	Default	
users radius auth-server_ld <ld></ld>	ip-address		
Description IP address of the Ra Only "1" may be use	dius server d as the Id at present.		
Example users radius auth-se	users radius auth-server_Id 1 ip-address 192.168.0.250		

Dot1x Authentication Commands

Command		Value range	Default
show dot1x-	authenticator global		
Description Displays the global dot1x mode.			
Example	show dot1x-authenticator global		

Command		Value range	Default
show dot1x-	authenticator port <port-no></port-no>		
Description	Shows the following parameters for Control Mode, Guest VLAN, Re-Au MAC Address, Status	dot1x on a selected port: thentication Mode, Re-Authentication Tin	neout, Last EAPOL
Example	show dot1x-authenticator port 5		

Command		Value range	Default	
dot1x-authenticator port <port-no> reauthenticate</port-no>				
Description Reauthenticate the client on the given port.				
Example	dot1x-authenticator port 10 reauthe	nticate		

Command		Value range	Default
dot1x-authe	nticator port <port-no></port-no>	1 - 65535 seconds	
reauthentication-period <value></value>			
Description Re-Authenticate client at regular interval defined by the period.			
Example	dot1x-authenticator port 10 reauthe	ntication-period 100	

Command		Value range	Default
dot1x-authenticator port <port-no></port-no>			
reauthentica	tion-mode {enable disable}		
Decerintien	Enable Re-Authentication mode to authenticate the client at regular interval defined by Re-		
Description	Authentication Period.	-	-
Example	dot1x-authenticator port reauthentication-mode enable		

Command		Value range	Default
dot1x-authenticator port <pre>port-no> control- made (aute ferrer authenticate ferrer </pre>			
unauthentica	ate}		
Description	ription Configure 802.1x on this port. Force Authenticate: Authenticate all the devices on this port. (Disable 802.1x) Force Unauthenticate: Do not authenticate any device on this port.		es on this port. nis port.
Example	dot1x-authenticator port 10 control-mode force-authenticate		

Command		Value range		Default
dot1x-authe	nticator global {enable disable}			
Description Enable or Disable dot1x authenticator globally.				
Example	dot1x-authenticator global enable			

System Commands

Command		Value range	Default
show version			
Description	Display the device description and I Serial number Hardware version Firmware version Bootloader version	hardware information:	
Example	show version		

Command		Value range	Default
show sys-info			
Description	Display the system information: Device name Object ID Device description Contact person Device location		
Example	show sys-info		

Command		Value range	Default
device-ident	ity name <name></name>	<name> max. 256 chars</name>	SmartE
Description Change the device name			
Example	device-identity name Switch-xyzzy		

Command		Value range	Default	
device-ident	ity description <description></description>	<description> max. 256 chars</description>		
Description Change the device description				
Example	xample device-identity description Switch dilvish			

Command		Value range	Default	
device-ident	ity location <location></location>	<location> max. 256 chars</location>		
Description Change the device location				
Example	ample device-identity location Nakatomi tower			

Command		Value range	Default	
device-identity contact <contact></contact>		<contact> max. 256 chars</contact>		
Description Change the contact person for the device				
Example	le device-identity contact Thomas A. Anderson			

Command		Value range	Default
snapshot tri	gger		
Description Trigger the snaphot function to capture the current runtime parameters.			
Example	snapshot trigger		

Command		Value range	Default
show snaps	hot status		
Description	Description Shows the status of the SnapShot file (not present / busy / present / error).		
Example	show snapshot status		

Command		Value range	Default
show snapshot timestamp			
Description Shows the timestamp of the last snapshot.			
Example	show snapshot timestamp		

Command		Value range	Default
show transfe	er-status		
Description Shows the status of the currently running snapshot transfer			
Example	show transfer-status		

Command		Value range	Default	
snapshot tri	gger			
Description Creates a snapshot with the currently applied parameters.				
Example	snapshot trigger			

Command		Value range	Default	
file-transfer snapshot <i< th=""><th><method> read-from-device paddress> <file-name></file-name></method></th><th></th><th></th></i<>	<method> read-from-device paddress> <file-name></file-name></method>			
Description Starts the download of the snapshot from the device				
Example	file-transfer tftp read-from-device sr	napshot 192.168.1.40 Snap1		

Command		Value range	Default
show syslog	message-group		
Description Shows the activation status of the group messages.			
Example	show syslog message-group		

Command		Value range	Default
show syslog	status		
Description Shows the activation status of the syslog function on the switch.			
Example	show syslog status		

Command		Value range	Default
show syslog server			
Description Shows the syslog server parameters			
Example	show syslog server		

Command		Value range	Default
syslog statu	s {enable disable}		
Description	Activate or deactivate the syslog function. The deactivated syslog prevents any communication		
	to a syslog server.		
Example	syslog status enable		

Command	Value range	Default
syslog server <value> ip-address <ip address<="" td=""><th>></th><th></th></ip></value>	>	
Description Configure the IP address of the syslog server.		
Example syslog server 1 ip-address 192.16	58.1.200	

Command		Value range	Default
syslog server <value> udp-port <port></port></value>			
Description Configure the UDP port of the syslog server.			
Example	syslog server 1 udp-port 10		

Command		Value range	Default
syslog send-test-message			
Description Send a test message to test the configuration.			
Example	syslog send-test-message		

Command	Value range	Default
syslog message-group <value> {enable </value>	1 Connectivity	
disable}	2 Diagnosis	
	3 Automation protocol	
	4 System information	
	5 Redundancy	
	6 Security	
Description Enable / disable a message group		
Example syslog message-group 1 disable		

Event Table Commands

Command		Value range	Default
show event-table			
Description	Display the event table with the following columns: Index Event Device runtime		
Example	show event-table		

Command		Value range	Default
clear event-table			
Description Delete/clear the event table			
Example	clear event-table		

MAC Address Table Commands

Command		Value range	Default
show mac-address-table			
Description Display the MAC address table			
Example	show mac-address-table		

Command		Value range	Default
clear mac-address-table			
Description Clear the MAC address table.			
Example	clear mac-address-table		

FW Image Handling Commands

Command		Value range	Default
file-transfer tftp write-to-device firmware <ip-< th=""><th><ip-address> IP address</ip-address></th><th></th></ip-<>		<ip-address> IP address</ip-address>	
address> <filename></filename>		(XXX.XXX.XXX.XXX)	
Description	Transfer of a firmware image file to the device. The firmware update is performed immediately,		
Description	the device then restarts and the CLI connection is terminated.		
Example	ample file-transfer tftp write-to-device firmware 192.168.0.1 SMARTE_v1_00.bin		

Script Handling Commands

Command		Value range	Default	
show script				
Description				
Example	show script			

Network Commands

Command		Value range	Default
show network			
Description	Display the current network parame IP address assignment (static, Boot IP address Network mask Default gateway Management VLAN Address Conflict Detection (ACD) n	eters: iP, DHCP) node	
Example	show network		

Command		Value range	Default
network parms <ip-address> <netmask></netmask></ip-address>		<ip-address> (xxx.xxx.xxx.xxx)</ip-address>	0.0.0.0
[gateway]		<netmask> (xxx.xxx.xxx.xxx)</netmask>	0.0.0.0
		[gateway] (xxx.xxx.xxx.xxx)	0.0.0.0
	Change the network parameters:		
Description	IP address		
Description	Network mask		
	Default gateway		
Example	network parms 192.168.0.150 255.255.255.0		

Command		Value range	Default
network protocol {bootp dhcp none}			bootp
Description Change the IP address assignment			
Example	network protocol dhcp		

Command		Value range	Default
network mg	mt-vlan <vlan-id></vlan-id>	VLAN ID (1 - 4000)	1
Description Change the management VLAN			
Example	network mgmt-vlan 2		

Command		Value range	Default
network acd-mode {acd none}			None
Description Change the ACD (Address Conflict Detection) mode			
Example	network acd-mode acd		

Command		Value range	Default	
network dns-server <1 2> <ip address=""></ip>		<1 2> Primary or secondary DNS		
		server (xxx.xxx.xxx.xxx)		
Description Configure the DNS server				
Example	network dns-server 1 192.168.1.250			

Command		Value range	Default	
network hostname resolution {enable disable}			enable	
Description Activate / deactivate host name resolution.				
Example	network hostname resolution disabl	le		

Command		Value range	Default	
network hostname name <hostname></hostname>				
Description	escription Configure the host name of the device.			
Example	ple network hostname name Glamdring			

Command		Value range	Default
lldp initial-ip-port			
Description Configure topology based initial IP port.			
Example	lldp initial-ip-port		

Services Commands

Command		Value range	Default
show service	e {sntp general}		
Description	Status indicator for all of the followin Sntp Network time protocol Primary SNTP server Primary server description Primary server name Secondary SNTP server Secondary server description Secondary server name UTC offset Synchronization Status Last SNTP synchronization General Web server SNMP server CLI service CLI network scripting UI (CLI com	ng services: mand entry via URL)	
Example	show service sntp		

Command		Value range	Default
service cli-service {telnet ssh disable}			Telnet
Description Change the CLI service protocol.			
Example	service cli-service telnet		

Command		Value range	Default
service cli-network-script-ui {enable disable}			enable
Description	Description Activation/deactivation of the CLI network scripting UI (CLI command entry via URL)		
Example	service cli-network-script-ui disable		

Command		Value range	Default
service web-server {disable http https}			http
Description Change the web server protocol			
Example	service web-server https		

Command		Value range	Default
service snmp-agent {disable snmp-v2 snmp-			snmp-v2
v3}			
Description	Description Change the SNMP server		
Example	service snmp-agent snmp-v2		

Command		Value range	Default
service login-expire <time></time>		60 – 3600 seconds	1200
Description Configure login expire time.			
Example	service login-expire 3600		

Command		Value range	Default
service snmpv2-read-comm {tx}		Max. 255 characters	
Description	Description Configure SNMPv2 read community.		
Example	service snmpv2-read-comm 100		

Command		Value range	Default
service conf	idential-web-view {enable disable}		
Description	Description Enable Disable a required user login for the web site access.		
Example	service confidential-web-view enable	le	

Command	Value range	Default
service smart-mode {enable disable}		
Description Enable Disable smart mode (mode button).		
Example service smart-mode disable		

Command		Value range	Default
service persistent-evt-log {enable disable}			enable
Description	Description Enable Disable persistent storage of event-table.		
Example	service persistent-evt-log enable		

Command		Value range	Default
service sntp status {enable disable}			disable
Description Activate / deactivate the global SNTP status.			
Example	service sntp status enable		

Command		Value range	Default
service sntp mode {unicast broadcast}			
Description	Description Set the SNTP mode.		
Example	service sntp mode broadcast		

Command		Value range	Default
service sntp primary-server <ip-address></ip-address>		(XXX.XXX.XXX.XXX)	
Description Set the IP address of the SNTP server.			
Example	Example service sntp primary-server 192.168.20.50		

Command		Value range	Default
service sntp primary-server description 		Max. 256 characters	
Description Set the description of the SNTP server.			
Example service	service sntp primary-server description alphaserver		

Command		Value range	Default
service sntp	backup-server <ip-address></ip-address>	(XXX.XXX.XXX.XXX)	
Description Set the IP address of the backup SNTP server.			
Example	service sntp backup-server 192.168	3.15.100	

Command		Value range	Default
service sntp	backup-server description		
<description< th=""><td>></td><td></td><td></td></description<>	>		
Description	Set the description of the backup S	NTP server.	
Example	service sntp backp-server description	on betaserver	

Command		Value range	Default
service system-time <"YYYY/MM/DD			
hh:mm:ss">			
Description Set the local system time.			
Example	le service system-time "2021/01/26 14:51:01"		

LLDP Services Commands

Command		Value range	Default
show lldp topology all			
Description	Tabular display of the LLDP topolog Local port Chassis ID of the connected device IP address of the connected device Remote port of the connected device Description of the remote port on the	y with the following columns: ce le connected device	
Example	show lldp topology all		

Command		Value range	Default
show lldp global			
Description	Display the configuration parameter LLDP status LLDP transmission interval LLDP transmit port LLDP receive port	rs:	
Example	le show lldp global		

Command		Value range	Default
show lldp to	pology port-no <port-no></port-no>		
Description	Display the topology information at Complete chassis ID Complete port name System name System description	a port:	
Example	show lldp topology port-no 3		

Command		Value range	Default
lldp status {e	enable disable}		enable
Description Change the LLDP status			
Example	lldp status enable		

Command		Value range	Default	
lldp tx-interv	al <value></value>	Interval in seconds (5 - 32768)	5	
Description Change the LLDP transmission interval				
Example	lldp tx-interval 10			

Command		Value range	Default	
lldp port-tx enable <port-list></port-list>		Comma-separated list of port numbers	All enable	
Description Activation of the LLDP transmit ports				
Example	lldp port-tx enable 3,4,8			

Command		Value range	Default	
lldp port-tx c	lisable <port-list></port-list>	Comma-separated list of port numbers	No disable	
Description Deactivation of the LLDP transmit ports				
Example	lldp port-tx disable 3,4,8			

Command		Value range	Default
lldp port-rx e	enable <port-list></port-list>	Comma-separated list of port numbers	All enable
Description Activation of the LLDP receive ports			
Example	lldp port-rx enable 3,4,8		

Command		Value range	Default
lldp port-rx o	lisable <port-list></port-list>	Comma-separated list of port numbers	No disable
Description Deactivation of the LLDP receive ports			
Example	lldp port-rx disable 3,4,8		

Port Features Commands

Command		Value range	Default
show port-info all			
Description	Display the basic parameters of all Port number Port name Port type Port status Port mode	ports:	
Example	show port-info all		

Command		Value range	Default
show port-info port-no <port-no></port-no>			
Description	Display the basic parameters of one Port number Port name Port type Port status Port mode Status flow control Status link monitoring	e port:	
Example	show port-info port-no 3		

Command		Value range	Default	
show port-stat port-no <port-no></port-no>				
Description Display the port statistics of one port				
Example	show port-stat port-no 5			

Command		Value range	Default
show port-util port-no <port-no></port-no>			
Description Display the RX and TX utilization of one port			
Example	show port-util port-no 1		

Command		Value range	Default	
show port-util all				
Description Display the RX and TX utilization of all ports				
Example	show port-util all			

Command		Value range	Default
port <port-ne< td=""><td>o> admin-mode {enable disable}</td><td></td><td>all enable</td></port-ne<>	o> admin-mode {enable disable}		all enable
Description	Description Activation/deactivation of a port		
Example	port 3 admin-mode disable		

Command		Value range	Default	
port <port-no> modus autoneg</port-no>				
Description Activation/deactivation of auto-negotiation on one port				
Example	port 3 modus autoneg			

Command		Value range	Default
port <port-net< th=""><th>o> modus auto10_100</th><th></th><th></th></port-net<>	o> modus auto10_100		
Description Activation/deactivation of auto-negotiation on one port (only 10/100 Mbps, not 1000 Mbps)			ot 1000 Mbps)
Example	port 3 modus auto10_100		

Command		Value range	Default	
port <port-no< td=""><td>> modus speed <speed> {half-</speed></td><td><speed> Transmission speed in Mbps</speed></td><td></td></port-no<>	> modus speed <speed> {half-</speed>	<speed> Transmission speed in Mbps</speed>		
duplex full-duplex}		{10 100 1000})		
Description Change the transmission speed and duplex mode on one port				
Example	port 3 modus speed 100 half-duple	X		

Command		Value range	Default
port <port-no> modus faststartup</port-no>			
Description Activation/deactivation of Fast Startup mode on one port.			
Example	port 3 modus faststartup		

Command		Value range	Default
port <port-ne< td=""><td>o> description <text></text></td><td>(0 - 31 chars)</td><td></td></port-ne<>	o> description <text></text>	(0 - 31 chars)	
Description Change the port name			
Example	port 3 description RingPortGrue		

Command		Value range	Default	
port <port-ne< td=""><td>o> link-monitoring {enable disable}</td><th></th><td>all disable</td></port-ne<>	o> link-monitoring {enable disable}		all disable	
Description	Description Activation/deactivation of link monitoring on one port			
Example	port 3 link-monitoring disable			

Command		Value range	Default	
port <port-no> flow-control {enable disable}</port-no>			All disable	
Description Activation/deactivation of flow control on one port				
Example	port 3 flow-control disable			

Command		Value range	Default		
port <port-no> jumbo-frames {enable disable}</port-no>			disable		
Description	Description Enable or disable Jumbo frames.				
Example	port 5 jumbo-frames enable				

Command		Value range	Default	
port <port-n< td=""><td>o> mtu <value></value></td><td>Number of bytes 1522 to 9600</td><td>1536</td></port-n<>	o> mtu <value></value>	Number of bytes 1522 to 9600	1536	
Description Set the maximum jumbo frame size in bytes.				
Example	port 4 mtu 1522			

Command		Value range	Default	
port <port-no> crc-threshold <value></value></port-no>			40000	
Description Set the threshold for CRC errors on the selected port.				
Example	port 2 crc-threshold 30000			

Command		Value range	Default	
clear port-stat port-no <port-no></port-no>				
Description Resets the port statistics counters for the selected port back to 0.				
Example	clear port-stat port-no 3			

Command		Value range	Default	
clear port-stat all				
Description Resets the port statistics counters for all ports to 0				
Example	le clear port-stat all			

Port Mirroring Commands

Command		Value range	Default
show port-m	hirror		
Description	Display the port mirroring paramete Global status Receive port (mirroring port) Mirrored ports (incoming traffic) Mirrored ports (outgoing traffic)	ers:	
Example	show port-mirror		

Command		Value range	Default		
port-mirror status {enable disable}			disable		
Description	Description Activation/deactivation of the global port mirroring status				
Example	port-mirror status enable				

Command		Value range	Default	
port-mirror o	lest <port-no></port-no>		1	
Description Change the receive port (mirroring port)				
Example	port-mirror dest 8			

Command		Value range	Default		
port-mirror in	ngress enable <port-list></port-list>	Comma-separated list of port numbers	all disable		
Description	Description Activation of RX port mirroring (incoming traffic) on multiple ports				
Example	port-mirror ingress enable 3,4,8				

Command		Value range	Default		
port-mirror in	ngress disable <port-list></port-list>	Comma-separated list of port numbers	all disable		
Description	Description Deactivation of RX port mirroring (incoming traffic) on multiple ports				
Example	port-mirror ingress disable 3,4,8				

Command		Value range	Default		
port-mirror	egress enable <port-list></port-list>	Comma-separated list of port numbers	all disable		
Description	Description Activation of TX port mirroring (outgoing traffic) on multiple ports				
Example	port-mirror egress enable 3,4,8				

Command		Value range	Default
port-mirror e	gress disable <port-list></port-list>	Comma-separated list of port numbers	all disable
Description Deactivation of TX port mirroring (outgoing traffic) on multiple ports			
Example	port-mirror egress disable 3,4,8		

VLAN Commands

Command		Value range	Default
show vlan global			
Description Display the current VLAN mode			
Example	show vlan global		

Command		Value range	Default
show vlan static-table			
Description	Display the static VLAN table: VLAN ID VLAN name Device ports (untagged) Device ports (tagged)		
Example	show vlan static-table		

Command		Value range	Default
show vlan c	urrent-table		
Description	Display the current VLAN table: VLAN ID VLAN name Device ports (untagged) Device ports (tagged)		
Example	show vlan current-table		

Command		Value range	Default
show vlan port-table			
Description	Display the port-based static VLAN VLAN ID VLAN name Device ports (untagged) Device ports (tagged)	table for all ports:	
Example	show vlan port-table		

Command		Value range	Default
show vlan port <port-no></port-no>			
Description	Display the port-based static VLAN VLAN ID VLAN name Device ports (untagged) Device ports (tagged)	table for one port:	
Example	show vlan port 3		

Command		Value range	Default
show vlan vlan-id <vlan-id></vlan-id>		(1 - 4000)	
Description	Display the VLAN information for a VLAN ID VLAN name Device ports (untagged) Device ports (tagged)	VLAN:	
Example	show vlan vlan-id 3		

Command		Value range	Default
vlan status {transparent tagged}			transparent
Description	Change the VLAN mode		
Example	Vlan status tagged		

Command		Value range	Default	
vlan create <vlan-id></vlan-id>		(1 - 4000)		
Description Create a new static VLAN				
Example	Vlan create 5			

Command		Value range	Default	
vlan delete <vlan-id></vlan-id>		(1 - 4000)		
Description Delete a static VLAN				
Example	vlan delete 5			

Command		Value range	Default
vlan static <vlan-id> name <vlan-name></vlan-name></vlan-id>		(1 - 4000), (0 - 31 chars)	
Description	Description Change the name of a static VLAN		
Example	vlan static 5 name VLAN_5		

Command		Value range	Default	
vlan static <vlan-id> tagged-mem-ports</vlan-id>		(1 - 4000)		
<port-list></port-list>		Comma-separated list of port numbers		
Description Assignment of device ports (tagged) to a VLAN				
Example	vlan static 5 tagged-mem-ports 2,5			

Command		Value range	Default	
vlan static <vlan-id> untagged-mem-ports</vlan-id>		(1 - 4000)		
<port-list></port-list>		Comma-separated list of port numbers		
Description Assignment of device ports (untagged) to a VLAN				
Example	vlan static 5 untagged-mem-ports 2,5			

Command		Value range	Default	
vlan static <vlan-id> no-member <port-list></port-list></vlan-id>		(1 - 4000)		
		Comma-separated list of port numbers		
Description Removal of device ports from a VLAN				
Example vlan static 5 no-	member 3,5			

Command		Value range	Default	
vlan port <port-no> vlan <vlan-id></vlan-id></port-no>		(1 - 4000)		
Description Assignment of a default VLAN ID to a port				
Example	vlan port 3 vlan 5			

Command		Value range	Default	
vlan port <port-no> priority <value></value></port-no>		(0 - 7)	0	
Description Assignment of a default priority to a port				
Example	vlan port 3 priority 7			

Command	Value range	Default		
vlan port <port-no> ingress-filter {enable </port-no>		all disable		
disable}				
Description Activation/deactivation of the ingress filter at a port				
Example vlan port 3 ingress-filter disable				

Command		Value range	Default	
vlan routing	add <vlan-id> <interface-no></interface-no></vlan-id>			
Description Creates a routing VLAN from a VLAN and assigns this to a Layer 3 interface.				
Example	vlan routing add 200 2			

Command		Value range	Default	
vlan routing delete <vlan-id></vlan-id>				
Description Removes the routing VLAN and makes it a Layer 2 VLAN.				
Example	vlan routing delete 200			

Multicast Commands

Command		Value range	Default
show multic	ast igmp		
Description	Display the IGMP snooping informa Status IGMP Snooping Snoop Aging Time IGMP Query Version Query interval Status of IGMP extension FUQ Status of IGMP extension BUQ Status of IGMP extension auto que List of static query ports	ition: ry port	
Example	show multicast igmp		

Command		Value range	Default
show multicast static-groups			
Description	Tabular display of the static multicast groups with the following columns: Multicast address VLAN ID Member ports including status		
Example	show multicast static-groups		

Command		Value range	Default
show multic	ast current-groups		
Description Tabular display of the current multic VLAN ID Multicast address Port member Port member		cast groups with the following columns:	
Example	show multicast current-groups		

Command		Value range	Default	
multicast igmp snoop	status {enable disable}		disable	
Description Activation/deactivation of IGMP snooping				
Example multicas	t igmp snoop status enable)		

Command		Value range		Default
multicast igr	np snoop aging <value></value>	Aging time in seconds (30 - 3600)	300
Description Change the aging time				
Example	multicast igmp snoop aging 100			

Command		Value range	Default
multicast igr	np querier version {disable v1 v2}		disable
Description Change the querier version			
Example	multicast igmp querier version v2		

Command		Value range	Default
multicast igr	np querier interval <value></value>	Querier interval in seconds (10 - 3600)	125
Description	Change the querier interval		
Example	multicast igmp querier interval 500		

Command		Value range	Default
multicast igr	np extension fuq {enable disable}		enable
Description Activation/deactivation of the IGMP extension FUQ			
Example	multicast igmp extension fuq enable	9	

Command		Value range	Default
multicast igr	np extension buq {enable disable}		enable
Description Activation/deactivation of the IGMP extension BUQ			
Example	multicast igmp extension buq enabl	e	

Command		Value range	Default
multicast ign disable}	np extension auto-query {enable		enable
Description	Description Activation/deactivation of the IGMP extension auto query port		
Example			

Command		Value range	Default	
multicast igmp extension clear-auto-query				
Description Delete all auto query ports				
Example	Example multicast igmp extension clear-auto-query			

Command		Value range	Default	
multicast igr	np extension static-query-port add	Comma-separated list of port numbers		
<port-list></port-list>				
Description Add static query ports				
Example	multicast igmp extension static-query-port add 2,4			

Command		Value range	Default	
mutlicast igr	np extension static-query-port	Comma-separated list of port numbers		
remove <po< td=""><td>rt-list></td><td></td><td></td></po<>	rt-list>			
Description Delete static query ports				
Example	multicast igmp extension static-query-port remove			

Command		Value range	Default
multicast static create <mac-address> <vlan-id></vlan-id></mac-address>			
Description Generate a new static multicast group			
Example	mple multicast static create 01:00:5e:00:18:0e 1		

Command		Value range	Default
multicast static delete <mac-address> <vlan-id></vlan-id></mac-address>			
Description Delete an existing static multicast group			
Example	multicast static delete 01:00:5e:00:18:0e 1		

Command		Value range	Default	
multicast sta	tic configure <mac-address></mac-address>	<port-list> Comma-separated list of</port-list>		
<vlanid> sta</vlanid>	tic-mem-ports <port-list></port-list>	port numbers		
Description Add ports to a static multicast group				
Example	Example multicast static configure 01:00:5e:00:18:0e 1 static-mem-ports 3,5,8			

Command	Value range	Default		
multicast static configure <mac-address> <vlanid> forbidden-mem-ports <port-list></port-list></vlanid></mac-address>	<port-list> Comma-separated list of port numbers</port-list>			
Description Forbid membership of ports in a static multicast group				
Example multicast static configure 01:00:5	Example multicast static configure 01:00:5e:00:18:0e 1 forbidden-mem-ports 3,5,8			

Command	Value range	Default		
multicast static configure <mac-address></mac-address>	<port-list> Comma-separated list of</port-list>			
<vlanid> no-member <port-list></port-list></vlanid>	port numbers			
Description Delete ports from a static multicast group				
Example multicast static configure 01:00:	5e:00:18:0e 1 no-member 3,5,8			

RSTP Commands

Command		Value range	Default
show spanning-tree global			
Description	Display the RSTP information: Status RSTP Mode Status Large Tree Support Status Fast Ring Detection Bridge Priority Bridge Hello Time Bridge Forward Delay Bridge Max Age MAC address of the root Root Port Root Cost Number of topology changes Last topology change Hello Time Forward Delay Max Age		
Example	show spanning-tree global		

Command	Value range	Default
show spanning-tree port port-no <port-no></port-no>		
Display the RSTP information for a Status RSTP Mode Admin Path Cost Operating Path Cost Status Auto Edge Status Admin Edge Description Status Operating Edge Priority Number of forward transitions MAC address of the root MAC address of the bridge Port ID Cost	specific port:	
Example show spanning-tree port port-no 10		

Command		Value range	Default
show spanning-tree port all			
Tabular display of the RSTP informa Port number Status RSTP Mode Description Path Cost Operating Edge Blocking State Protocol Role		ation for a specific port with the following	columns:
Example	show spanning-tree port all		

Command		Value range	Default
spanning-tre	ee status {disable 802.1w}		802.1w
Description Activation/deactivation of RSTP			
Example	spanning-tree status 802.1w		

Command		Value range	Default
spanning-tre	ee Its {enable disable}		disable
Description Activation/deactivation of Large Tree Support			
Example	spanning-tree Its enable		

Command		Value range	Default
spanning-tre	ee frd {enable disable}		disable
Description Activation/deactivation of Fast Ring Detection			
Example	spanning-tree frd enable		

Command		Value range	Default
spanning-tre	ee bdg-prio <value></value>	(0 - 61440 in increments of 4096)	32768
Description Change the Bridge Priority			
Example	spanning-tree bdg-prio 4096		

Command		Value range	Default
spanning-tre	ee hello-time <value></value>	Hello time in seconds (1 - 10)	2
Description Change the Bridge Hello Time			
Example	spanning-tree hello-time 3		

Command		Value range	Default
spanning-tre	ee fwd-delay <value></value>	Bridge Forward Delay in seconds (4 - 30)	15
Description Change the Bridge Forward Delay			
Example	spanning-tree fwd-delay 20		

Command		Value range	Default
spanning-tree max-age <value></value>		Bridge Max Age in seconds (6 - 40)	20
Description	Change the Bridge Max Age		
Example	spanning-tree max-age 25		

Command		Value range	Default
spanning-tre disable}	e port <port-no> status {enable </port-no>		all enable
Description Activation/deactivation of RSTP for a specific port			
Example	spanning-tree port 3 status disable		

Command	Value range	Default		
spanning-tree port <port-no> path-ost <value></value></port-no>	Path cost (0 = automatic detection based on the current port speed; 1 - 200000000 = manual setting)	0		
Description Change the path cost for a specific port				
Example spanning-tree port 3 path-cost 2000	le spanning-tree port 3 path-cost 20000			

Command		Value range	Default
spanning-tree port <port-no> auto-edge {enable</port-no>			all enable
disable}			
Description Activation/deactivation of Auto Edge for a specific port			
Example	spanning-tree port 3 auto-edge enable		

Command		Value range	Default
spanning-tree	e port <port-no> admin-edge</port-no>		all non-edge
{edge non-e	dge}		-
Description Activation/deactivation of Admin Edge for a specific port			
Example s	Example spanning-tree port 3 admin-edge non-edge		

Command		Value range	Default	
spanning-tre	e port <port-no> priority <value></value></port-no>	Priority (0 - 240 in increments of 16)	128	
Description Change the priority for a specific port				
Example	spanning-tree port 3 priority 192			

Command		Value range	Default	
spanning-tre	ee port <port-no> force-rstp</port-no>			
Description Force change from STP to RSTP for a specific port				
Example	spanning-tree port 3 force-rstp			

Port Channel Commands

Command		Value range	Default
show port-cl	nannel trunk-id <name></name>		
Description	Displays the trunk ID, trunk name, admin mode, spanning tree mode, algorithm and associated		
	ports for the selected trunk.		
Example	show port-channel trunk-id Redtrun	k1	

Command		Value range	Default
show port-c	hannel all		
Description Shows all trunks in a table with trunk ID, trunk name, admin mode and status.			
Example	show port-channel all		

Command		Value range	Default
port-channe	l create <name></name>		
Description Create a trunk with the configured name.			
Example	port-channel create Portch1		

Command		Value range	Default
port-channe	l delete <name></name>		
Description Delete a trunk with the configured name.			
Example	port-channel delete Portch1		

Command	Value range	Default		
port-channel config <name> admin- mode {enable disable}</name>				
Description Configuration of the port channel admin mode.				
Example port-channel config PortCh1 adm	port-channel config PortCh1 admin-mode enable			

Command		Value range	Default
port-channel config <name> spann-tree {enable disable}</name>			
Description Configuration of the Port Channel Spanning Tree mode.			
Example	port-channel config PortCh1 spann	-tree enable	

Command		Value range	Default
port-channe	l config <name> chg-name <name></name></name>		
Description Change a port channel name			
Example	Example port-channel config PortCh1 chg-name PortCh2		

Command		Value range	Default
port-channe port add <po< th=""><th>l config <name> member- ort-list></name></th><th></th><th></th></po<>	l config <name> member- ort-list></name>		
Description Add member ports to the port channel. Ports are listed in a comma separated list.			
Example	port-channel config PortCh2 member-port add 1,2,8		

Command		Value range	Default
port-channe port del <po< th=""><th>l config <name> member- rt-list></name></th><th></th><th></th></po<>	l config <name> member- rt-list></name>		
Description Delete member ports from the port channel. Ports are listed in a comma separated list.			
Example	port-channel config PortCh2 memb	er-port del 1,2	

Command		Value range	Default
port-channe mode mode	l config <name> trunk- {LIST-OF-MODES}</name>	Static, lacp-active and lacp-passive	lacp-active
Description	Configuration of the port selection for the selected port channel. Static, lacp-active and lacp- passive are supported.		
Example	port-channel config PortCh2 trunk-mode mode static		

Command		Value range	Default
port-channe OF-ALGOR	l global-algorithm algorithm {LIST- ITHMS}	Src MAC, Dst MAC, Src and Dst MAC, Src/Dst IP and TCP/UDP port, Src/Dst MAC, IP and TCP/UDP port	Src/Dst MAC, IP and TCP/UDP port
Description	Configuration of the load balancing algorithm for all port channels of the device.		
Example	port-channel global-algorithm algorithm Src and Dst MAC		

Security Context Commands

Command		Value range	Default
show sec-context			
Description Display the security context status			
Example	show sec-context		

Command		Value range	Default
sec-context generate			
Description Generate a security context			
Example	sec-context generate		

Command	Value range	Default	
file-transfer {tftp http} {write-to-device read- from-device} sec-context <ip-ad-dress></ip-ad-dress>	(XXX.XXX.XXX.XXX)		
<filename></filename>			
Description Transfer of a root CA certificate file to the device or from the device to the PC.			
Example file-transfer tftp write-to-device sec	file-transfer tftp write-to-device sec-context 192.168.0.1 cacert.cer		

DHCP Commands

Command		Value range	Default
show dhcp global			
Description Display the global DHCP status			
Example	show dhcp global		

Command		Value range	Default
show dhcp server current-lease			
Description	Tabular display of the current DHCF Number Assigned IP address MAC address of the device Local port Status	P leases (assigned IP addresses):	
Example	show dhcp server current-lease		

Command		Value range	Default
show dhcp s	server static-lease		
Description	Tabular display of the current static DHCP leases (assigned IP addresses): Number Assigned IP address MAC address of the device		
Example	show dhcp server static-lease		

Command		Value range	Default
show dhcp server port-local <port-no></port-no>			
Description	Display the port-based DHCP serve Port Status of the port-based DHCP serve IP address Subnet mask Default gateway DNS server	er information: ver	
Example	show dhcp server port-local 3		

Command		Value range	Default
dhcp-service service {none relay-agent			
server}			
Description Set the operating mode of the DHCP server			
Example	dhcp-service service server		

Command		Value range	Default	
dhcp-service	e relay-agent remote-id {ip mac}		ір	
Description Change the relay agent remote ID				
Example	Example dhcp-service relay-agent remote-id mac			

Command		Value range	Default	
dhcp-service	e relay-agent server <ip-address></ip-address>		0.0.0.0	
Description Change the DHCP server in relay agent mode				
Example	dhcp-service relay-agent server 192	2.168.0.2		

Command		Value range	Default	
dhcp-service relay-agent port-mode enable <port-list></port-list>		Comma-separated list of port numbers		
Description Activation of the relay agent on multiple ports				
Example	Example dhcp-service relay-agent port-mode enable 3,4,8			

Command		Value range	Default	
dhcp-service relay-agent port-mode disable <port-list></port-list>		Comma-separated list of port numbers		
Description Deactivation of the relay agent on multiple ports				
Example	dhcp-service relay-agent port-mode disable 3,4,8			

Command		Value range	Default
dhcp-service	e server pool-start-addr <ip-ddress></ip-ddress>		0.0.0.0
Description	Change the start address of the DH	ICP pool	
Example	dhcp-service server pool-start-addr	192.168.0.3	

Command		Value range	Default
dhcp-service server pool-size <size></size>		DHCP pool size (depends on subnet)	32
Description Change the maximum number of IP addresses specified by the DHCP server (size of the address pool)			
Example	dhcp-service server pool-size 20		

Command		Value range	Default
dhcp-service server net-mask <net-mask></net-mask>			0.0.0.0
Description Change the subnet mask that is assigned to the DHCP clients			
Example	dhcp-service server net-mask 255.2	255.255.0	

Command		Value range	Default	
dhcp-service	e server router-ip <ip-address></ip-address>		0.0.0.0	
Description Change the default gateway that is assigned to the DHCP clients				
Example	xample dhcp-service server router-ip 192.168.0.1			

Command		Value range	Default
dhcp-service server dns-ip <ip-address></ip-address>			0.0.0.0
Description Change the DNS server that is assigned to the DHCP clients			
Example	dhcp-service server dns-ip 192.168	.10.10	

Command		Value range	Default	
dhcp-service	e server lease-time <value></value>	DHCP lease time in seconds (300 - 2592000)	3600	
Description Change the DHCP lease time (validity of the IP address assignment)				
Example	ample dhcp-service server lease-time 3600			

Command		Value range	Default
dhcp-service server accept-bootp {enable			enable
disable}			
Description Activation/deactivation of the acceptance of BootP requests by the DHCP server			
Example	dhcp-service server accept-bootp enable		

Command		Value range	Default
dhcp-service ser	rver static-lease create		
<ip-address> <client-mac-address> Description Create a static IP assignment (DHCP lease) for a defined client address (MAC address)</client-mac-address></ip-address>			
Example dhc	p-service server static-lease cre	ate 192.168.0.20 XX:XX:XX:6C:D2:05	•

Command		Value range	Default
dhcp-service server static-lease delete			
<ip-address></ip-address>			
Description Delete a statically assigned IP address (DHCP lease)			
Example	ple dhcp-service server static-lease delete 192.168.0.20		

Command		Value range	Default
dhcp-service server static-lease clear			
Description Delete all static IP assignments (DHCP lease)			
Example	dhcp-service server static-lease clear		

Command		Value range	Default
dhcp-service server port-local <port-no> status {enable disable}</port-no>			all disable
Description Activation/deactivation of a port-based DHCP server			
Example	dhcp-service server port-local 3 sta	tus enable	

Command		Value range	Default
dhcp-service server port-local <port-no> local-ip <ip-address></ip-address></port-no>			0.0.0.0
Description Change an IP address assigned by a port-based DHCP server			
Example	Example dhcp-service server port-local 3 local-ip 192.168.0.30		

Command		Value range	Default
dhcp-service server port-local <port-no></port-no>			0.0.0.0
Description Change a subnet mask assigned by a port-based DHCP server			
Example	Example dhcp-service sercer port-local 3 net-mask 255.255.255.0		

Command		Value range	Default
dhcp-service server port-local <port-no></port-no>			0.0.0.0
router-ip <ip-address></ip-address>			
Description	Description Change a default gateway address assigned by a port-based DHCP server		
Example	xample dhcp-service server port-local 3 router-ip 192.168.0.1		

Command		Value range	Default
dhcp-service server port-local <port-no> dns-ip</port-no>			0.0.00
<ip-address></ip-address>			
Description Change a DNS server address assigned by a port-based DHCP server			
Example	dhcp-service server port-local 3 dns	s-ip 192.168.10.10	

Command		Value range	Default
dhcp-service server port-local-clear			
Description Delete all port-based DHCP servers			
Example	dhcp-service server port-local-clear		
Alarm Output Commands

Command		Value range	Default
show alarm-output <output-no></output-no>		Alarm contact number	
Description	Display the alarm contact informatic Alarm contact status Alarm contact output status (error s Event status power supply interrupt Event status link down	on: tate) ed	
Example	show alarm-output 1		

Command		Value range	Default
alarm-output <output-no> global {enable </output-no>			enable
disable}			
Description Change alarm contact status			
Example a	alarm-output 1 global enable		

Command		Value range	Default
alarm-output <output-no> pow-supply-lost</output-no>			enable
enable disable}			
Description Change event status power supply interrupted			
Example	alarm-output 1 pow-supply-lost ena	ble	

Command	Value range		Default
alarm-output <output-no> link</output-no>	-down {enable		disable
disable}			
Description Change event status link down			
Example alarm-output 1 lir	ık-down enable		

Command	Value range	Default	
alarm-output <output-no> plug-mem</output-no>	n-miss	disable	
{enable disable}			
Description Change event status configuration memory missing			
Example alarm-output 1 plug-me	ple alarm-output 1 plug-mem-miss enable		

QoS Commands

Command		Value range	Default
show broadcast-limiter			
Description	Display the broadcast limiter inform Status of the broadcast limiter Broadcast threshold value Status of the multicast limiter Multicast threshold value Status of the unknown unicast limite Unknown unicast threshold value	ation: er	
Example	show broadcast-limiter		

Command		Value range	Default
show quality	v-of-service profile		
Description Shows the Quality of Service information.			
Example	show quality-of-service profile		

Command		Value range	Default
quality-of-se	rvice profile {universal ethernet-ip}		universal
Description	Set predifined priority mapping and	queue usage for certain traffic class.	
Example	quality-of-service profile universal		

Command		Value range	Default
broadcast-limiter broadcast status {enable			disable
disable}			
Description Change the broadcast limiter status			
Example	broadcast-limiter broadcast status e	enable	

Command		Value range	Default	
broadcast-li	miter broadcast threshold <value></value>	Threshold value in frames per second (0 - 1048576 in increments of 1024)	1024	
Description Change the broadcast limiter threshold				
Example	e broadcast-limiter broadcast threshold 2048			

Command		Value range	Default	
broadcast-limiter multicast status {enable			disable	
disable}				
Description Change the multicast limiter status				
Example	Example broadcast-limiter multicast status enable			

SmartE Series

Command		Value range	Default	
broadcast-lir	niter multicast threshold <value></value>	Threshold value in frames per second (0 - 1048576 in increments of 1024)	1024	
Description Change the multicast limiter threshold				
Example	le broadcast-limiter multicast threshold 2048			

Command		Value range	Default
broadcast-limiter unicast status {enable			disable
disable}			
Description Change the unknown unicast limiter status			
Example	broadcast-limiter unicast status ena	able	

Command		Value range	Default	
broadcast-li	miter unicast threshold <value></value>	Threshold value in frames per second (0 - 1048576 in increments of 1024)	1024	
Description Change the broadcast limiter threshold				
Example	mple broadcast-limiter unicast threshold 2048			

Trap Manager Commands

Command		Value range	Default
show snmp-	trap		
Description	Tabular display of the SNMP trap st Trap Name Status	ates with the following columns:	
Example	show snmp-trap		

Command		Value range	Default
snmp-trap status {enable disable}			disable
Description Change the global SNMP status			
Example	snmp-trap status enable		

Command		Value range	Default
snmp-trap server add <ip-address></ip-address>			
Description Add an SNMP trap server			
Example	snmp-trap server add 192.168.0.50		

Command		Value range	Default
snmp-trap s	erver remove <ip-address></ip-address>		
Description Delete an SNMP trap server			
Example	Example snmp-trap server remove 192.168.0.50		

Command	Value range	Default	
snmp-trap trap <trap> {enable disable}</trap>	Traps separated by comma: user-config-chg - User config change event-tbl-oflow - Event Table Overflow crc-peak-increase - CRC proportion peak increased crc-status-critical - CRC status change to critical crc-status-warning - CRC status change to warning crc-status-ok - CRC status change to ok ip-conflict - Set IP conflict presisted dlr-ring-chg - DLR ring change fw-status-chg - firmware status changed port-sec-violation - Port security violation link-up - Link Up link-down - Link Down rstp-top-chg - RSTP Topology Change rstp-new-root - RSTP New Root rstp-link-fail - RSTP Link Failure pow-src-chg - Power source changed fw-config - Firmware configuration auth-fail - Authentication failure user-pwd-chg - User password changed config-diff - Configuration differ warm-start - Warm start cold-start - Cold start	all enable	
Example snmp-trap trap link-up,auth-fail,warm-start enable			

Command		Value range	Default
snmp-trap send-test-trap			
Description Send a test trap			
Example	snmp-trap send-test-trap		

SmartE Series

Contact Information

EtherWAN System, Inc.

www.etherwan.com

USA Office

2301 E. Winston Road Anaheim, CA 9280 Tel: +1-714-779-3800 Email: info@etherwan.com

Pacific Rim Office

8F., No.2, Alley 6, Lane 235, Baoqiao Rd. Xindian District, New Taipei City 231 Taiwan Tel: +886 -2- 6629-8986 Email: info@etherwan.com.tw

EtherWAN has made a good faith effort to ensure the accuracy of the information in this document and disclaims the implied warranties of merchantability and fitness for a particular purpose, and makes no express warranties, except as may be stated in its written agreement with and for its customers.

EtherWAN shall not be held liable to anyone for any indirect, special or consequential damages due to omissions or errors. The information and specifications in this document are subject to change without notice.

Copyright 2021. All Rights Reserved.

All trademarks and registered trademarks are the property of their respective owners

SmartE Series September 2, 2021