Industrial Ethernet IEC-61850-3 Switches

Manual

for

IE-SW-SL20M-8GT-12GESFP

of

SubstationLine

Fifth Edition, March 2025

Weidmüller

Industrial Ethernet managed Switches Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright ©2016 Weidmüller Interface GmbH & Co. KG
All rights reserved.
Reproduction without permission is prohibited.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Weidmüller.

Weidmüller provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Weidmüller reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Weidmüller assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Contact Information

Weidmüller Interface GmbH & Co. KG
Postfach 3030
32760 Detmold
Klingenbergstraße 26
32758 Detmold
Germany

Phone +49 (0) 5231 14-0
Fax +49 (0) 5231 14-2083
E-Mail info@weidmueller.com
Internet www.weidmueller.com

Table of Contents

1. About this Manual

Thank you for purchasing a Weidmüller managed Industrial Ethernet switch. Read this user's manual to learn how to connect your Weidmüller switch to Ethernet-enabled devices used for industrial applications.

The following chapters are covered in this user manual:

☐ **Getting Started**

This chapter summarizes the main hardware and software features of the IE-SW-SL20M-8GT-12GESFP Switch. The information related with the Installation of the Switch (Front / Rear side elements description and Connections) is described in the Hardware Installation Guide delivered with every device and available in our online catalogue.

☐ **Web Management**

There are three ways to access the Weidmüller switch's configuration settings: serial console, Telnet console, or web console. The Web console is the most user-friendly way for configuring and monitoring and is fully described in this chapter.

The description of the Command Line Interface (CLI) Management using serial console or Telnet console has its own specific manual (User Manual Command Line Interface for Substation Line Switches) that is also available in our online catalogue.

2. Getting Started

The IE-SW-SL20M-8GT-12GESFP Switch is specially designed to operate in harsh environments like Substations thanks to its IEC 61850-3 and IEEE 1613 compliance. The product comes with an IP30 rugged case, redundant power supply, alarm relay and wide operating temperature range from -40 to 85ºC. There are two variants of the Switch (HV and LV) to meet any power supply requirement.

2.1 Hardware features

- 8 x 10/100/1000Base-T(X) ports
- 12 x 100/1000BaseSFP
- RS232 interface with RJ45 connector for console access
- Redundant power supply; two product variants with different power input range
  - 12 to 52 Vdc (Low Voltage model)
  - 88 to 373Vdc and 85 to 264Vac (High Voltage model)
- Alarm relay contact
- Operating temperature from -40 to 85ºC
- IEC 61850-3 and IEEE 1613 compliance

2.2 Software features

- Management
  - Web-interface (HTTP / HTTPS)
  - SNMP v1/v2c/v3
  - Telnet console
  - Command Line Interface (CLI)
  - Upload of a configuration file via web-interface or external backup module
- Network redundancy
  - Spanning Tree Protocol (STP)
  - Rapid Spanning Tree Protocol (RSTP)
  - Multiple Spanning Tree Protocol (MSTP)
  - Media Redundancy Protocol (MRP)
  - O-Ring (optimized protocol for ring topologies; recovery time < 10ms)
  - O-Chain (allows multiple redundant network topologies; recovery time < 10ms)
  - Link Aggregation Control Protocol (LACP)
  - Fast Recovery
- IP-address management
  - Static
  - DHCP-Client
  - DHCP-Server (port based, pool based)
  - DHCP Option 82
  - DHCP-Relay
- Time synchronization management
  - SNTP
  - PTPv2
- Monitoring functions
  - SNMP v1/v2c/v3
  - Link Layer Discovery Protocol (LLDP)
  - Port mirroring
  - Port statistics
  - Port monitoring
  - RMON
  - Syslog
  - Event based warning (via e.mail / via output relay / via SNMP trap)
  - Ethernet cable diagnosis on RJ-45 ports
- Network traffic filter
  - Quality of Service (QoS)
  - Class of Service (CoS) according to IEEE 802.1p
  - Class of Service applicable to GOOSE and Sampled Value messages
  - Type of Service (ToS) / Differentiated Services Code Point (DSCP)
  - Port / Tag based VLAN
  - IGMP v2/v3
  - MLD
  - Multicast VLAN Registration (MVR)
  - Traffic Rate Limiting
- Security functions
  - VLAN segmentation
  - Enable / Disable ports
  - TACACS+ and RADIUS User Authentication
  - Access Control (port based via IEEE 802.1X)
  - Access Control List (IP based / MAC based)
  - Loop protection

- Management access security via privilege level configuration for different user roles
- Industrial protocols
  - Modbus TCP slave
  - Profinet Conformance Class B
  - MMS server

3. Web Management

In this chapter, we explain how to access the Weidmüller Switch's through the Web console as well as all the configuration, monitoring, and administration functions available when using this interface.

3.1 Accessing the Web interface via HTTP

The Ethernet Switch's web browser interface provides a convenient way to modify the switch's configuration and access the built-in monitoring and network administration functions. The web browsers Microsoft Edge, Google Chrome and Mozilla Firefox can be used to manage the Substation Line switches.

NOTE: To use the Switch's management and monitoring functions from a PC host connected to the same LAN as the switch, you must make sure that the PC host and the Switch are on the same logical subnet.

NOTE: If the Weidmüller switch is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

NOTE: Before accessing the Switch's web browser interface, first connect one of its RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can establish a connection with either a straight-through or cross-over Ethernet cable.

NOTE: The Weidmüller switch's default IP address is **192.168.1.110**.

The default username / password are **admin** / **Detmold**

After making sure that the Weidmüller switch is connected to the same LAN and logical subnet as your PC, open the switch's web console as follows:

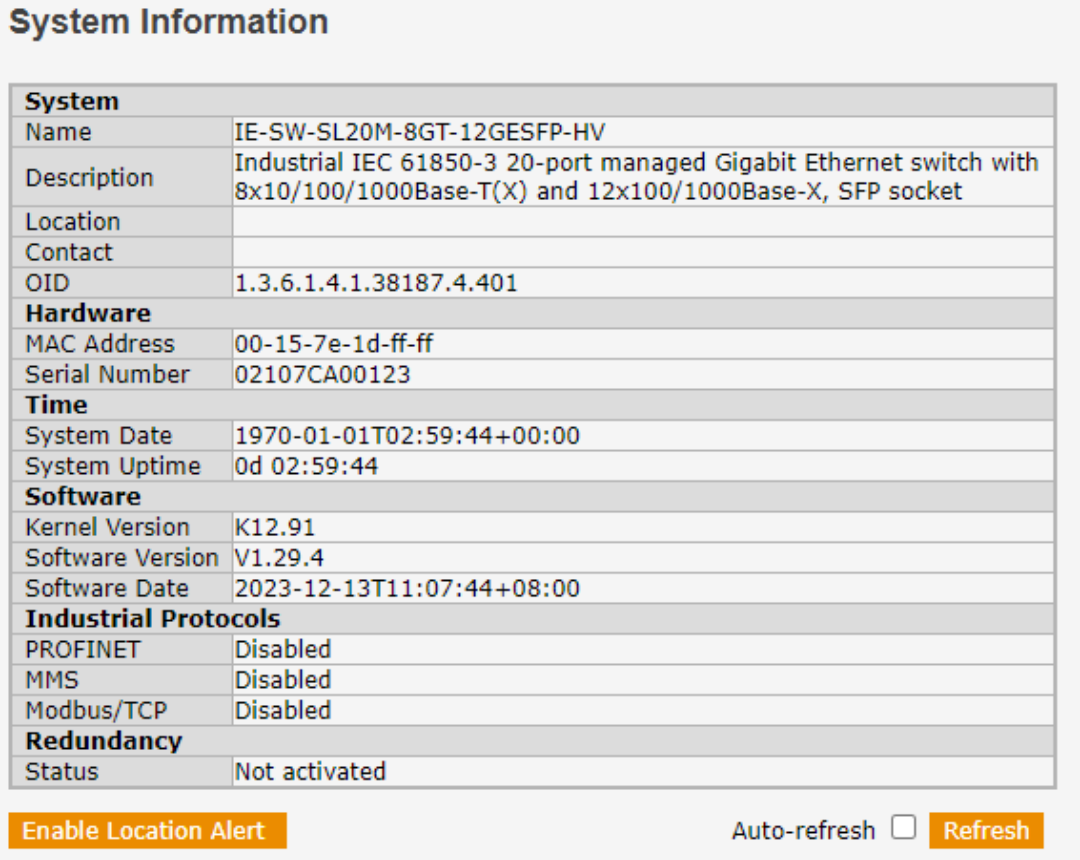
Open your web browser and type the Switch's IP address in the **Address** or **URL** field. Press **Enter** to establish the connection.

The web login page will open. Enter the default user name **“admin”** and password **“Detmold”**, and then click **OK** to continue.

After logging in, the main general information of the switch is shown including, among others, System Name, Software version, MAC address and Serial number. It is also displayed the front side of the switch (showing the active ports) in the right navigation panel.

In this home page is also available the button **Enable location alert**. When pressing it, the front LEDs starts to flash and an acoustic signal is heard (periodic change of the output relay). When clicking **Disable location alert**, the LEDs will stop flashing and the output relay will remain in its original position.

Use the menu tree in the left navigation panel to open the function pages to access each of Ethernet Switch's functions.



System Information

System	
Name	IE-SW-SL20M-8GT-12GESFP-HV
Description	Industrial IEC 61850-3 20-port managed Gigabit Ethernet switch with 8x10/100/1000Base-T(X) and 12x100/1000Base-X, SFP socket
Location	
Contact	
OID	1.3.6.1.4.1.38187.4.401
Hardware	
MAC Address	00-15-7e-1d-ff-ff
Serial Number	02107CA00123
Time	
System Date	1970-01-01T02:59:44+00:00
System Uptime	0d 02:59:44
Software	
Kernel Version	K12.91
Software Version	V1.29.4
Software Date	2023-12-13T11:07:44+08:00
Industrial Protocols	
PROFINET	Disabled
MMS	Disabled
Modbus/TCP	Disabled
Redundancy	
Status	Not activated

Enable Location Alert Auto-refresh Refresh

NOTE: The pages of the Web interface include a **Help** button that describes the parameters and functions that can be programmed or monitored in each web page.

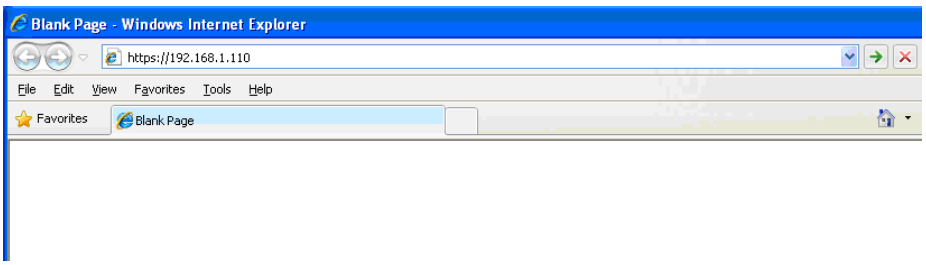
NOTE: After changing any parameter / function in a web page the button **Apply** activates the change but **does not save it**. The changes have to be saved using the **Save/Manage Configuration** option of the menu.

NOTE: The pages of the Web interface include also a **Reset** button closed to the Apply one. If the user modifies any parameter of a web page but still has not applied the changes, the Reset button can be used to recover the previous default values of the page. Once the button Apply is pressed, the default values of the page are the new ones.

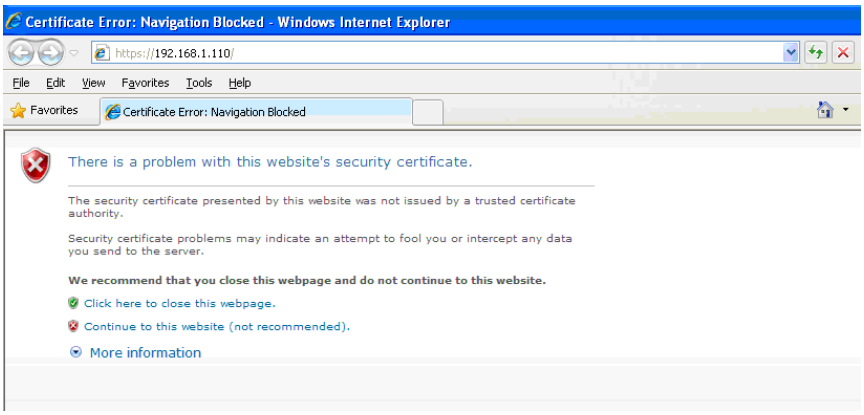
3.2 Accessing the Web interface via HTTPS

To secure your HTTP access, the Weidmüller switch supports HTTPS to encrypt all HTTP traffic. Perform the following steps to access the Weidmüller switch web browser interface via HTTPS/SSL.

Open Internet Explorer and enter **https://<Switch´s IP address>** in the address field. Press Enter to establish the connection.



Warning messages will pop out to warn the user that the security certificate was issued by a company they have not chosen to trust.



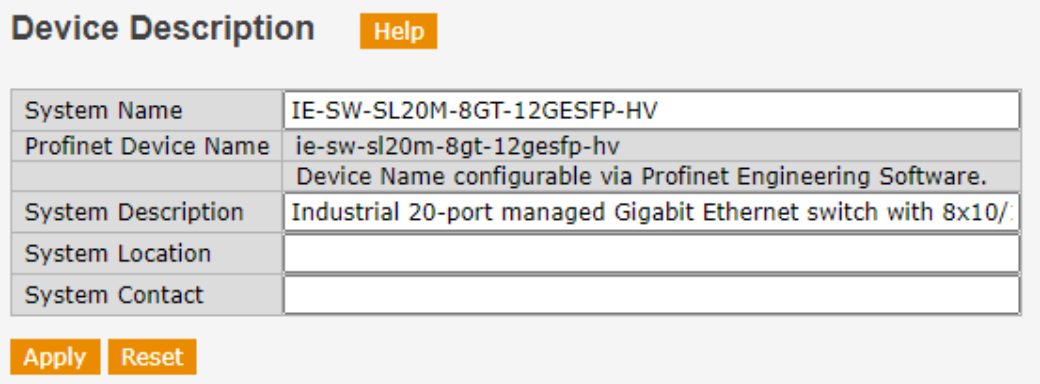
Select "**Continue to this website"** to enter the Weidmüller switch´s web browser interface and access the web browser interface secured via HTTPS.

3.3 Basic Settings

The Basic Settings section includes the most common settings required by administrators to maintain and control a Weidmüller switch.

3.3.1 Device Description

The device description items are displayed at the top of the web page. You can configure the System Identification items to make it easier to identify different switches that are connected to your network.



System Name

Setting	Description	Factory Default
Max. 255 characters	This option is useful for recording a name of the unit. A text string consisting of alphabets (A-Z, a-z), digits (0-9), and minus (-), period (.) or underline (_).	Name of type

Profinet Device Name

Setting	Description	Factory Default
Information only	This field is only shown if Profinet protocol is enabled in the switch and is showing the Profinet name of the switch. It is also indicated that this name can only be modified via Profinet Engineering Software.	Name of type

System Description

Setting	Description	Factory Default
Max. 255 characters	This option is useful for recording a more detailed description of the unit.	Description of type

System Location

Setting	Description	Factory Default
Max. 255 characters	This option is useful for differentiating between the locations of different units. Example: Bay 1. The allowed content is the ASCII characters from 32 to 126.	None

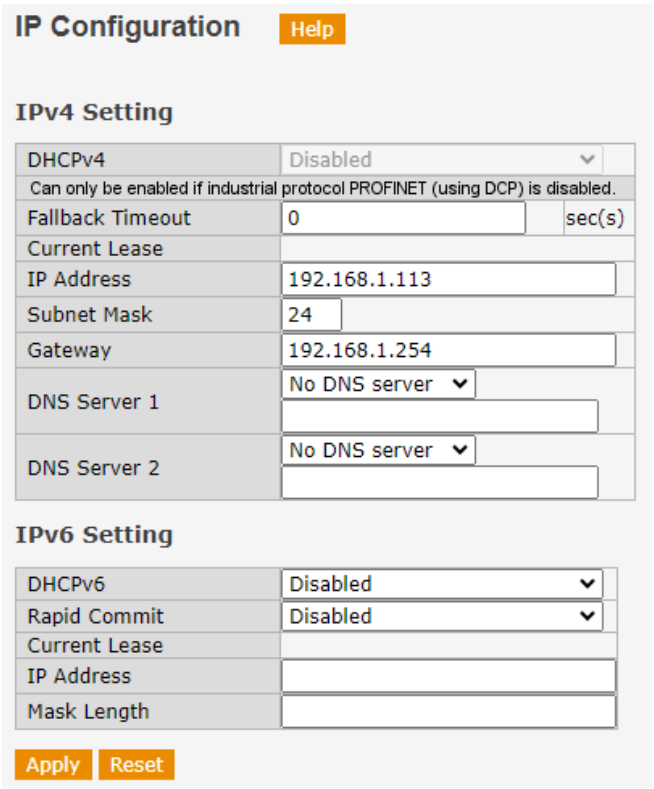
System contact

Setting	Description	Factory Default
Max. 255 characters	This option is useful for providing information about who is responsible for maintaining this unit and how to contact this person. The allowed content is the ASCII	None

	characters from 32 to 126.	

3.3.2 IP Configuration

The IP settings allow the user to set manually the IP parameters or by means of a DHCP server (for both IPv4 and IPv6).



See a brief explanation of each configuration item below.

IPv4 Setting

DHCPv4

Setting	Description	Factory Default
Disabled	The Weidmüller switch's IP address must be set manually.	Disabled
Enabled	The Weidmüller switch's IP address will be assigned automatically by the network's DHCPv4 server. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.	

Fallback Timeout

Setting	Description	Factory Default
Number between 0 and 4294967295 sec	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A	0

	value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained.	

Current Lease

Setting	Description	Factory Default
No setting (display)	For DHCPv4 interface with an active lease, this column shows the current interface address, as provided by the DHCPv4 server.	None

IP Address

Setting	Description	Factory Default
IPv4 address for the Weidmüller Switch	Assigns the Weidmüller Switch´s IPv4 address on a TCP/IP network. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.	192.168.1.110

Subnet Mask

Setting	Description	Factory Default
Subnet mask for the Weidmüller Switch	The IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for an IPv4 address. If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.	24

Gateway

Setting	Description	Factory Default
IP address for the gateway	The IP address of the router that connects the LAN to an outside network.	192.168.1.254

DNS Server 1

Setting	Description	Factory Default
1st DNS Server's IP address	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address you can input, for example, a hostname (instead of an IP address) to access to an NTP server in the Time settings option.	None

DNS Server 2

Setting	Description	Factory Default
2nd DNS Server's	The IP address of the secondary DNS Server used by your network. The Switch will use the 2nd DNS Server	None

IP address	if the 1st DNS Server fails to connect.	

IPv6 Setting

DHCPv6

Setting	Description	Factory Default
Disabled	The Weidmüller switch's IP address must be set manually.	Disabled
Enabled	The Weidmüller switch's IP address will be assigned automatically by the network's DHCPv6 server.	

Rapid Commit

Setting	Description	Factory Default
Disabled	DHCPv6 Rapid Commit option disabled.	Disabled
Enabled	The DHCPv6 client terminates the waiting process as soon as a Reply message with Rapid Commitment option is received.	

Current Lease

Setting	Description	Factory Default
No setting (display)	For DHCPv6 interface with an active lease, this column shows the current interface address, as provided by the DHCPv6 server.	None

IP Address

Setting	Description	Factory Default
IPv6 address for the Weidmüller Switch	Assigns the Weidmüller Switch´s IPv6 address on a TCP/IP network. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address. This field may be left blank if IPv6 operation on the interface is not desired.	None

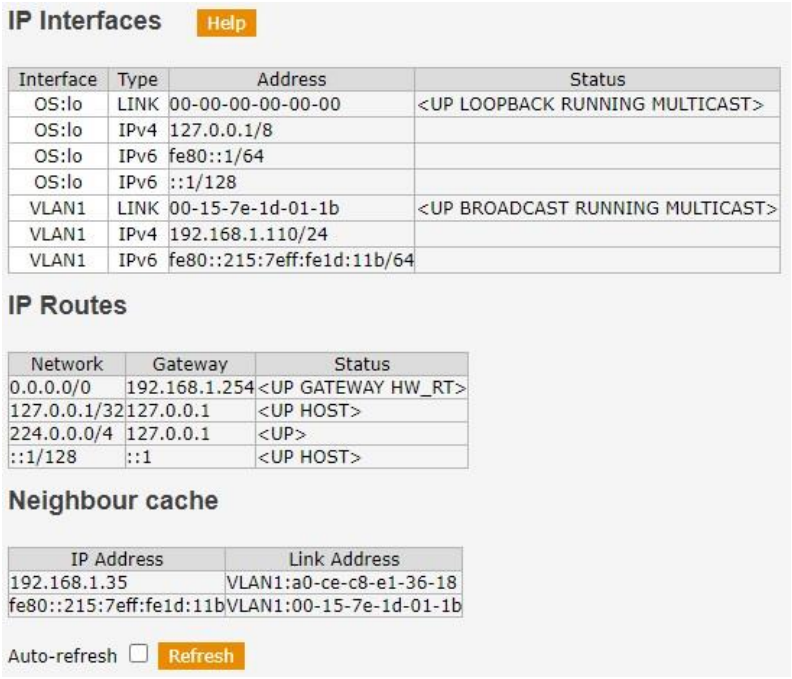
Mask Length

Setting	Description	Factory

		Default
Subnet mask for the Weidmüller Switch	The IPv6 network mask, in number of bits (*prefix length*). Valid values are between 1 and 128 bits for an IPv6 address. This field may be left blank if IPv6 operation on the interface is not desired.	None

3.3.3 IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbor cache (ARP cache) status.



The tables displays the following information:

IP Interfaces

Interface	The name of the interface.
Type	The address type of the entry. This may be LINK, IPv4 or IPv6.
Address	The current address of the interface (of the given type).
Status	The status flags of the interface (and/or address).

IP Routes

Network	The destination IP network or host address of this route.
Gateway	The gateway address of this route.
Status	The status flags of the route.

Neighbor Cache

IP Address	The IP address of the entry.

Link Address	The Link (MAC) address for which a binding to the IP address given exists.

3.3.4 Access Management

3.3.4.1 Login Methods

The Login Methods page allows the user to restrict the remote management of the switch. It is possible to block any specific kind of management (eg: web or telnet).

SSH

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable SSH mode operation.	Enabled

Telnet

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Telnet access.	Disabled

Web Interface Access

Setting	Description	Factory Default
Only HTTP	HTTPS mode operation disabled and web access only HTTP.	HTTP/HTTPS
Only HTTPS	HTTP mode operation disabled and web access only HTTPS.	
HTTP/HTTPS	HTTP and HTTPS mode operation enabled.	
HTTPS with HTTP auto-redirect	Automatically redirects web browser to an HTTPS connection.	

Certificate Maintain

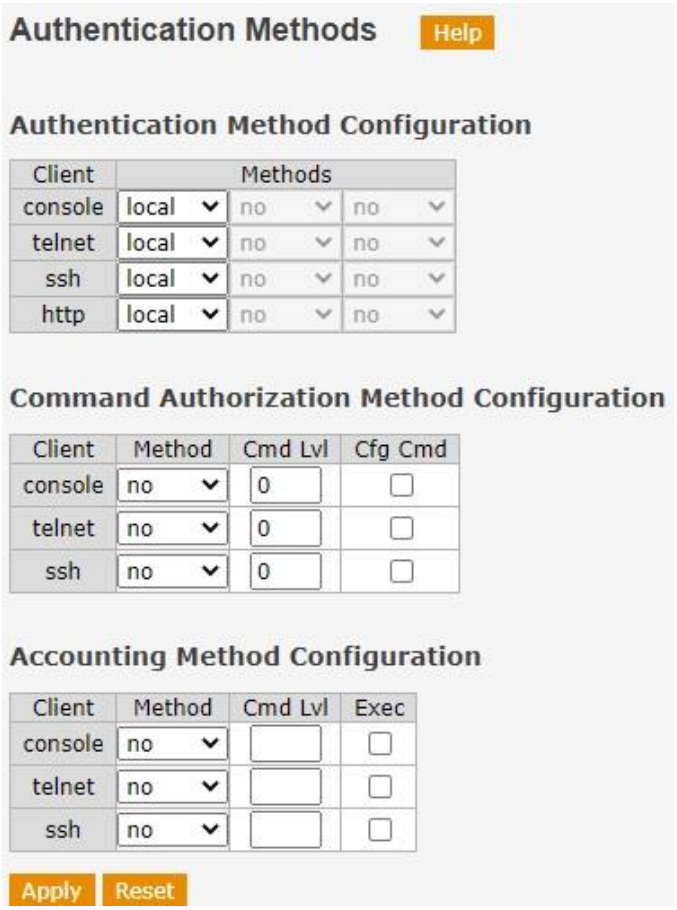
Setting	Description	Factory Default
None	No operation of certificate maintenance.	None
Delete	Delete the current certificate.	
Upload	Upload a certificate PEM file through a web browser or URL. A pass phrase has to be entered if the uploading certificate is protected by a specific passphrase.	
Generate	Generate a new self-signed RSA certificate.	

The **Certificate Status** field displays the current status of certificate on the switch. The possible status are:

- Switch secure HTTP certificate is presented.
- Switch secure HTTP certificate is not presented.
- Switch secure HTTP certificate is generating ...

3.3.4.2 Authentication Methods

The Authentication Methods option allows the administrator to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



Authentication Method Configuration

For each client type (console, telnet, ssh and http) the method to authenticate the user can be programmed:

Setting	Description	Factory Default
no	Authentication is disabled and login is not possible.	local
local	Use the local user database on the switch for authentication.	
radius	Use remote RADIUS server for authentication.	
tacacs	Use remote TACACS+ server for authentication.	

When a method involving a remote server is selected (“radius” or “tacacs”), an additional method can be programmed as backup. Up to three different authentication methods can be programmed and each one is tried from left to right until a user is either accepted or rejected.

NOTE: If a remote server is used for primary authentication, it is recommended to configure secondary authentication as “local”. This will enable the management client to login via the local user database if none of the configured authenticated servers are alive.

Command Authorization Method Configuration

The command authorization method section allows the administrator to limit the CLI commands available to a user. For each client type (console, telnet and ssh) the following parameters can be programmed:

Method

Setting	Description	Factory Default
no	Command authorization is disabled. User is granted access to CLI commands according to his privilege level.	no
tacacs	Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.	

Cmd Lvl

Setting	Description	Factory Default
0 to 15	Authorize all commands with a privilege level higher	0

	than or equal to this level.	

Cfg Cmd

Setting	Description	Factory Default
Check / Uncheck	Also authorize configuration commands.	Unchecked

Accounting Method Configuration

The accounting section allows the administrator to configure command and exec (login) accounting. For each client type (console, telnet and ssh) the following parameters can be programmed:

Method

Setting	Description	Factory Default
no	Accounting is disabled.	no
tacacs	Use remote TACACS+ server(s) for accounting.	

Cmd Lvl

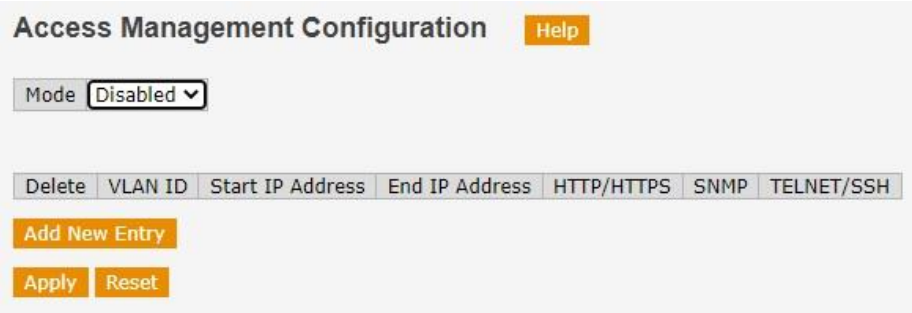
Setting	Description	Factory Default
0 to 15	Enable accounting for all commands with a privilege level higher than or equal to this level.	0

Exec

Setting	Description	Factory Default
Check / Uncheck	Enable exec (login) accounting.	Unchecked

3.3.4.3 Access Security

In this option the user can program the allowed IP addresses that can access to the management of the switch (Access Management). A table of up to 16 different entries can be created using the **Add New Entry** button.



Mode

Setting	Description	Factory Default
Disabled / Enabled	Enable or Disable the access management mode operation.	Unchecked

If the Access Management Mode is Enabled, for each entry of the table, the following fields have to be programmed:

VLAN ID

Setting	Description	Factory Default
1 to 4095	The VLAN ID for the access management entry.	1

Start IP address

Setting	Description	Factory Default
IP address	The start IP address for the access management entry.	None

End IP address

Setting	Description	Factory Default
IP address	The end IP address for the access management entry.	None

HTTP/HTTPS

Setting	Description	Factory Default
Check / Uncheck	The host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.	Unchecked

SNMP

Setting	Description	Factory Default
Check / Uncheck	The host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.	Unchecked

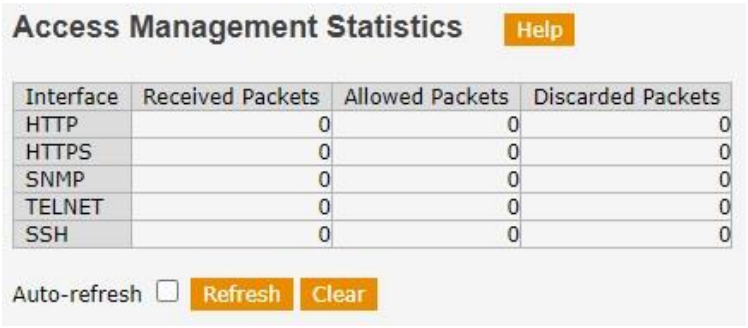
TELNET/SSH

Setting	Description	Factory Default
Check / Uncheck	The host can access the switch from TELNET/SSH interface if the host IP address matches the IP	Unchecked

	address range provided in the entry.	

3.3.4.4 Access Statistics

This page provides statistics for access management if the Mode is Enabled in the Access Security page.



In the table shown on the page is displayed the following information:

Interface	The interface type through which the remote host can access the switch.
Received Packets	Number of received packets from the interface.
Allowed Packets	Number of allowed packets from the interface.
Discarded Packets	Number of discarded packets from the interface.

3.3.5 Users

By default, the switch default's user name is "admin" (password is "Detmold") and has the highest privilege level (15). But is possible to create additional users / delete existing users and configure different privilege levels for each created user.

3.3.5.1 Configuration

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

When pressing the **Add New User** button, new fields are shown:

User Name

Setting	Description	Factory Default
Max. 31 characters	Enter the new user name. The valid user name is a combination of letters, numbers and underscores.	None

Password

Setting	Description	Factory Default
Max. 31 characters	Enter the password of the new user. Any printable characters are acceptable (letters, numbers, symbols and punctuation marks). The checkbox **Show Password** allows the user to display the written password.	None

Password (again)

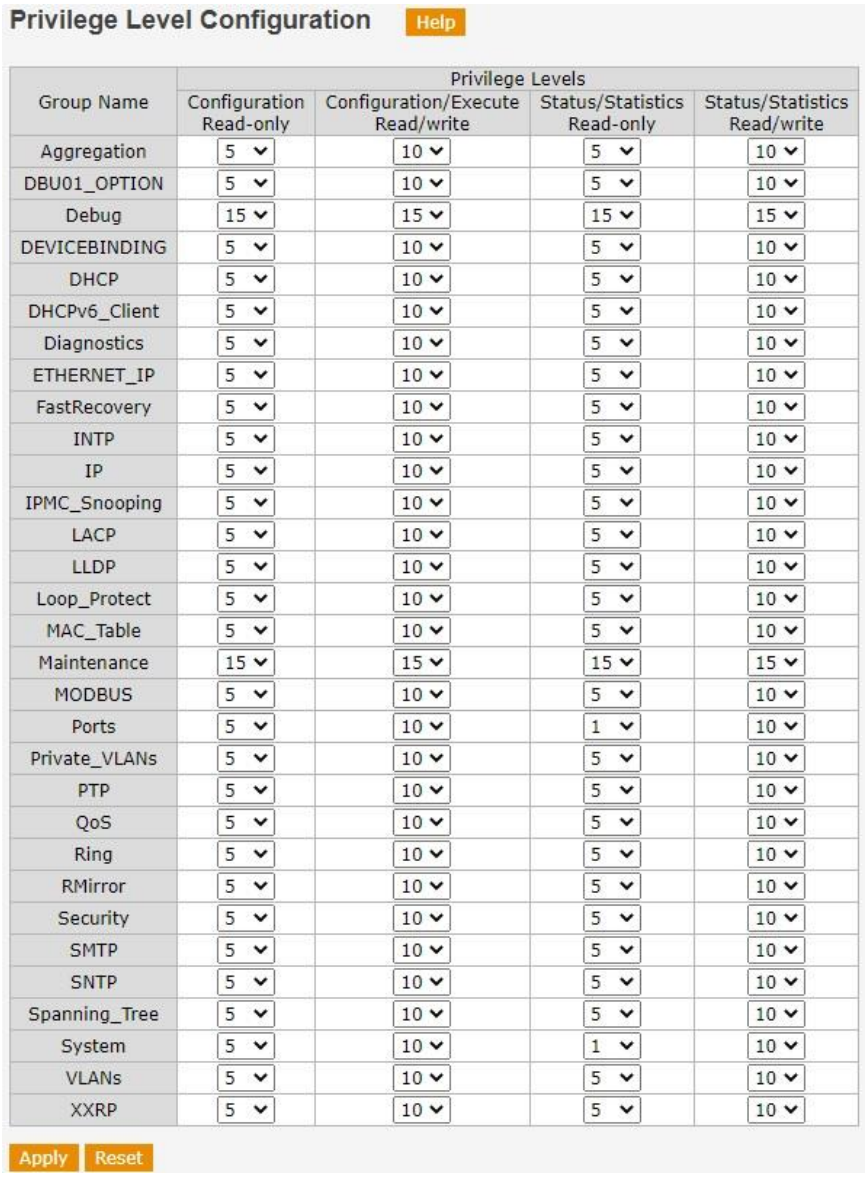
Setting	Description	Factory Default
Max. 31 characters	Enter the new password of the new user again to confirm.	None

Privilege Level

Setting	Description	Factory Default
0 to 15	The privilege level of the new user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have the access of that group. By default, the group privilege level of 5 has the read-only access and the privilege level of 10 has the read-write access. System maintenance (software upload, factory defaults, etc.) requires the user privilege level of 15. Generally, the privilege level of 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.	0

3.3.5.2 Privilege Levels

This page provides an overview of the default privilege levels required to perform specific actions in the switch. It also allows the administrator to modify these default values.



Privilege Level Configuration Help

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
DBU01_OPTION	5	10	5	10
Debug	15	15	15	15
DEVICEBINDING	5	10	5	10
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ETHERNET_IP	5	10	5	10
FastRecovery	5	10	5	10
INTP	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
MODBUS	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
PTP	5	10	5	10
QoS	5	10	5	10
Ring	5	10	5	10
RMirror	5	10	5	10
Security	5	10	5	10
SMTP	5	10	5	10
SNTP	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
VLANs	5	10	5	10
XXRP	5	10	5	10

Apply Reset

The page shows a table with the following fields:

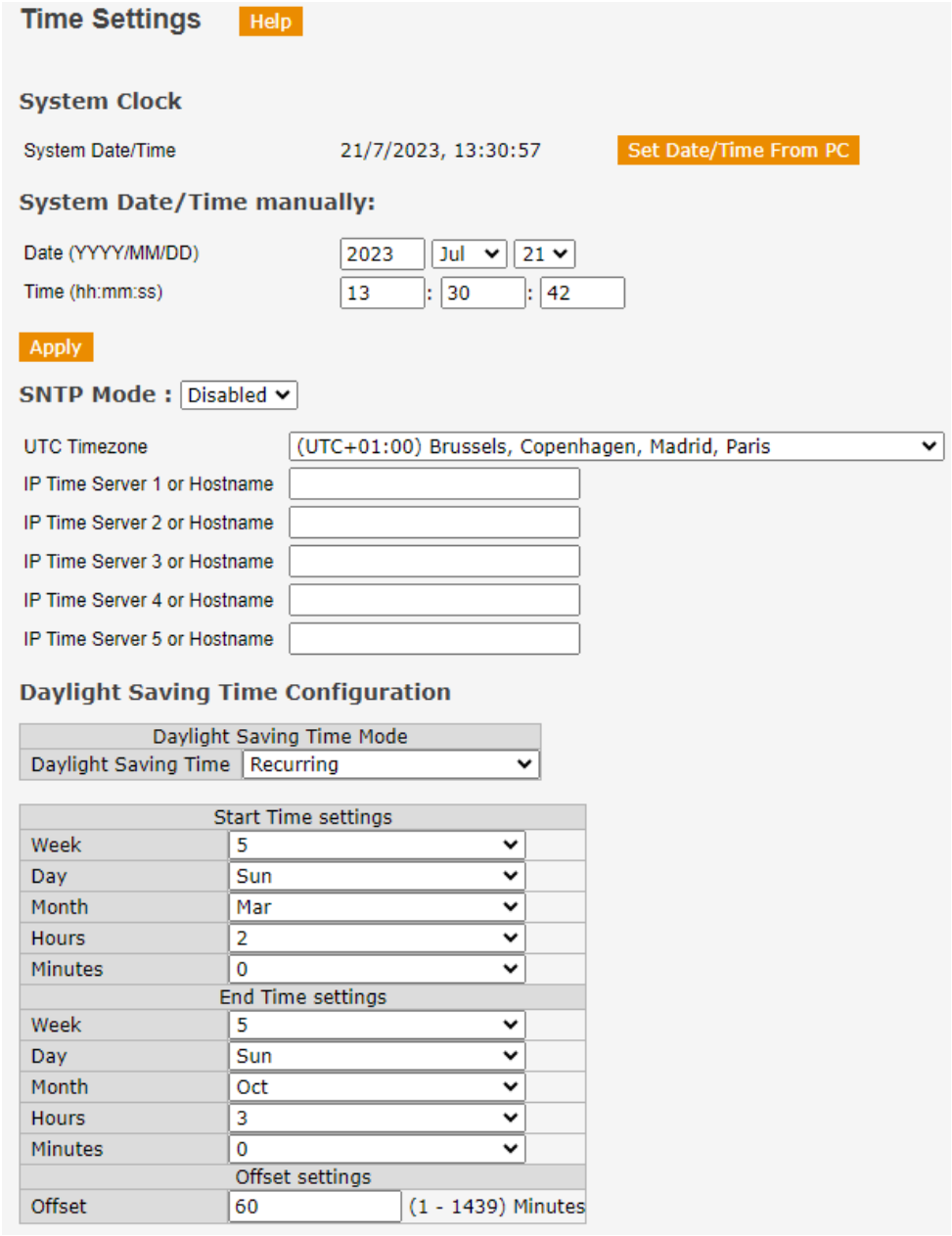
Group Name	The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details: **System**: Contact, Name, Location, Timezone, Daylight Saving Time, Log. **Security**: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, IP source guard. **IP**: Everything except 'ping'. **Port**: Everything except 'VeriPHY'. **Diagnostics**: 'ping' and 'VeriPHY'. **Maintenance**: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load.

	Web- Users, Privilege Levels and everything in Maintenance. **Debug**: Only present in CLI.

Privilege Levels	Every group has an authorization privilege level for the following subgroups: **Configuration Read-only** **Configuration/Execute Read/write** **Status/Statistics Read-only** **Status/Statistics Read/write** User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

3.3.6 Time Setting

The **Time Setting** configuration page lets users set the time, date, and other settings. An explanation of each setting is given below the figure.



NOTE: The Weidmüller switch does not have a real time clock. The user must update the Current Time and Current Date to set the initial time for the Weidmüller switch after each reboot, especially when the network does not have an Internet connection for an SNTP server or there is no SNTP server on the LAN.

System clock

Setting	Description	Factory Default
System Date/Time	Possibility to set the time of the switch directly from the management laptop using the button **Get Date/Time from PC** and then **Apply**. NOTE: The buttons **Get Date/Time from PC** and **Apply** are disabled if the SNTP mode is programmed	None

	as Server or Client.	

Set System Date Time manually

Setting	Description	Factory Default
System Date	Allows configuration of the local date in yyyy-mm-dd format.	None
System Time	Allows configuration of the local time in 24-hour format.	None

SNTP mode

Setting	Description	Factory Default
Disabled	No SNTP used in the switch.	Disabled
Server	The Weidmüller switch can synchronize other switches of the network with its programmed time clock.	
Client	The Weidmüller Switch will synchronize its clock with one of the Server IP Addresses fields.	

UTC Timezone

Setting	Description	Factory Default
User selectable time zone	Specifies the time zone, which is used to determine the local time offset from UTC (Universal Time Coordinated).	UTC (Universal Time Coordinated)

Server IP Addresses

Setting	Description	Factory Default
Time Server IP (1 to 5)	IP address of the SNTP servers. If the 1st SNTP Server fails to connect, the Weidmüller Switch will try to locate the 2nd, 3rd, 4th and 5th Servers indicated.	None

Daylight Saving Time Mode

Setting	Description	Factory Default
Disabled / Recurring / Non-Recurring	Automatically set the Weidmüller switch's time forward or backward according to national standards. When "Recurring" is selected, the configured Daylight Saving Time duration will be repeated every year whilst if "Non-Recurring" is selected, the configuration will only be applied for a single time.	Disabled

Start Time Settings

Setting	Description	Factory

		Default
Week / Day / Month / Hours / Minutes	Specifies the starting time to apply the Daylight Saving Time.	None

End Time Settings

Setting	Description	Factory Default
Week / Day / Month / Hours / Minutes	Specifies the ending time to apply the Daylight Saving Time.	None

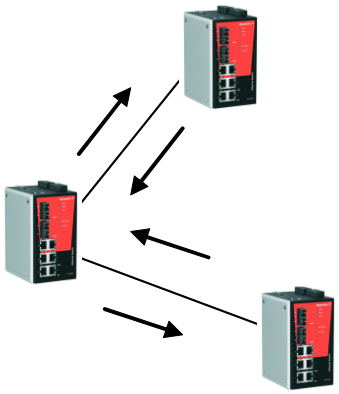
Daylight Saving Offset

Setting	Description	Factory Default
0 to 1440 minutes	Specifies the number of minutes that the time should be set forward during Daylight Saving Time.	None

3.3.7 LLDP Function

3.3.7.1 Overview

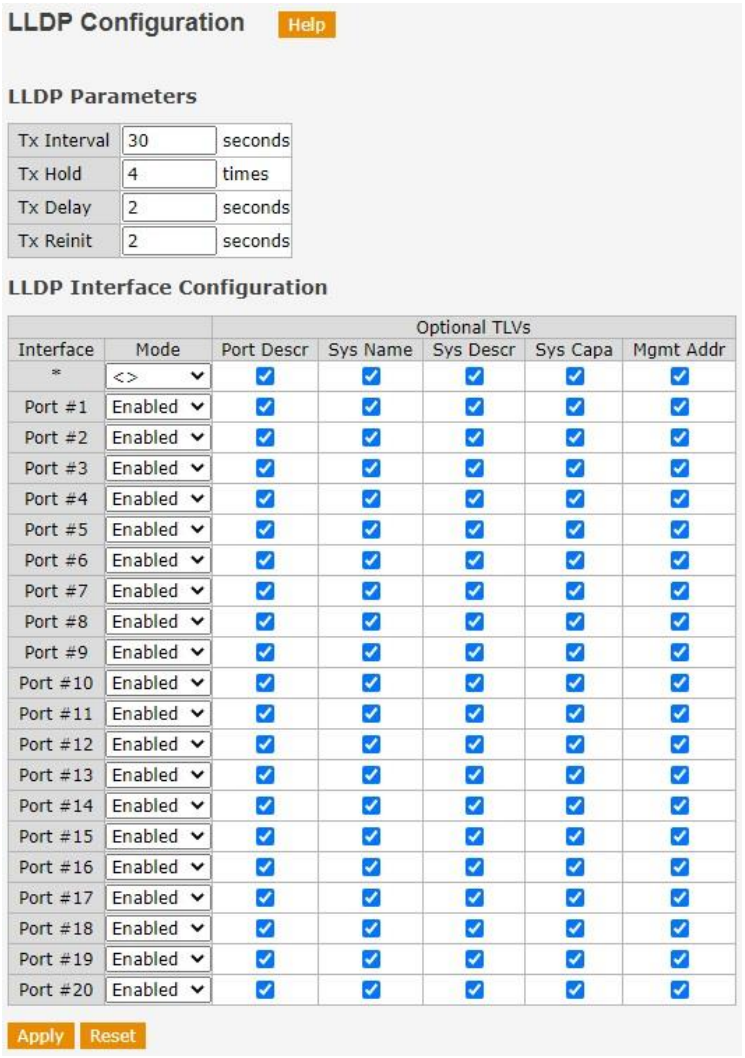
Defined by IEEE 802.11AB, LLDP is an OSI Layer 2 Protocol that standardizes the methodology of self-identity advertisement. It allows each networking device, e.g. a Weidmüller managed switch, to periodically inform its neighbors about its self-information and configurations. As a result, all of the devices would have knowledge about each other; and through SNMP, this knowledge can be transferred to a Network Management Software for auto-topology and network visualization.



From the switch's web interface, users have the option of either enabling or disabling the LLDP, as well as setting the LLDP transmit interval (as shown in the figure below). In addition, users are able to view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows a Network Management Software to automatically display the network's topology as well as system setup details such as VLAN, and Trunking for the entire network.

3.3.7.2 Configuration

This page allows the user to inspect and configure the current LLDP port settings.



LLDP Parameters

Tx Interval

Setting	Description	Factory Default
5 to 32768 sec	The switch periodically transmits LLDP frames to its neighbors to update the network discovery information. The interval between each LLDP frame is determined by the Tx Interval value.	30 (sec)

Tx Hold

Setting	Description	Factory Default
2 to 10 times	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds.	4 (times)

Tx Delay

Setting	Description	Factory Default
1 to 8192 sec	If some configuration is changed (e.g. the IP address), a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value.	2 (sec)

Tx Reinit

Setting	Description	Factory Default
1 to 10 sec	When an interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization.	2 (sec)

LLDP Interface Configuration

For each port of the switch the user can configure:

Mode

Setting	Description	Factory Default
Rx only	The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.	Enabled
Tx only	The switch will drop LLDP information received from neighbors, but will send out LLDP information.	
Disabled	The switch will not send out LLDP information, and will drop LLDP information received from neighbors	
Enabled	The switch will send out LLDP information, and will analyze LLDP information received from neighbors	

Port Descr

Setting	Description	Factory Default
Check / Uncheck	Optional TLV: When checked, the "port description" is included in LLDP information transmitted.	Checked

Sys Name

Setting	Description	Factory

		Default
Check / Uncheck	Optional TLV: When checked, the "system name" is included in LLDP information transmitted.	Checked

Sys Descr

Setting	Description	Factory Default
Check / Uncheck	Optional TLV: When checked, the "system description" is included in LLDP information transmitted.	Checked

Sys Capa

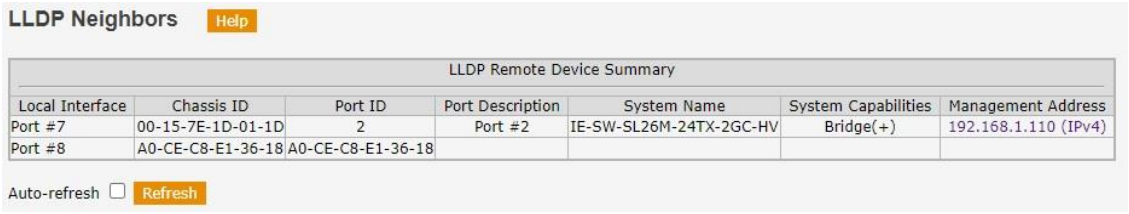
Setting	Description	Factory Default
Check / Uncheck	Optional TLV: When checked, the "system capability" is included in LLDP information transmitted.	Checked

Mgmt Addr

Setting	Description	Factory Default
Check / Uncheck	Optional TLV: When checked, the "management address" is included in LLDP information transmitted.	Checked

3.3.7.3 Neighbors

This page provides a status overview for all LLDP neighbors.



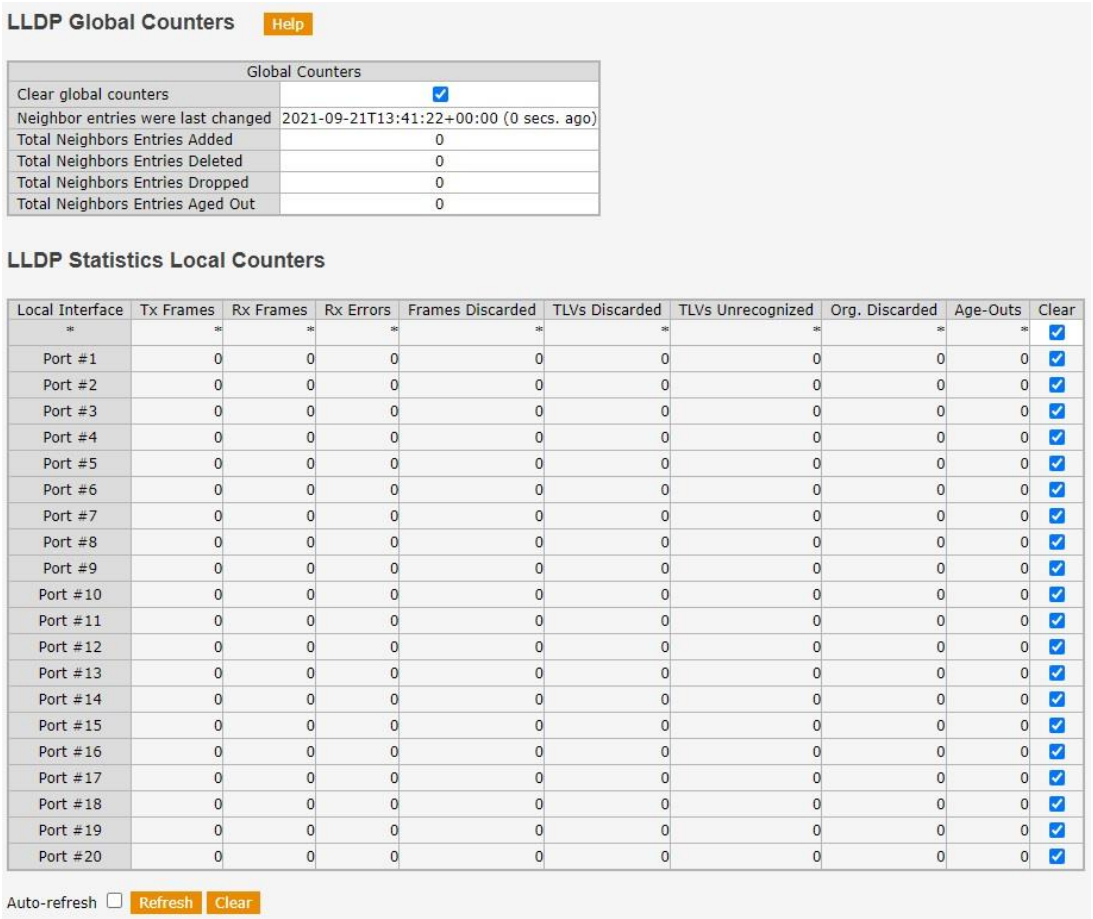
The displayed table contains information for each port on which an LLDP neighbor is detected:

Local Interface	The interface/port on which the LLDP frame was received.
Chassis ID	The identification of the neighbor's LLDP frames.
Port ID	The identification of the neighbor port.
Port Description	The port description advertised by the neighbor unit.
System Name	The name advertised by the neighbor unit.
System Capabilities	The neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS Cable Device

	8. Station Only 9. Reserved When a capability is enabled, a (+) will be displayed. If the capability is disabled, a (-) will be displayed.
Management Address	The neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

3.3.7.4 Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters refer to the whole switch, whilst local counters refer to specific interfaces/ports of the switch.



LLDP Global Counters Help

Global Counters	
Clear global counters	☑
Neighbor entries were last changed	2021-09-21T13:41:22+00:00 (0 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	☑
Port #1	0	0	0	0	0	0	0	0	☑
Port #2	0	0	0	0	0	0	0	0	☑
Port #3	0	0	0	0	0	0	0	0	☑
Port #4	0	0	0	0	0	0	0	0	☑
Port #5	0	0	0	0	0	0	0	0	☑
Port #6	0	0	0	0	0	0	0	0	☑
Port #7	0	0	0	0	0	0	0	0	☑
Port #8	0	0	0	0	0	0	0	0	☑
Port #9	0	0	0	0	0	0	0	0	☑
Port #10	0	0	0	0	0	0	0	0	☑
Port #11	0	0	0	0	0	0	0	0	☑
Port #12	0	0	0	0	0	0	0	0	☑
Port #13	0	0	0	0	0	0	0	0	☑
Port #14	0	0	0	0	0	0	0	0	☑
Port #15	0	0	0	0	0	0	0	0	☑
Port #16	0	0	0	0	0	0	0	0	☑
Port #17	0	0	0	0	0	0	0	0	☑
Port #18	0	0	0	0	0	0	0	0	☑
Port #19	0	0	0	0	0	0	0	0	☑
Port #20	0	0	0	0	0	0	0	0	☑

Auto-refresh ☐ Refresh Clear

LLDP Global Counters

Clear global counters	If checked, the global counters are cleared when the button **Clear** is pressed.
Neighbor entries were last changed	Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.

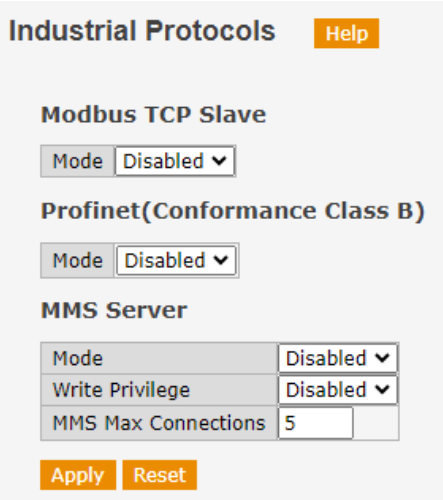
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to full entry table.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to expired time-to-live.

LLDP Statistics Local Counters

Local Interface	The port that receives or transmits LLDP frames.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If a port receives an LLDP frame, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given interface's links is down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (Type Length Value). If a TLV is malformed, it will be counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	If an LLDP frame is received with an organizationally TLV but the TLV is not supported, the TLV is counted and discarded.
Age-Outs	Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age-out time, the LLDP information is removed and the value of the age-out counter is incremented.
Clear	If checked, the counters for the specific interface are cleared when the button **Clear** is pressed.

3.3.8 Industrial Protocols

In this page the user can activate the industrial protocols supported by the switch: Modbus TCP, Profinet and MMS.



3.3.8.1 Modbus TCP

Introduction

MODBUS TCP is a protocol commonly used for the integration of a SCADA system. It is also a vendor-neutral communication protocol used to monitor and control industrial automation equipment such as PLCs, sensors, and meters. In order to be fully integrated into industrial systems, Weidmüller's switches support Modbus TCP/IP protocol for real-time monitoring in a SCADA system.

Configuring MODBUS/TCP on Weidmüller Switches

Modbus TCP is disabled by default. To enable Modbus TCP, select **Enable** in **Mode** and then click **Apply**. In the Appendix B, Modbus Register Table, the user can find all the available registers of the switch.

3.3.8.2 Profinet

Introduction

PROFINET is a communication standard for automation of PROFIBUS & PROFINET International (PI). It is 100% Ethernet-compatible as defined in IEEE standards. With PROFINET, applications can be implemented for production and process automation, safety applications, and the entire range of drive technology. With its integrated Ethernet-based communication, PROFINET satisfies a wide range of requirements, from data-intensive parameter assignment to extremely fast I/O data transmission.

PROFINET I/O is used for data exchange between I/O controllers (PLC, etc.) and I/O devices (field devices). This specification defines a protocol and an application interface for exchanging I/O data, alarms, and diagnostics. And its real-time (RT) solution allows response time in the range of 5 ms, which corresponds to today's PROFIBUS DP applications. The Weidmüller switch is a PROFINET I/O device.

Configuring Profinet on Weidmüller Switches

Profinet is enabled by default. It can be disabled by selecting **Disable** in **Mode** and clicking **Apply**. The user can get the GSDML (Generic Station Description Markup Language) File in in the

Weidmüller Online Product Catalogue. Select or search for device name or part number and refer to section ‘Donwloads’.

3.3.8.3 MMS

Introduction

MMS (Manufacturing Message Specification) is a client/server protocol included in the IEC 61850 standard for the communication between IEDs (Intelligent Electronic Devices) and SCADA system. The data model used by MMS is based on Logical Nodes. The Logical Nodes of an Ethernet Switch are defined in the technical report IEC 61850-90-4 (bridge model).

Configuring MMS on Weidmüller Switches

MMS is disabled by default. The user can enable it by selecting **Enabled** in **Mode** and then clicking **Apply**. After this, an MMS client can access to the switch to read and monitor its available data objects. Additionally, the user can also enable the **Write Privilege**.

NOTE: MMS protocol does not provide any authentication mechanism so by enabling the MMS Write Privilege any MMS client (TCP/IP protocol) may change the settings of the switch. Enable only MMS Write Privilege if additional measures to avoid unauthorized access have been taken (ex: Firewall).

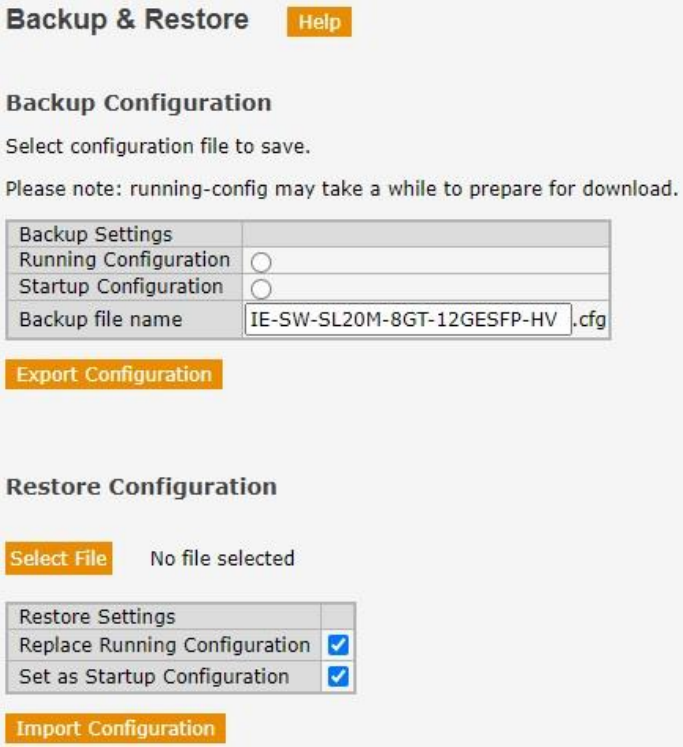
In the field **MMS Max Connections** the user can select the maximum number of allowed TCP connections to the MMS server (between 1 and 10).

In the Appendix C, Supported Logical Nodes (MMS), the user can find all the available Logical Nodes of the switch. Additionally, the user can get the ICD (IED Capability Description) File in in the Weidmüller Online Product Catalogue. Select or search for device name or part number and refer to section ‘Donwloads’.

3.3.9 Backup & Restore

Following saving and restoring functions are available in this web page.

- Save the current configuration file in connected PC
- Save the startup configuration file in connected PC
- Loading a new configuration by importing a file already saved in connected PC
- Set as startup configuration a configuration file already saved in connected PC



Backup Configuration

The switch stores its configuration in a number of text files. The files are either virtual (RAM-based) or stored in flash on the switch. The available files are:

- Running Configuration: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- Startup Configuration: The startup configuration of the switch read at boot time. If this file does not exist at boot time, the switch will start up in default configuration.
- Default Configuration: A read-only file with vendor-specific configuration. This file is read when the system is restored to default values.

It is possible to save either the Running Configuration file or the Startup Configuration file of the switch to the PC. The name of the file has to be entered in the field **Backup file name** and then the button **Export Configuration** has to be pressed.

Restore Configuration

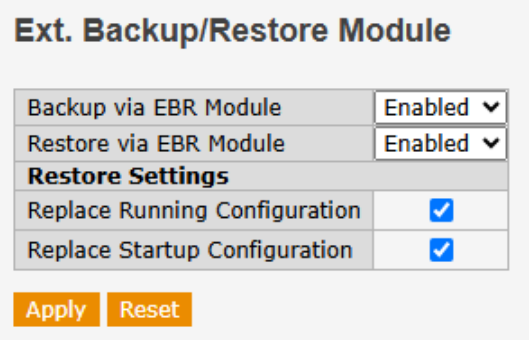
It is possible to upload a configuration file from the PC to all the files on the switch, except the Default Configuration one which is read-only. Press the button **Select File,** select the file saved on the PC, check in the web page the configuration file to be restored (Running Configuration and/or Startup Configuration) and press **Import Configuration**.

3.3.10 Ext. Backup/Restore Module

The Weidmüller's external backup and restore module IE-EBR-MODULE-RS232-ALM (Part No. 2682610000) is a standalone electronic unit that can be used to backup and restore the configuration of managed Weidmüller switches. The device will be connected to the switch's serial console port and is powered via the console port.

This module allows the user to save and restore configuration files without PC. It is also a very useful tool for creating cloned devices based on a stored Master Switch configuration to speed up mass configuration.

The web page Ext. Backup/Restore Module allows the user to enable or disable the use of this IE-EBR-MODULE-RS232-ALM module in the switch.



Backup via EBR module

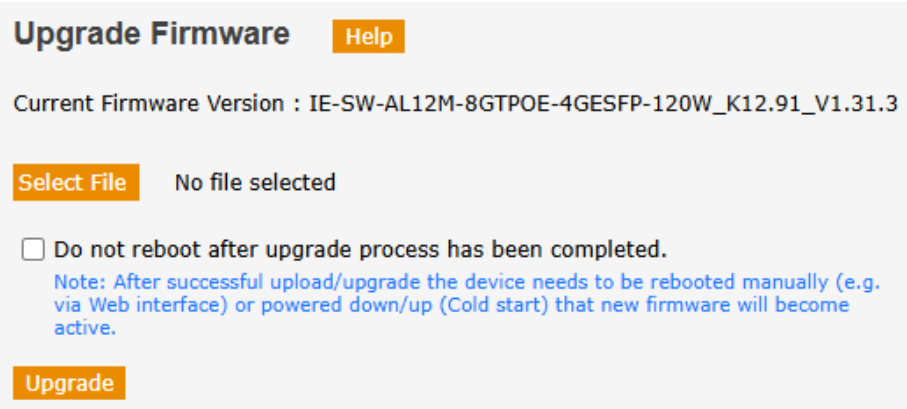
Setting	Description	Factory Default
Enabled/Disabled	When Enabled, the IE-EBR-MODULE-RS232-ALM can be used in the switch to download the configuration file.	Enabled

Restore via EBR module

Setting	Description	Factory Default
Enabled/Disabled	When Enabled, the IE-EBR-MODULE-RS232-ALM can be used in the switch to upload a stored configuration file. The user can select the restored configuration (running configuration, startup configuration or both).	Enabled

3.3.11 Upgrade Firmware

This option is used to upgrade the firmware of the switch when a new version is available.



The page already shows the current firmware version stored on the switch. To import a new firmware file into the Weidmüller switch, press the button **Select File** to select the firmware file that is saved on your computer. The upgrade procedure will proceed automatically after pressing **Upgrade**.

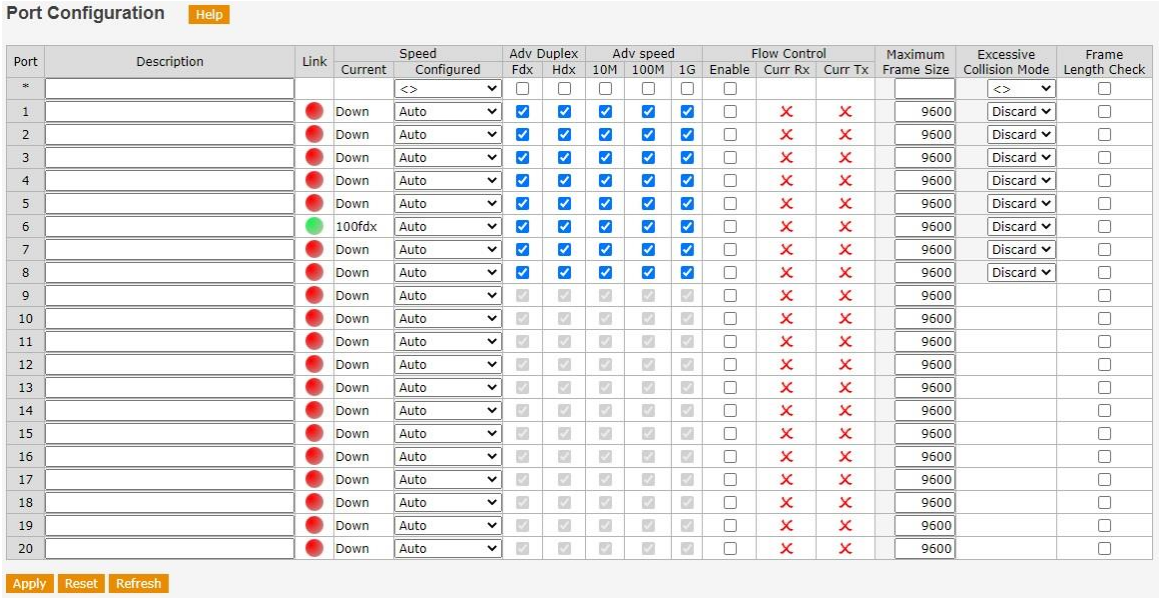
Once the upgrade process is completed, the switch will be automatically rebooted. If the user wants to avoid this automatic reboot, the checkbox “Do not reboot after upgrade process has been completed” has to be selected. Then the user will have to reboot the device manually to become active the new firmware.

3.4 Port Settings

Port settings are included to give the user control over the different ports of the switch. Through this menu the user can also configure Port trunking and Loop protection.

3.4.1 Port Configuration

This page displays current port configurations. Ports can also be configured here.



Description

Setting	Description	Factory Default
Max. 256 characters	Name of the port. Example: Main Busbar Protection Relay.	None

Link

Setting	Description	Factory Default
Graphic display of link status (no setting)	Green indicates the link is up and red that it is down.	Current Status

Current Link Speed

Setting	Description	Factory Default
Speed	Provides the current link speed of the port.	Current

(no setting)		Speed

Configured Link Speed

Setting	Description	Factory Default
Disabled	Immediately shuts off port access.	Auto
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	
10 Mbps HDX	Forces the RJ45 port in 10Mbps half-duplex mode.	
10 Mbps FDX	Forces the RJ45 port in 10Mbps full-duplex mode.	
100 Mbps HDX	Forces the RJ45 port in 100Mbps half-duplex mode.	
100 Mbp FDX	Forces the RJ45 port in 100Mbps full-duplex mode.	
1 Gbps FDX	Forces the RJ45 port in 1Gbps full-duplex mode.	
Auto (SFP)	Automatically determines the speed of the SFP transceiver. Note: There is no standardized way for the SFP auto detect, so in the switch is done by reading the SFP ROM. Due to the missing standardized way of autodetection in SFP transceivers, some of them may not be detectable.	
100 Mbps FDX (SFP)	Forces the SFP port in 100Mbps full-duplex mode.	
1 Gbps FDX (SFP)	Forces the SFP port in 1Gbps full-duplex mode.	

NOTE: If a connected device or sub-network is wreaking havoc on the rest of the network, the **Disabled** option gives the administrator a quick way to shut off access through this port immediately.

Advertise Duplex

Setting	Description	Factory Default
Check / Uncheck Fdx, Hdx	When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex modes (Fdx or Hdx) to the link partner.	All checked

Advertise Speed

Setting	Description	Factory Default

Check / Uncheck 10M, 100M, 1G	When speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (10M 100M 1G) to the link partner.	All checked

Flow Control

Setting	Description	Factory Default
Enabled / Disabled	Enables or Disables flow control for this port. This setting is related to the setting for Configured Link Speed. When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation.	Disabled

Maximum Frame Size

Setting	Description	Factory Default
1518 to 9600 (bytes)	Enter the maximum frame size allowed for the switch port, including FCS.	9600 (bytes)

Excessive Collision Mode

Setting	Description	Factory Default
Discard / Restart	Configures the port transmission behavior with collisions: Discard: Discard frame after 16 collisions Restart: Restart backoff algorithm after 16 collisions	Discard

Frame Length Check

Setting	Description	Factory Default
Check / Uncheck	Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field	Unchecked

	doesn't match the actual payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch.	

3.4.2 Port Trunking

Link Aggregation allows one or more links to be aggregated together to form a Link Aggregation Group. A MAC client can treat Link Aggregation Groups as if they were a single link.

The Weidmüller switch's Port Trunking feature allows devices to communicate by aggregating several trunk groups (half of total number of ports), with a maximum of 16 ports for each group. If one of the 16 ports fails, the other 15 ports will provide back up and share the traffic automatically.

Port Trunking can be used to combine up to 16 ports between two Weidmüller switches. If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 3200 Mbps.

The Port Trunking protocol provides the following benefits:

- Gives you more flexibility in setting up your network connections, since the bandwidth of a link can be increased.
- Provides redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.
- Load sharing—MAC Client traffic may be distributed across multiple links.

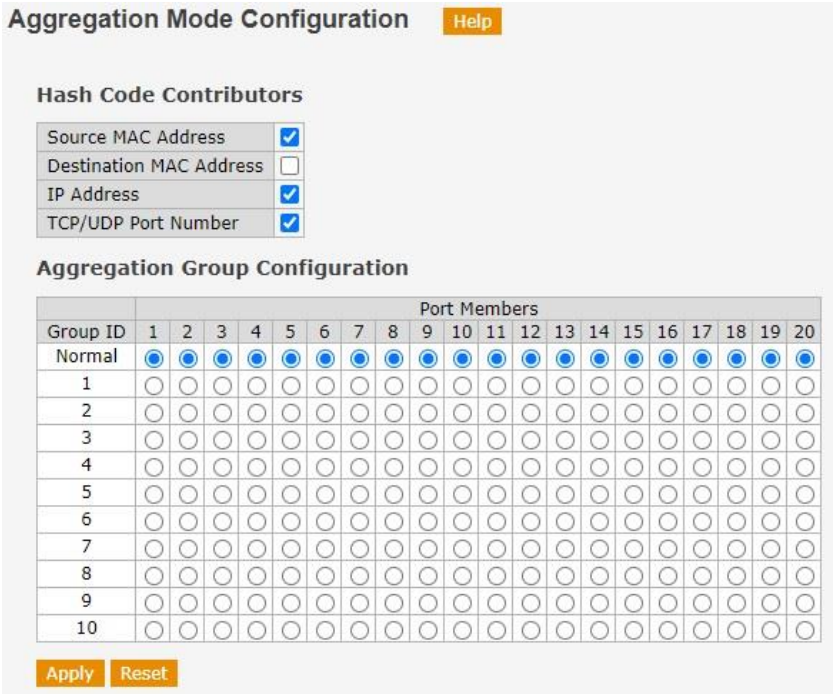
To avoid broadcast storms or loops in your network while configuring a trunk, first disable or disconnect all ports that you want to add to the trunk or remove from the trunk. After you finish configuring the trunk, enable or re-connect the ports.

When using a port link aggregation it also has to be considered that:

- None of the ports in a link aggregation can be configured as mirror source or mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in link aggregation as a whole.

3.4.2.1 Aggregation Mode

This page is used to configure the static aggregation mode and aggregation groups in the switch.



Hash Code Contributors

Source MAC Address

Setting	Description	Factory Default
Check / Uncheck	When enabled, the source MAC address is used to calculate the destination port for the frame.	Checked

Destination MAC Address

Setting	Description	Factory Default
Check / Uncheck	When enabled, the destination MAC address is used to calculate the destination port for the frame.	Unchecked

IP Address

Setting	Description	Factory Default
Check / Uncheck	When enabled, the IP address is used to calculate the destination port for the frame.	Checked

TCP/UDP Port Number

Setting	Description	Factory Default
Check / Uncheck	When enabled, theTCP/UDP port number is used to calculate the destination port for the frame.	Checked

Static Aggregation Group Configuration

Group ID

Setting	Description	Factory Default
Normal, 1 to half number of total ports	Indicates the ID of each aggregation group. Normal means no aggregation. Maximum number of groups is half number of the total ports and only one group ID is valid per port.	Normal

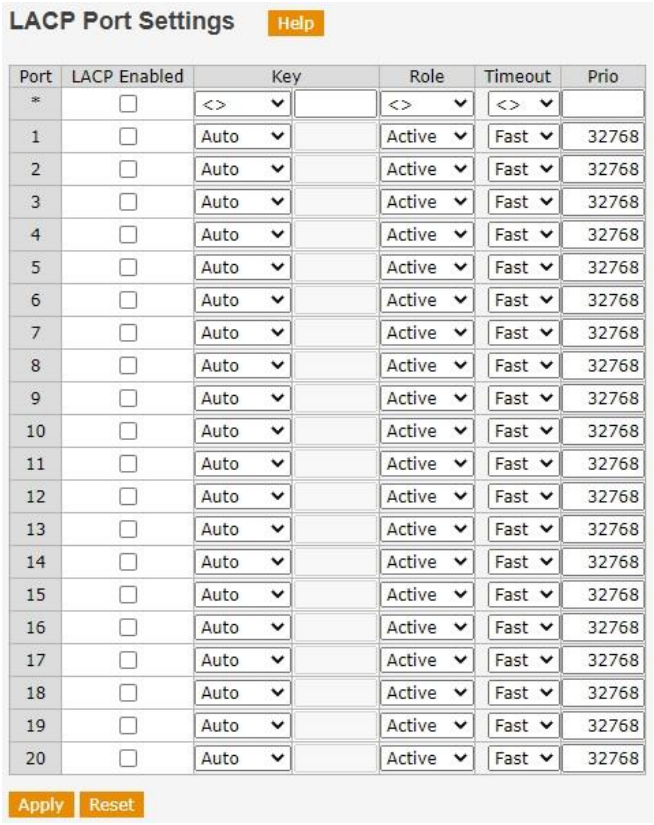
Port Members

Setting	Description	Factory Default
1 to total number of ports	Select ports to be included in an aggregation group. Only full duplex ports can join an aggregation group and all the ports must have the same speed in each group.	No ports belonging to any aggregation group

3.4.2.2 LACP Port Settings

LACP (Link Aggregation Control Protocol) trunks are similar to static port trunks but they are more flexible because LACP is compliant with the IEEE 802.3ad standard. Hence, it is interoperable with equipment from other vendors that also comply with the standard.

This page allows the user to enable LACP functions to group ports together to form single virtual links and change associated settings, thereby increasing the bandwidth between the switch and other LACP-compatible devices.



The following parameters can be configured for each port:

LACP Enabled

Setting	Description	Factory Default
Check / Uncheck	Controls whether LACP is enabled on the switch port. LACP will form an aggregation when two or more ports are connected to the same partner.	Unchecked

Key

Setting	Description	Factory Default
Auto / Specific	Ports with the same key value can join in the same aggregation group, while ports with different keys cannot. Auto: The key will be set according to the physical link speed (10Mb = 1, 100Mb = 2, 1Gb = 3). Specific. The user must enter the value of the key.	Auto
1 to 65535	Key value when Specific mode is set.	None

Role

Setting	Description	Factory Default
Active / Passive	Shows the LACP activity status. Active: Transmits packets every second. Passive: Waits for an LACP packet from a partner (speak if spoken to).	Active

Timeout

Setting	Description	Factory Default
Fast / Slow	Controls the period between BPDU transmissions. Fast: LACP packets are transmitted every second. Slow: LACP packets are transmitted every 30 seconds.	Fast

Priority

Setting	Description	Factory Default
1 to 65535	Controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.	32768

3.4.2.3 LACP System Status

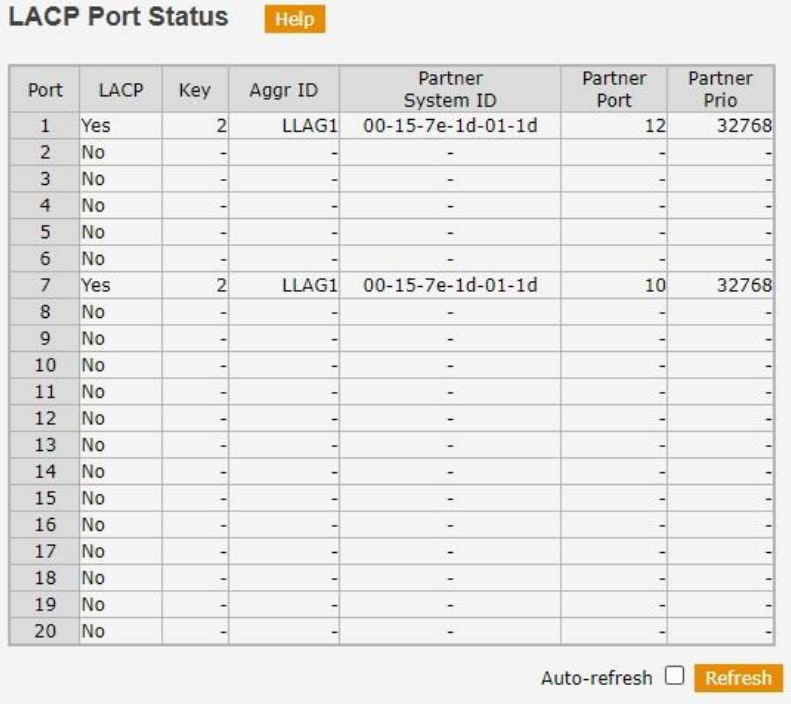
This page provides a status overview for all LACP instances.

The displayed table contains information about the different LACP groups created:

Aggr ID	The aggregation ID is associated with the aggregation instance.
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Partner Prio	The priority of the aggregation partner.
Last Changed	The time since this aggregation changed.
Local Ports	Shows which ports belong to the aggregation group of the switch.

3.4.2.4 LACP Port Status

This page provides an overview of LACP status of all ports.



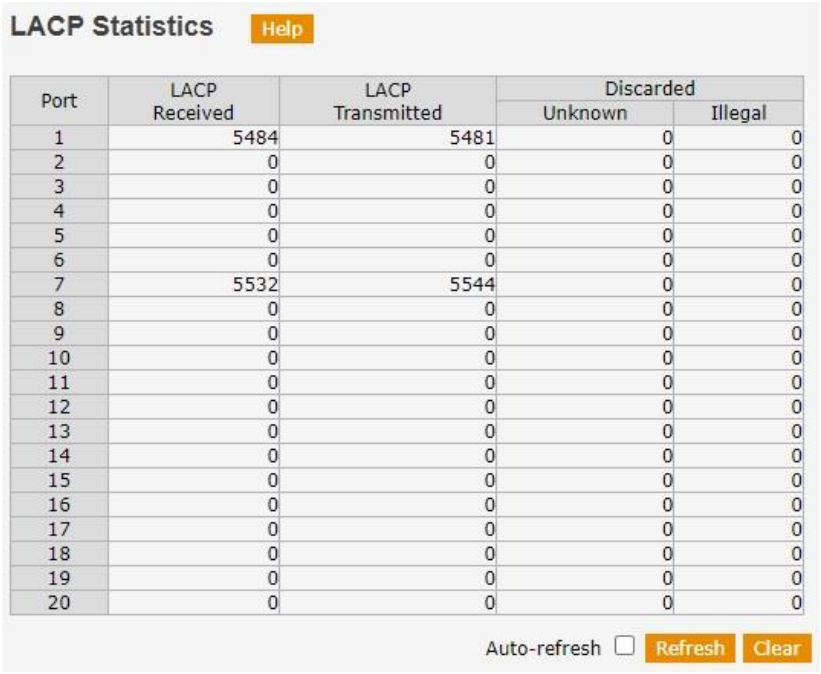
The displayed table contains information about the different LACP parameters of each port:

Port	The switch port number.
LACP	'Yes' means LACP is enabled and the port link is up. 'No' means LACP is not enabled or the port link is down. 'Backup' means the port cannot join in the aggregation group unless other ports are removed. Meanwhile its LACP status is disabled.
Key	The key assigned to the port. Only ports with the same key can aggregate together.

Aggr ID	The Aggregation ID assigned to this aggregation group.
Partner System ID	The partner's System ID (MAC address).
Partner Port	The partner's port number connected to this port.
Partner Prio	The partner's port priority.

3.4.2.5 LACP Statistics

This page provides an overview of the LACP statistics for all ports.



The displayed table shows the following information:

Port	The switch port number.
LACP Received	Shows how many LACP frames have been received at each port.
LACP Transmitted	Shows how many LACP frames have been sent from each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.

3.4.2.6 Aggregation Status

This page is used to see the status of ports in Aggregation groups.

The displayed table contains information about the different static and LACP aggregation groups created:

Aggr ID	The aggregation ID associated with this aggregation instance.

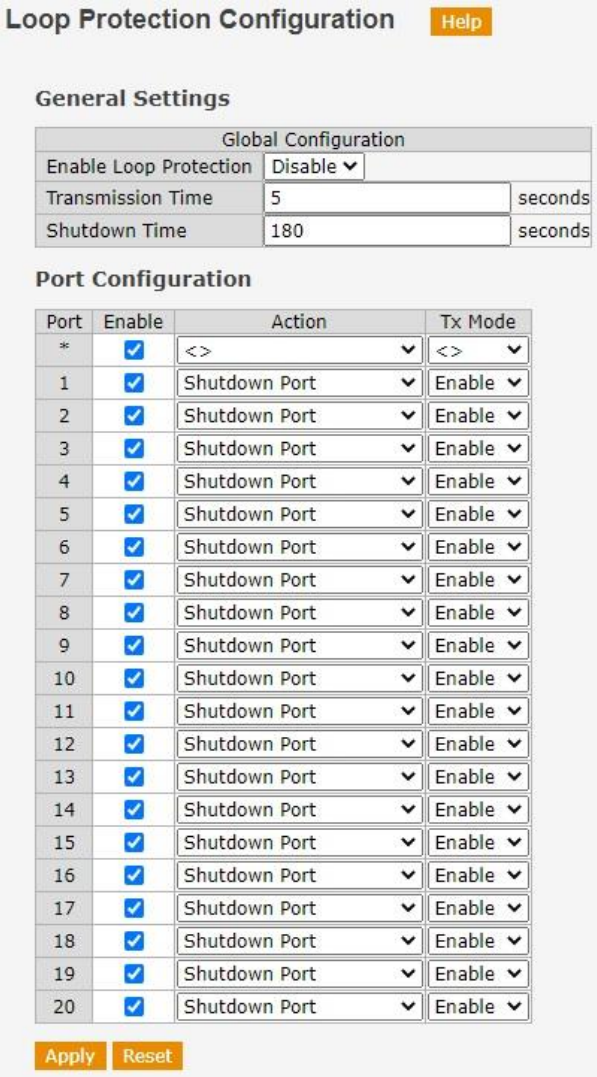
Name	Name of the aggregation group ID.
Type	Type of the aggregation group (static or LACP).
Speed	Speed pf the aggregation group.
Configured Ports	Configured member ports of the aggregation group.
Aggregated Ports	Aggregated member ports of the aggregation group.

3.4.3 Loop Protection

Avoid maintenance/installation crews from mistakenly placing one cable on the same switch generating a loop problem.

3.4.3.1 Configuration

This page allows the user to enable the Loop Protection function in the different ports of the switch.



General Settings

Enable Loop Protection

Setting	Description	Factory

		Default
Enable / Disable	Controls whether loop protection is enabled (as a whole).	Disable

Transmission Time

Setting	Description	Factory Default
1 to 10 (sec)	The interval between each loop protection PDU sent on each port.	5 (sec)

Shutdown Time

Setting	Description	Factory Default
0 to 604800 (sec)	The period (in seconds) for which a port will be kept disabled when a loop is detected (shutting down the port). A value of zero will keep a port disabled permanently (until the device is restarted). The maximum value is 604800 seconds (7 days).	180 (sec)

Port Configuration

Enable

Setting	Description	Factory Default
Check / Uncheck	Controls whether loop protection is enabled in this port. It is also necessary to enable the function in the General Setting section.	Checked

Action

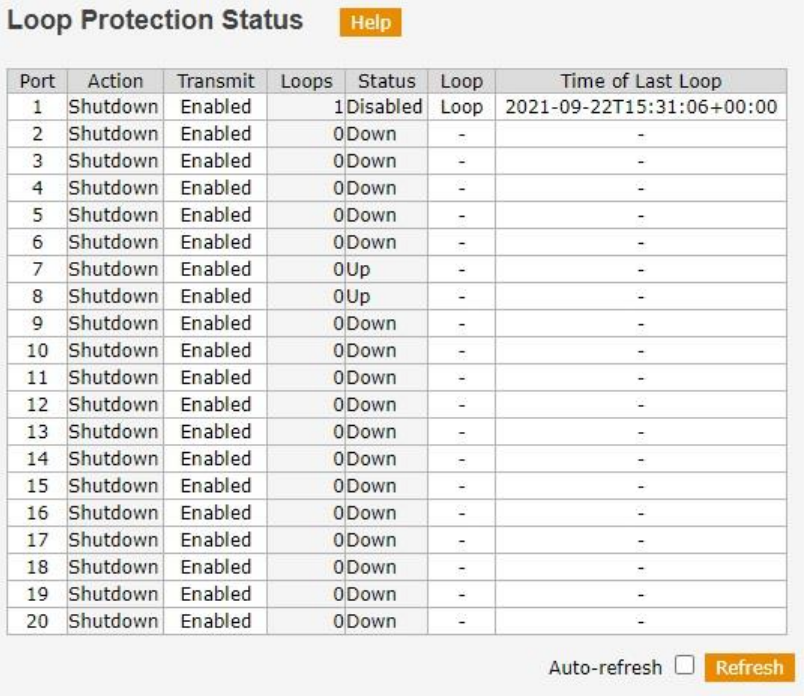
Setting	Description	Factory Default
Shutdown Port / Shutdown Port and Log / Log Only	Configures the action performed when a loop is detected on a port. It is possible to disable the port (shutdown), to log an event only or to take both actions (shutdown and log).	Shutdown Port

Tx Mode

Setting	Description	Factory Default
Enable / Disable	Controls whether the port is actively generating loop protection PDUs (Enable) or whether it is just passively looking for looped PDUs (Disable).	Enable

3.4.3.2 Status

This page displays the loop protection port status of the switch.



Loop Protection Status Help

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	1	Disabled	Loop	2021-09-22T15:31:06+00:00
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Up	-	-
8	Shutdown	Enabled	0	Up	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-
13	Shutdown	Enabled	0	Down	-	-
14	Shutdown	Enabled	0	Down	-	-
15	Shutdown	Enabled	0	Down	-	-
16	Shutdown	Enabled	0	Down	-	-
17	Shutdown	Enabled	0	Down	-	-
18	Shutdown	Enabled	0	Down	-	-
19	Shutdown	Enabled	0	Down	-	-
20	Shutdown	Enabled	0	Down	-	-

Auto-refresh Refresh

The displayed table contains information about the loop protection status in each port:

Port	The switch port number.
Action	The currently configured port action.
Transmit	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current loop protection status of the switch.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of last loop event detected.

3.5 DHCP Server/Relay

To reduce the effort required to set up IP addresses, the Weidmüller switch comes equipped with DHCP server.

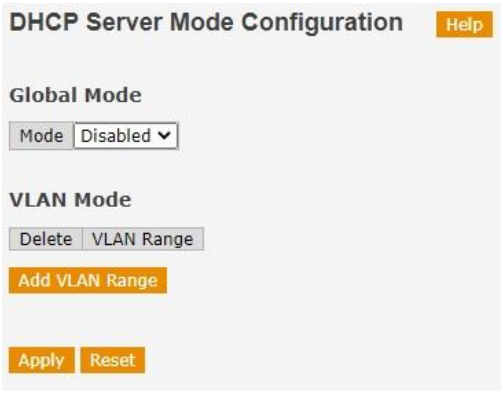
When enabled, the Weidmüller switch can assign specific IP addresses automatically to connected devices that are equipped with *DHCP Client*. In effect, the Weidmüller switch acts as a DHCP server by assigning a connected device with a specific IP address stored in its internal memory. Each time the connected device is switched on or rebooted, the Weidmüller switch sends the device the desired IP address.

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

3.5.1 DHCP Server

3.5.1.1 DHCP Server Mode Configuration

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.



Global Mode

Setting	Description	Factory Default
Enabled / Disabled	Enable / Disable DHCP server per system.	Disabled

VLAN Mode

Setting	Description	Factory Default
VLAN range	Indicate the VLAN range in which DHCP server is enabled or disabled.	None

3.5.1.2 DHCP Server Pool Configuration

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

Name

Setting	Description	Factory Default
Max 32 characters	Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.	None

Type

Setting	Description	Factory Default
Network / Host	Display the type of pool. Network: The pool defines a pool of IP addresses to service more than one DHCP client. Host: The pool services for a specific DHCP client identified by client identifier or hardware address. If '-' is displayed, it means not defined.	'-'

IP

Setting	Description	Factory Default
IP network address	Display the network number of the DHCP address pool. If "-" is displayed, it means not defined.	'-'

Subnet Mask

Setting	Description	Factory Default
Subnet mask	Display the subnet mask of the DHCP address pool. If "-" is displayed, it means not defined.	'-'

Lease Time

Setting	Description	Factory Default
Time in days / hours / minutes	Display the lease time of the pool.	1 day

3.5.1.3 DHCP Server Excluded IP Configuration

This page configures excluded IP addresses. DHCP server will never allocate these IP addresses to DHCP clients.

IP Range

Setting	Description	Factory Default
Range of IP addresses	Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just enter it in any of the fields (or in both).	None

3.5.1.4 DHCP Server Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

There are several tables on the page showing the following information:

Database Counters

Pool	Number of pools.
Excluded IP Address	Number of excluded IP address ranges.
Declined IP Address	Number of declined IP addresses.

Binding Counters

Automatic Binding	Number of bindings with network-type pools.c
Manual Binding	Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.
Expired Binding	Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

DISCOVER	Number of DHCP DISCOVER messages received.
REQUEST	Number of DHCP REQUEST messages received.
DECLINE	Number of DHCP DECLINE messages received.
RELEASE	Number of DHCP RELEASE messages received.
INFORM	Number of DHCP INFORM messages received.

DHCP Message Sent Counters

OFFER	Number of DHCP OFFER messages sent.
ACK	Number of DHCP ACK messages sent.
NAK	Number of DHCP NAK messages sent.

3.5.1.5 DHCP Server Binding IP

This page displays bindings generated for DHCP clients.

The displayed table shows the following information:

IP	IP address allocated to DHCP client.
Type	Type of binding. Possible types are Automatic, Manual, Expired.
State	State of binding. Possible states are Committed, Allocated, Expired.
Pool Name	The pool that generates the binding.
Server ID	Server IP address to service the binding.

In the page can also be found several buttons with the following functions:

Refresh	Click to refresh the page immediately. The Auto-refresh check refreshes the page automatically.
Clear Selected	Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to Expired. If the selected binding is Expired, then it is freed.
Clear Automatic	Click to clear all Automatic bindings and change them to Expired bindings.
Clear Manual	Click to clear all Manual bindings and change them to Expired bindings.
Clear Expired	Click to clear all Expired bindings and free them.

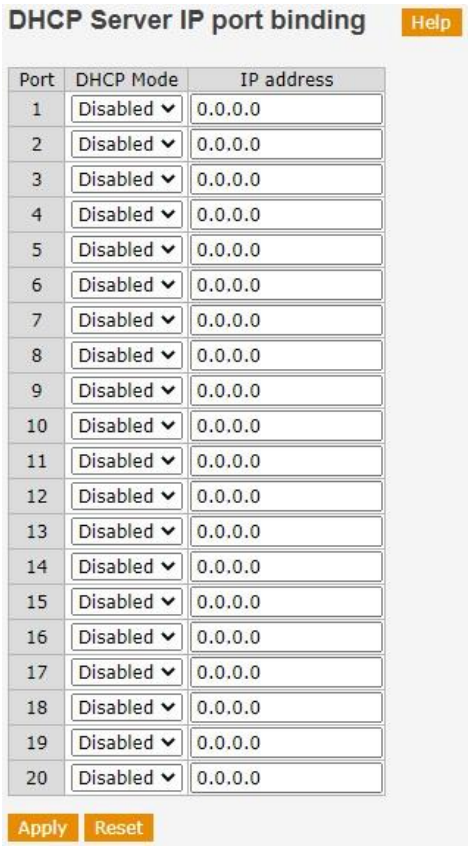
3.5.1.6 DHCP Server Declined IP

This page displays the IP addresses declined by DHCP clients.

The table shows a list of all IP addresses declined.

3.5.1.7 DHCP Server IP Port Binding

If is required to assign a fixed IP address to a client, this page allows to statically bind each port of the switch to an IP address in a DHCP address pool.



DHCP Mode

Setting	Description	Factory Default
Enabled / Disabled	Enable or Disable DHCP server in the port. It is also necessary to Enable DHCP server mode in Mode Configuration page.	Disabled

IP address

Setting	Description	Factory Default
IP address	The binding IP address on port. A DHCP client will always get the binding IP address of source port. Keep “0.0.0.0” to disable binding.	0.0.0.0

3.5.2 DHCP Relay Agent (Option 82)

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

DHCP Option 82 is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding

client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

When Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains 2 sub-options: Circuit ID and Remote ID, which define the relationship between end device IP and the DHCP Option 82 server. The **Circuit ID** is a 4-byte number generated by the Ethernet switch whilst the **Remote ID** is to identify the relay agent itself and it can be one of the following:

- The IP address of the relay agent.
- The MAC address of the relay agent.
- A combination of IP address and MAC address of the relay agent.
- A user-defined string.

3.5.2.1 DHCP Relay Configuration

This page configures DHCP Relay operation mode.

Relay Mode

Setting	Description	Factory Default
Enabled / Disabled	Indicates the DHCP relay mode operation. Enabled: Activates DHCP relay. When DHCP relay is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain to prevent the DHCP broadcast message from flooding for security considerations. Disabled: Disables DHCP relay.	Disabled

Relay Server

Setting	Description	Factory Default
IP address	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain.	0.0.0.0

Relay Information Mode

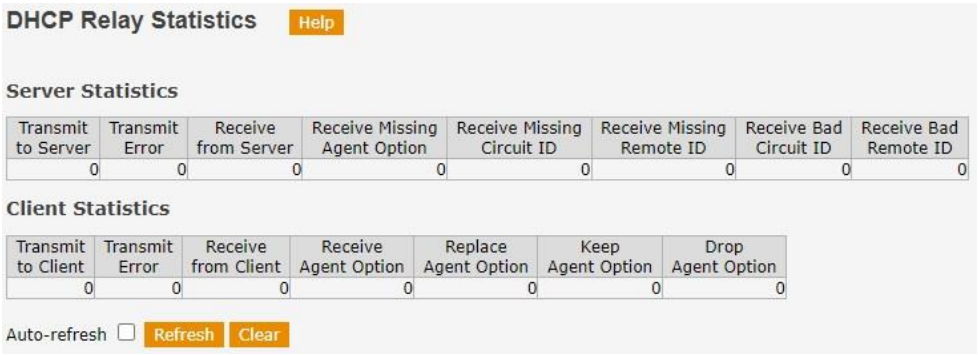
Setting	Description	Factory Default
Enabled / Disabled	Indicates the DHCP relay information mode option operation. Enabled: When DHCP relay information is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to a DHCP server and removes it from a DHCP message when transferring to a DHCP client. It only works when DHCP relay mode is enabled. Disabled: Disables DHCP relay information mode operation.	Disabled

Relay Information Policy

Setting	Description	Factory Default
Replace / Keep / Drop	Indicates the DHCP relay information option policy. When DHCP relay information mode is enabled, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. The “Replace” policy is invalid when relay information mode is disabled. Replace: Replace the original relay information when a DHCP message containing the information is received. Keep: Keep the original relay information when a DHCP message containing the information is received. Drop: Drop the package when a DHCP message containing the information is received.	Keep

3.5.2.2 DHCP Relay Statistics

This page provides statistics for DHCP Relay.



In the page can be displayed two tables showing Server and Client statistics.

Server Statistics

Transmit to Server	The number of packets relayed from the client to the server.
Transmit Error	The number of packets that resulted in errors while being sent to clients.
Receive from Server	The number of packets received from the server.
Receive Missing Agent Option	The number of packets received without agent information option.
Receive Missing Circuit ID	The number of packets received with the Circuit ID option missing.
Receive Missing Remote ID	The number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	The number of packets whose Circuit ID do not match the known circuit ID.
Receive Bad Remote ID	The number of packets whose Remote ID do not match the known Remote ID.

Client Statistics

Transmit to Client	The number of packets relayed from the server to the client.
Transmit Error	The number of packets that resulted in errors while being sent to server.
Receive from Client	The number of packets received from the client.
Receive Agent Option	The number of packets received containing agent information option.
Replace Agent Option	The number of packets replaced when received messages containing relay agent information.
Keep Agent Option	The number of packets whose relay agent information was retained.
Drop Agent Option	The number of packets dropped when received messages containing relay agent information.

3.5.3 DHCP Snooping

DHCP snooping inspects all incoming messages on the port of the switch. If an incoming message is not related to DHCP, the DHCP snooping lets it in. If an incoming message is related to DHCP, the DHCP snooping uses its logic. Based on its configuration, DHCP snooping either lets the message in or discards the message.

3.5.3.1 DHCP Snooping Configuration

Configure DHCP Snooping on this page.

Snooping Mode

Setting	Description	Factory Default
Enabled / Disabled	Indicates the DHCP snooping mode operation. Enabled: Activates DHCP snooping. When DHCP snooping is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. Disabled: Disables DHCP snooping mode operation.	Disabled

Port Mode Configuration

Setting	Description	Factory Default
Trusted / Untrusted	Indicates the DHCP snooping port mode. Trusted: Configures the port as trusted source of the DHCP messages. Untrusted: Configures the port as untrusted source of the DHCP messages.	Trusted

3.5.3.2 DHCP Snooping Table

This page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients that obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

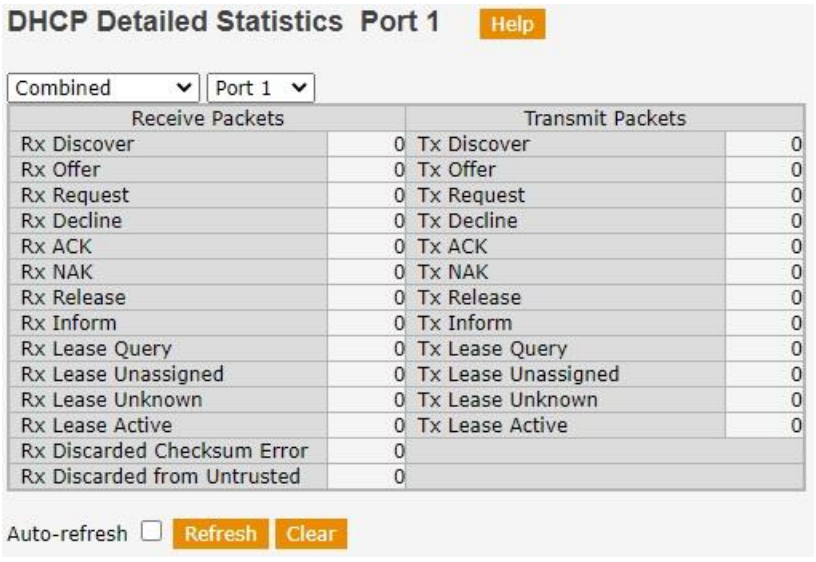
The page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The "MAC address" and "VLAN" input fields allow the user to select the starting point in the Dynamic DHCP snooping Table.

MAC Address	User MAC address of the entry.
VLAN ID	VLAN-ID in which the DHCP traffic is permitted.
Source Port	Switch port number for which the entries are displayed.
IP Address	User IP address of the entry.
IP Subnet Mask	User IP subnet mask of the entry.
DHCP Server	DHCP server address of the entry.

3.5.3.3 DHCP Snooping Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics is not increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.



The displayed table shows the following information for each port of the switch:

Rx and Tx Discover	The number of discover packets received and transmitted.
Rx and Tx Offer	The number of offer packets received and transmitted.
Rx and Tx Request	The number of request packets received and transmitted.
Rx and Tx Decline	The number of decline packets received and transmitted.
Rx and Tx ACK	The number of ACK packets received and transmitted.
Rx and Tx NAK	The number of NAK packets received and transmitted.
Rx and Tx Release	The number of release packets received and transmitted.
Rx and Tx Inform	The number of inform packets received and transmitted.
Rx and Tx Lease Query	The number of lease query packets received and transmitted.
Rx and Tx Lease Unassigned	The number of lease unassigned packets received and transmitted.
Rx and Tx Lease Unknown	The number of lease unknown packets received and transmitted.
Rx and Tx Lease Active	The number of lease active packets received and transmitted.
Rx Discarded Checksum Error	The number of discard packets that IP/UDP checksum is error.
Rx Discarded from Untrusted	The number of discard packets that are coming from untrusted ports.

3.6 Redundancy

3.6.1 Introduction to Communication Redundancy

Setting up Communication Redundancy on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum.

Communication Redundancy allows you to set up *redundant loops* in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This is a particularly important feature for T&D applications, since it could take several minutes to locate the disconnected or severed cable. For example, if the Weidmüller switch is used as a key communications component in the Protection & Control system of a Substation, several minutes of downtime are totally unacceptable. The Weidmüller switch supports following different protocols for communication redundancy:

- O-Ring
- MRP (Media Redundancy Protocol)
- O-Chain
- RSTP (Rapid Spanning Tree), MSTP (Multiple Spanning Tree) and STP (Spanning Tree Protocols) according to IEEE 802.1W/802.1S/802.1D-2004
- Fast Recovery

When configuring a redundant ring, all switches on the same ring must be configured to use the same redundancy protocol. You cannot mix the O-Ring, MRP or STP/RSTP/MSTP protocols on the same ring. The following table lists the key differences between the features of each protocol. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network.

	O-Ring	MRP	O-Chain	STP	RSTP/MSTP
Topology	Ring	Ring	Chain	Ring, Mesh	Ring, Mesh
Recovery Time	~ 10 ms	~ 200 ms	~ 40 ms	Up to 30 sec.	Up to 2 sec

By factory default, no redundancy protocol is activated.

Any network redundancy protocol should be configured well-done for all member switches of the redundant network before actually connecting any backup/redundant path in order to prevent the inadvertent generation of traffic loops.

At the same time only one redundancy protocol may be enabled via the web interface.

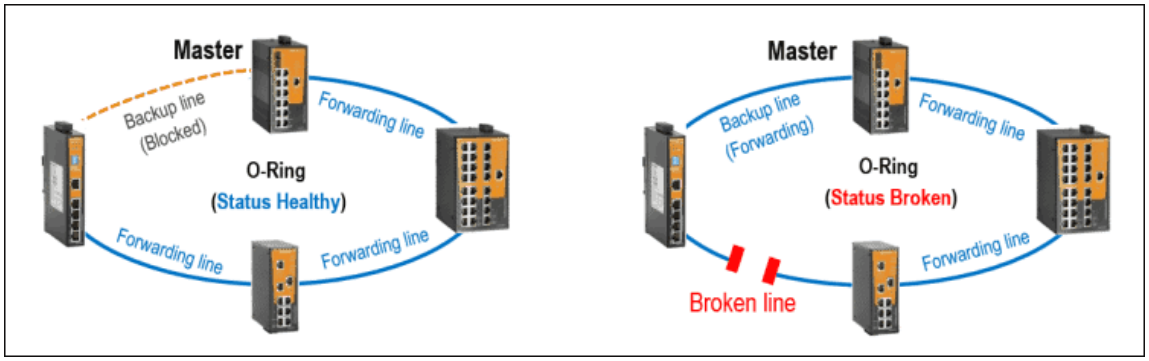
3.6.2 The O-Ring Concept

With the proprietary O-Ring protocol you can optimize communication redundancy and achieve a faster recovery time on the network.

In the O-Ring protocol one switch has to be the ***master*** of the network, and then automatically will block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically re-adjusts the ring so that the part of the network that was disconnected can re-establish the contact with the rest of the network.

3.6.2.1 Topology Setup for "O-Ring"

O-Ring protocol is a very fast network redundancy protocol that provides link fail-over protection with very fast self-healing recovery.



For failure detection the O-Ring protocol uses simultaneously two methods:

1. **Physical link change detection** (Ethernet link loss, e.g. caused by broken cable)
   This detection method is always active and triggers link losses of Fast Ethernet connections (Copper and Fiber) and Fiber Gigabit Ethernet connections. The typical link loss recognition for these connection types is about 2 – 5 ms resulting in an overall self-healing time of the ring structure of about 10 ms.

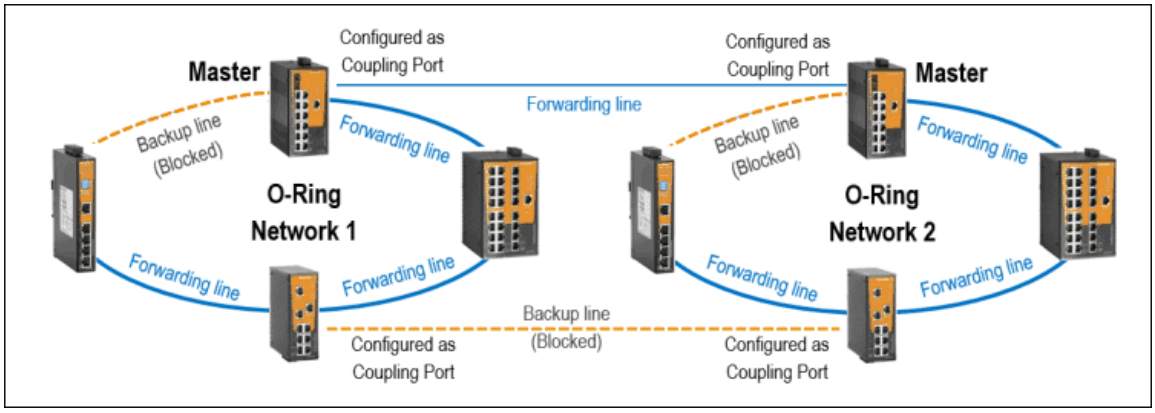
For copper-based Gigabit Ethernet connections the link loss detection is not used as trigger for ring topology change due to the physical design, as a link loss recognition takes a time of several hundred millisecond. Instead, for copper-based Gigabit Ethernet connections control packets are sent cyclic to achieve the fast recovery time of 30ms (Method 2).

2. **Cyclic sending of control packets by the Master** over all ring members and loop back detection via Master's blocked port.
   The ring is based on parameters "Hello Time" and "Max Age Count" (explained in section below *Configuring O-Ring*).
   Using control packets as additional method for ring check (besides link loss detection) can be very useful in cases of bad Ethernet signal quality. This can be caused by poor-quality cables and connectors, or EMC based impact leading to a lot of malformed Ethernet packets resulting in a significant decrease of the network payload. Such a situation can be detected via counting corruptive control packets forcing a ring topology change through there is no link loss (but packet losses).
   If triggered, the overall recovery time is ("Hello Time" * "Max Age Account") + (Topology change process time of about 10 ms). For factory default settings with "Hello Time" = 10 ms and "Max Age Account" = 2 the ring recovery time will be around 30 ms. For this setting, 100 control packets will be sent per second which burdens the ring network with an acceptable bandwidth of 51200 bps.
   For poor quality networks where packet loss easily can occur, smaller values of "Hello Time" and "Max Age Count" would trigger topology changes very often, which will cause a lot of short time network loops. It is recommended to increase these two parameters appropriately to adapt to the conditions of the network environment.

As both methods are running concurrently, a ring topology change will be initiated based on the error condition which will be triggered first.

3.6.2.2 Ring Coupling Configuration

In some applications it may not be convenient to connect all devices in the system to form one large redundant ring, though some devices are located in a remote area. For these systems, "**Ring Coupling"** can be used to separate the devices into two smaller redundant rings, but in such a way that they can still communicate with each other.



Ring Coupling provides a redundant connection between **two** O-Ring networks.

For coupling of two O-Ring networks at both sides the coupling ports must be selected and enabled. Any two switches within an O-Ring network can be selected being a ring coupling switch. The configured coupling switches automatically determine which of the both coupling connections will be the forwarding and the backup one.

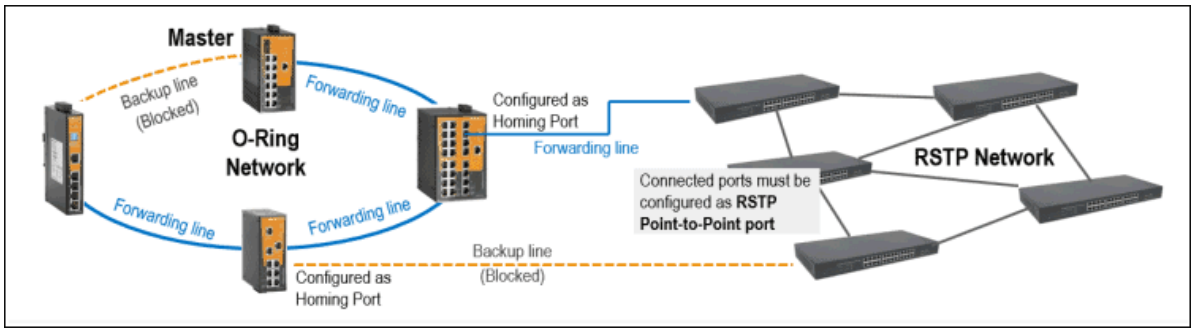
For failure detection of the coupling connection the same checking mechanisms are used as applied for the O-Ring protocol (Refer to section *"Topology setup for O-Ring"* above). Based on the used

methods (Physical link change detection and/or Cyclic sending of control packets every 10ms) the coupling backup line will be activated (including a topology change) after around 30 ms.

NOTE: Only for two switches of an O-Ring network **one** coupling port may be enabled.

3.6.2.3 Dual Homing Configuration

Dual Homing provides a redundant connection between an O-Ring network and an RSTP network.

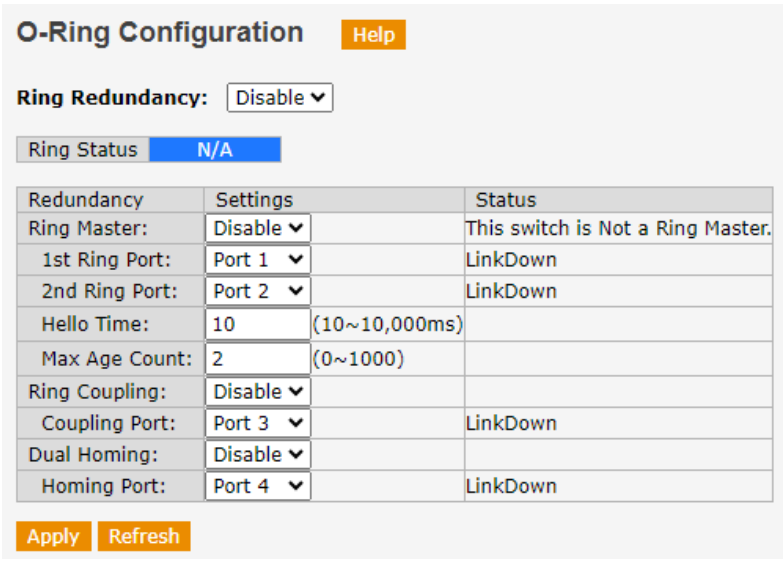


For a Dual Homing connection on any two switches inside of the O-Ring network a Homing port needs to be selected and enabled. Each configured Homing port must be connected to a RSTP enabled port on any switch of the RSTP network. Configure RSTP port being of type Point-to-Point (for switch interconnections). Do not configure as RSTP Edge Port (used for host connections). Dual Homing ports bypass BPDU packets sent from RSTP network switches resulting in normal state in a forwarding and blocked (discarding) line. In case of a ring failure or if the forwarding line will be interrupted, bypassing of BPDU packets will be stopped triggering a network topology change of the RSTP network and both Dual Homing connections will become forwarding lines.

NOTE: Only for two switches of an O-Ring network the Homing port may be enabled. Ensure that the connected network is RSTP enabled.

3.6.2.4 Configuring “O-Ring”

Use the **O-Ring** page of the Redundancy menu.



1. Select **Enable** in field **Ring Redundancy.**

2. If only a redundancy with 1 ring shall be created then do following:

- Enable '*Ring Master'* if the switch shall be assigned as ring master.
  For O-Ring configuration **one switch** needs to be configured as Ring Master. However, if two or more switches are set as Ring Master, the switch with the lowest MAC address will be the actual Ring Master and the others will be Backup Masters.
  If O-Ring redundancy on involved switches will be configured and applied but without setting any switch as Ring Master, then a loop will arise causing heavy data traffic when closing the ring cabling. This happens because there is no instance which controls and blocks the backup line. In this case all ring switches show a broken ring status.
- Select the *'Redundant ports'* which shall be used
- Configure the '*Hello Time'* and '*Max Age Count'* parameters (explained below)

3. If the switch is used to connect 2 O-Rings (Ring Coupling) then additionally do following:

- Enable '*Ring Coupling"*
- Select the *'Coupling port'* which shall be used to connect the two rings

4. If the switch is used to connect one O-Ring and a switch of a different redundant network using RSTP (Dual Homing) then additionally do following:

- Enable '*Dual Homing"*
- Select the *'Homing port'* which shall be used to connect the O-Ring with the RSTP switch

The **Ring Status** field indicates the operation of the ring. It shows **N/A** if Ring Redundancy is Disabled, shows **Healthy** if the ring is operating normally, and shows **Broken** if the any of the two links of the ring is not connected.

Explanation of *'Setting'* and *'Status'* items

Ring Master

Setting	**Description**	**Factory Default**
Enable	Select this Switch as Master.	Disable
Disable	Do not select this Switch as Master.	
Status	**Description**	**Factory Default**
This switch is a Ring Master	Switch programmed as Master.	This switch is Not a Ring Master
This switch is Not a Ring Master	Switch not programmed as Master or O-Ring redundancy disabled.	

Redundant Ports

Setting	**Description**	**Factory Default**
1st Ring Port	Select any port of the Switch to be one of the redundant ports.	Port 01
2nd Ring Port	Select any port of the Switch to be one of the redundant ports.	Port 02
Status	**Description**	**Factory Default**
Inactive	O-Ring disabled and this port is connected.	LinkDown
LinkDown	No connection in this port.	
Forwarding	Normal transmission in this port.	
Discarding	The port is connected to a backup path and the path is blocked.	

Hello Time

Setting	Description	Factory Default
10 to 10,000ms	Cyclic time of control packets sent by Master in the failure detection method 2 of the switch.	10ms

Max Age Count

Setting	Description	Factory Default
0 to 1000	Number of lost control packets for initiating a ring topology change.	2

Ring Coupling

Setting	Description	Factory Default
Enable	Enables the Ring Coupling operation in the Switch.	Disable
Disable	Does not enable the Ring Coupling operation in the Switch.	

Coupling Port

Setting	Description	Factory Default
Coupling Port	Select any port of the Switch to be the coupling port.	Port 03
Status	**Description**	**Factory Default**
Inactive	Coupling Port disabled and this port is connected.	LinkDown
Link down	No connection in this port.	
Forwarding	Normal transmission in this port.	
Discarding	The port is connected to a backup path and the path is blocked.	

Enable Dual Homing

Setting	Description	Factory Default
Enable	Enables the Dual Homing operation in the Switch.	Enable
Disable	Does not enable the Dual Homing operation in the Switch.	

Homing Port

Setting	Description	Factory Default
Homing Port	Select any port of the Switch to be the homing port.	Port 04
Status	**Description**	**Factory Default**
Inactive	Dual Homing disabled and this port is connected.	LinkDown
Link down	No connection in this port.	
Forwarding	Normal transmission in this port.	
Discarding	The port is connected to a backup path and the path is blocked.	

3.6.3 Media Redundancy Protocol (MRP)

MRP (IEC standard 62439-2) provides fast communication recovery in ring-based network topologies and is supported by several Industrial Ethernet switches of the market. Therefore, it is a good alternative to build rings of different branded switches. An MRP ring can support up to 50 devices and will enable a back-up link in 200 ms.

MRP in Weidmüller Ethernet Switches

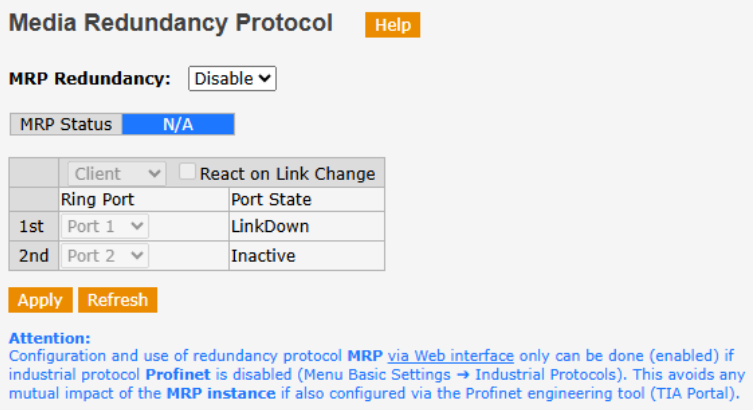
There is a dependency between the web-interface configurable instance and the PROFINET-based MRP instance which will be configured via a PROFINET engineering tool (like TIA portal).

For this reason, the web-interface based MRP redundancy can only be used if industrial protocol PROFINET is Disabled in the option Industrial Protocols of Basic Settings menu.

If one of the other redundancy protocols (O-Ring, O-Chain, MSTP/RSTP or Fast Recovery) will be used additionally to a running PROFINET MRP instance, the selected PROFINET MRP ports cannot be used in the other redundancy protocol configured via web-interface. For checking or reconfiguring the current PROFINET MRP settings of the switch, a PROFINET engineering tool like TIA Portal has to be used.

Configuring MRP via Web-Interface

Use the **MRP** page of the Redundancy menu.



MRP Redundancy

Setting	Description	Factory Default
Enable	Enables the web-interface controller MRP instance.	Disable
Disable	Disables the web-interface controller MRP instance.	

Role Manager / Client

Setting	Description	Factory Default
Manager	Only ONE device acting as Manager is required in any MRP topology. If two or more switches are set to be “Manager”, the MRP topology will fail.	Client
Client	Rest of devices of any MRP topology must be configured as Client.	

React on Link Change

Setting	Description	Factory Default
Enable	Enabling this function will cause MRP topology to converge more rapidly in case of a ring break. This option is only available on a switch with Manager role. This feature specifies whether the Manager reacts immediately or not on a 'MRP Link Change' frame received from any client which has detected any change (link down/up) at its ring ports. If activated, the Master directly accepts a broken status when receiving a 'MRP Link Change' frame. The backup port will be opened and a 'MRP Topology Change' frame immediately will be sent out on both ports towards all of the MRP clients in the ring. If deactivated, the Master - when receiving any 'MRP Link Change' frame - additionally checks the ring interruption by sending some MRP control packets to verify the ring fracture. If the reception of these frames also fail then the Master opens the backup port and sends out a 'MRP Topology Change' frame on both ports to inform all clients to update their MAC address tables.	Disable
Disable		

Ring Ports

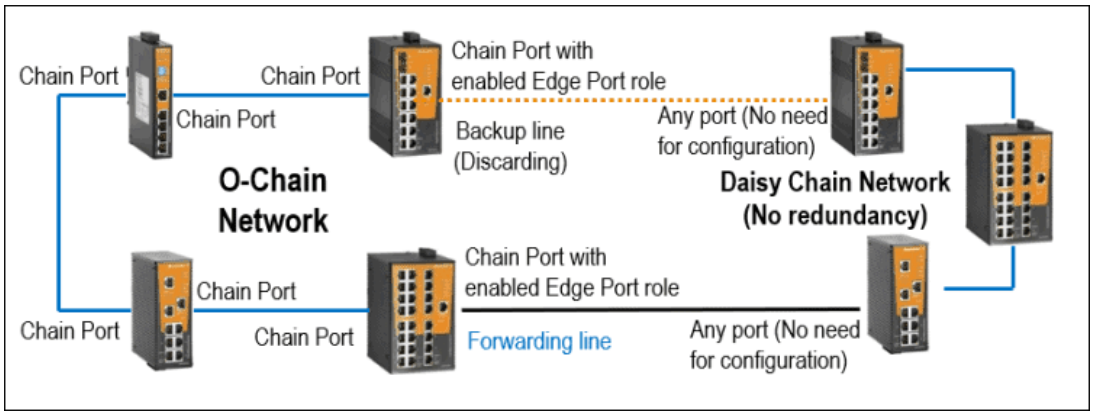
Setting	Description	Factory Default
1st MRP Port	Select any port of the Switch to be one of the redundant ports.	Port 01
2nd MRP Port	Select any port of the Switch to be one of the redundant ports.	Port 02
Status	**Description**	**Factory Default**
Link down	No connection in this port.	LinkDown
Forwarding	Normal transmission in this port.	
Discarding	The port is connected to a backup path and the path is blocked.	

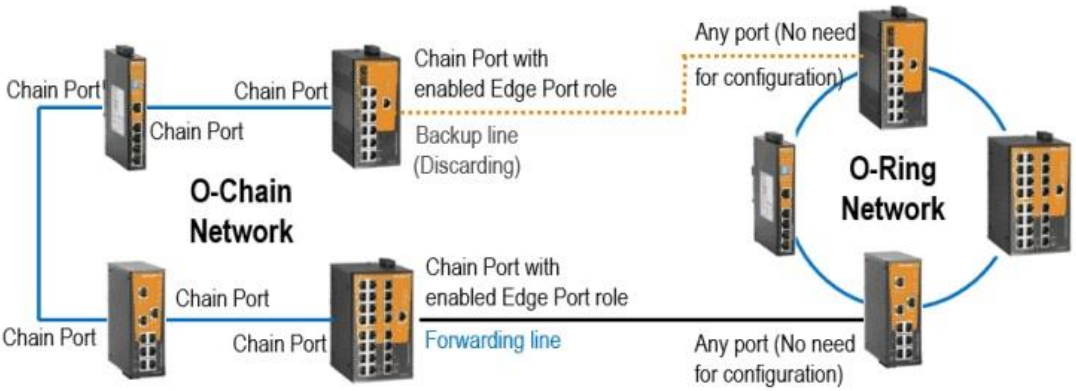
3.6.4 The O-Chain Concept

O-Chain is an advanced software-technology that offers a highly flexible method for providing a redundant network extension to any kind of existing switch network.

By using O-Chain technology the additional switches forming a chain will be connected redundantly to a single switch, to daisy chained switches or to other redundant network topologies. A redundant O-Chain simply will be configured by enabling chain redundancy on each switch, selecting the switch interconnection ports as chain port and enable the edge port role for the ports of the two switches which shall be connected to the existing network. For failure detection (broken chain) the O-Chain protocol uses a similar method as used for O-Ring technology resulting in a healing time of the chain of around 30 milliseconds. In terms of the entire network infrastructure the overall healing time (performing a network topology update after the chain has been broken) depends on the network to which the O-Chain is connected.

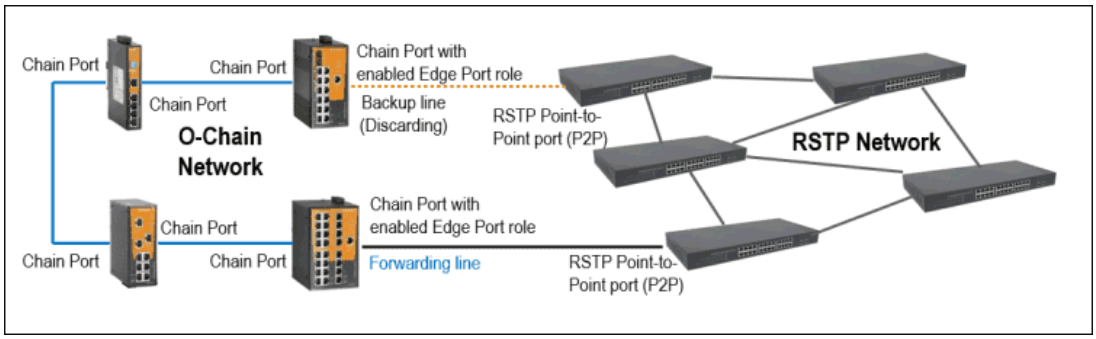
Recovery time for O-Chain connected to Daisy Chain of Weidmüller's Substation/Advanced Line switches OR to an O-Ring network of Substation/Advanced Line switches





For both above illustrated scenarios the overall network healing time can be calculated roughly to around 40 ms based on a proprietary method to force a MAC address table update for all connected Weidmüller switches.

Recovery time for O-Chain connected to an RSTP network



For a connection to an RSTP network the overall time for topology update after the chain is broken can be estimated as the calculated healing time of the used RSTP redundancy settings plus around 30 milliseconds for chain topology update.

Generally, RSTP network ports connected to O-Chain Edge ports shall be configured as Point-to-Point (P2P) RSTP port. This type is used to connect to other switches. Do not configure those ports as RSTP Edge port because it is designed for host connection and do not allow passing any BPDU control packet.

Interaction of O-Chain and RSTP network in terms of overall network topology update:

- If the chain is healthy the O-Chain Edge port of the switch with lowest MAC address always becomes the blocking (discarding) state and the other Edge port will be the forwarding one.
- BPDU control packets which will be sent cyclic from RSTP network to the O-Chain Edge ports will be blocked by both Edge ports as long as the chain is healthy. As result the RSTP network does not recognize any loop and sets for both RSTP ports the forwarding state.
- When learning new MAC addresses for unknown traffic sent via both RSTP ports, only the one connected to forwarding O-Chain Edge port will learn the path to devices connected to the O-Chain. The other RSTP port, though also having forwarding status, never will participate in any traffic due to the blocked O-Chain Edge port. This ensures a unique traffic flow via the forwarding O-Chain Edge port.
- In case of a broken chain (means any interruption in the chain behind the O-Chain Edge switches) both O-Chain Edge ports go to state forwarding and send additionally a TCN BPDU packet (Topology Change Notification) to their connected RSTP ports. This will trigger a fast network topology change of the RSTP network resulting in fast renewed accessibility of devices at both parts of the broken chain. In this case, both RSTP ports stay in state forwarding. Only for an interrupted connection between O-Chain Edge port and RSTP port the state on both sides will change to link down.

Recovery time for O-Chain connected to any non-redundant Daisy Chain network or to a proprietary 3rd party network

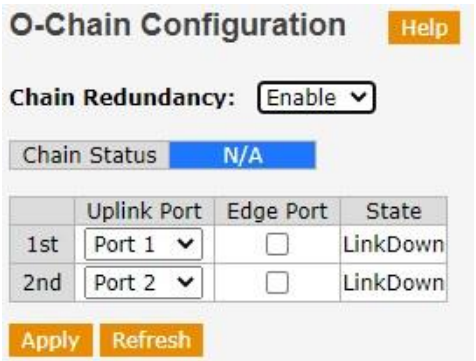
For connections to unmanaged switches, to a non-redundant daisy chain network or to a redundant proprietary 3rd party network the overall network topology recreation time depends worst case on the remaining MAC address aging time of the 3rd party switches (when the chain becomes broken). For those devices there is no mechanism to inform them about a broken chain and to flush their MAC address tables immediately. Only the O-Chain switches flush their MAC address tables after around 30 ms providing all devices connected to O-Chain switches, immediately an update path for Ethernet communication to any target device. However already established communication relations, originally initiated from 3rd party network devices to O-Chain connected devices, do not longer work until the MAC address tables of the 3rd party switches will be renewed after the remaining aging-time has been expired.

Configuring O-Chain

How to configure O-Chain generally:

1. Enable the Chain Redundancy in all the switches of the daisy chain.
2. Determine the switches that shall be used as edge switches.
3. Configure at all the switches of the daisy Chain the ports that will be part of the chain.
4. In the two edge switches, additionally configure the edge port (port which is connected to the counterpart part of the other network).

There is no need to change anything in the configuration of the network on which the O-Chain switches will be attached.



Explanation of *'Setting'* and *'Status'* items

Chain Redundancy

Setting	Description	Factory Default
Enable	Enable the O-Chain operation.	Disable
Disable	Disable the O-Chain operation.	
Status	**Description**	**Factory Default**
N/A	O-Chain redundancy disabled.	N/A
Healthy	The Chain is operating normally.	
Broken	Any of the two links of the Chain is not connected.	

Chain Ports

Setting	Description	Factory Default
1st Chain Port	Select any port of the Switch to be one of the ports of the daisy Chain.	Port 01
2nd Chain Port	Select any port of the Switch to be one of the ports of the daisy Chain.	Port 02
Status	**Description**	**Factory Default**
Link down	No connection in this port.	LinkDown
Forwarding	Normal transmission in this port.	
Discarding	The port is connected to a backup path and the path is blocked.	

Edge Port

Setting	Description	Factory Default
Check	Configure a port of the daisy Chain as edge port.	Not checked
Uncheck	Does not configure a port of the daisy Chain as edge port.	

3.6.5 STP / RSTP / MSTP

3.6.5.1 The STP / RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures on a network, and provide an automatic means of avoiding loops. This is particularly important for networks that have a complicated architecture, since unintended loops in the network can cause broadcast storms. Weidmüller switches' STP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every Weidmüller switch connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE 802.1D-2004. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy.

For example:

- Defaults to sending 802.1D style BPDUs if packets with this format are received.
- STP (802.1D) and RSTP (802.1w) can operate on different ports of the same switch, which is particularly helpful when switch ports connect to older equipment such as legacy switches.

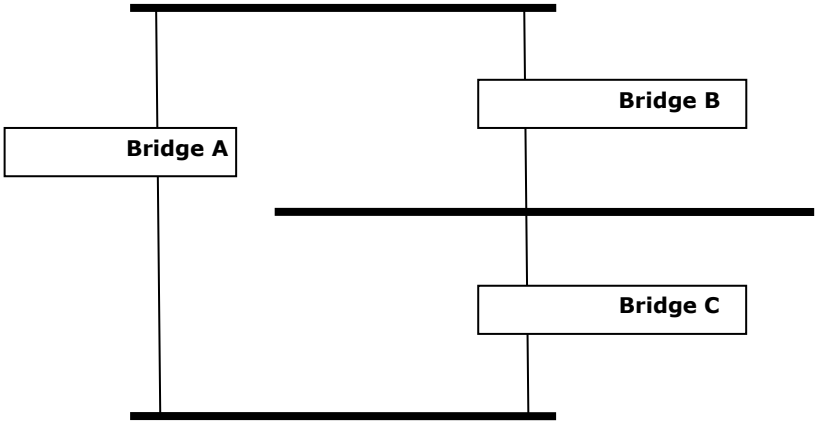
You get essentially the same functionality with RSTP and STP. To see how the two systems differ, see section '*Differences between STP and RSTP*' later in this chapter.

NOTE: The STP protocol is part of the IEEE Std 802.1D, 2004 Edition bridge specification. The following explanation uses “bridge” instead of “switch.”

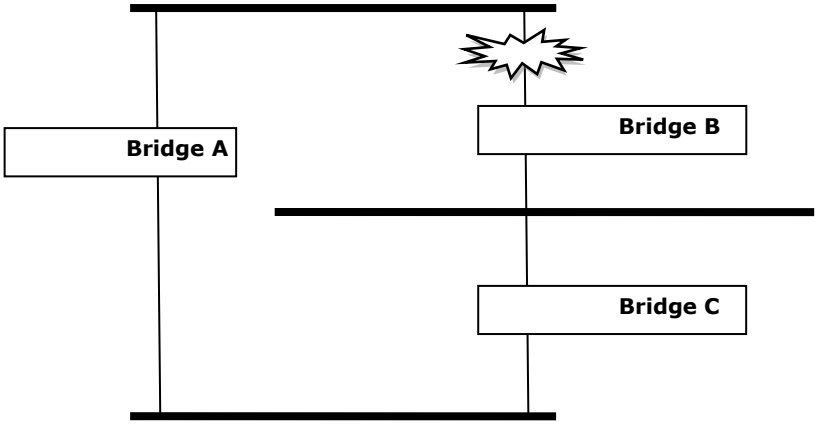
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- Locate and then disable less efficient paths (i.e., paths that have a lower bandwidth).
- Enable one of the less efficient paths if a more efficient path fails.

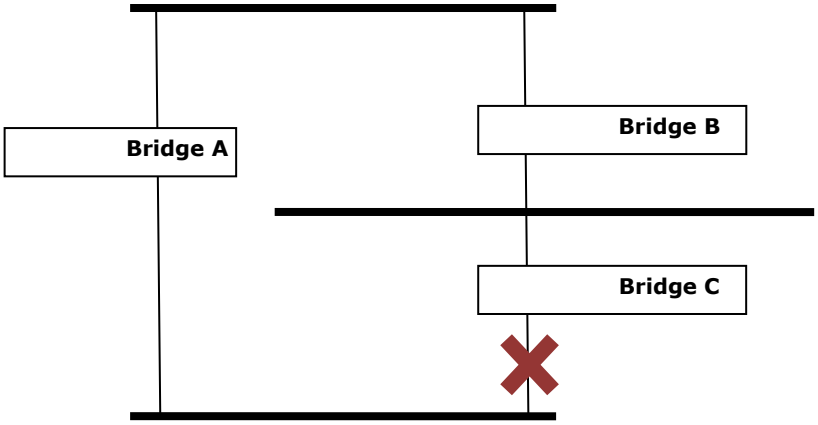
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



If STP is enabled, it will detect duplicate paths and prevent, or *block*, one of the paths from forwarding traffic. In the following example, STP determined that traffic from LAN segment 2 to LAN segment 1 should flow through bridges C and A since this path has a greater bandwidth and is therefore more efficient.



What happens if a link failure is detected? As shown in next figure, the STP process reconfigures the network so that traffic from LAN segment 2 flows through bridge B.



STP will determine which path between each bridged segment is most efficient, and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous 3 figures, STP first determined that the path through bridge C was the most efficient, and as a result, blocked the path through bridge B. After the failure of bridge C, STP re-evaluated the situation and opened the path through Bridge B.

3.6.5.2 How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the sections below.

STP Requirements

Before STP can configure the network, the system must satisfy the following requirements:

- All bridges must be able to communicate with each other. The communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. For example, the default priority setting of Weidmüller switches is 32768.
- Each port has a cost that specifies the efficiency of each link. The efficiency cost is usually determined by the bandwidth of the link, with less efficient links assigned a higher cost. The following table shows the default port costs for a switch:

Port Speed	Path Cost 802.1D, 1998 Edition	Path Cost 802.1w-2001
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1000 Mbps	4	20,000

STP Calculation

The first step of the STP process is to perform calculations. During this stage, each bridge on the network transmits BPDUs. The following items will be calculated:

- Which bridge should be the **Root Bridge**. The Root Bridge is the central reference point from which the network is configured.
- The **Root Path Costs** for each bridge. This is the cost of the paths from each bridge to the Root Bridge.
- The identity of each bridge's **Root Port**. The Root Port is the port on the bridge that connects to the Root Bridge via the most efficient path. In other words, the port connected to the Root Bridge via the path with the lowest Root Path Cost. The Root Bridge, however, does not have a Root Port.
- The identity of the **Designated Bridge** for each LAN segment. The Designated Bridge is the bridge with the lowest Root Path Cost from that segment. If several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge. Traffic transmitted in the direction of the Root Bridge will flow through the Designated Bridge. The port on this bridge that connects to the segment is called the **Designated Bridge Port**.

STP Configuration

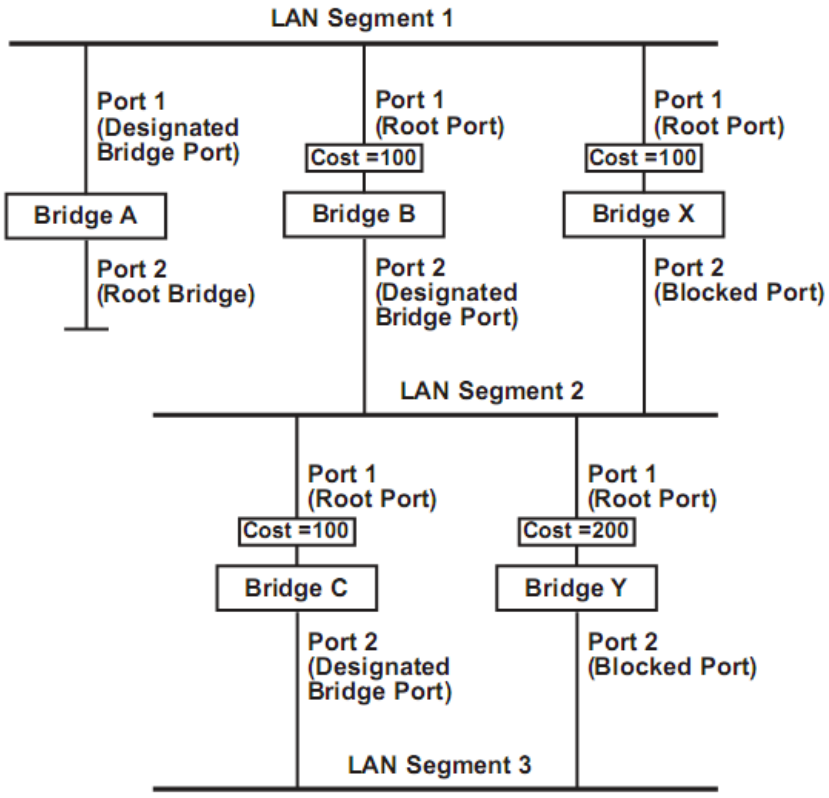
After all of the bridges on the network agree on the identity of the Root Bridge, and all other relevant parameters have been established, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they will not be allowed to receive or forward traffic.

STP Reconfiguration

Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has ceased to function. This will trigger the bridge to reconfigure the network to account for the change. If you have configured an SNMP trap destination, when the topology of your network changes, the first bridge to detect the change will send out an SNMP trap.

STP Example

The LAN shown in the following figure has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.



- Bridge A has been selected as the Root Bridge, since it was determined to have the lowest Bridge Identifier on the network.
- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.
- Ports 1 of Bridges B, C, X, and Y are all Root Ports since they are nearest to the Root Bridge, and therefore have the most efficient path.
- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B was selected as the Designated Bridge for that segment since it has a lower Bridge Identifier. Port 2 on Bridge B is selected as the Designated Bridge Port for LAN Segment 2.
- Bridge C is the Designated Bridge for LAN segment 3, because it has the lowest Root Path Cost for LAN Segment 3:
  - The route through bridges C and B costs 200 (C to B=100, B to A=100)
  - The route through bridges Y and B costs 300 (Y to B=200, B to A=100)
- The Designated Bridge Port for LAN Segment 3 is port 2 on bridge C.

Differences between STP and RSTP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

The MSTP concept

Multiple Spanning Tree Protocol (MSTP) is a standard protocol based on IEEE 802.1S. It defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). The calculations of

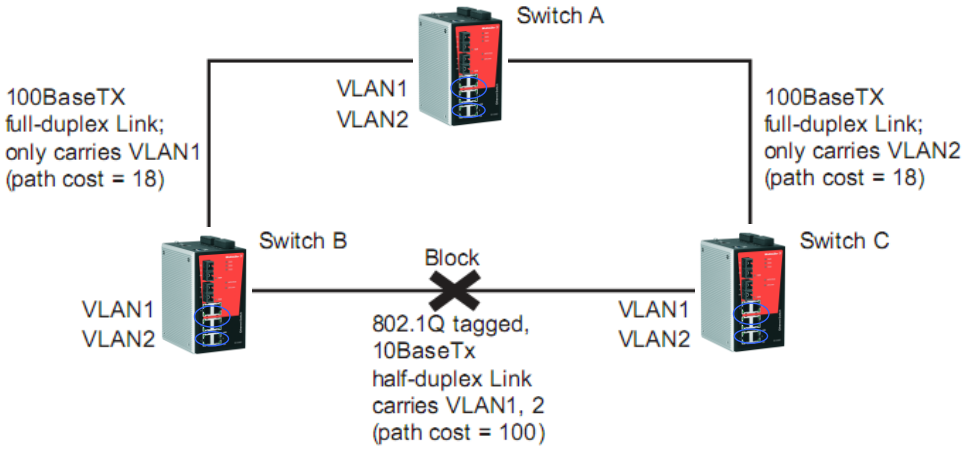
STP/RSTP only depend on the physical connections, whilst MSTP configures separate Spanning Tree instances for different VLAN groups.

The main concepts that are specific of MSTP when comparing with STP/RSTP are:

- **Multiple Spanning Tree Instances (MSTIs)**. An MST instance (MSTI) is a particular set of VLANs that are all using the same spanning tree.
- **Regions**. An MST region is a set of interconnected switches that all have the same values for all following MST configuration elements:
    - MST configuration name
    - Revision level
    - Mapping of which VLANs are mapped to which MST instances

  Each of the MST instances created are identified by an MSTI number that identifies them only inside the MST region. Therefore, an MSTI will never span across MST regions.
- **Common and Internal Spanning Tree (CIST)**. The CIST is the default spanning tree of MSTP, i.e. all VLANs that are not members of particular MSTIs are members of the CIST. Also, the spanning tree that runs between MST regions is the CIST.

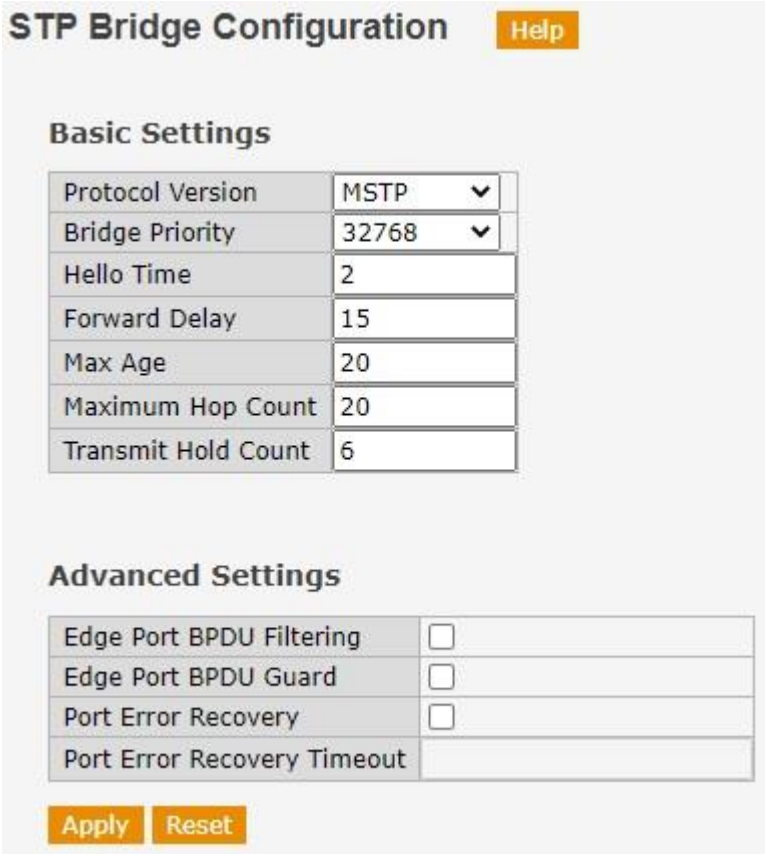
The following figure shows an example of an STP/RSTP network that contains VLANs 1 and 2. The VLANs are connected using the 802.1Q-tagged link between switch B and Switch C. By default, this link has a port cost of 100 and is automatically blocked by STP/RSTP because the other switch-to-switch connections have a port cost of 36 (18+18). This means that both VLANs are now subdivided—VLAN 1 on switches A and B cannot communicate with VLAN 1 on switch C, and VLAN 2 on switches A and C cannot communicate with VLAN 2 on switch B.



The above situation can be rectified by using MSTP. With MSTP, VLAN 1 and VLAN 2 can be mapped to different MSTIs. Hence, each instance can have a topology independent of other spanning tree instances.

3.6.5.3 Configuring STP / RSTP / MSTP – Bridge Settings

The following figure indicates the STP / RSTP / MSTP parameters that can be configured. A more detailed explanation of each parameter follows.



Basic Settings

Protocol version

Setting	Description	Factory Default
STP / RSTP / MSTP	The version of the STP protocol. Valid values are STP, RSTP and MSTP.	MSTP

Bridge Priority

Setting	Description	Factory Default
Scroll list with acceptable values	Controls the bridge priority. Lower numeric values have higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.	32768

Hello time (sec)

Setting	Description	Factory Default
Numerical value input by user (1 to 10)	The root of the Spanning Tree topology periodically sends out a “hello” message to other devices on the network to check if the topology is healthy. The “hello time” is the amount of time the root waits between sending hello messages.	2

Forward Delay (sec)

Setting	Description	Factory Default
Numerical value input by user (4 to 30)	The amount of time this device waits before checking to see if it should change to a different state.	15

Max. Age (sec)

Setting	Description	Factory Default
Numerical value input by user (6 to 40)	If this device is not the root, and it has not received a hello message from the root in an amount of time equal to “Max. Age,” then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20

Maximum Hop Count

Setting	Description	Factory Default
Numerical value input by user (6 to 40)	The maximum number of hops in the MST Region. It defines how many bridges a root bridge can distribute its BPDU information.	20

Transmit Hold Count

Setting	Description	Factory Default
Numerical value input by user (1 to 10)	The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed.	6

Advanced Settings

Edge Port BPDU Filtering

Setting	Description	Factory Default
Check / Uncheck	Control whether a port explicitly configured as Edge will transmit and receive BPDUs..	Unchecked

Edge Port BPDU Guard

Setting	Description	Factory Default
Check / Uncheck	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state and will be removed from the active topology..	Unchecked

Port Error Recovery

Setting	Description	Factory Default
Check / Uncheck	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.	Unchecked

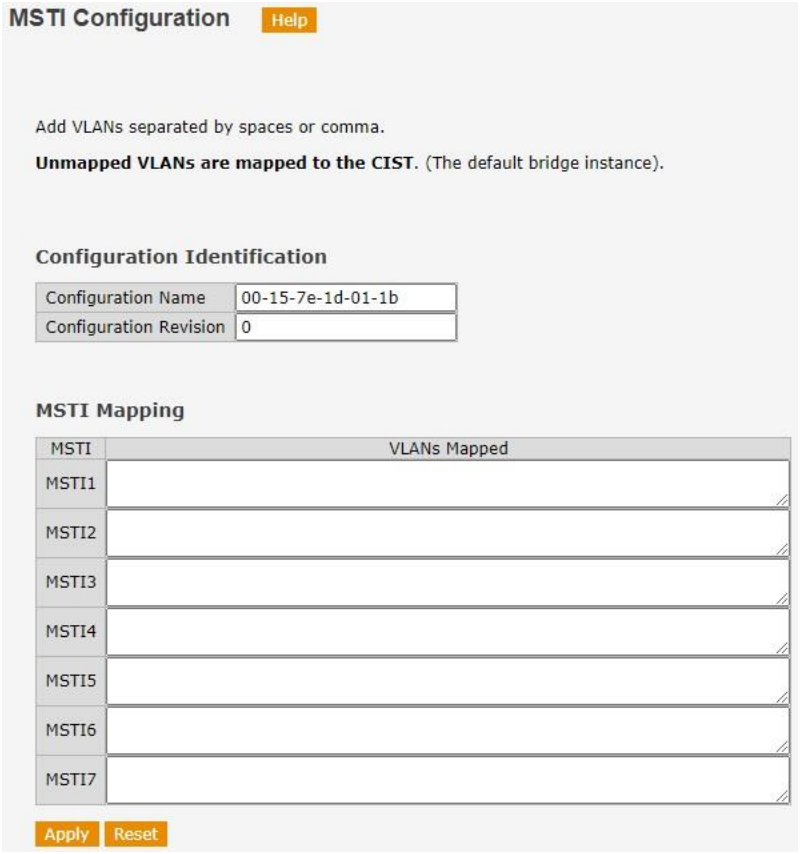
Port Error Recovery Timeout (sec)

Setting	Description	Factory Default
Numerical value input by user (30 to 86400)	This field is only enabled if Port Error Recovery is checked. It sets the time to pass before a port in the error-disabled state can be enabled.	None

3.6.5.4 MSTI Mapping

NOTE: This page only has to be programmed if the redundancy protocol programmed is MSTP. It is not applicable to STP/RSTP.

The page allows the user to inspect and change the current MST Configuration Name, the Revision level and the mapping of VLANs in MSTIs.



Configuration Identification

Configuration Name

Setting	Description	Factory Default
Max. of 32 characters	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configurations in order to share spanning trees for MSTIs (intra-region).	MAC address

Configuration Revision

Setting	Description	Factory Default
Numerical value input by user (0 to 65535)	The revision of the MSTI configuration named above.	0

MSTI Mapping

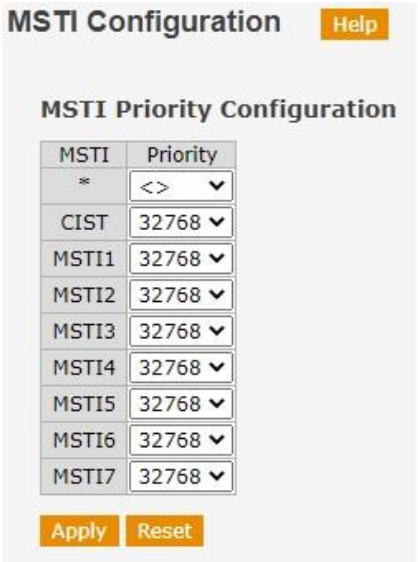
VLANs Mapped

Setting	Description	Factory Default
VLAN number by the user (1 to 4094)	The list of VLANs mapped to the different MSTIs. The VLANs must be separated with commas and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI will be left empty (ex. without any mapped VLANs).	None

3.6.5.5 MSTI Priorities

NOTE: This page only has to be programmed if the redundancy protocol programmed is MSTP. It is not applicable to STP/RSTP.

The page allows the user to inspect and change the current MSTI bridge instance priority configurations.



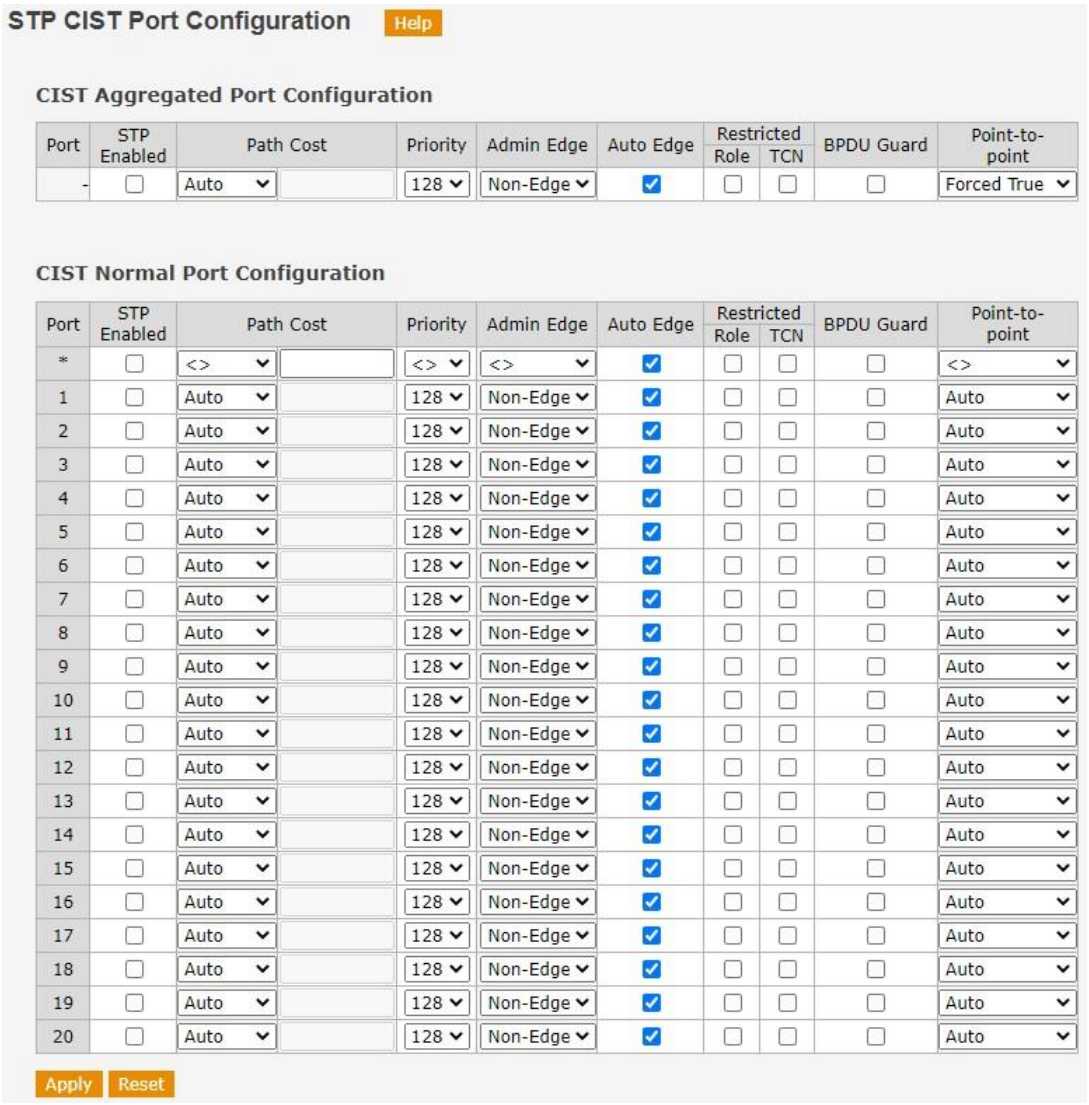
It is possible to program the priority for each MSTI as well as for the CIST.

Priority

Setting	Description	Factory Default
Scroll list with acceptable values	Controls the bridge priority. Lower numeric values have higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.	32768

3.6.5.6 CIST Ports

This page allows the user to inspect and change the current CIST port configurations.



STP CIST Port Configuration Help

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
-	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
*	☐	<>	<>	<>	☑	☐	☐	☐	<>
1	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
2	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
3	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
4	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
6	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
7	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
8	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
9	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
10	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
11	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
12	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
13	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
14	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
15	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
16	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
17	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
18	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
19	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
20	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto

Apply Reset

For each port of the switch, the user can program the following parameters:

STP Enabled

Setting	Description	Factory Default
Checked / Unchecked	Controls whether STP/RSTP is enabled on this switch port.	Unchecked

Path Cost

Setting	Description	Factory Default
Auto / Specific	Configures the path cost incurred by the port. Auto will set the path cost according to the physical link speed by using the 802.1D-recommended values. Specific allows the user to enter a user-defined value (1 to 200000000). The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports.	Auto

Priority

Setting	Description	Factory Default
Scroll list with acceptable values	Configures the priority for ports having identical path cost.	128

Admin Edge

Setting	Description	Factory Default
Edge / Non-Edge	Configures the operEdge flag to start as set or cleared (the initial operEdge state when a port is initialized). The operEdge is a flag indicating whether the port is connected directly to edge devices or not (no bridges attached). Transiting to the forwarding state is faster for edge ports (operEdge set to true) than other ports.	Non-Edge

Auto Edge

Setting	Description	Factory Default
Checked / Unchecked	Check to enable the bridge to detect edges at the bridge port automatically. This allows operEdge to be derived from whether BPDUs are received on the port or not.	Checked

Restricted Role

Setting	Description	Factory Default
Checked / Unchecked	When checked, the port will not be selected as root port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.	Unchecked

Restricted TCN

Setting	Description	Factory Default
Checked / Unchecked	When checked, the port will not propagate received topology change notifications and topology changes to other ports. If set, it can cause temporary loss of connectivity after changes in spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.	Unchecked

BPDU Guard

Setting	Description	Factory Default
Checked / Unchecked	If checked, causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port Edge status does not effect this setting.	Unchecked

Point-to-Point

Setting	Description	Factory Default
Auto	Automatic detection if the link port is point to point or not (connected to a point-to-point LAN or to a shared media).	Auto
Forced True	The port link is point to point and then is a candidate for rapid transition to the forwarding state.	
Forced False	The port link is not point to point.	

3.6.5.7 MSTI Ports

NOTE: This page only has to be programmed if the redundancy protocol programmed is MSTP. It is not applicable to STP/RSTP.

This page allows the user to inspect and change the current MSTI port configuration. An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

By selecting the specific MSTI and pressing the Get button, we can see the page shown below:

Path Cost

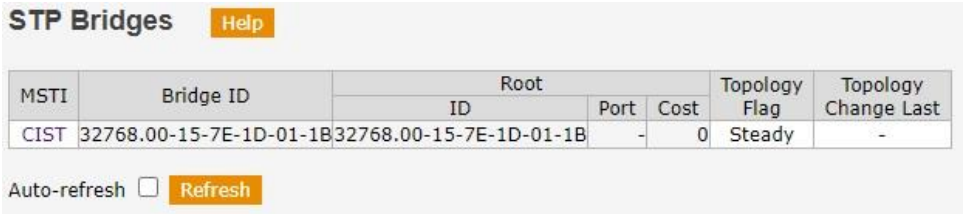
Setting	Description	Factory Default
Auto / Specific	Configures the path cost incurred by the port. Auto will set the path cost according to the physical link speed by using the 802.1D-recommended values. Specific allows the user to enter a user-defined value (1 to 200000000). The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports.	Auto

Priority

Setting	Description	Factory Default
Scroll list with acceptable values	Configures the priority for ports having identical path cost.	128

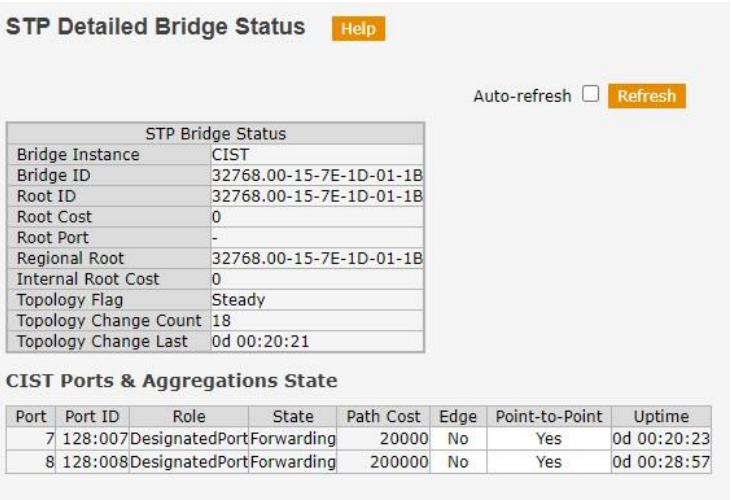
3.6.5.8 Bridge Status

This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the information that can be seen in the screen below:



MSTI	The bridge instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The bridge ID of this bridge instance.
Root ID	The bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root path cost. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.
Topology Flag	The current state of the topology change flag for this bridge instance.
Topology Change Last	The time since last topology change occurred.

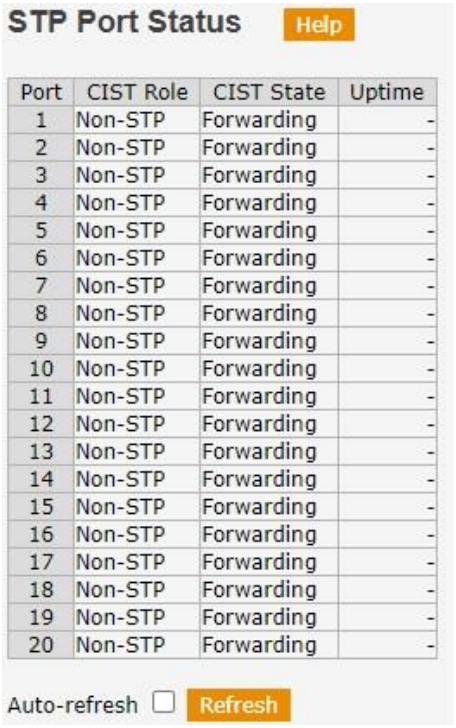
By clicking on the bridge instance of the column MST0I the user can check the detailed bridge status. In the figure below can be seen the screen shown when CIST is pressed.



Port	The port of the switch.
Port ID	The port identifier used by the STP protocol, consisting of the priority and the logical port index of the bridge port.
Role	The role of a port is assigned based on whether it is part of the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port); or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed.
State	Displays the current state of this port in the Spanning Tree.
Path Cost	The path cost of the port contributed to the paths towards the spanning tree root which include this port. It can be a value assigned by the Auto setting or any explicitly configured value.
Edge	The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.
Point-to-Point	Indicates a connection to exactly another bridge. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP states.
Uptime	The time since the bridge port was last initialized.

3.6.5.9 Port Status

This page displays the STP CIST port status for physical ports of the switch.



In the table shown on the page is displayed the following information for each port:

CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort Disabled Non-STP
CIST State	The current STP port state of the CIST port. The port state can be one of the following values: Disabled Learning Forwarding
Uptime	The time since the bridge port was last initialized.

3.6.5.10 Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

The page includes a table with the following information:

Port	The switch port number of the logical STP port.
MSTP	The number of MSTP BPDUs transmitted/received on the port.
RSTP	The number of RSTP BPDUs transmitted/received on the port.
STP	The number of legacy STP Configuration BPDUs transmitted/received on the port.
TCN	The number of (legacy) Topology Change Notifications BPDUs transmitted/received on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDUs received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDUs received (and discarded) on the port.

3.6.6 Fast Recovery

Fast Recovery is a function for port redundancy. Multiple ports can be connected to one or more switches providing redundant links but only one of these ports will be active and the others will be blocked.

Mode

Setting	Description	Factory Default
Enabled/Disabled	Select to enable the Fast Recovery function.	Disabled

Recovery Priority

Setting	Description	Factory Default
Not included, 1 to 20	Select the priority (number from 1 to 20) of each port. The connected port with the highest priority (lowest number) will be the active one and the others will be blocked.	Not included

When the Fast Recovery is Enabled, the page shows an additional text indicating the active port of the switch. Besides the priority programmed, the switch will also consider the ports status to establish the active port for the Fast Recovery. If a port is not connected (link down), it will never be the active port regardless the priority programmed.

3.7 Virtual LAN

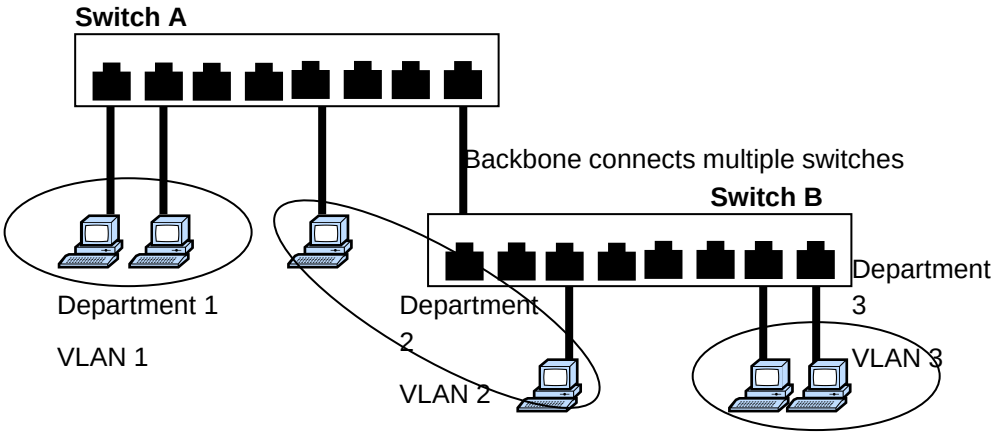
Setting up Virtual LANs (VLANs) on your Weidmüller switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

3.7.1 The Virtual LAN (VLAN) Concept

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. With VLANs you can segment your network according into:

- **Departmental groups**—You could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups**—You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—You could have one VLAN for email users and another for multimedia users.



Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend most of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host on VLAN Marketing, for example, is moved to a port in another part of the network, and retains its original subnet membership, you only need to specify that the new port is on VLAN Marketing. You do not need to carry out any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on VLAN Marketing needs to communicate with devices on VLAN Finance, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs

Your Weidmüller switch provides support for VLANs using IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-1998 standard allows each port on your Weidmüller switch to be placed in:

- On a single VLAN defined in the Weidmüller switch
- On several VLANs simultaneously using 802.1Q tagging

The standard requires that you define the *802.1Q VLAN ID* for each VLAN on your Weidmüller switch before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized Weidmüller contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- *VLAN Name*—Management VLAN ID
- *802.1Q VLAN ID*—1 (if tagging is required)

Communication between VLANs

If devices connected to a VLAN need to communicate to devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

The Weidmüller switch supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical (backbone, trunk) link. When setting up VLANs you need to understand when to use untagged and tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, tagged membership must be defined.

A typical host (e.g., clients) will be untagged members of one VLAN, defined as "Access Port" in the Weidmüller switch, while inter-switch connections will be tagged members of all VLANs, defined as "Trunk Port" in the Weidmüller switch.

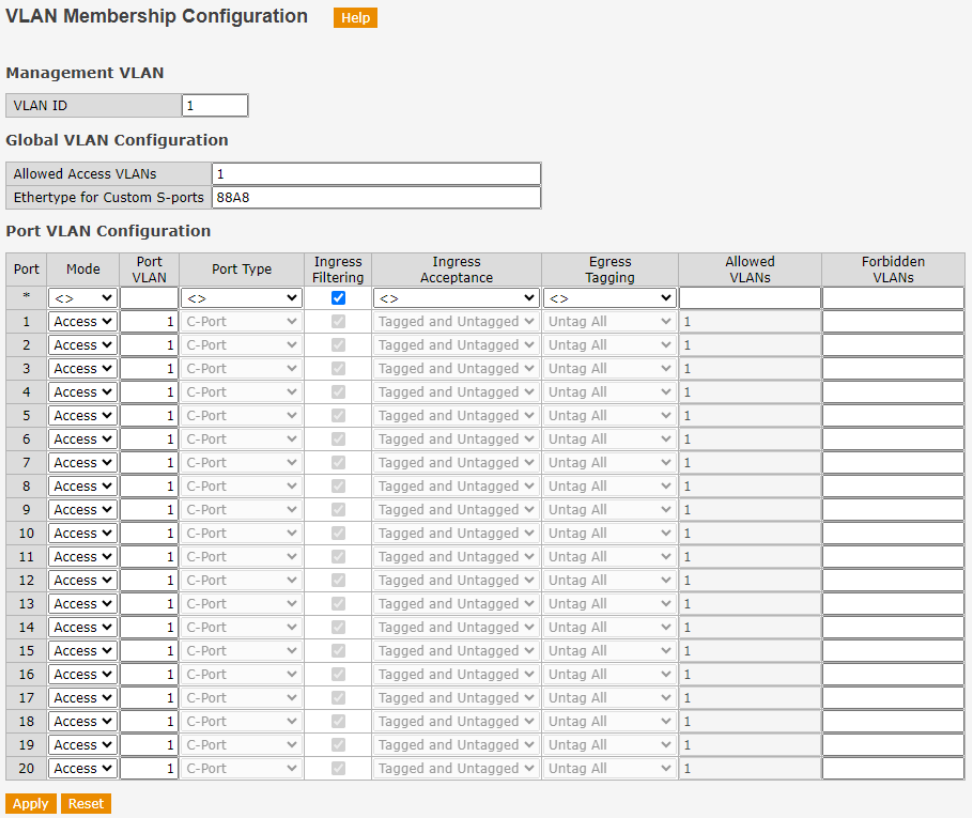
The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs. If a frame is carrying the additional information, it is known as a *tagged* frame.

To carry multiple VLANs across a single physical (backbone, trunk) link, each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong to which VLAN. To communicate between VLANs, a router must be used.

3.7.2 Configuring Virtual LAN

3.7.2.1 VLAN Membership

This page allows the user to configure VLANs on the switch. The page is divided into a section to configure the Management VLAN, a global section and a per-port configuration section.



Management VLAN

VLAN ID

Setting	Description	Factory Default
Number between 1 and 4095	Identifier for the Management VLAN.	1

Global VLAN Configuration

Allowed Access VLANs

Setting	Description	Factory Default
Numerical value between 1 and 4095	This field shows the allowed Access VLANs, it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field (Port VLAN Configuration section). By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.	1

Ethertype for Custom S-ports

Setting	Description	Factory Default
Hexadecimal value between 0x600 and FFFF	This field specifies the ethertype/TPID used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.	88A8

Port VLAN Configuration

Mode

Setting	**Description**	**Factory Default**
Access	Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics: • Member of exactly one VLAN, the Port VLAN (Access VLAN), which by default is 1 • Accepts untagged and C-tagged frames • Discards all frames that are not classified to the Access VLAN • On egress all frames classified to the Access VLAN are transmitted untagged	Access
Trunk	Trunk ports can carry traffic on multiple VLANs simultaneously and are normally used to connect to other switches. Trunk ports have the following characteristics: • By default, a trunk port is member for all VLANs (1-4095)	

	• The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Frames classified to a VLAN that the port is not a member of are discarded • By default, all frames but frames classified to the Port VLAN (Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress • Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress	
Hybrid	Hybrid ports resemble trunk ports in many ways, but add additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Ingress filtering can be controlled • Ingress acceptance of frames and configuration of egress tagging can be configured independently	

ATTENTION

For communication redundancy in the VLAN environment, set **Redundant Port**, **Coupling Port**, and **Homing Port** as "Trunk Port," since these ports act as the "backbone" to transmit all packets of different VLANs to different Weidmüller switches.

Port VLAN

Setting	Description	Factory Default
VID ranges from 1 to 4095	Determines the port's VLAN ID (PVID). On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called "Access VLAN" for ports in Access mode and “Native VLAN” for ports in Trunk or Hybrid mode.	1

Port type

Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

Setting	Description	Factory Default
Unaware	On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. This port type can only be selected if port mode is Hybrid.	C-Port
C-Port	On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.	
S-Port	On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. If frames must be tagged on egress, they will be tagged with an S-tag. This port type can only be selected if port mode is Hybrid.	
S-Custom-Port	On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. If frames must be tagged on egress, they will be tagged with the custom S-tag.	

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

Setting	Description	Factory Default
Checked / Unchecked	If checked (ingress filtering enabled), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled (unchecked), frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.	Checked

Ingress Acceptance

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Setting	Description	Factory Default
Tagged and Untagged	Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged.	Tagged and Untagged
Tagged Only	Only frames tagged with the corresponding Port Type tag are accepted on ingress.	
Untagged Only	Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.	

Egress Tagging

Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Setting	Description	Factory Default
Untag Port VLAN	Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.	Untag All
Tag All	All frames, whether classified to the Port VLAN or not, are transmitted with a tag.	
Untag All	All frames, whether classified to the Port VLAN or not, are transmitted without a tag. Only available for Hybrid ports.	

Allowed VLANs

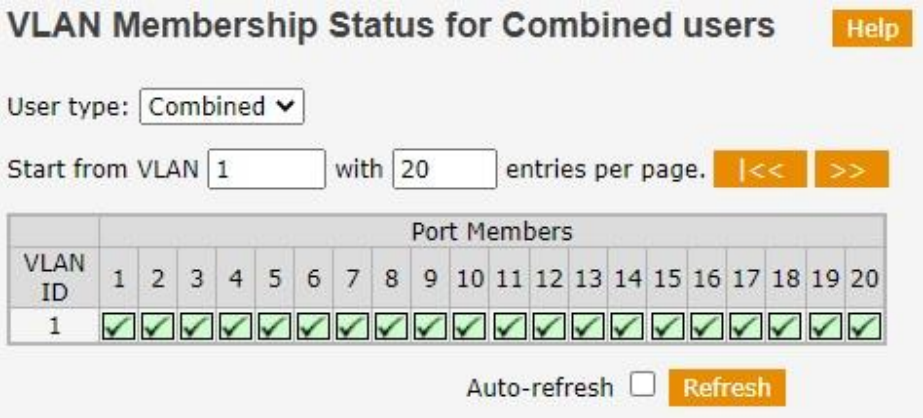
Setting	Description	Factory Default
VID ranges from 1 to 4095	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port will not become member of any VLAN.	1

Forbidden VLANs

Setting	Description	Factory Default
VID ranges from 1 to 4095	A port may be configured to never become member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. By default, the field is left blank, which means that the port may become a member of all possible VLANs.	None

3.7.2.2 VLAN Membership Status

This page provides an overview of membership status of VLAN users.



User Type

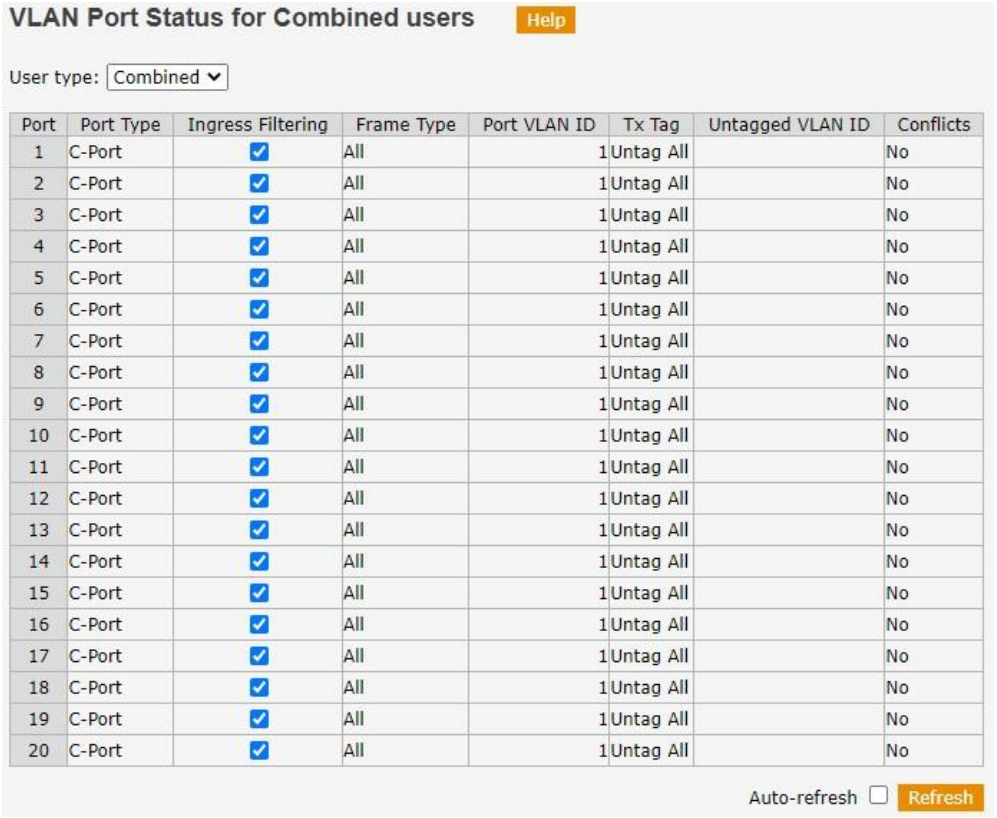
Setting	Description	Factory Default
Scroll list with acceptable user types	Various internal software modules may use VLAN services to configure VLAN memberships on the fly. It is possible to show VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.	Combined

The table displayed on the page shows the port members of each programmed VLAN ID.

VLAN ID	VLAN ID for which the Port members are displayed.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, the image ✓ will be displayed. If a port is in the forbidden port list, the image ✗ will be displayed. If a port is in the forbidden port list and at the same time attempted to be included in the VLAN (ex: dynamically by GVRP), the image ✗ will be displayed indicating that there is a conflict in the port. The port will not be a member of the VLAN in this case.

3.7.2.3 VLAN Port Status

This page provides VLAN port status information.



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag All		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No
11	C-Port	☑	All	1	Untag All		No
12	C-Port	☑	All	1	Untag All		No
13	C-Port	☑	All	1	Untag All		No
14	C-Port	☑	All	1	Untag All		No
15	C-Port	☑	All	1	Untag All		No
16	C-Port	☑	All	1	Untag All		No
17	C-Port	☑	All	1	Untag All		No
18	C-Port	☑	All	1	Untag All		No
19	C-Port	☑	All	1	Untag All		No
20	C-Port	☑	All	1	Untag All		No

The following information is shown on the table:

User Type	Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. It is possible to show VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.
Port	The logical port for the settings contained in the same row.
Port Type	Shows the port type (Unaware, C-Port, S-Port or S-Custom-Port).
Ingress Filtering	Shows whether the ingress filtering is enabled or not.
Frame Type	Shows the acceptable frame types for the port (All, Tagged, Untagged).
Port VLAN ID	Shows the PVID setting for the port.
Tx Tag	Shows the egress Tag requirements (Tag All, Tag PVID, Untag All, …) for the port.
Untagged VLAN ID	If Tx Tag is overridden in the port and is set to UVID (Untagged VLAN ID), then this field will show the VLAN ID the user wants to untag on egress.
Conflicts	Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other

	software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority. If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module. The "Combined" user reflects what is actually configured in hardware.

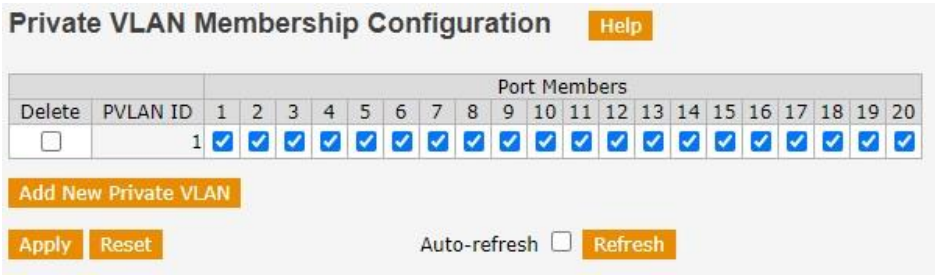
3.7.2.4 Private VLAN Membership

The private VLAN membership configuration for the switch can be monitored and modified from this page. Private VLANs can be added or deleted and port members of each private VLAN can also be added or removed.

Private VLANs are based on the source port mask and there are no connections to VLANs. This means that VLAN IDs and private VLAN IDs can be identical.

A port must be a member of both a VLAN and a private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and private VLAN 1.

A VLAN-unaware port can only be a member of one VLAN, but it can be a member of multiple private VLANs.



Press the button **Add New Private VLAN** to add a new private VLAN ID. An empty row is added to the table and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted and a warning message appears.

The **Delete** button can be used to undo the addition of new private VLANs.

PVLAN ID

Setting	Description	Factory Default
PVLAN ID ranges from 1 to 20	Indicate the Private VLAN ID number.	None

Port Membership

Setting	Description	Factory Default
Check/Uncheck	A row of check boxes for each port is displayed for each private VLAN ID. Check the box to include a port in a private VLAN. To remove or exclude the port from the private VLAN, make sure the box is unchecked.	Unchecked

3.7.2.5 Private VLAN Port Isolation

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other ports on the same VLAN and Private VLAN.

Port Number

Setting	Description	Factory Default
Check/Uncheck	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port.	Unchecked

3.7.2.6 GVRP Configuration

GVRP (GARP VLAN Registration Protocol) is a protocol that allows automatic VLAN configuration between the switch and nodes.

In the figure below can be seen the GVRP configuration settings that are commonly applied to all GVRP enabled ports.

GVRP

Setting	Description	Factory Default
Disabled/Enabled	GVRP feature globally enabled or disabled.	Disabled

Join-time

Setting	Description	Factory Default
Numerical value between 1 and 20 (hundreds of sec)	GVRP protocol timer.	20

Leave-time

Setting	Description	Factory Default
Numerical value between 60 and 300 (hundreds of sec)	GVRP protocol timer.	60

LeaveAll-time

Setting	Description	Factory Default
Numerical value between 1000 and 5000 (hundreds of sec)	GVRP protocol timer.	1000

Max VLANs

Setting	Description	Factory Default
Numerical value between 1 and 4094	The maximum number of VLANs supported by GVRP. This number can only be changed when GVRP is disabled.	20

3.7.2.7 GVRP Port Configuration

This configuration can be performed either before or after GVRP is configured globally. The protocol operation will be the same.

For each port it has to be configured whether GVRP is enabled or not.

Port Mode

Setting	Description	Factory Default
Disabled / GVRP Enabled	Turns the GVRP feature off or on for the port in question.	Disabled

3.8 SNMP

Weidmüller managed Switches support SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community strings *public* and *private* by default. SNMP V3 requires that you select an authentication level of MD5 or SHA and is the most secure protocol. You can also enable data encryption to enhance data security.

Supported SNMP security modes and levels are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication.
SNMP V3	No-Auth	No	No	Uses an account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key (DES or AES128). 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

These parameters are configured on the SNMP page. A more detailed explanation of each parameter is given in the following sections.

3.8.1 SNMP System

This page allows the user to configure the general SNMP settings.

Mode

Setting	Description	Factory Default
Enabled/Disabled	Enables or disables SNMP operation mode.	Enabled

Version

Setting	Description	Factory Default
V1 / V2c / V3	Specifies the SNMP protocol version used to manage the switch.	V2c

Read Community (SNMPv1 and SNMP v2c only)

Setting	Description	Factory Default
Max. 255 characters	Specifies the community string to authenticate the SNMP agent for read-only access. The SNMP agent will access all objects using this community string. The field only suits to SNMPv1 and SNMPv2c. If SNMPv3 is used, this setting has to be made using the option SNMP Community.	public

Write Community (SNMPv1 and SNMP v2c only)

Setting	Description	Factory Default
Max. 255 characters	Specifies the community string to authenticate the SNMP agent for read/write access. The SNMP agent will access all objects using this community string. The field only suits to SNMPv1 and SNMPv2c. If SNMPv3 is used, this setting has to be made using the option SNMP Community.	private

Engine ID

Setting	Description	Factory Default
Information only	Indicates the SNMPv3 engine ID.	Enterprise number and MAC address

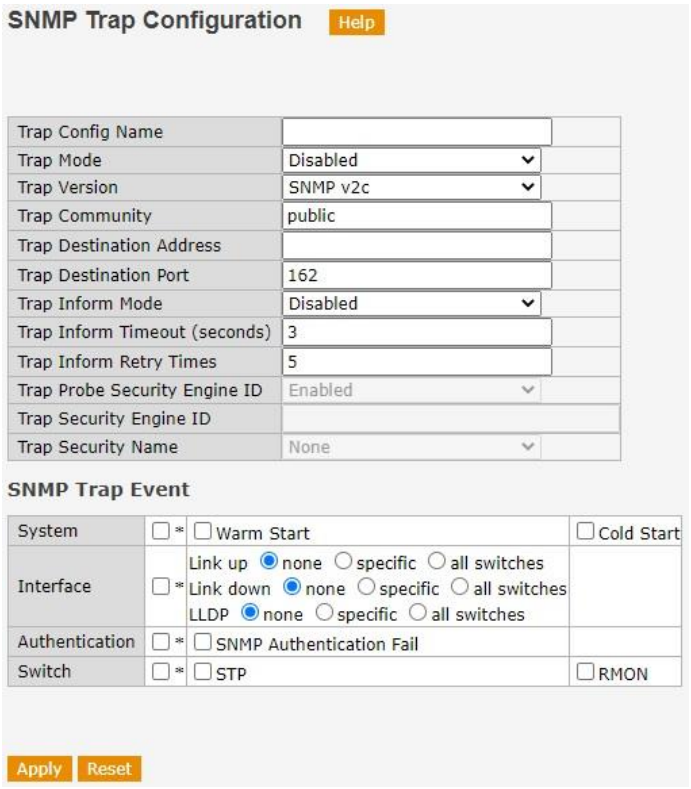
3.8.2 SNMP Trap

This page allows the user to configure the general SNMP traps.

Mode

Setting	Description	Factory Default
Disabled/Enabled	Enables or disables SNMP traps in the switch.	Disabled

Pressing the button **Add New Entry** the SNMP Trap configuration page appears.



SNMP Trap Configuration

Trap Config Name

Setting	Description	Factory Default
Max. 255 characters	Indicates the trap Configuration's name.	None

Trap Mode

Setting	Description	Factory Default
Disabled/Enabled	Enables or disables SNMP traps in the switch.	Disabled

Trap Version

Setting	Description	Factory Default
V1 / V2c / V3	Specifies the SNMP protocol version used to manage the traps.	V2c

Trap Community

Setting	Description	Factory Default
Max. 255 characters	Indicates the community access string when sending SNMP trap packets.	public

Trap Destination Address

Setting	Description	Factory Default
IP address	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').	None

Trap Destination Port

Setting	Description	Factory Default
Port number (1 to 65535)	Indicates the SNMP trap destination port. SNMP Agent will send SNMP messages via this port.	162

Trap Inform Mode

Setting	Description	Factory Default
Disabled/Enabled	Enables or disables SNMP trap inform mode.	Disabled

Trap Inform Timeout

Setting	Description	Factory Default
Numerical value between 0 and 2147 (sec)	Configures the SNMP trap inform timeout.	3

Trap Inform Retry Times

Setting	Description	Factory Default
Numerical value between 0 and 255	Configures the retry times for SNMP trap inform	5

Trap Probe Security Engine ID

Setting	Description	Factory Default
Disabled/Enabled	This field can only be programmed if the selected trap version is SNMPv3. Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.	Disabled

Trap Security Name

Setting	Description	Factory Default
Max. 255 characters	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.	None

SNMP Trap Event

System

Setting	Description	Factory Default
Check/Uncheck	Enable/Disable the traps related with the complete system. It is possible to enable traps for cold start, for warm start of for both events.	Unchecked

Interface

Setting	Description	Factory Default
Check/Uncheck	Enable/Disable the traps related with the interfaces/ports of the switch. It is possible to enable traps for link up, for link down, for LLDP of for all events.	Unchecked

Authentication

Setting	Description	Factory Default
Check/Uncheck	Enable/Disable the traps related with the SNMP authentication failure event.	Unchecked

Switch

Setting	Description	Factory Default
Check/Uncheck	Enable/Disable the traps related with the STP redundancy.	Unchecked

3.8.3 SNMP Community Configuration

This page allows the user to configure SNMP community table. The entry index key is Community.

Press the button **Add New Entry** to create a new Community.

Community

Setting	Description	Factory Default
Max. 32 characters	Indicates the community access string to permit access to SNMP agent	None

Source IP

Setting	Description	Factory Default
IP address	Indicates the SNMP source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.	None

Source Mask

Setting	Description	Factory Default
Subnet Mask	Indicates the SNMP access source address mask.	None

3.8.4 SNMP Users Configuration

NOTE: This page only has to be configured if SNMPv3 is programmed in the switch.

This page allows the user to configure SNMPv3 user table. The entry index keys are Engine ID and User Name.

A default user is already created but is possible to create additional ones with different security levels. Press the button **Add New Entry** to create a new User.

Engine ID

Setting	Description	Factory Default
Octet string	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses User-based Security Model (USM) for message security and View-based Access Control Model (VACM) for access control. For the USM entry, the **usmUserEngineID** and **usmUserName** are the entry keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID is the same as system engine ID, then it is local user; otherwise it's remote user.	None

User Name

Setting	Description	Factory Default
Max 32 characters	A string identifying the user name that this entry should belong to.	None

Security Level

Setting	Description	Factory Default
NoAuth, NoPriv	No authentication and no encryption required.	Auth, Priv
Auth, NoPriv	Authentication is required but no encryption.	
Auth, Priv	Authentication and encryption required.	

Authentication Protocol

Setting	Description	Factory Default
MD5	Authentication will be based on the MD5 algorithms.	MD5
SHA	Authentication will be based on the SHA algorithms.	

Authentication Password

Setting	Description	Factory Default
String between 8 and 32 characters (MD5) or between 8 and 40 (SHA)	A string identifying the authentication pass phrase.	None

Privacy Protocol

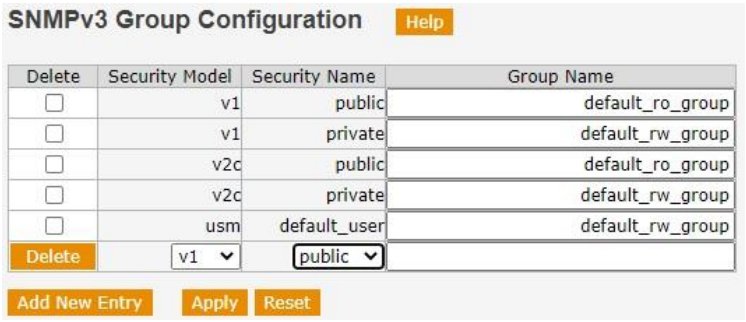
Setting	Description	Factory Default
DES	Encryption will be based on DES protocol.	DES
AES	Encryption will be based on AES protocol.	

Privacy Password

Setting	Description	Factory Default
String between 8 and 32 characters	A string identifying the encryption pass phrase.	None

3.8.5 SNMP Groups Configuration

This page allows the user to configure SNMP group table. The entry index keys are Security Model and Security Name.



There are several Groups already created but is possible to create additional ones. Press the button **Add New Entry** to create a new Group.

Security Model

Setting	Description	Factory Default
V1	Reserved for SNMPv1.	V1
V2c	Reserved for SNMPv2c.	
usm	User-based Security Model (usm): SNMPv3.	

Security Name

Setting	Description	Factory Default
Max. 32 characters	A string identifying the security name that this entry should belong to. This Security Name must be one of the created users names in the SNMP Users Configuration option.	None

Group Name

Setting	Description	Factory Default
Max. 32 characters	A string identifying the group name that this entry should belong to.	None

Group Table – Group Name

Setting	Description	Factory Default
Max. 32 characters	A string identifying the name of the Group.	None

3.8.6 SNMP View Configuration

NOTE: This page only has to be configured if SNMPv3 is programmed in the switch.

This page allows the user to configure SNMPv3 views table. The entry index keys are View Name and OID Subtree.

A default view is already created but is possible to create additional ones. Press the button **Add New Entry** to create a new View.

View Name

Setting	Description	Factory Default
Max. 32 characters	A string identifying the view name that this entry should belong to.	None

View Type

Setting	Description	Factory Default
Included	Indicates that the created view subtree should be included.	Exact
Excluded	Indicates that the created view subtree should be excluded.	

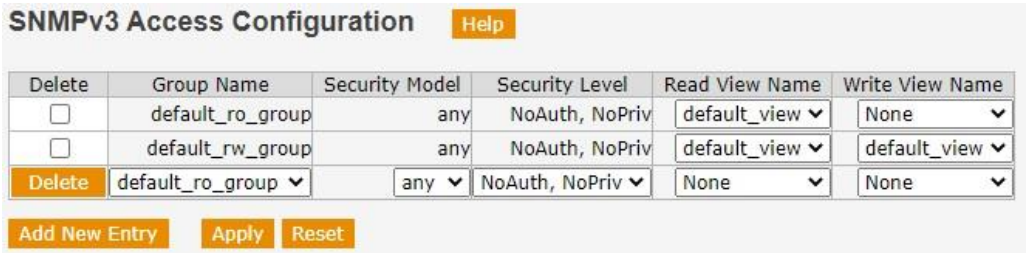
OID Subtree

Setting	Description	Factory Default
Number (OID)	The object identifier (OID) value for the created view table. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).	None

3.8.7 SNMP Access Configuration

NOTE: This page only has to be configured if SNMPv3 is programmed in the switch.

This page allows the user to configure SNMPv3 accesses table. The entry index keys are Group Name, Security Model and Security Level.



Two default views are already created but is possible to create additional ones based on the SNMPv3 users / groups / views created. Press the button **Add New Entry** to create a new Access.

Group Name

Setting	Description	Factory Default
Max. 32 characters	A string identifying the group name that this entry should belong to. It should be one of the created groups in the SNMP Groups Configuration option.	None

Security Model

This Security Model must be selected in accordance with the one defined for the User of the selected Group Name.

Setting	Description	Factory Default
V1	Reserved for SNMPv1.	any

V2c	Reserved for SNMPv2c.	
usm	User-based Security Model (usm): SNMPv3.	
any	Accepted any Security model.	

Security Level

This Security Level must be selected in accordance with the one defined for the User of the selected Group Name.

Setting	Description	Factory Default
NoAuth, NoPriv	No authentication and no encryption required.	NoAuth, NoPriv
Auth, NoPriv	Authentication is required but no encryption.	
Auth, Priv	Authentication and encryption required.	

Read View Name

Setting	Description	Factory Default
Max. 32 characters	The name of the MIB View defining the MIB objects for which this request may get the current values. It should be one of the created views in the SNMP Views Configuration option.	None

Write View Name

Setting	Description	Factory Default
Max. 32 characters	The name of the MIB View defining the MIB objects for which this request may set new values. It should be one of the created views in the SNMP Views Configuration option.	None

3.9 RMON

Remote Monitoring (RMON) is an extension of SNMP and is a method of monitoring network traffic. So, while SNMP tracks network devices, RMON tracks traffic. In tandem, SNMP and RMON help network administrators to monitor network performance and troubleshoot issues.

RMON is deployed as an SNMP MIB. The RMON MIB is composed of data associated with Ethernet traffic activity to help identify and address performance issues.

3.9.1 RMON Statistics Configuration

This page allows the user to configure RMON Statistics.

Press the button **Add New Entry** to create a new entry to get RMON statistics in any port of the switch.

ID

Setting	Description	Factory Default
Numeric value between 1 and 65535	Indicates the index of the entry.	None

Data Source

Setting	Description	Factory Default
Number (OID)	Indicates the port ID which wants to be monitored. The value of the switch must add 1000000*(switch ID-1). For example, if we want to monitor switch 3 port 5, the value is 2000005.	None

3.9.2 RMON History Configuration

The user can configure RMON History table on this page.

Press the button **Add New Entry** to create a new entry to get history RMON statistics in any port of the switch.

ID

Setting	Description	Factory Default
Numeric value between 1 and 65535	Indicates the index of the entry.	None

Data Source

Setting	Description	Factory Default
Number (OID)	Indicates the port ID which wants to be monitored. The value of the switch must add 1000000*(switch ID-1). For example, if we want to monitor switch 3 port 5, the value is 2000005.	None

Interval

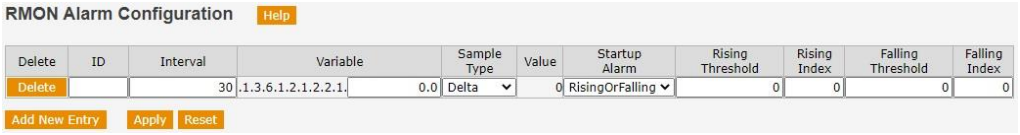
Setting	Description	Factory Default
Time between 1 and 3600 sec	Indicates the interval in seconds for sampling the history statistics data.	1800

Buckets

Setting	Description	Factory Default
Numeric value between 1 and 3600	Indicates the maximum data entries associated this History control entry stored in RMON.	50

3.9.3 RMON Alarm Configuration

The user can configure RMON Alarm table on this page.



Press the button **Add New Entry** to create a new entry to define RMON alarms.

ID

Setting	Description	Factory Default
Numeric value between 1 and 65535	Indicates the index of the entry.	None

Interval

Setting	Description	Factory Default
Time between 1 and 2^{31}-1 (sec)	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.	30

Variable

Setting	Description	Factory Default
Number (OID)	Indicates the particular variable to be sampled, the possible variables are:	None

	InOctets: The total number of octets received on the interface, including framing characters. InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol. InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. InDiscards: The number of inbound packets that are discarded even the packets are normal. InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol. OutOctets: The number of octets transmitted out of the interface , including framing characters. OutUcastPkts: The number of uni-cast packets that request to transmit. OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit. OutDiscards: The number of outbound packets that are discarded even the packets are normal. OutErrors: The number of outbound packets that could not be transmitted because of errors. OutQLen: The length of the output packet queue (in packets).	

Sample Type

Setting	Description	Factory Default
Delta / Absolute	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Absolute: Get the sample directly. Delta: Calculate the difference between samples.	Delta

Value

Setting	Description	Factory Default
Information only	The value of the statistic during the last sampling period.	None

Startup Alarm

Setting	Description	Factory Default
Rising / Falling / Rising Or Falling	The activation of the alarm. Rising when the first value is larger than the rising threshold. Falling when the first value is lower than the falling threshold.	Rising Or Falling

	Rising Or Falling when the first value is larger than the rising threshold or lower than the falling threshold.	

Rising Threshold

Setting	Description	Factory Default
Numeric value between -2^{31} and $2^{31}-1$	Rising threshold value.	0

Rising Index

Setting	Description	Factory Default
Numeric value between 1 and 65535	Rising event index.	0

Falling Threshold

Setting	Description	Factory Default
Numeric value between -2^{31} and $2^{31}-1$	Falling threshold value.	0

Falling Index

Setting	Description	Factory Default
Numeric value between 1 and 65535	Falling event index.	0

3.9.4 RMON Event Configuration

The user can configure RMON Event table on this page.

Press the button **Add New Entry** to create a new entry to define RMON events.

ID

Setting	Description	Factory Default
Numeric value between 1 and 65535	Indicates the index of the entry.	None

Desc

Setting	Description	Factory Default
Max. 127 characters	Description of the event.	None

Type

Setting	Description	Factory Default
None	The event is not notified.	None
Log	SNMP log is created when the event is triggered.	
SNMPtrap	SNMP trap is sent when the event is triggered.	
Logandtrap	SNMP log is created and SNMP trap is sent when the event is triggered.	

Community

Setting	Description	Factory Default
Max. 127 characters	Specify the community when trap is sent.	public

Event Last Time

Setting	Description	Factory Default
Information only	Indicates the value of sysUpTime at the time this event entry last generated an event.	None

3.9.5 RMON Statistics Status

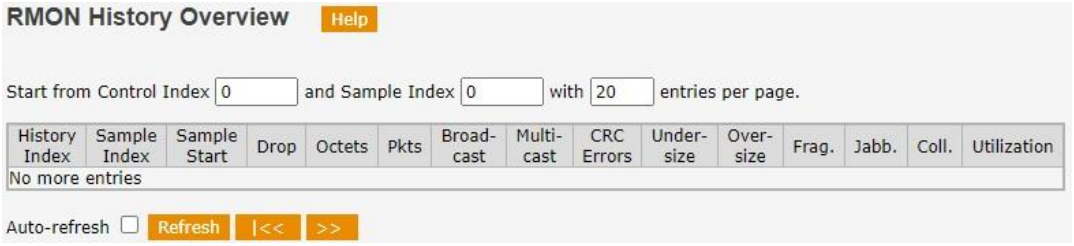
This page provides an overview of RMON Statistics entries. The page shows up to 99 entries from the Statistics table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table. The **Start from Control Index** field allows the user to select the starting point in the Statistics table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Statistics table match.

The page includes a table with the following information:

ID	Indicates the index of Statistics entry.
Data Source	The port ID which wants to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-Cast	The total number of good packets received that were directed to the broadcast address.
Multi-Cast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-Size	The total number of packets received that were less than 64 octets.
Over-Size	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
64 Bytes	The total number of packets (including bad packets) received that were 64 octets in length.
65~127	The total number of packets (including bad packets) received that are between 65 to 127 octets in length.
128~255	The total number of packets (including bad packets) received that are between 128 to 255 octets in length.
256~511	The total number of packets (including bad packets) received that are between 256 to 511 octets in length.
512~1023	The total number of packets (including bad packets) received that are between 512 to 1023 octets in length.
1024~1588	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

3.9.6 RMON History Status

This page provides an overview of RMON History entries. The page shows up to 99 entries from the History table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table. The **Start from Control Index** field allows the user to select the starting point in the Statistics table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Statistics table match.



The page includes a table with the following information:

History Index	Indicates the index of History control entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	The total number of good packets received that were directed to the broadcast address.
Multi-cast	The total number of good packets received that were directed to a multicast address.
CRC Error	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-size	The total number of packets received that were less than 64 octets.
Over-size	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames whose size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames whose size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this segment.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

3.9.7 RMON Alarm Status

This page provides an overview of RMON Alarm entries. The page shows up to 99 entries from the Alarm table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table. The **Start from Control Index** field allows the user to select the starting point in the Statistics table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Statistics table match.

The page includes a table with the following information:

ID	Indicates the index of Alarm control entry.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
Variable	Indicates the particular variable to be sampled
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
Value	The value of the statistic during the last sampling period.
Startup Alarm	The alarm that may be sent when this entry is first set to valid.
Rising Threshold	Rising threshold value.
Rising Index	Rising threshold index.
Filing Threshold	Falling threshold value.
Falling Index	Falling event index.

3.9.8 RMON Event Status

This page provides an overview of RMON Event entries. The page shows up to 99 entries from the Event table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table. The **Start from Control Index** field allows the user to select the starting point in the Statistics table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Statistics table match.

The page includes a table with the following information:

Event Index	Indicates the index of the event entry.
Log Index	Indicates the index of the log entry.
Log Time	Indicates Event log time
LogDescripi	Indicates the Event description.

3.10 Traffic Prioritization

The Weidmüller switch's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The Weidmüller switch can inspect both IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 ToS information to provide consistent classification of the entire network. The implemented QoS capability improves the performance and determinism of industrial networks for mission critical applications.

What is Traffic Prioritization?

Traffic prioritization allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- Improve network performance by controlling a wide variety of traffic and managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or business-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP, and minimize traffic delay and jitter.
- Improve network performance as the amount of traffic grows. This will save cost by reducing the need to keep adding bandwidth to the network.

How Traffic Prioritization Works

Traffic prioritization uses the eight traffic queues that are present in your Weidmüller managed Switch to ensure that high priority traffic is forwarded on a different queue from lower priority traffic. This is what provides Quality of Service (QoS) to your network.

Weidmüller managed Switch traffic prioritization depends on two industry-standard methods:

- **IEEE 802.1D** → A layer 2 marking scheme.
- **Differentiated Services (DiffServ)** → A layer 3 marking scheme.

IEEE 802.1D Traffic Marking

The IEEE Std 802.1D, 1998 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. The 4-byte tag immediately follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D, 1998 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame. The priority marking scheme determines the level of service that this type of traffic should receive. Refer to the table below for an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority Level	IEEE 802.1D Traffic Type
0	Best Effort (default)
1	Background
2	Standard (spare)
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (interactive media); less than 100 milliseconds of latency and jitter
6	Voice (interactive voice); less than 10 milliseconds of latency and jitter
7	Network Control Reserved traffic

Even though the IEEE 802.1D standard is the most widely used prioritization scheme in the LAN environment, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional for Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.
- It is only supported on a LAN and not across routed WAN links, since the IEEE 802.1Q tags are removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to store the packet priority information. DSCP is an advanced intelligent method of traffic marking that allows you to choose how your network prioritizes different types of traffic. DSCP uses 64 values that map to user-defined service levels, allowing you to establish more control over network traffic.

The advantages of DiffServ over IEEE 802.1D are:

- You can configure how you want your switch to treat selected applications and types of traffic by assigning various grades of network service to them.
- No extra tags are required in the packet.
- DSCP uses the IP header of a packet to preserve priority across the Internet
- DSCP is backward compatible with IPV4 ToS, which allows operation with existing devices that use a layer 3 ToS enabled prioritization scheme.

Traffic Prioritization

Weidmüller managed Switches classify traffic based on layer 2 of the OSI 7 layer model, and the switch prioritizes received traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1D frame and is assigned to the appropriate priority queue based on the IEEE 802.1p service level value defined in that packet. Service level markings (values) are defined in the IEEE 802.1Q 4-byte tag, and consequently traffic will only contain 802.1p priority markings if the network is configured with VLANs and VLAN tagging. The traffic flow through the switch is as follows:

- A packet received by the switch may or may not have an 802.1p tag associated with it. If it does not, then it is given a default 802.1p tag (which is usually 0). Alternatively, the packet may be marked with a new 802.1p value, which will result in all knowledge of the old 802.1p tag being lost.
- As the 802.1p priority levels are fixed to the traffic queues, the packet will be placed in the appropriate priority queue, ready for transmission through the appropriate egress port. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port is tagged for that VLAN. If it is, then the new 802.1p tag is used in the extended 802.1D header.
- The Weidmüller Switch will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based upon the IEEE 802.1p value (service levels) in that tag. It is this 802.1p value that determines to which traffic queue the packet is mapped to.

Traffic Queues

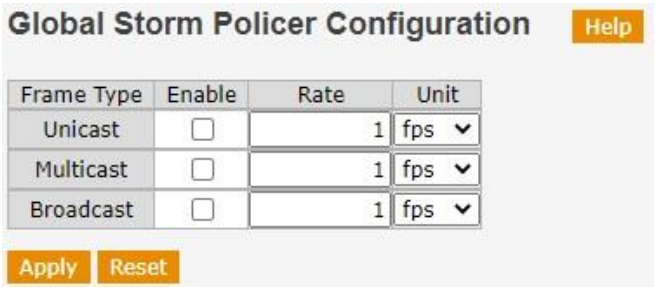
The hardware of Weidmüller switches has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the Weidmüller switch without being delayed by lower priority traffic. As each packet arrives in the Weidmüller switch, it passes through any ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue.

The Weidmüller switches support two different queuing mechanisms:

- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weight Fair method gives high priority precedence over low priority, but in the event that high priority traffic does not reach the link capacity, lower priority traffic is not blocked.
- **Strict:** This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. The Strict method always gives precedence to high priority over low priority.

3.10.1 Storm Control

Global storm policers for the switch are configured on this page. There is a unicast storm rate control, multicast storm rate control and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a VLAN ID-DMAC pair not present on the MAC Address table.



For each frame type (Unicast / Multicast / Broadcast) is possible:

Enable

Setting	Description	Factory Default
Check / Uncheck	Enable or disable the storm control status for the given frame type.	Unchecked

Rate

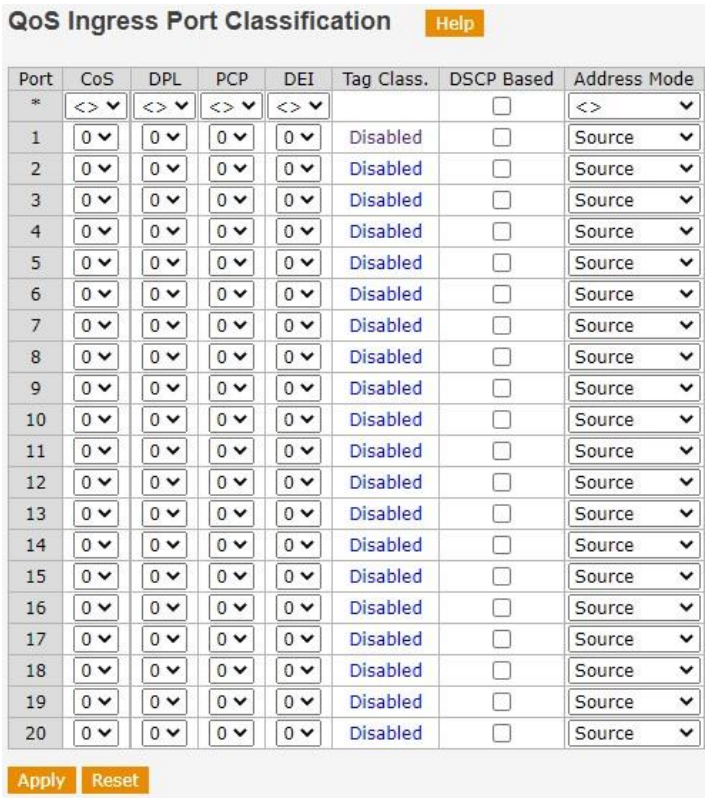
Setting	Description	Factory Default
Numeric value	Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer.	1

Unit

Setting	Description	Factory Default
fps / kfps	Controls the unit of measure for the storm control rate. Fps stands for frames per second and kfps means kilo-frames per second.	fps

3.10.2 Port Classification

This page allows the user to configure the basic QoS Ingress Classification settings for all switch ports.



The following settings can be applied to any port of the switch:

COS

Setting	Description	Factory Default
0 to 7	Controls the **default class of service**. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Classification is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to this default CoS.	0

DPL

Setting	Description	Factory Default
0 to 1	Controls the **default drop precedence level**. All frames are classified to a drop precedence level. If the port is VLAN aware, the frame is tagged and Tag Classification is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to this default DPL.	0

PCP

Setting	Description	Factory Default
0 to 7	Controls the **default priority code point (PCP)** value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to this default PCP value.	0

DEI

Setting	Description	Factory Default
0 to 1	Controls the **default drop eligible indicator (DEI)** value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.	0

Tag Class

Setting	Description	Factory Default
Enabled / Disabled	Shows the classification mode for tagged frames on this port. Disabled: Use default QoS class and DP level for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. Click on the mode to configure the mode and/or mapping. This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN-unaware ports are always classified to the default CoS class and DPL.	Disabled

DSCP Based

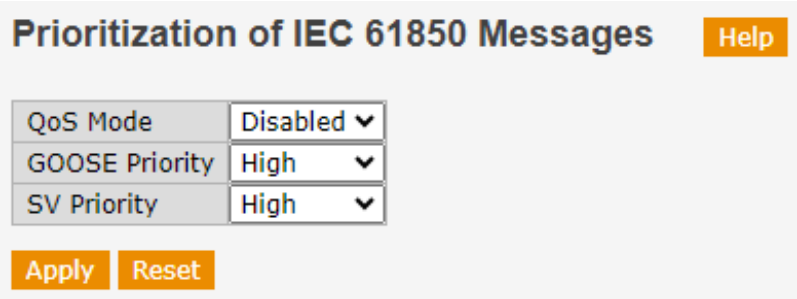
Setting	Description	Factory Default
Checked / Unchecked	Check to enable DSCP Based ToS Ingress Port Classification	Unchecked

Address Mode

Setting	Description	Factory Default
Source / Destination	The IP/MAC address mode specifies whether the QoS Control List (QCL) classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. Accordingly: Source: Enables SMAC/SIP matching. Destination: Enables DMAC/DIP matching.	Source

3.10.3 IEC 61850 Messages

This page allows the user to prioritize only the GOOSE and Sampled Value messages that the switch could receive from IEDs (Intelligent Electronic Devices).



QoS Mode

Setting	Description	Factory Default
Enabled / Disabled	Enable or Disable the prioritization applicable to GOOSE and Sampled Value (SV) messages.	Disabled

GOOSE priority

Setting	Description	Factory Default
High / Medium / Low	Forwarding priority applied to the GOOSE messages received by the switch. The GOOSE messages are identified by the switch with the Ethertype value (0x88B8) and destination address (multicast). If priority is set to High, the switch will use for these messages the queue with highest priority (7). Medium priority will use the queue 4 and Low priority will use the queue 0.	High

SV priority

Setting	Description	Factory Default
High / Medium / Low	Forwarding priority applied to the Sampled Value (SV) messages received by the switch. The SV messages are identified by the switch with the Ethertype value (0x88BA) and destination address (multicast). If priority is set to High, the switch will use for these messages the queue with highest priority (7). Medium priority will use the queue 4 and Low priority will use the queue 0.	High

3.10.4 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

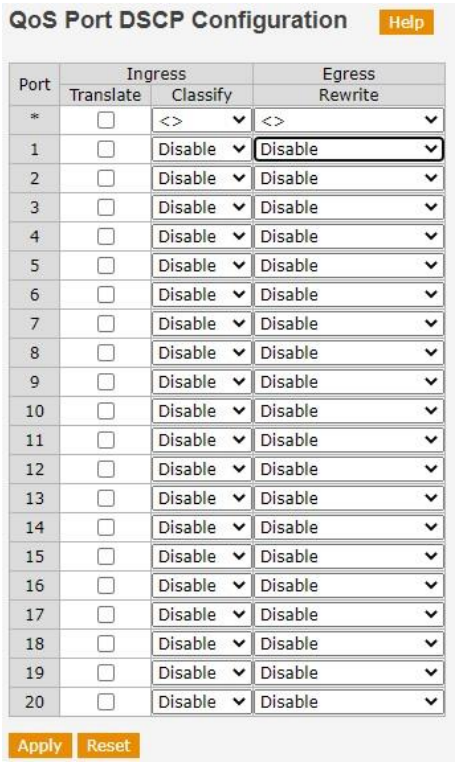
The user can set the tag remarking mode of each port:

Tag Class

Setting	Description	Factory Default
Classified / Default / Mapped	Shows the tag remarking mode for this port: Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of CoS and DPL.	Disabled

3.10.5 Port DSCP

This page allows the user to configure the basic ToS DSCP Configuration settings for all switch ports.



Ingress Translate

Setting	Description	Factory Default
Check / Uncheck	Check to enable ingress translation.	Unchecked

Ingress Classify

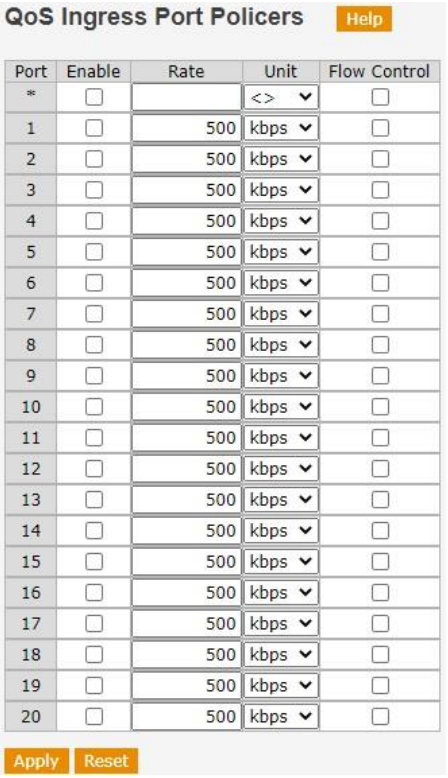
Setting	Description	Factory Default
Disable / DSCP=0 / Selected / All	The classification of a port has four different values: Disable: No ingress DSCP classification. DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP translation window for the specific DSCP. All: Classify all DSCP.	Disable

Egress Rewrite

Setting	Description	Factory Default
Disable / Enable / Remap DP Unaware / Remap DP Aware	Port egress rewriting can be one of the following options: Disable: No egress rewrite. Enable: Rewrite enable without remapping. Remap DP Unaware: DSCP from the analyzer is remapped and the frame is remarked with a remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. Remap DP Aware: DSCP from the analyzer is remapped and the frame is remarked with a remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.	Disable

3.10.6 Port Policing

This page allows the user to configure the Policer settings for all switch ports.



Enable

Setting	Description	Factory Default
Check / Uncheck	Check to enable the policer on the switch port.	Unchecked

Rate

Setting	Description	Factory Default
Numerical value	Configures the rate of each policer. This value is restricted to 100 to 3276700 when the Unit is kbps or fps, and is restricted to 1 to 3276 when the Unit is Mbps or kfps.	500

Unit

Setting	Description	Factory Default
kbps / Mbps / fps / kfps	Configures the unit of measure for each policer rate.	kbps

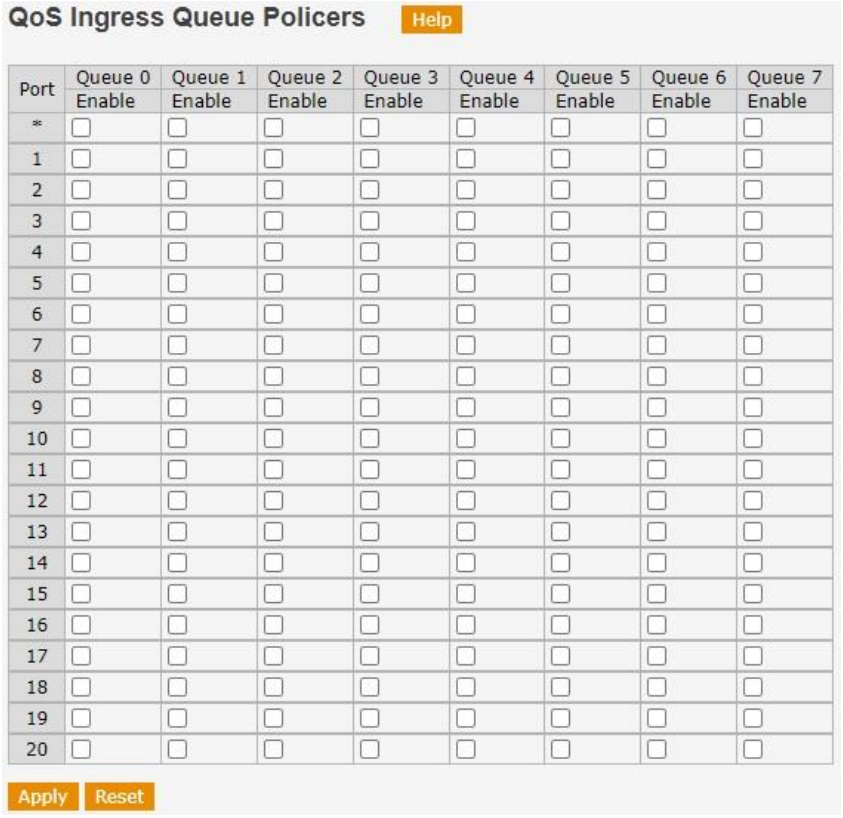
Flow Control

Setting	Description	Factory Default
Check /	If enabled and the port is in Flow Control mode, then	Unchecked

Uncheck	pause frames are sent instead of being discarded.	

3.10.7 Queue Policing

This page allows the user to configure Queue Policer settings for all switch ports.



Enable

Setting	Description	Factory Default
Check / Uncheck	Check to enable the queue policer on the switch port.	Unchecked

Rate

Setting	Description	Factory Default
Numerical value	Configures the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if the queue policer is enabled.	500

Unit

Setting	Description	Factory Default
kbps / Mbps	Controls the unit of measure for the queue policer rate as kbps or Mbps.	kbps

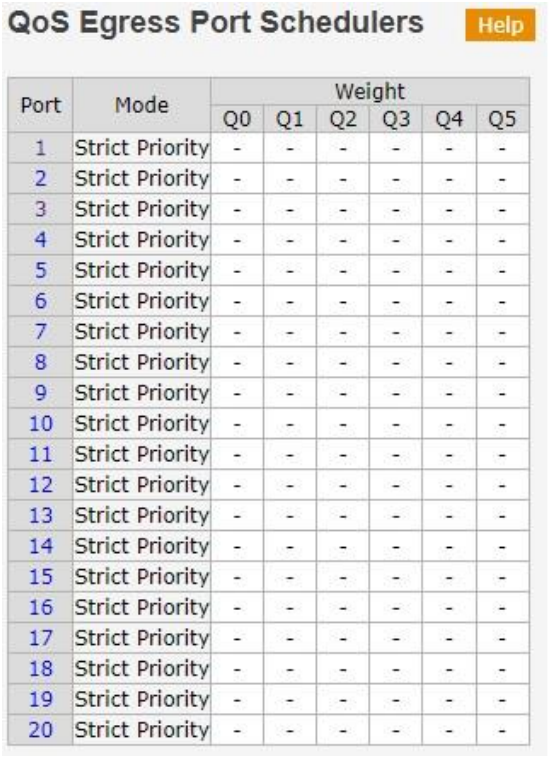
	This field is only shown if the queue policer is enabled.	

3.10.8 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

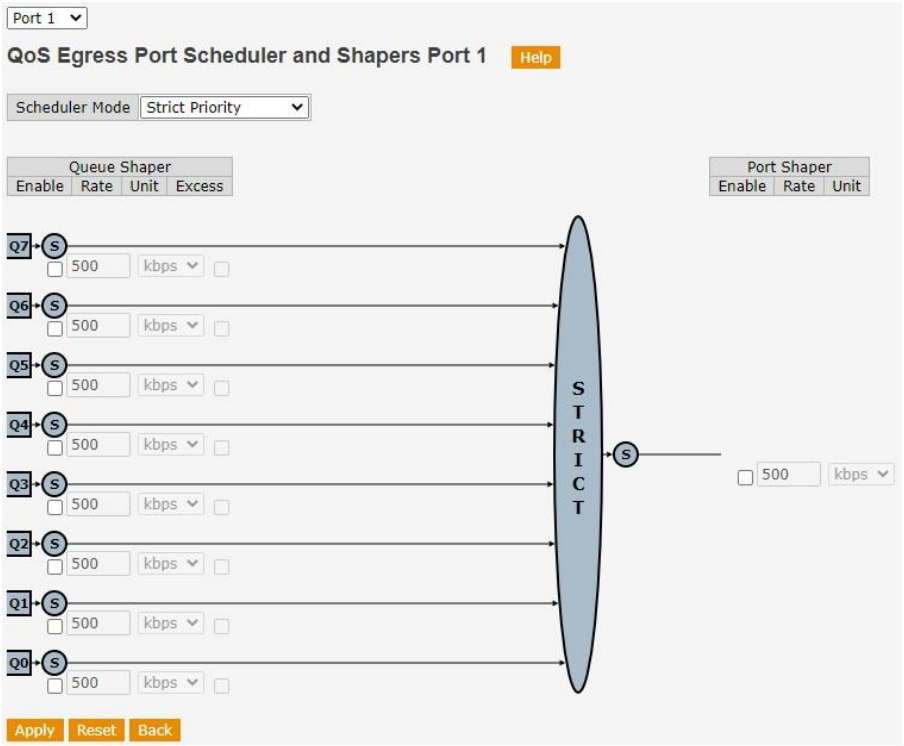
The following information of each port is displayed on the page:

Mode	Shows the scheduling mode (Strict Priority or Weighted).
Weight Q0 – Q5	Shows the weight for this queue and port.



Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-
17	Strict Priority	-	-	-	-	-	-
18	Strict Priority	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-

When clicking on any port number, a new page is loaded to configure the Scheduler and Shapers for that specific port of the switch.



Scheduler Mode

Setting	Description	Factory Default
Strict Priority / 6 Queues Weighted	Configures the scheduler mode on this switch port.	Strict Priority

Queue Shaper Enable

Setting	Description	Factory Default
Check / Uncheck	Controls whether the queue shaper is enabled for this queue on this switch port.	Unchecked

Queue Shaper Rate

Setting	Description	Factory Default
Numerical value	Controls the rate for the queue shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper. It can only be programmed if queue shaper is enabled.	500

Queue Shaper Unit

Setting	Description	Factory Default
kbps / Mbps	Controls the unit of measure for the queue shaper rate. It can only be programmed if queue shaper is enabled.	kbps

Queue Shaper Excess

Setting	Description	Factory Default
Check / Uncheck	Controls whether the queue is allowed to use excess bandwidth. It can only be programmed if queue shaper is enabled.	Unchecked

Queue Scheduler Weight

Setting	Description	Factory Default
Numerical value between 1 and 100	Controls the weight for this queue. This parameter is only shown if "Scheduler Mode" is set to "6 Queues Weighted".	17

Queue Scheduler Weight

Setting	Description	Factory Default
Information only	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "6 Queues Weighted".	16%

Port Shaper Enable

Setting	Description	Factory Default
Check / Uncheck	Controls whether the port shaper is enabled for this switch port.	Unchecked

Queue Shaper Rate

Setting	Description	Factory Default
Numerical value	Controls the rate for the port shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.	500

Queue Shaper Unit

Setting	Description	Factory Default
kbps / Mbps	Controls the unit of measure for the port shaper rate as kbps or Mbps.	kbps

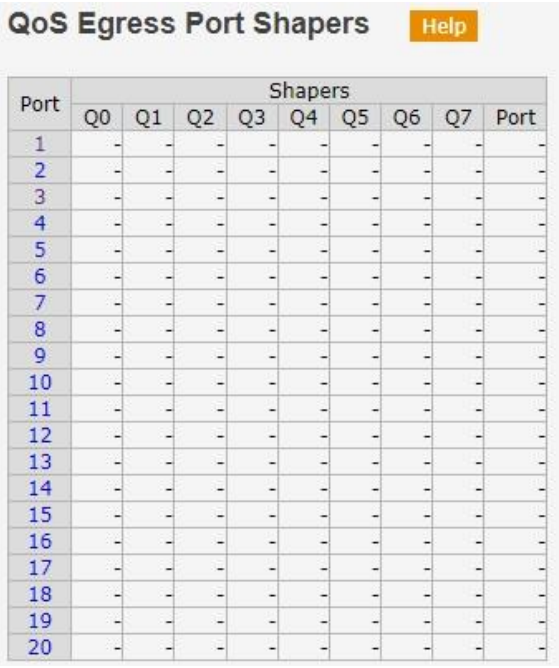
3.10.9 Port Shaper

This page provides an overview of QoS Egress Port Shapers for all switch ports.

The following information of each port is displayed on the page:

Q0 – Q7	Shows "-" if port shaper disabled or actual queue shaper rate - e.g. "800 Mbps"

Port	Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".



When clicking on any port number, a new page is loaded to configure the Scheduler and Shapers for that specific port of the switch. The page is the same one loaded from the Port Scheduler option and all its settings are already explained in the previous section of this manual.

3.10.10 DSCP-Based QoS

This page allows the user to display and configure the basic DSCP based QoS Ingress Classification settings for the switch. For the 64 DSCP values is possible to set:

Trust

Setting	Description	Factory Default
Check / Uncheck	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.	Unchecked

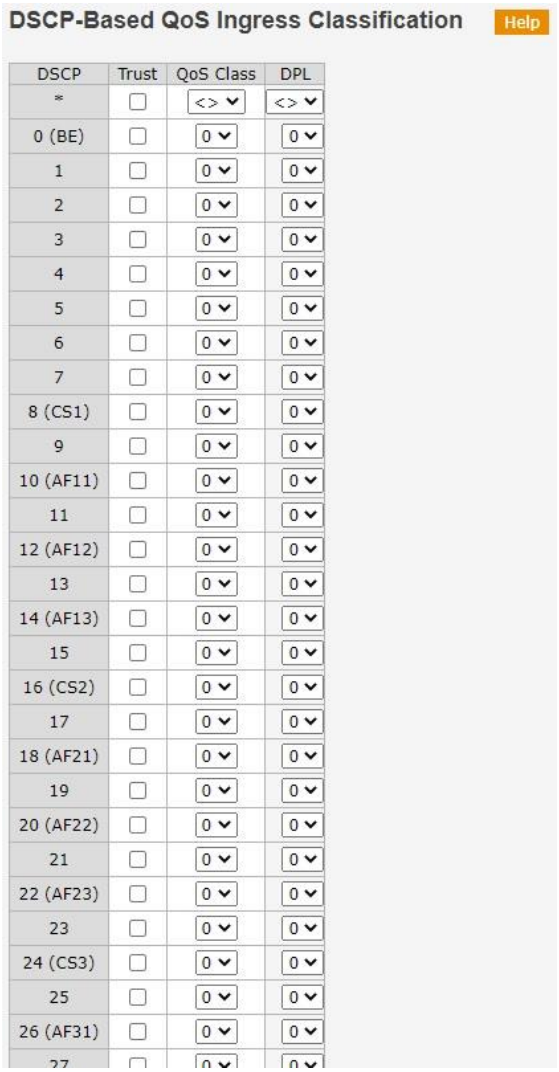
QoS Class

Setting	Description	Factory Default
0 to 7	Quality of Service Class value (CoS). A CoS of 0 (zero) has the lowest priority.	0

DPL

Setting	Description	Factory Default
0 to 1	Drop precedence level (DP). A DP level of 0 corresponds to committed frames and a DP level of 1	0

	corresponds to discard eligible frames.	



3.10.11 DSCP Translation

This page allows the user to configure QoS DSCP translation settings for the switches. DSCP translation can be done in Ingress or Egress.

For the 64 DSCP values is possible to set:

Ingress Translate

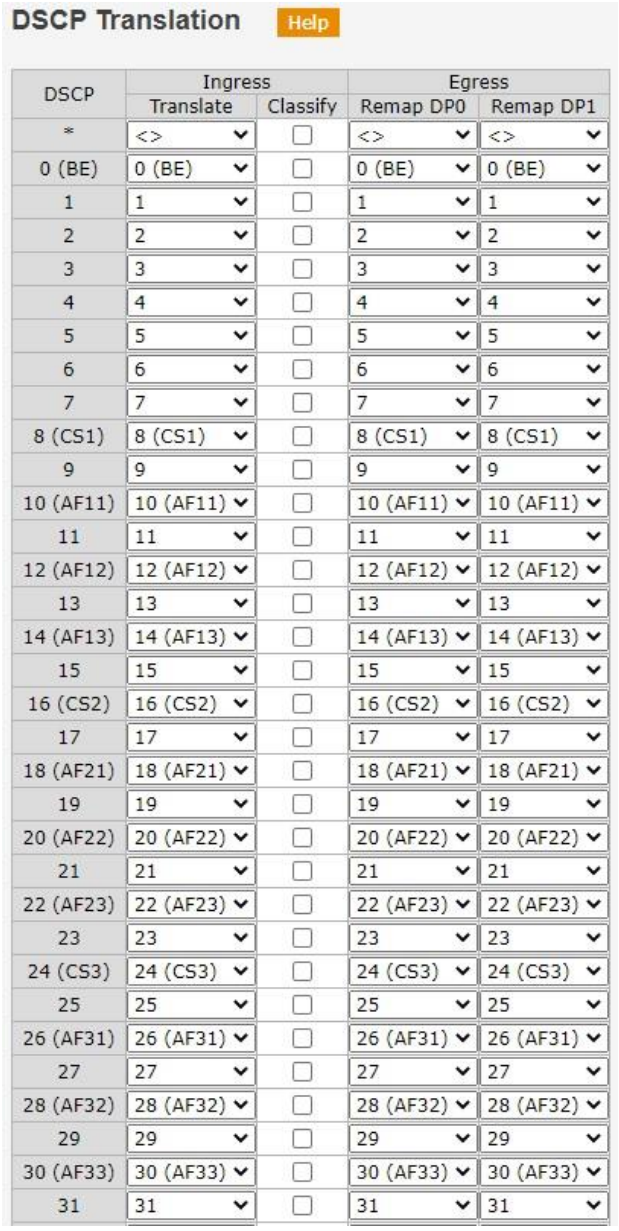
Setting	Description	Factory Default
0 to 63	Before using the DSCP for classification is possible to first translate the ingress side DSCP to new DSCP values.	0 to 63

Ingress Classification

Setting	Description	Factory Default
Check / Uncheck	Check to enable classification at ingress side.	Unchecked

Egress Remap DP0 and DP1

Setting	Description	Factory Default
0 to 63	Controls the remapping for frames with DP level 0 and DP level 1. The user can select the DSCP value from a selected menu to which is desired to remap.	0 to 63



3.10.12 DSCP Classification

This page allows the user to configure the mapping of QoS class and Drop Precedence Level to DSCP value.

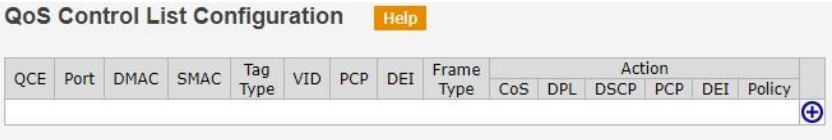
For the actual QoS (0 to 7) the user can set the classified DSCP value.

DSCP DP0 and DP1

Setting	Description	Factory Default
0 to 63	Select the classified DSCP value for frames with Drop Precedence Level 0 and Drop Precedence Level 1.	0

3.10.13 QoS Control List

This page shows the QoS Control List, which is made up of the QCEs (QoS Control Entry). Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.



Clicking the plus sign, a new web page is loaded and can be used to any QCE.

Port Members

Setting	Description	Factory Default
Check/Uncheck	A row of check boxes for each port. Check the box to include the port in the QCL entry.	Checked

Key Parameters - DMAC

Setting	Description	Factory Default
Any / Unicast / Multicast / Broadcast	Indicates the destination MAC address for incoming frames. Any: All types of DMAC addresses are allowed. Unicast: Only Unicast DMAC addresses are allowed. Multicast: Only Multicast DMAC addresses are allowed. Broadcast: Only Broadcast DMAC addresses are allowed.	Any

Key Parameters - SMAC

Setting	Description	Factory Default
Any / Specific	Indicates the source MAC address for incoming frames. Any: All types of SMAC addresses are allowed. Specific: Type the specific source MAC address allowed.	Any

Key Parameters - Tag

Setting	Description	Factory Default
Any / Untagged / Tagged / C-Tagged / S-Tagged	Indicates the tag type for incoming frames. Any: Untagged and tagged frames are allowed. Untagged: Only untagged frames are allowed. Tagged: Only tagged frames are allowed. C-Tagged: Only C-tagged frames are allowed. S-tagged: Only S-tagged frames are allowed.	Any

Key Parameters - VID

Setting	Description	Factory Default
Any / 1 to 4095	Valid value of VLAN ID. Can be any value in the range 1-4095 or ‘Any’.	Any

Key Parameters - PCP

Setting	Description	Factory Default
Any / 0 to 7 / ranges	Valid value of Priority Code Point (PCP). Can be any value in the range 1-7 or 'Any'.	Any

Key Parameters - DEI

Setting	Description	Factory Default
Any / 0 / 1	Valid value of Drop Eligible Indicator (DEI). Can be 'Any', 0 or 1.	Any

Key Parameters – Frame Type

Setting	Description	Factory Default
Any / Ethertype / LLC / SNAP / IPv4 / IPv6	Indicates the type of incoming frame allowed among the several possibilities.	Any

Key Parameters – Frame Type - Ethertype

Setting	Description	Factory Default
Any / Specific	Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.	Any

Key Parameters – Frame Type - LLC

Setting	Description	Factory Default
DSAP address / SSAP address / Control	DSAP address: Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'. SSAP address: Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'. Control: Valid Control field can vary from 0x00 to 0xFF or 'Any'.	Any

Key Parameters – Frame Type - SNAP

Setting	Description	Factory Default
Any / Specific	Valid PID (Parameter Identification) values can range from 0x00 to 0xFFFF or 'Any'.	Any

Key Parameters – Frame Type – IPv4

Setting	Description	Factory Default
Protocol	TCP, UDP, Other (value from 0 to 255) or 'Any'. When selecting TCP or UDP, the following additional parameters have to be configured: Sport (Source TCP/UDP Port): Specific value (0 to 65535) or 'Any'. Dport (Destination TCP/UDP Port): Specific value (0 to 65535) or 'Any'.	Any
SIP	Specific Source IP address in value/mask format or 'Any'.	Any
IP fragment	IPv4 frame fragmented options are 'Yes', 'No' or 'Any'.	Any
DSCP	It can be a specific value, a range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.	Any

Key Parameters – Frame Type – IPv6

Setting	Description	Factory Default
Protocol	TCP, UDP, Other (value from 0 to 255) or 'Any'. When selecting TCP or UDP, the following additional parameters have to be configured: Sport (Source TCP/UDP Port): Specific value (0 to 65535) or 'Any'. Dport (Destination TCP/UDP Port): Specific value (0 to 65535) or 'Any'.	Any
SIP	Specific Source IP address (32LS bits in value/mask format) or 'Any'.	Any
DSCP	It can be a specific value, a range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.	Any

Action Parameters

Indicate the classification action taken on ingress frame if the parameters configured in the QCE match with the frame's content.

Action Parameters - CoS

Setting	Description	Factory Default
Default, 0 to 7	Classified Class of Service. 'Default' means that the default classified value is not modified by this QCE.	Default

Action Parameters – DPL

Setting	Description	Factory Default
Default, 0 or 1	Drop Precedence Level 0, 1 or Default. 'Default' means that the default classified value is not modified by this QCE.	Default

Action Parameters – DSCP

Setting	Description	Factory Default
Default, 0 to 63	DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) or Default. 'Default' means that the default classified value is not modified by this QCE.	Default

Action Parameters – PCP

Setting	Description	Factory Default
Default, 0 to 7	PCP from 0 to 7 or Default. 'Default' means that the default classified value is not modified by this QCE.	Default

Action Parameters – DEI

Setting	Description	Factory Default
Default, 0 or 1	DEI 0, 1 or Default. 'Default' means that the default classified value is not modified by this QCE.	Default

Action Parameters – Policy

Setting	Description	Factory Default
0 to 255	ACL Policy number (0 to 255) or empty field.	None

3.10.14 QoS Statistics

This page provides statistics for the different queues for all switch ports.

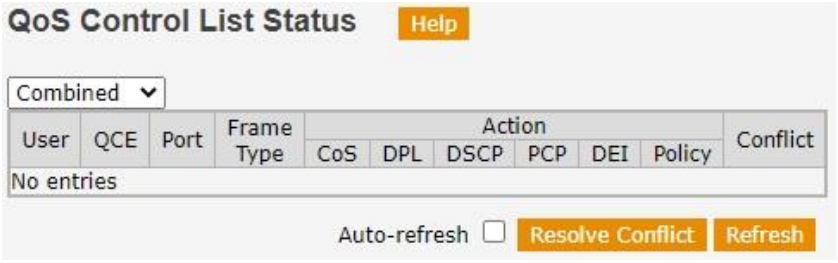
The following information of each port is displayed on the page:

Q0 – Q7	There are 8 queues per port. Q0 is the lowest priority queue.
Rx / Tx	The number of received and transmitted packets per queue.

3.10.15 QCL Status

This page shows the QCL (Quality of Service Control List) status by different QCL users. Each row describes the QCE (Quality of Service Control Entry) that is defined. The maximum number of QCEs is 256 on each switch.

As HW resources are shared by multiple applications, it may happen that resources required to add a QCE may not be available. In that case, the page shows conflict status as 'Yes'; otherwise it is always 'No'. The conflict can be resolved by releasing the HW resources required to add the QCL entry on pressing **Resolve Conflict** button.



The following information can be displayed on the page:

User	Indicates the QCL user.
QCE	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: Any: The QCE will match all frame type. Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC: Only (LLC) frames are allowed. SNAP: Only (SNAP) frames are allowed. IPv4: The QCE will match only IPV4 frames.

	IPv6: The QCE will match only IPV6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are six action fields: CoS: Classified QoS class; if a frame matches the QCE, it will be put in the queue. DPL: Drop Precedence Level; if a frame matches the QCE, then DP level will set to a value displayed under DPL column. DSCP: If a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column. PCP: : If a frame matches the QCE, then PCP will be classified with the value displayed under PCP column. DEI: If a frame matches the QCE, then DEI will be classified with the value displayed under DEI column. Policy: If a frame matches the QCE, then ACL policy number will be displayed under Policy column.
Conflict	Displays ‘Yes’ if there is a HW conflict related with the created QCE. Otherwise displays ‘No’.

3.11 Multicast

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your Weidmüller switch.

3.11.1 The Concept of Multicast Filtering

What is an IP Multicast?

A *multicast* is a packet sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations on a LAN or VLAN that belong to the multicast group. Multicast group members can be distributed across multiple subnets, so that multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only *one* copy of the desired information across the network until the delivery path that reaches group members diverges. To make more efficient use of network bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

The benefits of using IP multicast are:

- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- It works with other IP protocols and services, such as Quality of Service (QoS).

Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of

traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all end-stations would cause a substantial reduction in network performance. Furthermore, the GOOSE messages and SAMPLED VALUES defined in the IEC 61850 standard are multicast and use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic.

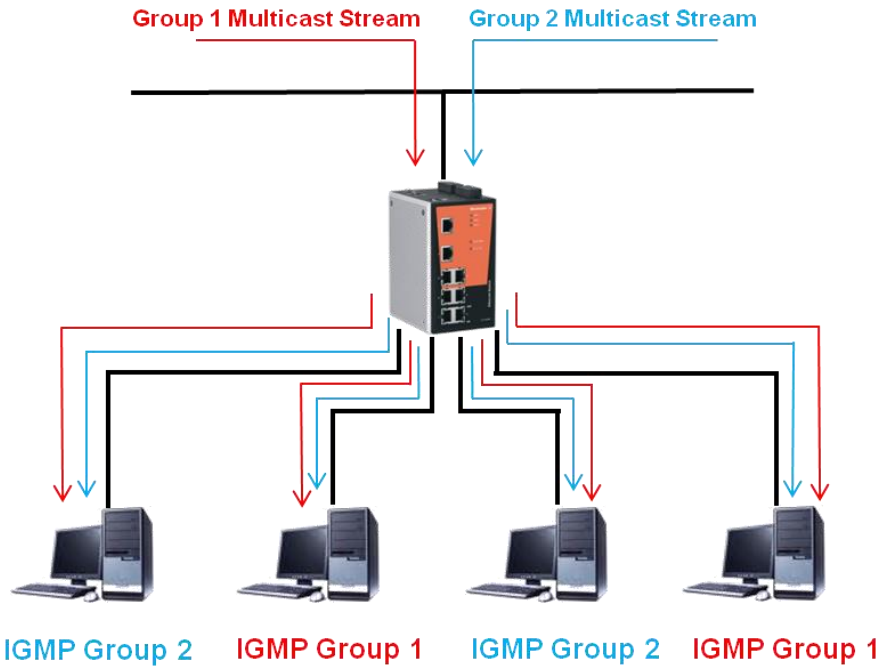
IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves without multicast filtering, and with multicast filtering.

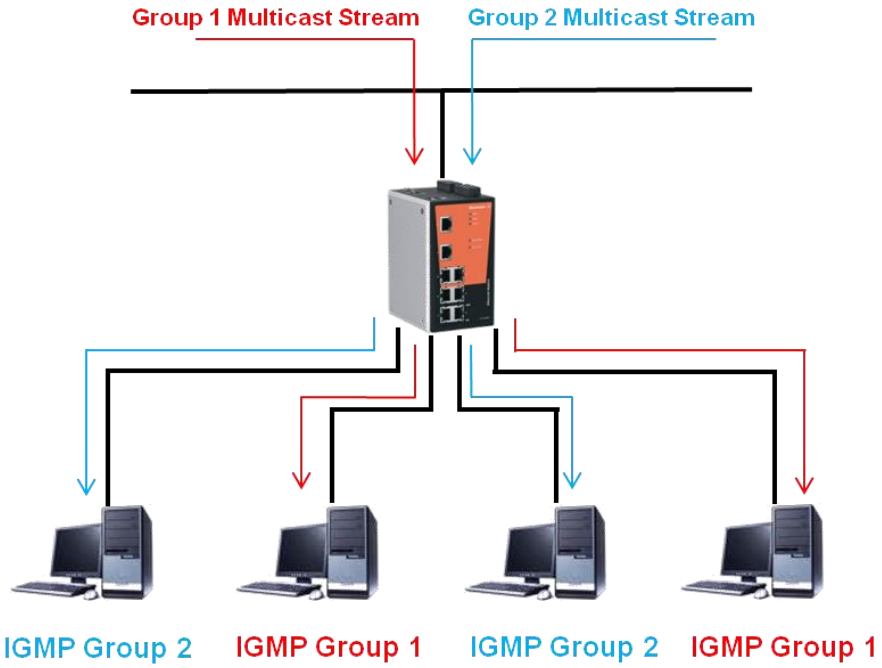
Network without multicast filtering

All hosts receive the multicast traffic, even if they don't need it.



Network with multicast filtering

Hosts only receive dedicated traffic from other hosts belonging to the same group.



The Weidmüller switch supports multicast filtering with both IGMP (Internet Group Management Protocol) Snooping and MLD (Multicast Listener Discovery) Snooping. MLD is the IPv6 equivalent of IGMP.

IGMP / MLD

Snooping Mode

Snooping Mode allows your switch to forward multicast packets only to the appropriate ports. The switch "snoops" on exchanges between hosts and an IGMP/MLD device, such as a router, to find those ports that want to join a multicast group, and then configure its filters accordingly.

Querier Mode

Querier mode allows the Weidmüller switch to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs. Enable query mode to run multicast sessions on a network that does not contain IGMP/MLD routers (or queriers).

IGMP Multicast Filtering

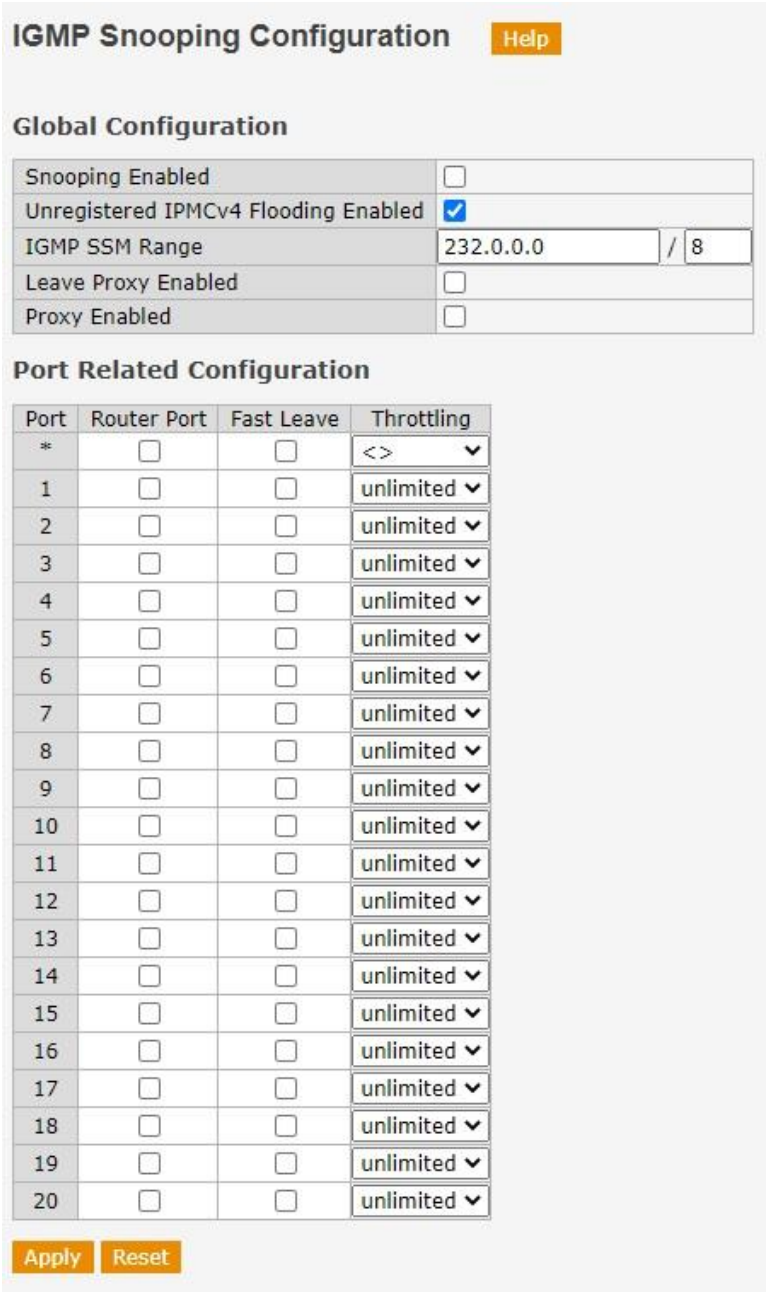
IGMP/MLD is used by IP-supporting network devices to register hosts with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router, and on other network devices that support multicast filtering.

- The IP router (or querier) periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with IP address lower than the IP address of any other IGMP/MLD querier connected to the LAN or VLAN can become the IGMP/MLD querier.
- When an IP host receives a query packet, it sends a report packet back that identifies the multicast group that the end-station would like to join.
- When the report packet arrives at a port on a switch with IGMP/MLD Snooping enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.

- When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
- When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

3.11.2 IGMP Snooping Basic Configuration

IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.



Global Configuration

Snooping Enabled

Setting	Description	Factory Default
Check/Uncheck	Enable the IGMP Snooping function globally.	Unchecked

Unregister IPMCv4 Flooding Enabled

Setting	Description	Factory Default
Check/Uncheck	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.	Checked

IGMP SSM Range

Setting	Description	Factory Default
IP address and prefix length	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.	232.0.0.0/8

Leave Proxy Enabled

Setting	Description	Factory Default
Check/Uncheck	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.	Unchecked

Proxy Enabled

Setting	Description	Factory Default
Check/Uncheck	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.	Unchecked

Port Related Configuration

Router Port

Setting	Description	Factory Default
Check/Uncheck	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.	Unchecked

Fast Leave

Setting	Description	Factory Default
Check/Uncheck	Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the leave message without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.	Unchecked

Throttling

Setting	Description	Factory Default
Unlimited / 1 to 10	The user can limit the number of multicast groups to which a port/switch port can belong.	Unlimited

3.11.3 IGMP Snooping VLAN Configuration

The page shows up to 99 entries from the VLAN table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN table. The first displayed will be the one with the lowest VLAN ID found in the VLAN table. The **Start from Control Index** field allows the user to select the starting point in the VLAN table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN table match.

Press the button **Add New IGMP VLAN** to create a new entry enabling per-VLAN IGMP snooping.

VLAN ID

Setting	Description	Factory Default
VLAN ID number	The VLAN ID of the entry.	None

Snooping Enabled

Setting	Description	Factory Default
Check/Uncheck	Enable the per-VLAN IGMP snooping. Up to 32 VLANs can be selected.	Unchecked

Querier Election

Setting	Description	Factory Default
Check/Uncheck	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.	Checked

Querier Address

Setting	Description	Factory Default
IP address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address.	None

Compatibility

Setting	Description	Factory Default
IGMP-Auto / Forced IGMPv1 / Forced IGMPv2 / Forced IGMPv3	Select the IGMP version. Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.	IGMP-Auto

PRI

Setting	Description	Factory Default
0 to 7	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic (0-best effort to 7-highest).	0

RV

Setting	Description	Factory Default
1 to 255	Robustness Variable. It allows tuning for the expected packet loss on a network.	2

QI

Setting	Description	Factory Default
1 to 31774 (sec)	Query Interval. It is the interval (in sec) between General Queries sent by the Querier.	125

QRI

Setting	Description	Factory Default
1 to 31774 (tenths of sec)	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.	100 (10 sec)

LLQI

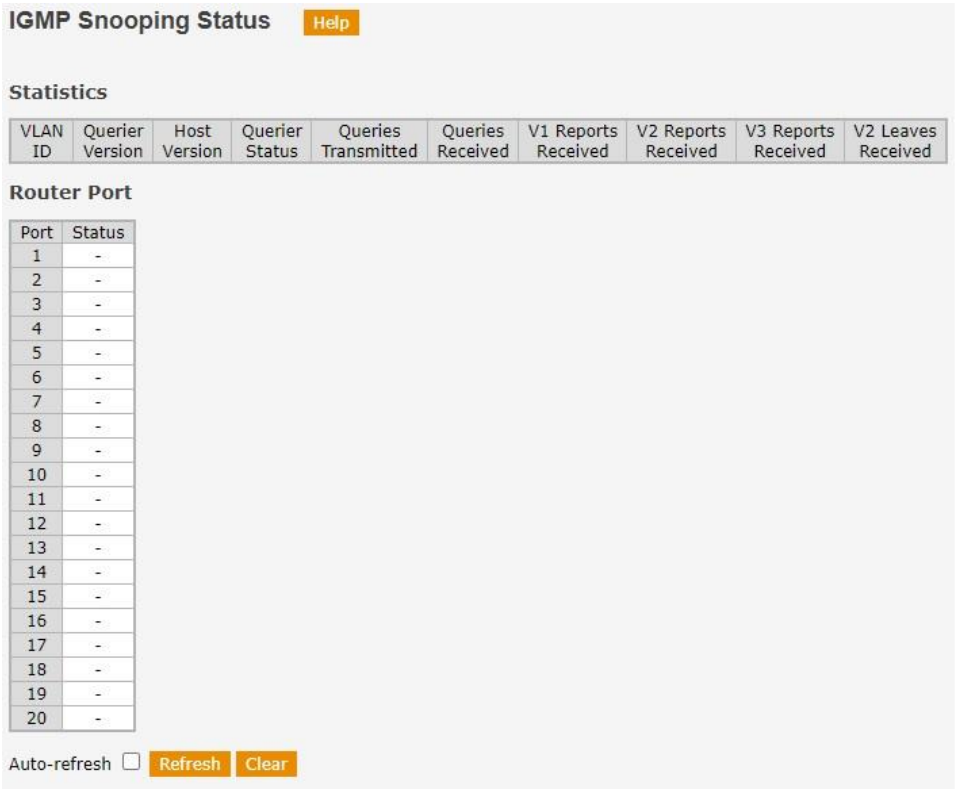
Setting	Description	Factory Default
1 to 31774 (tenths of sec)	Last Member Query Interval. It is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.	10 (1 sec)

URI

Setting	Description	Factory Default
1 to 31774 (sec)	Unsolicited Report Interval. It is the time between repetitions of a host's initial report of membership in a group.	1

3.11.4 IGMP Snooping Status

This page provides IGMP Snooping status.



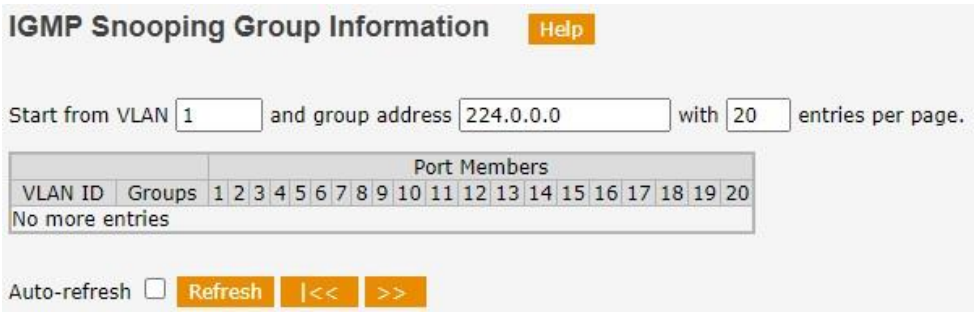
The following information can be displayed on the page:

VLAN ID	The VLAN ID of the entry.
Querier Version	Current working Querier version.
Host Version	Current working Host version.
Querier Status	Querier status (ACTIVE or IDLE).
Querier Transmitted	The number of transmitted queriers.
Querier Received	The number of received queriers.

V1 Reports Received	The number of received V1 reports.
V2 Reports Received	The number of received V2 reports.
V3 Reports Received	The number of received V3 reports.
V2 Leaves Received	The number of received V2 leave packets.
Port	Switch port number.
Status	Indicates whether the specific port is a router port or not.

3.11.5 IGMP Snooping Group Information

The page shows up to 99 entries from the IGMP Group table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group table. The **Start from VLAN** and **Group Address** fields allows the user to select the starting point in the IGMP Group table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest IGMP Group table match.



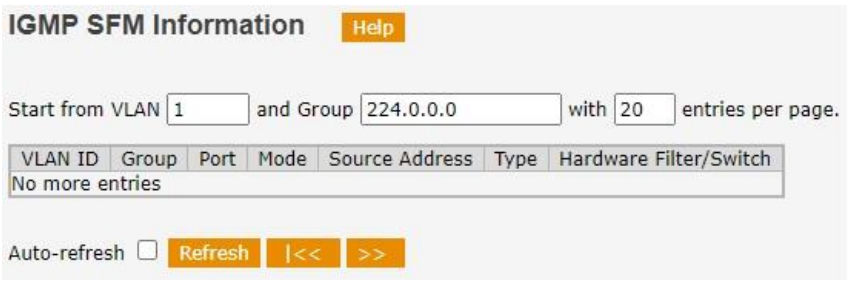
The following information can be displayed on the page:

VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

3.11.6 IGMP SFM Information

The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belonging to the same group are treated as single entry.

The page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information table. The **Start from VLAN** and **Group** fields allows the user to select the starting point in the IGMP SFM Information table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest IGMP SFM Information table match.

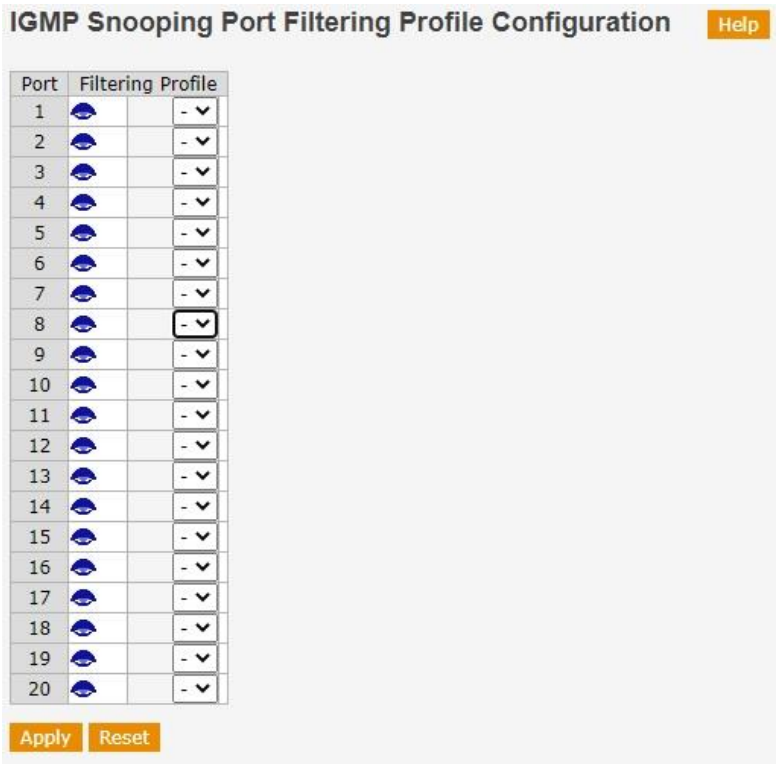


The following information can be displayed on the page:

VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per basis (VLAN ID, port number, Group Address). It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is not any source filtering address, the text "None" is shown in the Source Address field.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

3.11.7 IGMP Snooping Port Group Filtering

In this page the user can apply the created IPMC entries to specific ports of the switch. IPMC entries are created in the option “IPMC Profile Configurations” described in the next section of this manual.



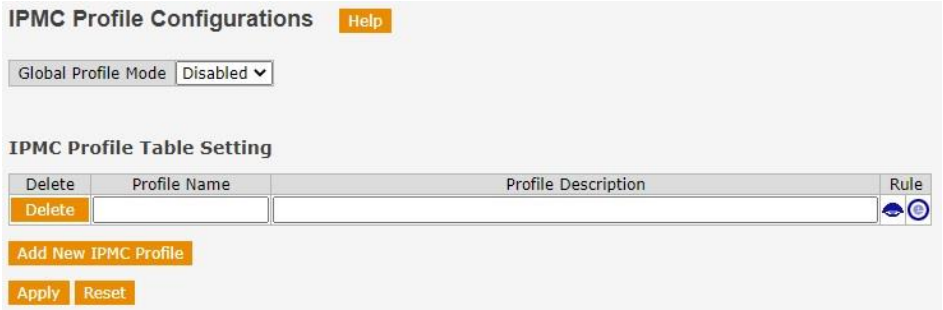
For each port of the switch, the user can select the Filtering profile:

Filtering profile

Setting	Description	Factory Default
Select IPMC profile entry from a list	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button. Note: No available IPMC Profiles by default. It is necessary to create them with the option IPMC Profile Configurations.	None

3.11.8 IPMC Profile Configurations

In certain applications, the administrator may want to control the multicast services that are available to end users. The IPMC (IP Multicast) profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with a maximum of 128 corresponding rules for each.



Global Profile Mode

Setting	Description	Factory Default
Enabled/Disabled	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.	Disabled

Using the **Add New IPMC Profile** button the user can create the different Profile entries.

Profile Name

Setting	Description	Factory Default
Max 16 characters	The name used for indexing the profile table. Each entry must have a unique name (at least one alphabet character).	None

Profile Description

Setting	Description	Factory Default
Max 64 characters	Additional description about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.	None

Rule

Setting	Description	Factory Default
Rule setting	When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons: : List the rules associated with the designated profile. : Adjust the rules associated with the designated profile. Note: The address entry required for the IPMC profile has to be created in the section “IPMC Profile Address Configuration”.	None

3.11.9 IPMC Profile Address Configuration

This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create a maximum of 128 address entries in the system.

Using the **Add New Address (Range) Entry** button the user can create the different Profile entries.

Entry Name

Setting	Description	Factory Default
Max 16 characters	The name used for indexing the address entry table. Each entry must have a unique name (at least one alphabet character).	None

Start Address / End address

Setting	Description	Factory Default
Multicast IP address	The starting and ending IPv4/IPv6 Multicast Group Addresses that will be used as an address range.	None

3.11.10 MLD Snooping

The same options described for IGMP in previous sections (Basic Configuration, VLAN Configuration, Status, Groups Information, IP SFM Information and Port Group Filtering) are also available for MLD protocol in case multicast of IPv6 traffic in required.

3.12 Security

Security can be categorized in two levels: the user name/password level, and the port access level.

For both levels Weidmüller switches provide a wide range of options that allow the user to meet the security requirements of different applications.

For user name/password level security, Weidmüller switches provide the possibility to enable/disable any possible access to the management of the device and also provide the login option through Terminal Access Controller Access-Control System Plus (TACACS+) or Remote Access Dial-In User Service (RADIUS). The TACACS+ and RADIUS mechanisms are centralized “AAA” (Authentication, Authorization and Accounting) systems for connecting to network services.

Regarding the port access level, the switches provide three kinds of Port-Based Access Control:

- **Static Port Lock, either using MAC or IP addresses**
- **Access Control Lists**
- **IEEE 802.1X**

Static Port Lock

In this case the Weidmüller switch can be configured to protect both static MAC and IP addresses for a specific port. With the different available functions (Device binding, IP source guard, Port security), these locked ports will only allow traffic from preset static MAC/IP addresses, helping to block hackers and careless usage.

Access Control Lists

The user can create specific access lists for any port of the switch. In these access lists is possible to permit or deny any kind of ingress Ethernet and/or IP traffic.

Access control according IEEE 802.1X

The IEEE 802.1X standard defines a protocol for client/server-based access control and authentication. The protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet, and which otherwise would be readily accessible. The purpose of the authentication server is to check each client that requests access to the port. The client is only allowed access to the port if the client's permission is authenticated.

Three components are used to create an authentication mechanism based on 802.1X standards: Client/Supplicant, Authentication Server, and Authenticator.

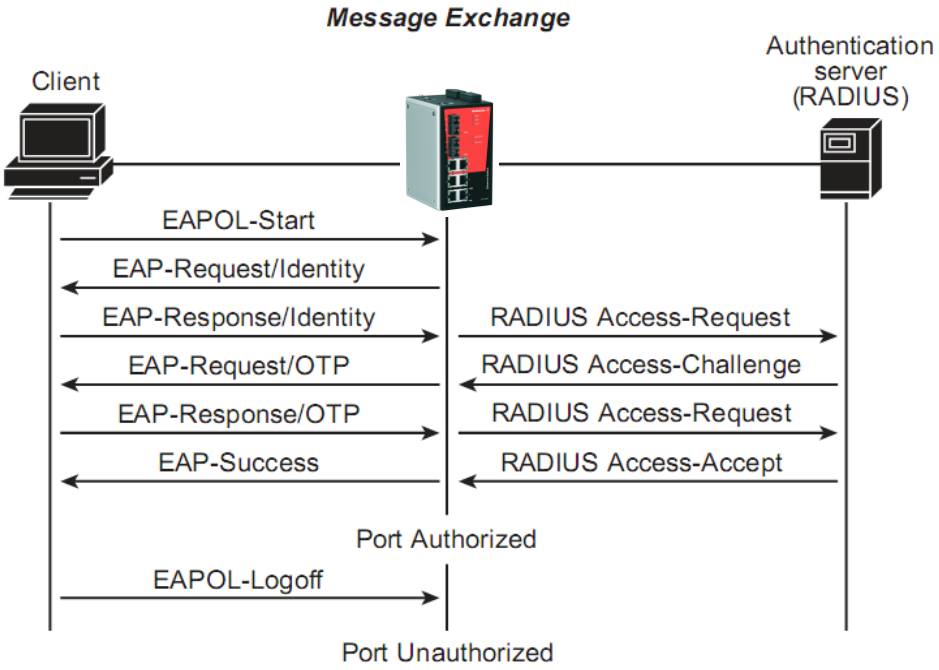
Client/Supplicant: The end station that requests access to the LAN and switch services and responds to the requests from the switch.

Authentication server: The server that performs the actual authentication of the supplicant.

Authenticator: Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant.

The Weidmüller switch acts as an authenticator in the 802.1X environment. A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other.

Authentication can be initiated either by the supplicant or the authenticator. When the supplicant initiates the authentication process, it sends an **EAPOL-Start** frame to the authenticator. When the authenticator initiates the authentication process or when it receives an **EAPOL Start** frame, it sends an **EAP Request/Identity** frame to ask for the username of the supplicant. The following actions are described below:

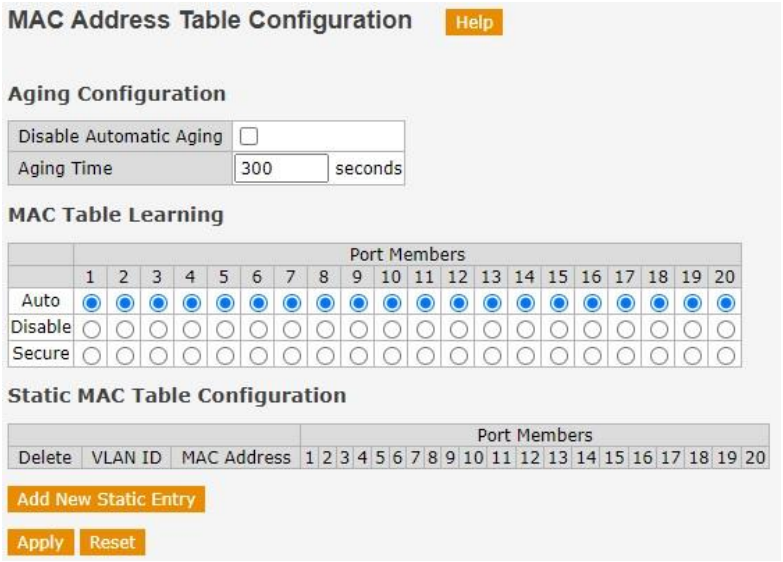


1. When the supplicant receives an "EAP Request/Identity" frame, it sends an "EAP Response/Identity" frame with its username back to the authenticator.
2. The authenticator relays the "EAP Response/Identity" frame from the supplicant by encapsulating it into a "RADIUS Access-Request" frame and sends to the RADIUS server. When the authentication server receives the frame, it looks up its database to check if the username exists. If the username is not present, the authentication server replies with a "RADIUS Access-Reject" frame to the authenticator if the server is a RADIUS server or just indicates failure to the authenticator if the Local User Database is used. The authenticator sends an "EAP-Failure" frame to the supplicant.
3. The RADIUS server sends a "RADIUS Access-Challenge," which contains an "EAP Request" with an authentication type to the authenticator to ask for the password from the client.
4. The authenticator sends an "EAP Request/Challenge" frame to the supplicant. The "EAP Request/Challenge" frame is retrieved directly from the "RADIUS Access-Challenge" frame.
5. The supplicant responds to the "EAP Request/Challenge" by sending an "EAP Response/Challenge" frame that encapsulates the user's password.
6. The authenticator relays the "EAP Response/ Challenge" frame from the supplicant by encapsulating it into a "RADIUS Access-Request" frame along with a "Shared Secret," which must be the same within the authenticator and the RADIUS server, and sends the frame to the RADIUS server. The RADIUS server checks against the password with its database, and replies with "RADIUS Access-Accept" or "RADIUS Access-Reject" to the authenticator.

7. The authenticator sends "EAP Success" or "EAP Failure" based on the reply from the authentication server.

3.12.1 MAC Address Table Configuration

The user can configure the MAC Address Table on this page. It is possible to set timeouts for entries in the dynamic MAC Table as well as configure the static MAC table.



Aging Configuration

Disable Automatic Aging

Setting	Description	Factory Default
Check / Uncheck	By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is called aging. It is possible to de-activate the automatic aging of dynamic entries by checking Disable Automatic Aging.	Unchecked

Aging time

Setting	Description	Factory Default
10 to 1000000 (sec)	Configure specific aging time.	300

MAC Table Learning

Port Members

Setting	Description	Factory Default
Auto / Disable / Secure	Each port can be configured to dynamically learn the MAC address based upon the following settings: Auto: Learning is done automatically as soon as a frame with unknown Source MAC address is received. Disable: No learning is done.	Auto

	Secure: Only static MAC entries are learned, all other frames are dropped.	

NOTE: If the setting of the port for the MAC Table Learning is Secure, make sure the link used for managing the switch is added to the static MAC table before saving. Otherwise the management link will be lost and can only be restored by using another non-secure port, by connecting to the switch via the serial interface or by restoring the default values.

NOTE: If the learning mode for a given port is grayed out, it means the user cannot change the configurations because of the current programming of the switch. An example of such programming is MAC-Based authentication under 802.1X.

Static MAC Table Configuration

Press the button **Add New Static Entry** to add a new entry to the static MAC address table. An empty row is added to the table and the static MAC entry can be configured as needed. The static MAC table can contain up to 64 entries.

The **Delete** button can be used to undo the addition of new static MAC entries.

VLAN ID

Setting	Description	Factory Default
1 to 4095	The VLAN ID of the entry.	1

MAC Address

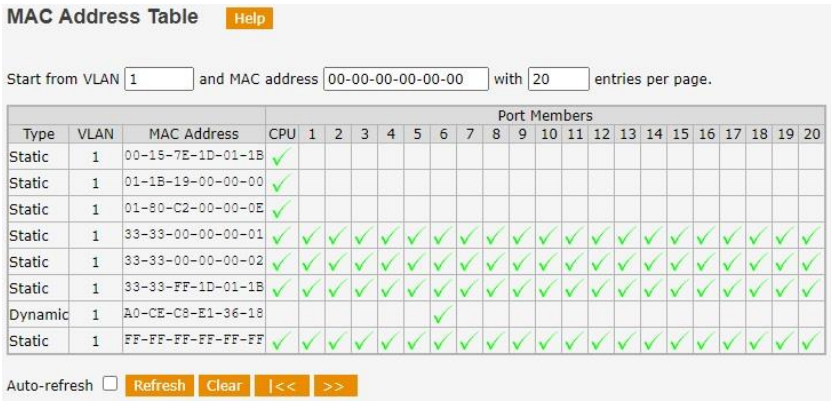
Setting	Description	Factory Default
MAC Address	The MAC address of the entry.	None

Port Members

Setting	Description	Factory Default
Check / Uncheck	Indicate (check) which ports are member of the entry.	Unchecked

3.12.2 MAC Address Table Status

This page provides an overview of the MAC table entries. The page shows up to 999 entries from the MAC table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC table. The first displayed will be the one with the lowest VLAN ID and lowest MAC found in the table. The **Start from MAC address** and **Start from VLAN ID** fields allow the user to select the starting point in the MAC table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest MAC table match.

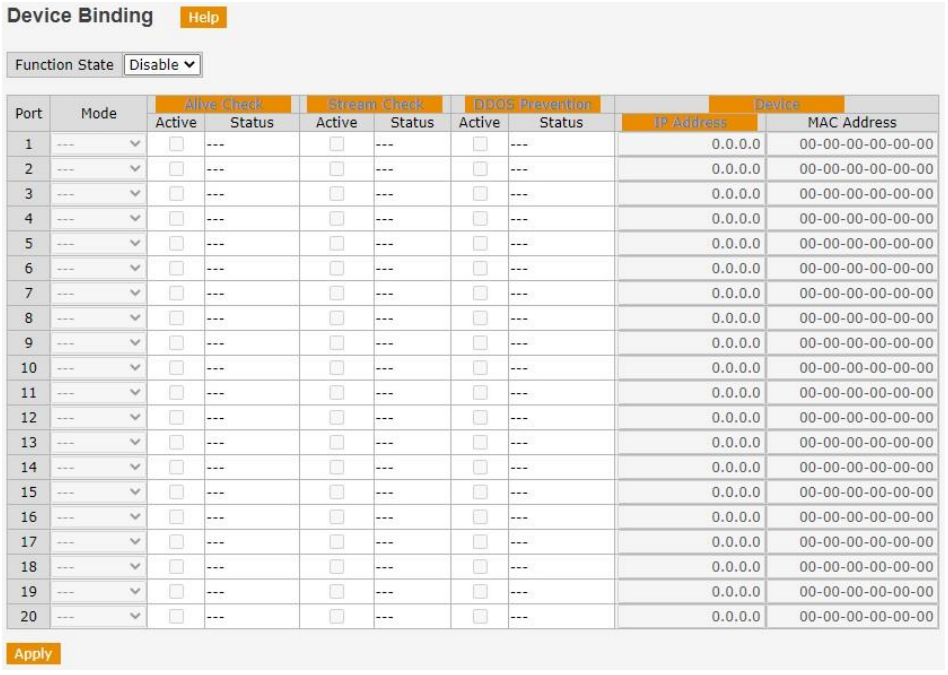


The page includes a table with the following information:

Type	Indicates whether the entry is static or dynamic.
VLAN	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	The ports that are members of the entry.

3.12.3 Device Binding

This page provides Device Binding related configuration. Device Binding is a powerful monitor tool for devices and network security.



Function State

Setting	Description	Factory Default
Enabled/Disabled	Enable/Disable Device Binding.	Disabled

Mode

Setting	Description	Factory Default
--- / Scan / Binding / Shutdown	The Mode configuration is only possible when Device Binding function is enabled. The possible states for each port are: ---: Device Binding disabled in that port. Scan: Scans IP/MAC automatically, but no binding function executed in the port. Binding: Binding function enabled in the port. Under this mode, any IP/MAC that does not match the entry will not be allowed to access the network. Shutdown: Disables the port (No Link).	---

Alive Check Active / Status

Setting	Description	Factory Default
Enable/Disable	When enabled, the switch will ping the device continuously. The Status column indicates the alive check status: Got Reply: Receiving ping reply from device. Lost Reply: Not receiving ping reply from device.	Disabled

Stream Check Active / Status

Setting	Description	Factory Default
Enable/Disable	When enabled, the switch will detect the stream change (getting low) from device. The Status column indicates the alive check status: Normal: The stream is normal. Low: The stream is getting low.	Disabled

DDOS Prevention Active / Status

Setting	Description	Factory Default
Enable/Disable	When enabled, the switch will monitor the device against DDOS (Distributed Denial of Service) attack. The Status column indicates the alive check status: Analyzing: Analyze the packet throughput for initialization. Running: Function ready. Attacked: DDOS attack happened.	Disabled

Device IP Address

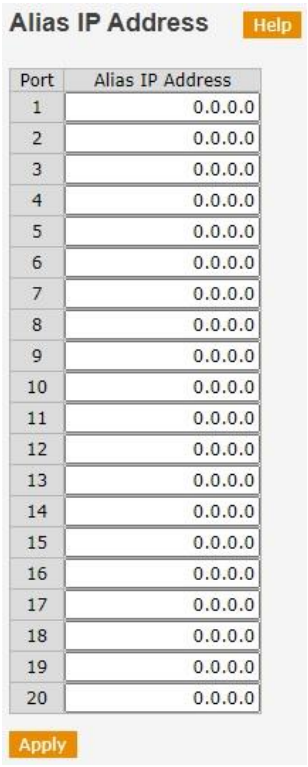
Setting	Description	Factory Default
IP address	If the Mode configuration is ‘Scan’, this field indicates the IP address detected. If the Mode configuration is ‘Binding’, this field must specify the IP address of the authorized device.	None

Device MAC Address

Setting	Description	Factory Default
MAC address	If the Mode configuration is ‘Scan’, this field indicates the MAC address detected. If the Mode configuration is ‘Binding’, this field must specify the MAC address of the authorized device.	None

3.12.3.1 Alias IP Address

Some devices might have more than one IP address. In this page is possible to specify alternative IP addresses (alias IP addresses).

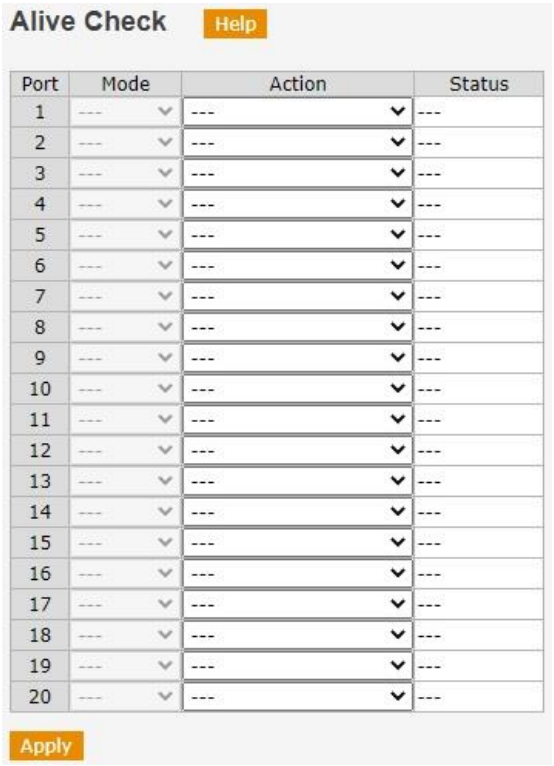


Alias IP Address

Setting	Description	Factory Default
IP address	Specify Alias IP address. Keep "0.0.0.0", if the device doesn't have alias IP address.	None

3.12.3.2 Alive Check

This page provides additional configuration options for the Alive Check function on each port.



Mode

Setting	Description	Factory Default
Enable / Disable	Enable or Disable (---) the Alive Check option on the port. Note: If the Binding function is not enabled on a port, it will not be possible to enable the Alive Check option. Binding function is enabled in the Device Binding page.	--- (Disabled)

Action

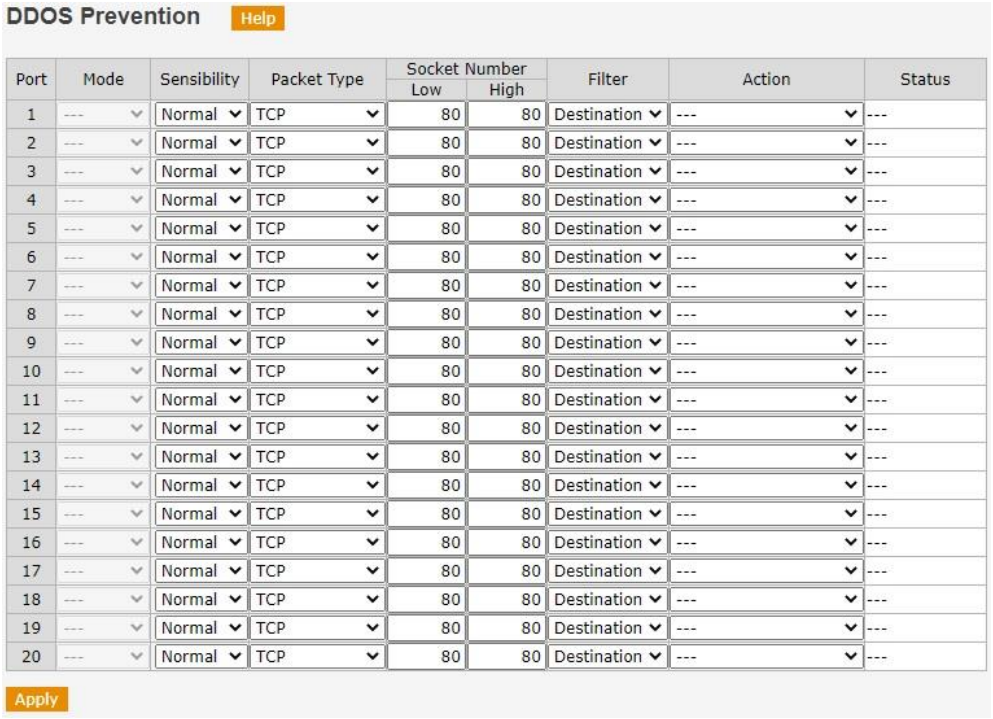
Setting	Description	Factory Default
Link Change / Only Log it / Shut Down the Port	Indicates the action when Alive check fails (Lost Reply). The possible actions to be configured are: Link Change: Link down the port and link up once. Only Log it: Just log the event. Shut Down the Port: Disable the port.	--- (Disabled)

Status

Setting	Description	Factory Default
Information only	Indicates the Alive Check status. ---: Disabled Got Reply: Receiving ping reply from device. Lost Reply: Not receiving ping reply from device.	--- (Disabled)

3.12.3.3 DDOS Prevention

This page provides DDOS (Distributed Denial of Service) Prevention related configuration options. The switch could monitor the ingress packets and do some actions when DDOS attack happened on any specific port.



Mode

Setting	Description	Factory Default
Enable / Disable	Enable or Disable (---) the DDOS Prevention option on the port. Note: If the Binding function is not enabled on a port, it will not be possible to enable the DDOS Prevention option. Binding function is enabled in the Device Binding page.	--- (Disabled)

Sensibility

Setting	Description	Factory Default
Low / Normal / Medium / High	Indicates the level of DDOS detection. Possible levels are: Low: Low sensibility. Normal: Normal sensibility. Medium: Medium sensibility. High: High sensibility.	Normal

Packet Type

Setting	Description	Factory Default
Low / Normal / Medium / High	Indicates the type of DDoS attack packets to be monitored. Possible types are: Rx Total: Total ingress packets.	TCP

	Rx Unicast: Unicast ingress packets. Rx Multicast: Multicast ingress packets. Rx Broadcast: Broadcast ingress packets. TCP: TCP ingress packets. UDP: UDP ingress packets.	

Socket Number

Setting	Description	Factory Default
Socket number	If the packed type is TCP or UDP, the socket number has to be specified. It is possible to specify a range (from Low to High) If the socket number is one, fill the same number in fields Low and High.	80

Filter

Setting	Description	Factory Default
Destination / Source	If the packet type is TCP or UDP, the socket direction has to be specified (Destination or Source).	Destination

Action

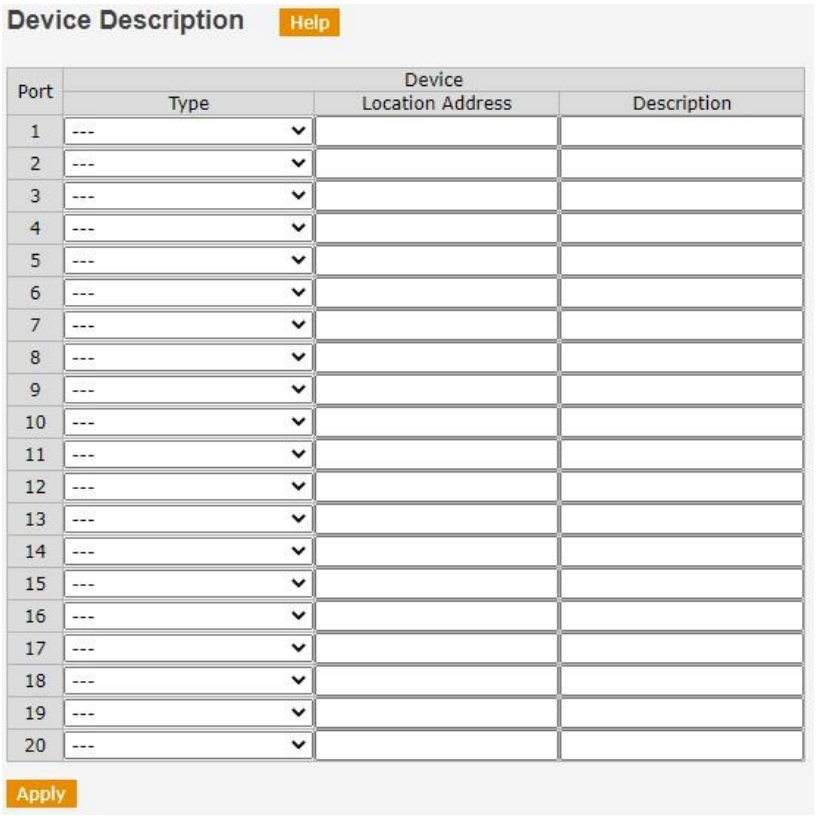
Setting	Description	Factory Default
Blocking 1 minute / Blocking 10 minutes / Blocking / Shut Down the Port / Only Log it	Indicates the action when DDOS attack happens. The possible actions to be configured are: ---: No action or Disabled Blocking 1 minute: Block the port for 1 minute and log the event.. Blocking 10 minutes: Block the port for 10 minutes and log the event. Blocking: Block the port and log the event. Shut Down the Port: Disable the port and log the event. Only Log it: Just log the event.	--- (Disabled)

Status

Setting	Description	Factory Default
Information only	Indicates the DDOS Prevention status. ---: Disabled Analyzing: Analyze the packet throughput for initialization. Running: Function ready. Attacked: DDOS attack happened.	--- (Disabled)

3.12.3.4 Device Description

From this option it can be specified a description and a location for each port to help administrators differentiate between different ports.



Type

Setting	Description	Factory Default
Select from a list	Indicates device types. Possible types are: --- (no specification), IP Camera, IP Phone, Access Point, PC, PLC, and Network Video Recorder.	None

Location Address

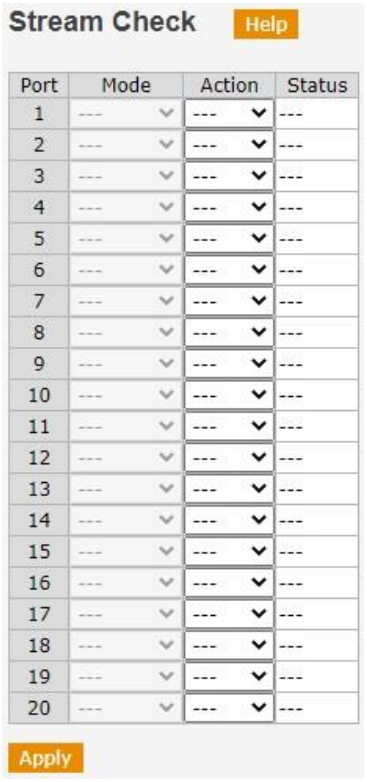
Setting	Description	Factory Default
Max. of 128 characters	Description of the location of the device connected to the port.	None

Description

Setting	Description	Factory Default
Max. of 128 characters	Description of the device connected to the port.	None

3.12.3.5 Stream Check

This page provides additional configuration options for the Stream Check function on each port.



Mode

Setting	Description	Factory Default
Enable / Disable	Enable or Disable (---) the Stream Check option on the port. Note: If the Binding function is not enabled on a port, it will not be possible to enable the Stream Check option. Binding function is enabled in the Device Binding page.	--- (Disabled)

Action

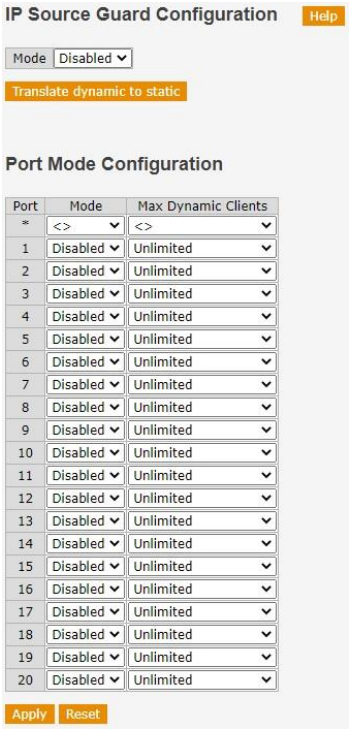
Setting	Description	Factory Default
--- / Log it	Indicates the action when stream getting low. The possible actions to be configured are: ---: No action Log it: Log the event.	--- (Disabled)

Status

Setting	Description	Factory Default
Information only	Indicates the Stream Check status. ---: Disabled Normal: The stream is normal. Low: The stream is getting low.	--- (Disabled)

3.12.4 IP Source Guard

IP Source Guard is a feature used to restrict IP traffic on DHCP snooping untrusted ports. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.



IP Source Guard Configuration

Mode

Setting	Description	Factory Default
Enabled/Disabled	Enable or Disable the IP Source Guard function globally in the switch. All configured ACEs (Access Control Entries) will be lost when the mode is enabled.	Disabled

The button **Translate dynamic to static** translates all dynamic entries to static entries (see following sections Static and Dynamic IP Source Guard Tables).

Port Mode Configuration

Mode

Setting	Description	Factory Default
Enabled/Disabled	Enable or Disable the IP Source Guard function in each specific port of the switch.	Disabled

Max Dynamic Clients

Setting	Description	Factory Default
Unlimited / 0 / 1 / 2	Specifies the maximum number of dynamic clients that can be learned on given port. If the port mode is enabled and the value of max dynamic client is equal	Unlimited

	to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.	

3.12.4.1 Static IP Source Guard Table

This page allows to create entries for the static IP source guard table.

Press the button **Add New Entry** to create an entry for the Static IP Source Guard Table.

Port

Setting	Description	Factory Default
1 to 20	The logical port for the entry.	1

VLAN ID

Setting	Description	Factory Default
1 to 4095	The VLAN ID for the entry.	None

IP Address

Setting	Description	Factory Default
IP address	Allowed source IP address for the entry.	None

MAC Address

Setting	Description	Factory Default
MAC address	Allowed source MAC address for the entry.	None

3.12.4.2 Dynamic IP Source Guard Table

The page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard table. The **Start from port, VLAN** and **IP Address** fields allow the user to select the starting point in the Dynamic IP Source Guard table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest IGMP Group table match.

The following information can be displayed on the page:

Port	Switch port number for which the entries are displayed.
VLAN ID	VLAN ID in which the traffic is permitted.
IP Address	User IP address of the entry.
MAC Address	Source MAC address.

3.12.5 Access Control List (ACL)

The switch has an Access Control List (ACL) where the user can create different Access Control Entries (ACEs) specifying individual frame types permitted or denied. Accordingly, ACL can be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are four ACE frame types (Ethernet Type, ARP, IPv4 and IPv6) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

In the following sections are described the options of the Web Management associated with the ACLs.

3.12.5.1 ACL Ports Configuration

This option allows the user to configure the ACL parameters of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

The parameters that can be configured for each port of the switch are:

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*		<>	<>	Disabled / Port 1 / Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	46597
7	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
13	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0

Policy ID

Setting	Description	Factory Default
0 to 255	Indicate the policy ID to apply to this port.	0

Action

Setting	Description	Factory Default
Permit / Deny	Select whether forwarding is permitted ("Permit") or denied ("Deny").	Permit

Rate Limiter ID

Setting	Description	Factory Default
Disabled / 1 to 16	Select which rate limiter to apply on this port (1 to 16). The value of the 1 to 16 Rate limiters ID is defined in the option ACL Rate Limiter Configuration.	Disabled

Port Redirect

Setting	Description	Factory Default
Disabled / Port number	Select which port frames are redirected on. It can't be set when action is permitted.	Disabled

Mirror

Setting	Description	Factory Default
Enabled/Disabled	Specifies the mirror operation of this port. Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored.	Disabled

Logging

Setting	Description	Factory Default
Enabled/Disabled	Specifies the logging operation of this port: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. Note: Consider that the System Log memory size and logging rate is limited.	Disabled

Shutdown

Setting	Description	Factory Default
Enabled/Disabled	Specifies the port shut down operation of this port. Enabled: If a frame is received on the port, the port will be disabled.	Disabled

	Disabled: Port shut down is disabled.	

State

Setting	Description	Factory Default
Enabled/Disabled	Specifies the state of this port. Enabled: To reopen ports by changing the volatile port configuration of the ACL user module. Disabled: To close ports by changing the volatile port configuration of the ACL user module.	Enabled

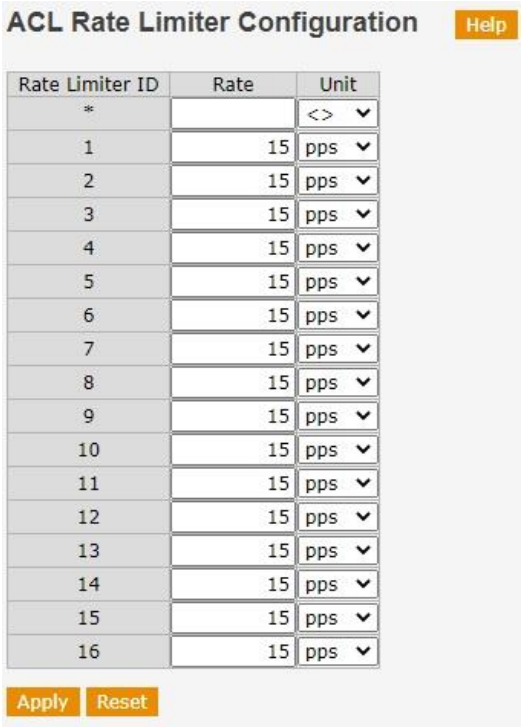
Counter

Setting	Description	Factory Default
Information only	Counts the number of frames that match this ACE.	None

3.12.5.2 ACL Rate Limiter Configuration

This option is used to define the Rate Limiters ID (from 1 to 16) that are used in the ACLs of the switch.

For each Rate Limited ID (1 to 16) it has be configured the maximum data rate.



Rate

Setting	Description	Factory Default
Maximum rate	The valid rate is 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.	15

Unit

Setting	Description	Factory Default
pps / kbps	Packets per second (pps) or Kilobits per second (kbps).	pps

3.12.5.3 ACL Configuration

This page shows the Access Control List (ACL), made up of the Access Control Entries (ACEs) defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol (ex: Device binding, Port mirroring, …), cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

The information displayed on the page is summarized in the following table:

ACE	Indicates the ACE ID.
Ingress Port	Indicates the ingress port of the ACE. It can be “All” (the ACE will match all ingress ports) or “Port” (the ACE will match a specific ingress port).
Policy / Bitmask	Indicates the policy number and bitmask of the ACE.
Frame Type	Indicates the frame type of the ACE. Possible types are: Any: The ACE will match any frame type. Ethernet Type: The ACE will match Ethernet type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match only ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match all IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match all IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match all IPv4 frames with TCP protocol. IPv4/Other: The ACE will match all IPv4 frames not being ICMP /UDP / TCP protocol. IPv6: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE: Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped. Filter: Frames matching the ACE are filtered.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect

	operation is disabled.
Mirror	Indicates the mirror operation of the ACE. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are Enabled (frames received on the port are mirrored) or Disabled (frames received on the port are not mirrored).
Counter	The counter indicates the number of times the ACE was hit by a frame.

The created ACEs of the table can be edited, removed and moved up/down on the list using the corresponding buttons:

: Inserts a new ACE before the current row.

: Edits the ACE row.

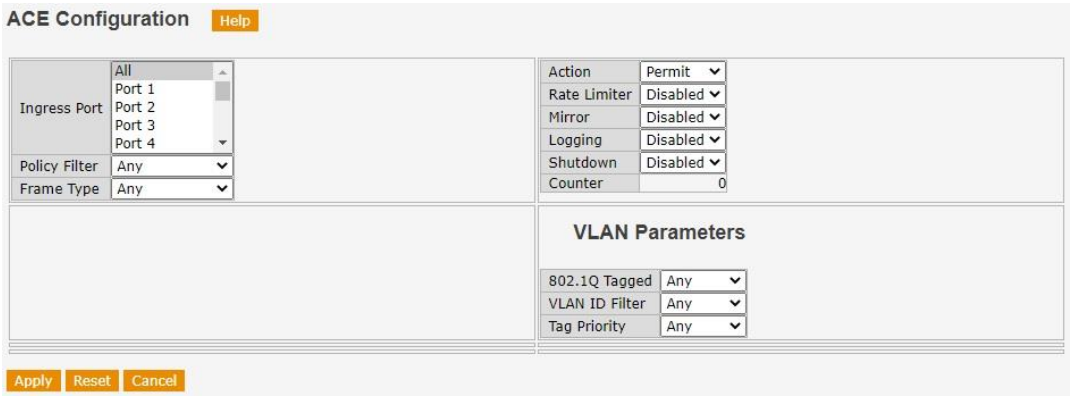
: Moves the ACE up the list.

: Moves the ACE down the list.

: Deletes the ACE.

The button **Clear** resets all the counters and the button **Remove All** deletes all the created ACEs.

When pressing the button , a new entry at the bottom of the ACE listings is added and its configuration page is loaded. On the figure below is shown the configuration page for the ACEs.



Ingress Port

Setting	Description	Factory Default
Any / Port n	Select the ingress port for which this ACE applies: All: The ACE applies to any port. Port n: The ACE applies to this port number, where n is the number of the switch port.	Any

Policy Filter

Setting	Description	Factory Default
Any / Specific	Specify the policy number filter for this ACE. Any: No policy filter is specified. Specific: Two field for entering a policy value and bitmask appear.	Any

Frame Type

Setting	Description	Factory Default
Any / Ethernet / ARP / IPv4 / IPv6	Select the frame type for this this ACE: Any: Any frame can match this ACE. Ethernet type: Only Ethernet type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6). ARP: Only ARP frames can match this ACE. Noe that the ARP frames won't match the ACE with ethernet type. IPv4: Only IPv4 frames can match this ACE. Note that the IPv4 frames won't match the ACE with ethernet type. IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type. Depending on the Type of Frame selected, new fields are shown in the page. At the end of this section are described all these additional fields.	Any

802.1Q Tagged

Setting	Description	Factory Default
Any / Enabled / Disabled	Specify whether frames can hit the action of this ACE according to the 802.1Q tagging. Any: Any value is allowed. Enabled: Tagged frame only. Disabled: Untagged frame only.	Any

VLAN ID Filter

Setting	Description	Factory Default
Any / Specific	Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. Specific: A field for entering the VLAN ID appears.	Any

Tag Priority

Setting	Description	Factory Default
Any / Specific priority	Specify the tag priority filter for this ACE. Any: No tag priority is specified. Specific: Allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7.	Any

Action

Setting	Description	Factory Default
Permit / Deny / Filter	Specify the action to take with a frame that hits this ACE. Permit: The frame that hits this ACE has granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped. Filter: Frames matching the ACE are filtered (the filtered ports can be selected).	Permit

Rate Limiter ID

Setting	Description	Factory Default
Disabled / 1 to 16	Specify the rate limiter in number of base units. Disabled indicates that the rate limiter operation is disabled.	Disabled

Mirror

Setting	Description	Factory Default
Enabled/Disabled	Specify the mirror operation of this port. When Enabled, frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. When disabled, frames received on the port are not mirrored.	Disabled

Logging

Setting	Description	Factory Default
Enabled/Disabled	Specify the logging operation of the ACE: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Note: Consider that the System Log memory size and logging rate is limited.	Disabled

Shutdown

Setting	Description	Factory Default
Enabled/Disabled	Specify the port shut down operation of the ACE. Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.	Disabled

Counter

Setting	Description	Factory Default
Information only	Counts the number of times the ACE was hit by a	None

	frame.	

Ethernet type parameters

If the type of frame selected is **Ethernet type**, additional parameters can be programmed:

SMAC Filter

Setting	Description	Factory Default
Any / Specific	Specify the source MAC address filter for this ACE. Any: No SMAC address filter is specified. Specific: A field for entering the SMAC address appears.	Any

DMAC Filter

Setting	Description	Factory Default
Any / MC / BC / UC / Specific	Specify the destination MAC address filter for this ACE. Any: No DMAC address filter is specified. MC: Frame must be multicast. BC: Frame must be broadcast. UC: Frame must be unicast. Specific: A field for entering the DMAC address appears.	Any

EtherType Filter

Setting	Description	Factory Default
Any / Specific	Specify the Ethernet type filter for this ACE. Any: No Ethernet type filter is specified. Specific: A field for entering the EtherType value appears. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6).	Any

ARP parameters

If the type of frame selected is **ARP**, several additional parameters can be programmed:

ARP/RARP

Setting	Description	Factory Default
Any / ARP / RARP / Other	Specify the available ARP/RARP opcode (OP) flag for this ACE: Any: No ARP/RARP opcode flag is specified. ARP: Frame must have ARP/RARP opcode set to ARP. RARP: Frame must have ARP/RARP opcode set to RARP. Other: Frame has unknown ARP/RARP Opcode flag.	Any

Request/Reply

Setting	Description	Factory Default
Any / Request / Reply	Specify the available Request/Reply opcode (OP) flag for this ACE. Any: No Request/Reply OP flag is specified. Request: Frame must have ARP Request or RARP Request OP flag set. Reply: Frame must have ARP Reply or RARP Reply OP flag.	Any

Sender IP Filter

Setting	Description	Factory Default
Any / Host / Network	Specify the sender IP filter for this ACE. Any: No sender IP filter is specified. Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.	Any

Target IP Filter

Setting	Description	Factory Default
Any / Host / Network	Specify the target IP filter for this specific ACE. Any: No target IP filter is specified. Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.	Any

ARP Sender MAC Match

Setting	Description	Factory Default
Any / 0 / 1	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. Any: Any value is allowed. 0: ARP frames where SHA is not equal to the SMAC address. 1: ARP frames where SHA is equal to the SMAC address.	Any

RARP Target MAC Match

Setting	Description	Factory Default
Any / 0 / 1	Specify whether frames can hit the action according to their target hardware address field (THA) settings.	Any

	Any: Any value is allowed. 0: RARP frames where THA is not equal to the target MAC address. 1: RARP frames where THA is equal to the target MAC address.	

IP/Ethernet Length

Setting	Description	Factory Default
Any / 0 / 1	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. Any: Any value is allowed. 0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04). 1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).	Any

IP

Setting	Description	Factory Default
Any / 0 / 1	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. Any: Any value is allowed. 0: ARP/RARP frames where the HLD is not equal to Ethernet (1). 1: ARP/RARP frames where the HLD is equal to Ethernet (1)	Any

Ethernet

Setting	Description	Factory Default
Any / 0 / 1	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings. Any: Any value is allowed. 0: ARP/RARP frames where the PRO is not equal to IP (0x800). 1: ARP/RARP frames where the PRO is equal to IP (0x800).	Any

IPv4 parameters

If the type of frame selected is **IPv4**, several additional parameters can be programmed:

IP Protocol Filter

Setting	Description	Factory Default
Any / ICMP / UDP	Specify the IPv4 protocol filter for this specific ACE.	Any

/ TCP	Any: No IPv4 protocol is specified. ICMP: IPv4 ICMP protocol frames. UDP: IPv4 UDP protocol frames. TCP: IPv4 TCP protocol frames. New fields are shown for the specific IPv4 protocols. At the end of this section the new fields are described.	

IP TTL

Setting	Description	Factory Default
Any / Non-zero / Zero	Specify the Time-to-Live settings for this ACE. Any: Any value is allowed. Zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. Non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.	Any

IP Fragment

Setting	Description	Factory Default
Any / Yes / No	Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. Any: Any value is allowed. No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.	Any

IP Option

Setting	Description	Factory Default
Any / Yes / No	Specify the option flag setting for this ACE. Any: Any value is allowed. No: IPv4 frames where the options flag is set must not be able to match this entry. Yes: IPv4 frames where the options flag is set must be able to match this entry.	Any

SIP Filter

Setting	Description	Factory Default
Any / Host / Network	Specify the source IP filter for this ACE. Any: No source IP filter is specified. Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP	Any

	Address and SIP Mask fields that appear.	

DIP Filter

Setting	Description	Factory Default
Any / Host / Network	Specify the destination IP filter for this ACE. Any: No destination IP filter is specified. Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.	Any

IPv6 parameters

If the type of frame selected is **IPv6**, several additional parameters can be programmed:

Next Header Filter

Setting	Description	Factory Default
Any Other / ICMP / UDP / TCP	Specify the IPv6 next header filter for this specific ACE. Any: No IPv6 next header filter is specified. Other: A field for entering a specific IPv6 next header filter appears (from 0 to 255). ICMP: IPv6 ICMP protocol frames. UDP: IPv6 UDP protocol frames. TCP: IPv6 TCP protocol frames. New fields are shown for the specific IPv6 protocols. At the end of this section the new fields are described.	Any

SIP Filter

Setting	Description	Factory Default
Any / Specific	Specify the source IPv6 filter for this ACE. Any: No source IPv6 filter is specified. Specific: Specify the source IPv6 address and source IPv6 mask in the fields that appear.	Any

Hop Limit

Setting	Description	Factory Default
Any / 0 / 1	Specify the hop limit settings for this ACE. Any: Any value is allowed. 0: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. 1: IPv6 frames with a hop limit field greater than zero must be able to match this entry.	Any

ICMP parameters

If the type of frame selected is **IPv4/ICMP** or **IPv6/ICMP**, several additional parameters can be programmed:

ICMP Type Filter

Setting	Description	Factory Default
Any / Specific	Specify the ICMP filter for this ACE. Any: No ICMP filter is specified. Specific: A field for entering an ICMP value (0 to 255) appears.	Any

ICMP Code Filter

Setting	Description	Factory Default
Any / Specific	Specify the ICMP code filter for this ACE. Any: No ICMP code filter is specified. Specific: A field for entering an ICMP code value (0 to 255) appears.	Any

TCP/UDP parameters

If the type of frame selected is **IPv4/TCP, IPv4/UDP**, **IPv6/TCP** or **IPv6/UDP**, several additional parameters can be programmed:

TCP/UDP Source Port Filter

Setting	Description	Factory Default
Any / Specific / Range	Specify the TCP/UDP source port filter for this ACE. Any: No TCP/UDP source port filter is specified. Specific: A field for entering a TCP/UDP source port value (0 to 65535) appears. Range: Two fields for entering a TCP/UDP source port range appear (0 to 65535).	Any

TCP/UDP Destination Port Filter

Setting	Description	Factory Default
Any / Specific / Range	Specify the TCP/UDP destination port filter for this ACE. Any: No TCP/UDP destination port filter is specified. Specific: A field for entering a TCP/UDP destination port value (0 to 65535) appears. Range: Two fields for entering a TCP/UDP destination port range appear (0 to 65535).	Any

TCP FIN

Setting	Description	Factory Default

Any / 0 / 1	Specify the TCP "No more data from sender" (FIN) value for this ACE. Any: Any value is allowed ("don't-care"). 0: TCP frames where the FIN field is set must not be able to match this entry. 1: TCP frames where the FIN field is set must be able to match this entry.	Any

TCP SYN

Setting	Description	Factory Default
Any / 0 / 1	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. Any: Any value is allowed ("don't-care"). 0: TCP frames where the SYN field is set must not be able to match this entry. 1: TCP frames where the SYN field is set must be able to match this entry.	Any

TCP RST

Setting	Description	Factory Default
Any / 0 / 1	Specify the TCP "Reset the connection" (RST) value for this ACE. Any: Any value is allowed ("don't-care"). 0: TCP frames where the RST field is set must not be able to match this entry. 1: TCP frames where the RST field is set must be able to match this entry.	Any

TCP PSH

Setting	Description	Factory Default
Any / 0 / 1	Specify the TCP "Push function (PSH) value for this ACE. Any: Any value is allowed ("don't-care"). 0: TCP frames where the PSH field is set must not be able to match this entry. 1: TCP frames where the PSH field is set must be able to match this entry.	Any

TCP ACK

Setting	Description	Factory Default
Any / 0 / 1	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. Any: Any value is allowed ("don't-care"). 0: TCP frames where the ACK field is set must not be able to match this entry. 1: TCP frames where the ACK field is set must be able	Any

	to match this entry.	

TCP URG

Setting	Description	Factory Default
Any / 0 / 1	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. Any: Any value is allowed ("don't-care"). 0: TCP frames where the URG field is set must not be able to match this entry. 1: TCP frames where the URG field is set must be able to match this entry.	Any

3.12.5.4 ACL Status

This page shows the ACL status by different ACL users. Each row describes the main information about each ACE that is defined. The maximum number of ACEs is 256 on each switch.

The table displayed on the page shows the following information:

User	Indicates the ACL user.
ACE	Indicates the ACE ID on local switch.
Frame Type	Indicates the frame type of the ACE: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE: Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped. Filter: Frames matching the ACE are filtered.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 o 16. When Disabled is displayed, the rate limiter operation is disabled.
Mirror	Indicates if the Mirror operation is included in the ACE (Enabled). When Disabled is displayed, the mirror operation is disabled.
CPU	Forward packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.

Conflict	Displays 'Yes' if there is a HW conflict related with the created ACE. Otherwise displays 'No'.

3.12.6 Authentication, Authorization and Accounting (AAA)

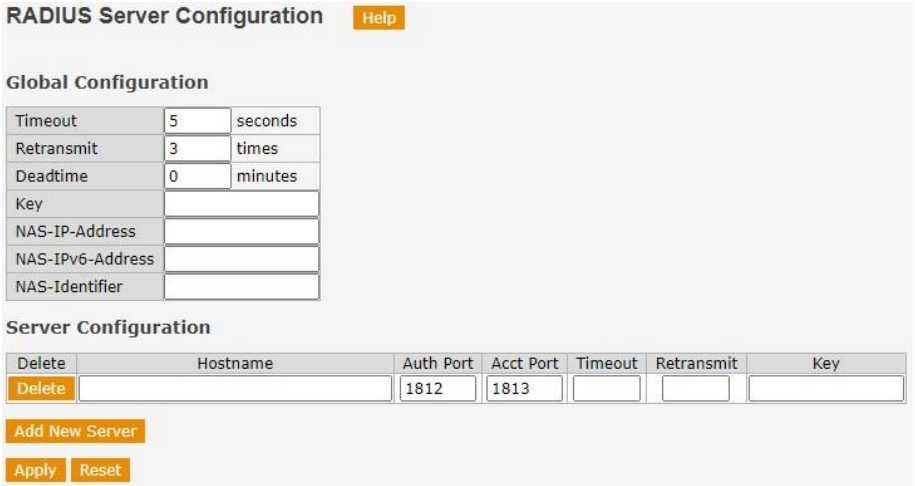
For user name/password level security, Weidmüller switches provide the possibility to enable/disable any possible access to the management of the device and also provide the login option through Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+). The RADIUS and TACACS+ mechanisms are centralized "AAA" (Authentication, Authorization and Accounting) systems for connecting to network services.

In the following sections of this chapter the different configuration options for RADIUS and TACACS+ operation are described.

NOTE: The Authentication, Authorization and Accounting preferred options for the switch (including RADIUS and TACACS+) are selected in the web page Authentication methods of the Basic Settings menu.

3.12.6.1 RADIUS Server Configuration

This page allows the user to configure the RADIUS servers.



Global Configuration

Timeout

Setting	Description	Factory Default
1 to 1000 (sec)	Number of seconds to wait for a reply from a RADIUS server before retransmitting the request.	5

Retransmit

Setting	Description	Factory Default
1 to 1000	Number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.	3

Deadtime

Setting	Description	Factory Default
1 to 1440 (minutes)	Deadtime is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.	0

Key

Setting	Description	Factory Default
Max 63 characters	The secret key shared between the RADIUS server and the switch.	None

NAS-IP-Address

Setting	Description	Factory Default
IP address	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.	None

NAS-IPv6-Address

Setting	Description	Factory Default
IPv6 address	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.	None

NAS-Identifier

Setting	Description	Factory Default
Max 253 characters	The identifier to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.	None

Server Configuration

Press the button **Add New Server** to add and configure a RADIUS server. Up to 5 servers are supported. The parameters that have to be configured for each server are:

Hostname

Setting	Description	Factory Default
IP address	The IP address of the RADIUS server.	None

Auth Port

Setting	Description	Factory Default
Port	The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.	1812

Acct Port

Setting	Description	Factory Default
Port	The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.	1813

Timeout

Setting	Description	Factory Default
1 to 1000 (sec)	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.	None

Retransmit

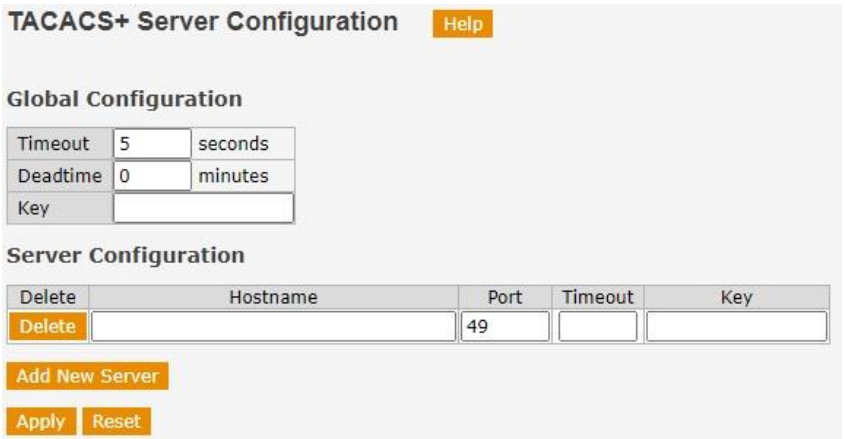
Setting	Description	Factory Default
1 to 1000	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.	None

Key

Setting	Description	Factory Default
Max 63 characters	This optional setting overrides the global key. Leaving it blank will use the global key.	None

3.12.6.2 TACACS+ Server Configuration

This page allows the user to configure the TACACS+ servers.



Global Configuration

Timeout

Setting	Description	Factory Default
1 to 1000 (sec)	Number of seconds to wait for a reply from a TACACS+ server before retransmitting the request.	5

Deadtime

Setting	Description	Factory Default
1 to 1440 (minutes)	Deadtime is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.	0

Key

Setting	Description	Factory Default
Max 63 characters	The secret key shared between the TACACS+ server and the switch.	None

Server Configuration

Press the button **Add New Server** to add and configure a TACACS+ server. Up to 5 servers are supported. The parameters that have to be configured for each server are:

Hostname

Setting	Description	Factory Default
IP address	The IP address of the TACACS+ server.	None

Port

Setting	Description	Factory Default
Port	The TCP port to use on the TACACS+ server for authentication.	49

Timeout

Setting	Description	Factory Default

1 to 1000 (sec)	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.	None

Key

Setting	Description	Factory Default
Max 63 characters	This optional setting overrides the global key. Leaving it blank will use the global key.	None

3.12.6.3 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configured in the switch.

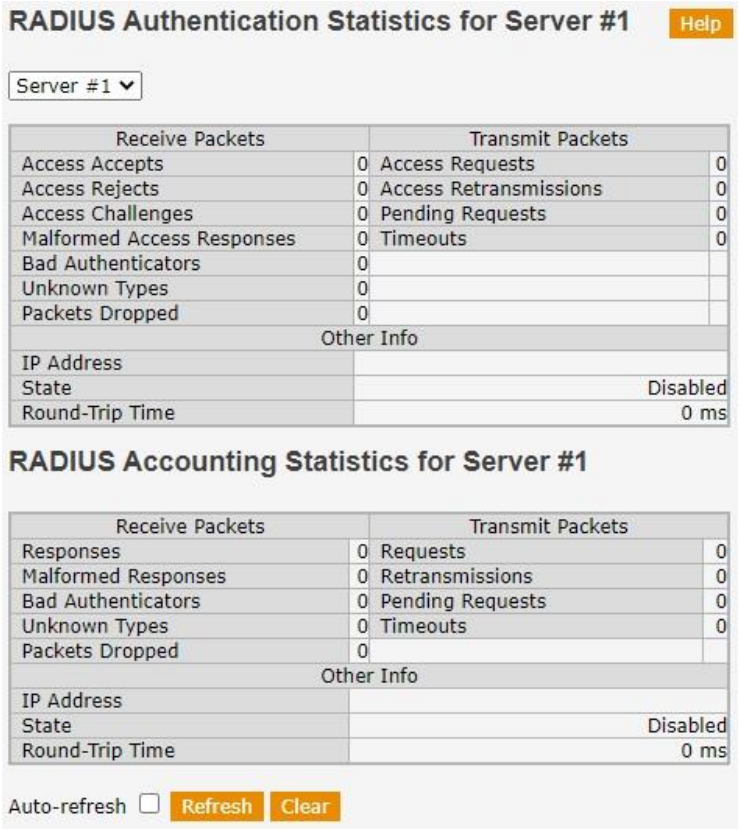
The table displayed on the page shows the following information:

#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address of this server.
Authentication Port	UDP port number for authentication.
Authentication Status	The current status of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Accounting Port	UDP port number for accounting.
Accounting Status	The current status of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server but it did not reply within the configured timeout. The server has temporarily

	been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

3.12.6.4 RADIUS Details

This page provides detailed statistics for a particular RADIUS server.



The statistics shown map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

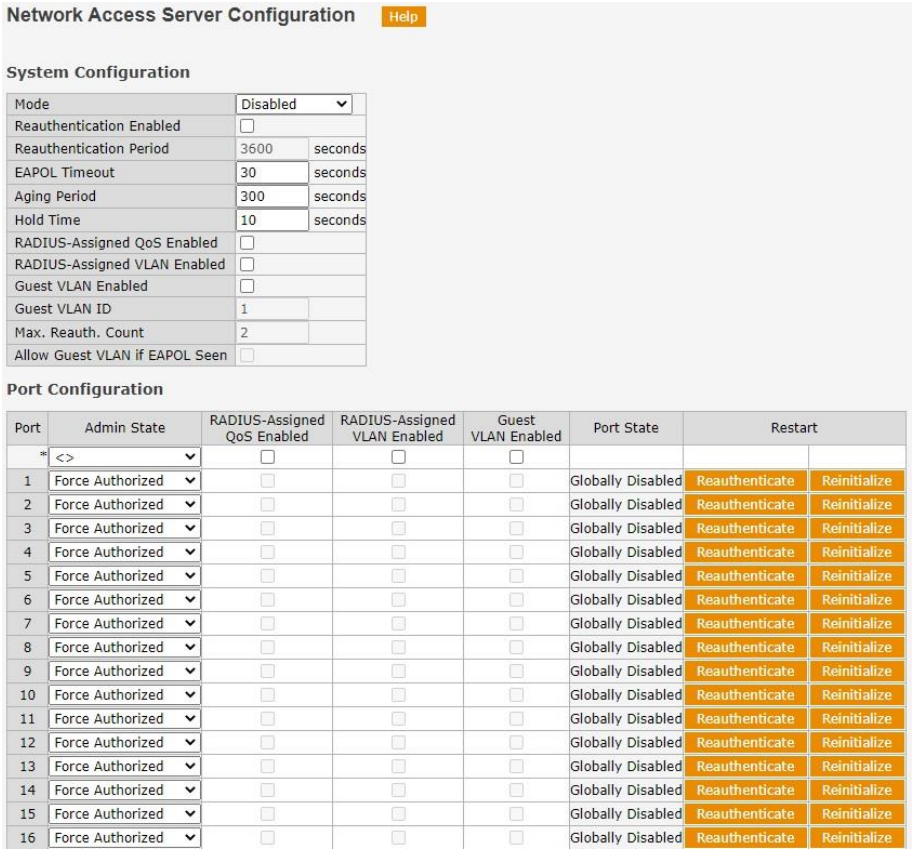
The **Help** button provides a description of all the different counters shown on the page.

3.12.7 Network Access Server (802.1X)

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers (the backend servers) determine whether the user is allowed access to the network.

3.12.7.1 Network Access Server (NAS) Configuration

This page allows the user to configure the IEEE 802.1X and MAC-based authentication system and port settings. The NAS configuration consists of two sections, a system- and a port-wide.



System Configuration

Mode

Setting	Description	Factory Default
Enabled / Disabled	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames. Note: The backend (RADIUS) servers are configured on the RADIUS Configuration page (Security/AAA menu).	Disabled

Reauthentication Enabled

Setting	Description	Factory Default
Check / Uncheck	Determines if connected clients must be reauthenticated (checked) or not (unchecked).	Unchecked

Reauthentication Period

Setting	Description	Factory Default
1 to 3600 (sec)	Period, in seconds, after which a connected client must be reauthenticated. It can only be programmed if Reauthentication Enabled is checked.	3600

EAPOL Timeout

Setting	Description	Factory Default
1 to 65535 (sec)	Determines the time for retransmission of Request Identity EAPOL frames. This has no effect for MAC-based ports.	30

Aging Period

Setting	Description	Factory Default
10 to 1000000 (sec)	This setting applies to the following Modes defined in Port Configuration (described below global settings): • Single 802.1X • Multi 802.1X • MAC-Based Auth. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this. If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.	300

Hold Time

Setting	Description	Factory Default
10 to 1000000 (sec)	This setting applies to the following modes Modes defined in Port Configuration (described below global settings): • Single 802.1X • Multi 802.1X • MAC-Based Auth. If a client is denied access, either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the RADIUS configuration page), the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.	10

RADIUS-Assigned QoS Enabled

Setting	Description	Factory Default
Check / Uncheck	The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.	Unchecked

RADIUS-Assigned VLAN Enabled

Setting	Description	Factory Default
Check / Uncheck	The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.	Unchecked

Guest VLAN Enabled

Setting	Description	Factory Default
Check / Uncheck	The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.	Unchecked

Guest VLAN ID

Setting	Description	Factory Default
1 to 4095	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.	1

Max. Reauth. Count

Setting	Description	Factory Default
1 to 255	The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.	2

Allow Guest VLAN if EAPOL seen

Setting	Description	Factory Default
Check / Uncheck	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.	Unchecked

Port Configuration

Admin State

Setting	Description	Factory Default
Force Authorized / Force Unauthorized / Port-based 802.1X / Single 802.1X / Multi 802.1X / MAC-based Auth	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: • Force Authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up and any client on the port will be network access allowed without authentication. • Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up and any client on the port will be network access disallowed. • Port-based 802.1X: In this mode, the switch will act as authenticator according to the IEEE 802.1X standard. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. • Single 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time.	Force Authorized

	If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. • Multi 802.1X: Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality. • MAC-based Auth: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.	

RADIUS-Assigned QoS Enabled

Setting	Description	Factory Default
Check / Uncheck	When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the	Unchecked

	switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. This option is only available for single-client modes (Port-based 802.1X and Single 802.1X).	

RADIUS-Assigned VLAN Enabled

Setting	Description	Factory Default
Check / Uncheck	When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. This option is only available for single-client modes (Port-based 802.1X and Single 802.1X).	Unchecked

Guest VLAN Enabled

Setting	Description	Factory Default
Check / Uncheck	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the following rules: When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port and, if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. This option is only available for EAPOL-based modes	Unchecked

	(Port-based 802.1, Single 802.1 and Multi 802.1X).	

Port state

Setting	Description	Factory Default
Information only	The current state of the port. It can undertake one of the following values: • Globally Disabled: NAS is globally disabled. • Link Down: NAS is globally enabled, but there is no link on the port. • Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. • Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. • X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.	Globally Disabled

The buttons **Reauthenticate** and **Reinitialize** are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

The **Reauthenticate** button schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

The **Reinitialize** button forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

3.12.7.2 Network Access Server (NAS) Switch Status

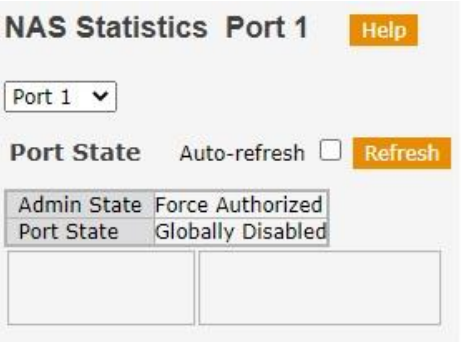
This page provides an overview of the current NAS port states.

The table displayed on the page shows the following information:

Port	The switch port number. Click to navigate to detailed NAS statistics for this port.
Admin State	The port's current administrative state. Possible values already explained in previous section (Admin State).
Port State	The current state of the port. Possible values already explained in previous section (Port State).
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
QoS Class	QoS Class assigned to the port by the RADIUS server if enabled.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

3.12.7.3 Network Access Server (NAS) Statistics

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics only. Use the port select box to select which port details to be displayed.



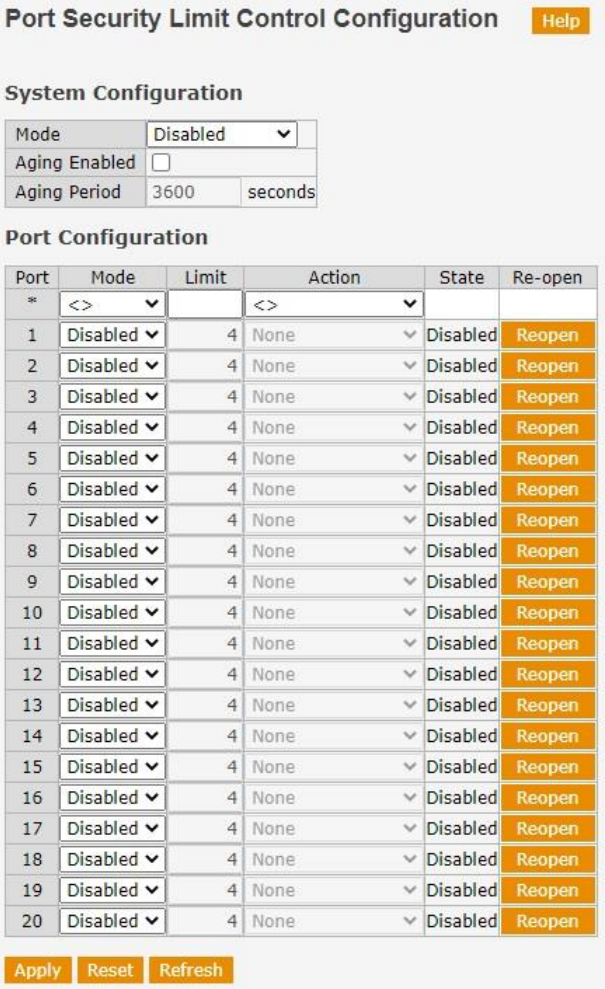
The page shows the Port State information including the parameters Admin State, Port State, QoS Class and Port VLAN ID already described in the previous section of this manual.

Additionally, the page also shows the Port Counters. The **Help** button provides a detailed description of all these counters shown on the page.

3.12.8 Port Security

3.12.8.1 Port Limit Control

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.



System Configuration

Mode

Setting	Description	Factory Default
Enabled / Disabled	Enable or Disable the Global limit control on the switch.	Disabled

Aging Enabled

Setting	Description	Factory Default
Check / Uncheck	If checked, secured MAC addresses are subject to aging according to the 'Aging Period' defined.	Unchecked

Aging Period

Setting	Description	Factory Default
10 to 10000000 (sec)	If Aging is enabled (checked) the user can specify the aging period of the MAC addresses in seconds.	3600

Port Configuration

Mode

Setting	Description	Factory Default
Enabled / Disabled	Controls whether Limit Control is enabled on this port. Both the Global Mode and Port Mode must be Enabled to activate the Limit Control.	Disabled

Limit

Setting	Description	Factory Default
1 to 1024	The maximum number of MAC addresses that can be secured on this port. If the limit is exceeded, the corresponding action is taken.	4

Action

Setting	Description	Factory Default
None / Trap / Shutdown / Trap & Shutdown	If the limit number is reached, the switch will take one of the following actions: None: Do not allow more than Limit MAC addresses on the port, but take no further action. Trap: If the limit number is exceeded on the port, an SNMP trap will be sent. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded. Shutdown: If the limit number is exceeded on the port,	None

	the port will be shut down. This implies that all secured MAC addresses will be removed from the port and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. Trap & Shutdown: If the limit number is exceeded on the port, both the “Trap” and the “Shutdown” actions described above will be taken. There are three ways to re-open a port that has been shut down: 1) Boot the switch, 2) Disable and re-enable Limit Control on the port or the switch, 3) Click the Reopen button.	

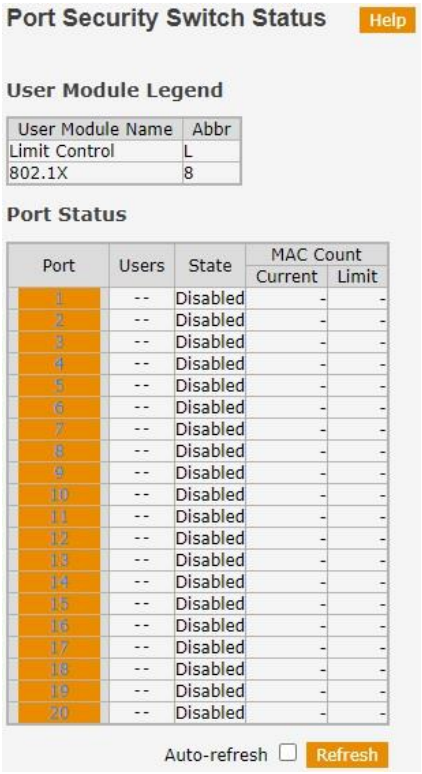
State

Setting	Description	Factory Default
Information only	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of the following four values: Disabled: Limit Control is either globally disabled or disabled on the port. Ready: The limit is not yet reached. This can be shown for all actions. Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap. Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.	Disabled

The **Reopen** button can be used to reopen a specific port that has been shut down due to exceeding the defined limit.

3.12.8.2 Port Security Status

When port security is enabled on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn checks all internal programming (user modules) whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.
The status page is divided into two sections - one with a legend of user modules and one with the actual port status.



User Module Legend

The table displayed shows the following information:

User Module Name	The full name of a user module that may request Port Security services.
Abbr	A one-letter abbreviation of the user module. This is used in the Users column in the Port Status table.

Port Status

Port	The port number for which the status applies. Click the port number to see additional information about the status of this particular port.
Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '- -' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
State	Shows the current state of the port which includes the following values: Disabled: No user modules are currently using the Port Security service. Ready: The Port Security service is in use by at least one user module and is awaiting frames from unknown MAC addresses to arrive. Limit Reached: The Port Security service is enabled by at least the Limit Control user module and that module has indicated that the limit is reached and no more MAC addresses should be taken in. Shutdown: The Port Security service is enabled by at least the Limit Control user module and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened.
MAC Count	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of

	MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

3.12.8.3 Port Status

This page shows the MAC addresses secured by the Port Security module.

The table displayed on the page shows the following information:

MAC Address	The MAC address that is seen on this port. If no MAC addresses are learned, a single row stating No MAC addresses attached is displayed.
VLAN ID	The VLAN ID that is seen on this port.
State	Indicates whether the corresponding MAC address is blocked or forwarding. If blocked, it will not be allowed to transmit or receive traffic.
Time of Addition	Shows the date and time when this MAC address was first seen on the port.
Age/Hold	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

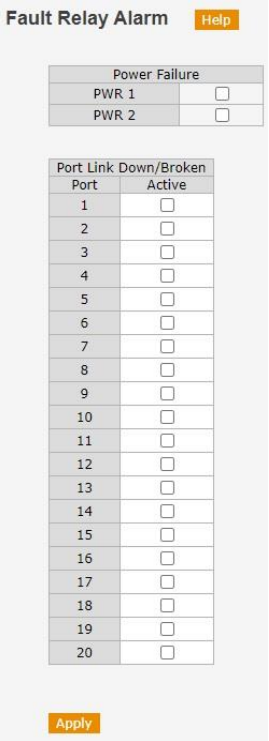
3.13 Warning/Event Settings

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet switch that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The Weidmüller switch supports different approaches to warn engineers automatically, such as email and relay output. It also allows to store the log data of events both locally and in a SYSLOG server.

3.13.1 Configuring Relay Warnings

The Fault Relay Alarm function uses relay output to alert the user when certain user-configured events take place.

Configuring Relay Warning Events Settings



Alarm event types can be divided into two basic groups: **Power Failure** and **Port Link Down/Broken**.

You can configure which events are related to the relay output.

NOTE: The events that are configured to activate the relay output also activate the amber light in the FAULT LED of the front-plate of the switch.

Power Failure	Warning Relay output is triggered when…
PWR 1	No power input in the first power supply module of the switch.
PWR 2	No power input in the second power supply module of the switch.

Port Link Down/Broken	Warning e-mail is sent when…
Port number	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).

3.13.2 Configuring Email Warning

The SMTP Setting function uses e-mail to alert the user when certain user-configured events take place. Two basic steps are required to set up the Auto Warning function:

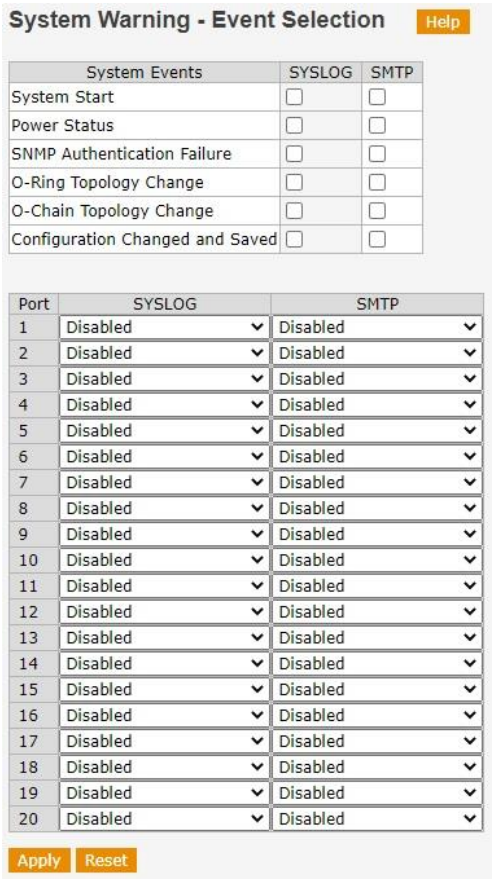
Configure Email Event Types

Select the desired **Event types** from the Event type page.

Configure Email Settings

To configure a Weidmüller switch's email setup, enter your Mail Server IP, Account Name, Account Password, Retype New Password, and the email addresses to which warning messages will be sent.

3.13.2.1 Event Selection



Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

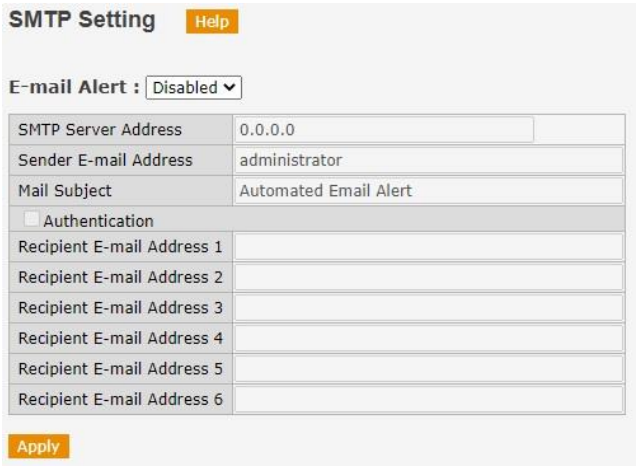
NOTE: For each event the user can decide if a log is registered (SYSLOG) and/or if a warning Email is sent (SMTP). Please, consider that the SYSLOG and SMTP sever must also be Enabled from the corresponding page.

System Events	Log is registered when / Warning e-mail is sent when…
System restart	Weidmüller switch is rebooted.
Power Status	Weidmüller switch is powered up or down.
SNMP Authentication Failure	Incorrect SNMP authentication.
O-Ring Topology Change	If the Master of the O-Ring has changed or the backup path is activated.
O-Chain Topology Change	If the configuration of the O-Chain has changed or the backup path is activated.

Configuration Changed and Saved	Any configuration item has been changed and saved.

Port Events	Log is registered when / Warning e-mail is sent when…
Disable	Never.
Link Up	The port is connected to another device.
Link Down	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Link Up & Link Down	The port is either connected or disconnected.

3.13.2.2 Email Settings



E-mail Alert

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Email warning function.	Disabled

SMTP Server Address

Setting	Description	Factory Default
IP address	The IP Address of your email server.	0.0.0.0

Sender E-mail Address

Setting	Description	Factory Default
E-mail address	Your email account	administrator

Mail Subject

Setting	Description	Factory Default
Max. of 45 characters	Subject of the email that will be sent.	Automated Email Alert

Authentication

Setting	Description	Factory Default
Check / Uncheck	Check if the SMTP server needs authentication.	Unchecked
Username	Type the username of the SMTP server.	None
Password	Type the password of the SMTP server.	None
Confirm password	Retype the password of the SMTP server.	None

Recipient Email Address

Setting	Description	Factory Default
Max. of 45 characters	You can set up to six email addresses to receive alarm emails from the Weidmüller switch.	None

3.13.3 SYSLOG Setting

Server Mode

Setting	Description	Factory Default
Client(Local)	Events are logged only in the switch.	Client(Local)
Client(Local) and Server(Remote)	Events are logged in the switch and in a remote SYSLOG server.	

Server Address

Setting	Description	Factory Default
IP address	The IP address of Syslog Server used by your network.	None

Syslog Level

Setting	Description	Factory Default
Informational / Error / Warning / Message	Select the severity level for the syslog messages to be logged: Informational: Send the specific messages which severity code is less or equal than Informational (6). Error: Send the specific messages which severity code is less or equal than Error (3). Warning: Send the specific messages which severity code is less or equal than Warning (4). Message: Send the specific messages which severity code is less or equal than Message (5).	Informational

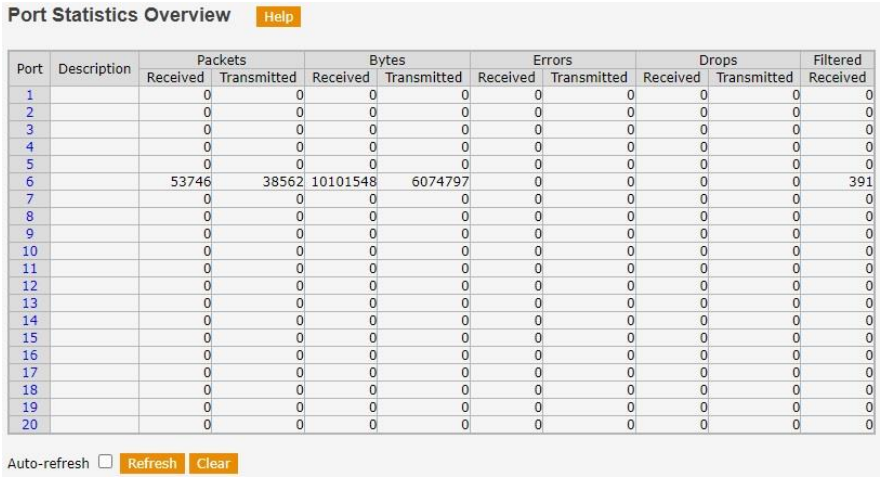
3.14 Monitoring and Diag

You can monitor statistics in real time from the Weidmüller switch as well as check its log register.

The Weidmüller switch also provides important tools for administrators to diagnose network systems.

3.14.1 Port Statistics Overview

This page provides an overview of general traffic statistics for all switch ports.



Port	Description	Packets Received	Packets Transmitted	Bytes Received	Bytes Transmitted	Errors Received	Errors Transmitted	Drops Received	Drops Transmitted	Filtered Received
1		0	0	0	0	0	0	0	0	0
2		0	0	0	0	0	0	0	0	0
3		0	0	0	0	0	0	0	0	0
4		0	0	0	0	0	0	0	0	0
5		0	0	0	0	0	0	0	0	0
6		53746	38562	10101548	6074797	0	0	0	0	391
7		0	0	0	0	0	0	0	0	0
8		0	0	0	0	0	0	0	0	0
9		0	0	0	0	0	0	0	0	0
10		0	0	0	0	0	0	0	0	0
11		0	0	0	0	0	0	0	0	0
12		0	0	0	0	0	0	0	0	0
13		0	0	0	0	0	0	0	0	0
14		0	0	0	0	0	0	0	0	0
15		0	0	0	0	0	0	0	0	0
16		0	0	0	0	0	0	0	0	0
17		0	0	0	0	0	0	0	0	0
18		0	0	0	0	0	0	0	0	0
19		0	0	0	0	0	0	0	0	0
20		0	0	0	0	0	0	0	0	0

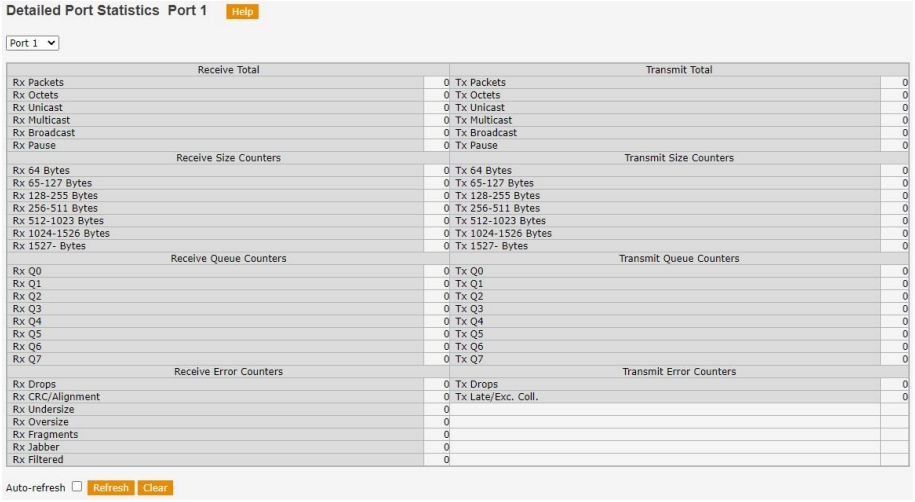
The table shown on the page includes the following information:

Port	The port number of the switch.
Description	The description of the port.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.

The **Clear** button allows the user to reset all the port counters.

3.14.2 Detailed Port Statistics

This page provides detailed traffic statistics for any specific switch port. Use the port select box to select which switch port details to display.



The tables shown on the page include the following information:

Receive and Transmit Total

Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes, including FCS but excluding framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	The number of MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short frames (frames smaller than 64 bytes) received with valid CRC.

Rx Oversize	The number of long frames (frames longer than the configured maximum frame length for this port) received with valid CRC.
Rx Fragments	The number of frames received with a length of more than 64 bytes and with an invalid FCS/CRC.
Rx Jabber	The number of frames received with a length of more than MaxSize bytes but with an invalid FCS/CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.

Transmit Error Counters

Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	The number of frames dropped due to excessive or late collisions.

The **Clear** button allows the user to reset all the port counters.

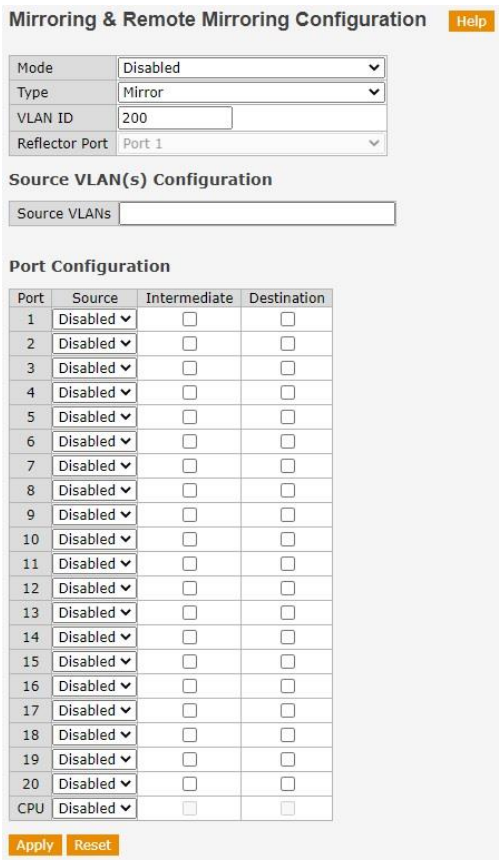
3.14.3 Port Monitoring

The user can configure port mirroring on this page. This function can be used by the administrator to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

As will be explained below, the traffic to be copied to the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring)
- All frames transmitted on a given port (also known as egress or destination mirroring)

Remote mirroring (RMirror) is an additional function available on the switch to extend the destination port to another switch of the network. So, the administrator can analyze the network traffic on several different switches.



Mode

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Mirroring or Remote mirroring function.	Disabled

Type

Setting	Description	Factory Default
Mirror	The source port(s) and destination port are located on this switch.	Mirror
Source (RMirror)	The source port(s) and intermediate port(s) are located on this switch.	
Intermediate (RMirror)	The intermediate ports are located on this switch.	
Destination (RMirror)	The destination port(s) and intermediate port(s) are located on this switch.	

VLAN ID

Setting	Description	Factory Default
1 to 4095	When Remote Mirroring is activated, the VLAN ID points out where the monitor packet will copy to.	200

Reflector port

Setting	Description	Factory Default
Port of the switch	The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled. The reflector port needs to be selected only on Source switch type and only supports pure copper ports.	Port 1

Source VLAN(s) Configuration

Setting	Description	Factory Default
1 to 4095	The switch can support VLAN-based mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.	200

Port Configuration

Source

Setting	Description	Factory Default
Disabled	Neither transmitted nor received frames are mirrored.	Disabled
Both	Transmitted and received frames are mirrored on the Destination or Intermediate port.	
Rx Only	Received frames are mirrored on the Destination or Intermediate port. Transmitted frames are not mirrored.	
Tx Only	Transmitted frames are mirrored on the Destination or Intermediate port. Received frames are not mirrored.	

Intermediate

Setting	Description	Factory Default
Check / Uncheck	Select intermediate port (applicable only to Remote Mirroring). The intermediate port is a port of the switch to connect to another switch.	Unchecked

Mode

Setting	Description	Factory Default
Check / Uncheck	Select destination port. The destination port is a port of the switch where is received a copy of traffic from the source port.	Unchecked

3.14.4 System Log Information

This page shows the Event Log Table stored in the switch. The page shows up to 999 entries, default being 20, selected through the **Entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Event Log table. The first displayed will be the one with the lowest ID found in the Event Log table. The **Start from ID** field allows the user to select the starting point in the Event Log table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Event Log table match.

In the Syslog are defined four different levels for the Event Log Table:

- **Error**: The system log entry belongs to error level
- **Warning**: The system log entry belongs to warning level
- **Notice**: The system log entry belongs to notice level
- **Informational**: The system log entry belongs to information level

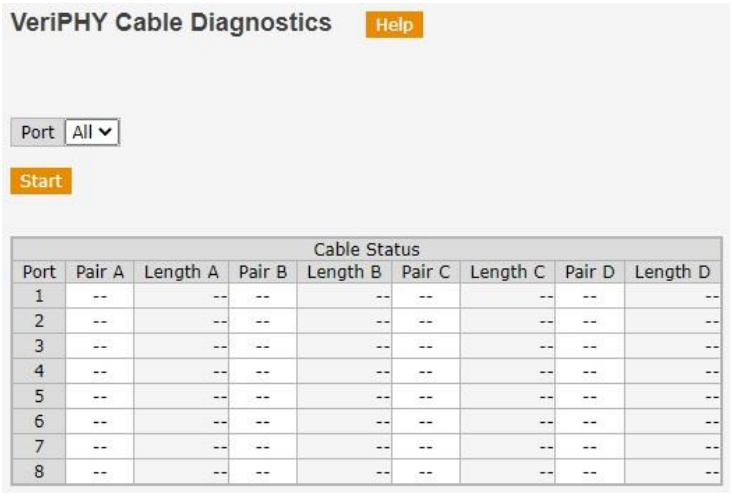
It is possible to display all the entries of the table or filtered by level. It is also possible to delete (clear) all the entries of the table or delete only by level.

The Event Log table shows the following information:

ID	The identification of the system log entry.
Level	The level of the system log entry (Error, Warning, Notice or Informational).
Time	The time of the system log entry.
Message	The description of the system log entry.

3.14.5 VeriPHY Cable Diagnostics

This page allows the user to perform Cable Diagnostics tests on copper wires.



Press the **Start** button to run the diagnostics. When completed, the page refreshes automatically and the cable diagnostics results are shown in the cable status table.

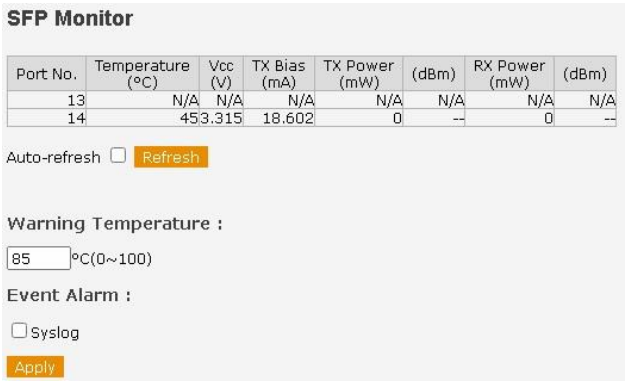
NOTE: The VeriPHY diagnostics tool is only accurate for cables 7 - 140 meters long. 10 and 100 Mbps ports will be disconnected while running VeriPHY diagnostics. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until diagnostic is completed.

The information shown on the table is:

Port	Port number where the diagnostic is performed.
Pair	The status of the cable pair: OK - Correctly terminated pair Open - Open pair Short - Shorted pair Short A - Cross-pair short to pair A Short B - Cross-pair short to pair B Short C - Cross-pair short to pair C Short D - Cross-pair short to pair D Cross A - Abnormal cross-pair coupling with pair A Cross B - Abnormal cross-pair coupling with pair B Cross C - Abnormal cross-pair coupling with pair C Cross D - Abnormal cross-pair coupling with pair D
Length	The length (in meters) of the cable pair. The resolution is 3 meters.

3.14.6 SFP Monitor

Optical fiber is commonly used for long distance data transmission. However, when link issues occur, it is very costly to trouble shoot the fiber cable and fiber transceiver at remote sites. To solve this problem, Weidmüller industrial Ethernet switches provide digital diagnostic and monitoring (DDM) functions on Weidmüller SFP optical fiber links and allow users to measure optical parameters and its performance from center site. This function can greatly facilitate the trouble shooting process for optical fiber links and reduce costs for onsite debug.



Parameter	Description
Port No.	Switch port number with SFP plugged in
Temperature (°C)	SFP casing temperature
Vcc (V)	Voltage supply to the SFP

Tx Bias (mA)	The bias current of the optical transmitter
Tx power (mW)	The amount of light being transmitted into the fiber optic cable in mW
(dBm)	The amount of light being transmitted into the fiber optic cable in dBm
Rx power (mW)	The amount of light being received from the fiber optic cable in mW
(dBm)	The amount of light being received from the fiber optic cable in dBm

Besides monitoring the SFP status, it is also possible to configure a high-temperature warning that can be logged in Syslog.

Warning Temperature

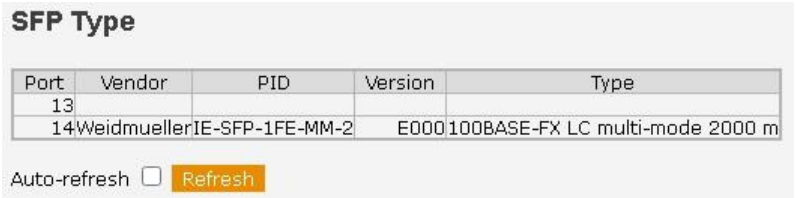
Setting	Description	Factory Default
Number between 0 and 100 ºC	Temperature threshold for warning event.	85 ºC

Event Alarm

Setting	Description	Factory Default
Syslog	Check to register the event in Syslog.	Unchecked

3.14.7 SFP Type

Besides the monitoring parameters described in the previous section, general information about the SFP transceivers can also be obtained from the web interface.



Parameter	Description
Port	Switch port number with SFP plugged in
Vendor	Provider of the SFP transceiver
PID	Product Identification of the SFP transceiver
Version	Version of the SFP transceiver
Type	General information about the SFP transceiver (Interface / Fiber optic type / Distance)

3.14.8 Ping and Ping6

The **Ping** function uses the *ping* command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the

Weidmüller switch itself. In this way, the user can essentially sit on top of the Weidmüller switch and send ping commands out through its ports.

To use the Ping function, type in the desired IP address (ICMPv4 or ICMPv6), and then click **Start**.

The payload size of the ICMP packet (8 to 1400 bytes) as well as its number can be programmed by the user. The sequence number and roundtrip time will be displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

3.15 PTP Synchronization

IEEE Std 1588-2008 specifies the second generation of the Precision Time Protocol (PTP), which is also known as “PTPv2” or “1588v2”. This is capable of very accurate time synchronization by using special Ethernet hardware that records the exact time a PTP synchronization message is received at the Ethernet card. It achieves clock accuracy in the sub-microsecond range, in contrast with NTP/SNTP protocol that achieves an accuracy around 1ms.

IEEE Std 1588-2008 defines a number of terms for PTP time synchronization systems:

- **Grandmaster clock**: The clock that is the ultimate source of time for synchronization using PTP and usually has a GPS receiver built-in
- **Master clock**: A clock that is the source of time that other clocks on the network synchronize to
- **Slave clock**: The end user of PTP (ex: Protection Relay)
- **Transparent clock**: An Ethernet switch that measures the time taken for a PTP synchronization message to transit the device and provides this information to clocks receiving the PTP event message
- **Boundary clock**: A clock that has multiple PTP ports and may serve as a source of time, i.e. be a slave clock to an upstream source and a master clock to downstream devices

Ethernet switches in a PTP network will generally be transparent clocks but it may also be possible for them to act as boundary clocks. Weidmüller switches can be programmed for both operation modes. Transparent clock operation may be configured as peer to peer or end to end. Peer to peer provides better accuracy but then is required that all the network devices are PTP complaint.

3.15.1 PTP Clock Configuration

This page allows the user to configure and inspect the current PTP clock settings.

When pressing the **Add New PTP Clock Configuration** button, the following fields have to be programmed:

Clock Instance

Setting	Description	Factory Default
0 to 3	Indicates the Instance of a particular Clock Instance. Click on the Clock Instance number to edit the Clock details.	0

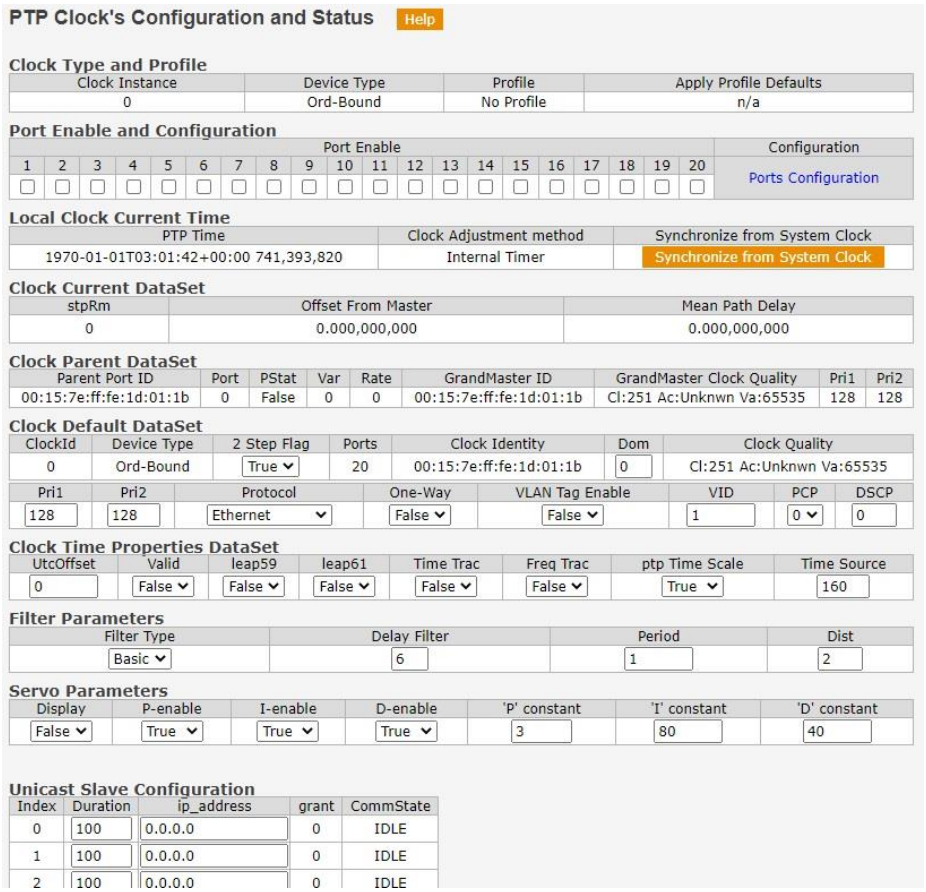
Device Type

Setting	Description	Factory Default
Inactive / Ord-Bound / P2pTransp / E2eTransp / Mastronly / Slaveonly	Indicates the Type of the Clock Instance. There are five Device Types. Ord-Bound: Clock's Device Type is Ordinary-Boundary Clock. P2p Transp: Clock's Device Type is Peer to Peer Transparent Clock. E2e Transp: Clock's Device Type is End to End Transparent Clock. Mastronly: Clock's Device Type is Master Only. Slaveonly:-Clock's Device Type is Slave Only. NOTE: The usual operation mode for an Ethernet Switch in a PTP network will be Transparent Clock or Boundary Clock.	Inactive

Profile

Setting	Description	Factory Default
No profile / 1588 / C37.238-2011 / 61850-9-3	Indicates the profile used by the clock.	No profile

Clicking on the clock instance number, a new page is loaded to configure all the necessary parameters.



Clock Type and Profile

The clock instance, device type and selected profile is shown. If the clock has been configured to use a profile (eg: 1588), clicking the **Apply** button will reset configured values to profile defaults.

Port Enable and Configuration

Select (check) the ports configured for this Clock Instance and click on **Ports Configuration** to edit all the data settings. The port data set is defined in the IEEE 1588 Standard and the **Help** button of the web page describes all the parameters that can be adjusted for each PTP port.

Local Clock Current Time

Shows the actual PTP time with nanosecond resolution and the actual clock adjustment method (depending on the available hardware on the network). The button **Synchronize from System Clock** is taking the switch clock reference as the PTP reference (if no Grandmaster clock available).

Clock Current DataSet

Shows information about the PTP network. Specifically, the number of PTP clocks traversed from the grandmaster to the local slave clock, the difference between the master clock and the local slave clock in nanosecond and the mean propagation time for the link between the master and the local slave.

Clock Parent DataSet

Shows dynamic information about the Grandmaster clock defined in the IEEE 1588 Standard. The **Help** button of the web page provides a description of all the displayed parameters.

Clock Default DataSet

The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here. The **Help** button of the web page provides a description of all the parameters that can be displayed and configured.

Clock Time Properties DataSet / Filter Parameters / Servo Parameters

Show specific information about the clock time properties. The user can modify the parameters if required. The **Help** button of the web page provides a description of all the parameters that can be displayed and configured.

Unicast Slave Configuration

When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master. The parameters that can be configured for each master are:

Duration

Setting	Description	Factory Default
10 to 1000 (sec)	The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.	100

IP Address

Setting	Description	Factory Default
IP address	The IPv4 address of the master clock.	None

Grant

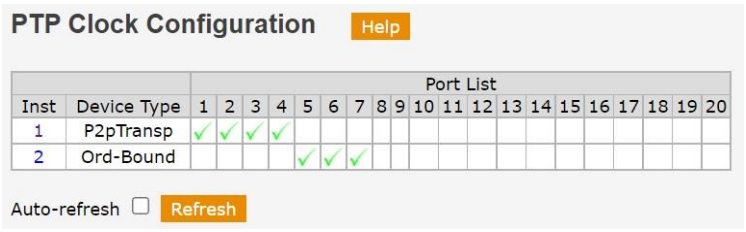
Setting	Description	Factory Default
Information only	The granted repetition period for the sync message.	None

CommState

Setting	Description	Factory Default
Information only	The state of the communication with the master, possible values are: IDLE : The entry is not in use. INIT : Announce is sent to the master (waiting for a response). CONN : The master has responded. SELL : The assigned master is selected as current master. SYNC : The master is sending Sync messages.	None

3.15.2 PTP Clock Status

This page shows an overview of the PTP clocks configured in the switch.



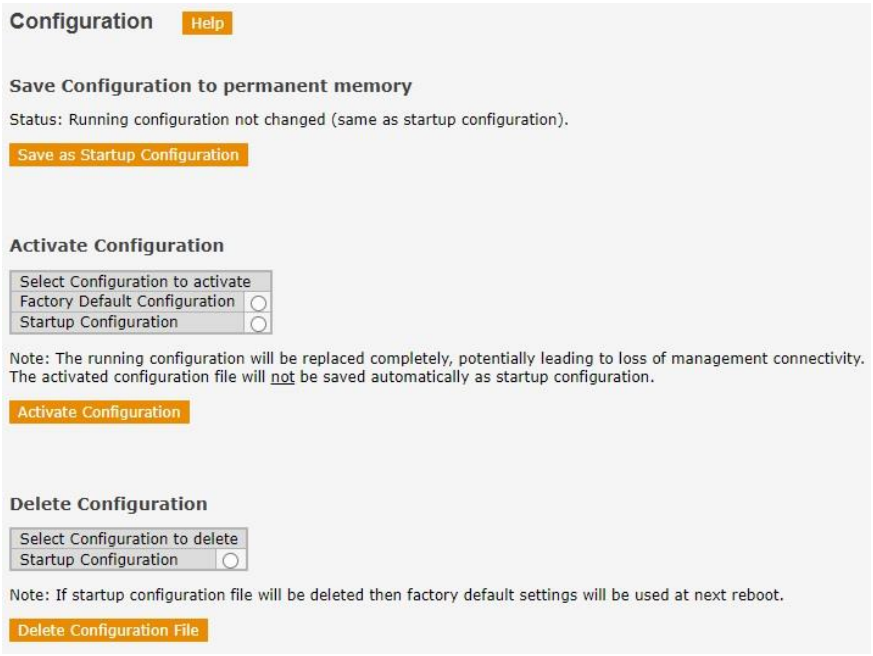
The table on the page shows the following information:

Inst	The particular clock instance.
Device Type	The type of clock for that particular instance. The five possible types are Transparent Clock (End to End or Peer to Peer), Boundary Clock, Master only or Slave only.
Port	The ports configured for that clock instance.

3.16 Save/Manage Configuration

After changing any parameter / function in a web page the button **Apply** activates the change but **does not save it**. The text *"Running configuration changed but not saved as startup configuration!*" is shown in all the pages of the web interface. It means the changes would be lost after restarting the switch.

The button **Save as Startup Configuration** permanently saves the applied changes to flash memory.

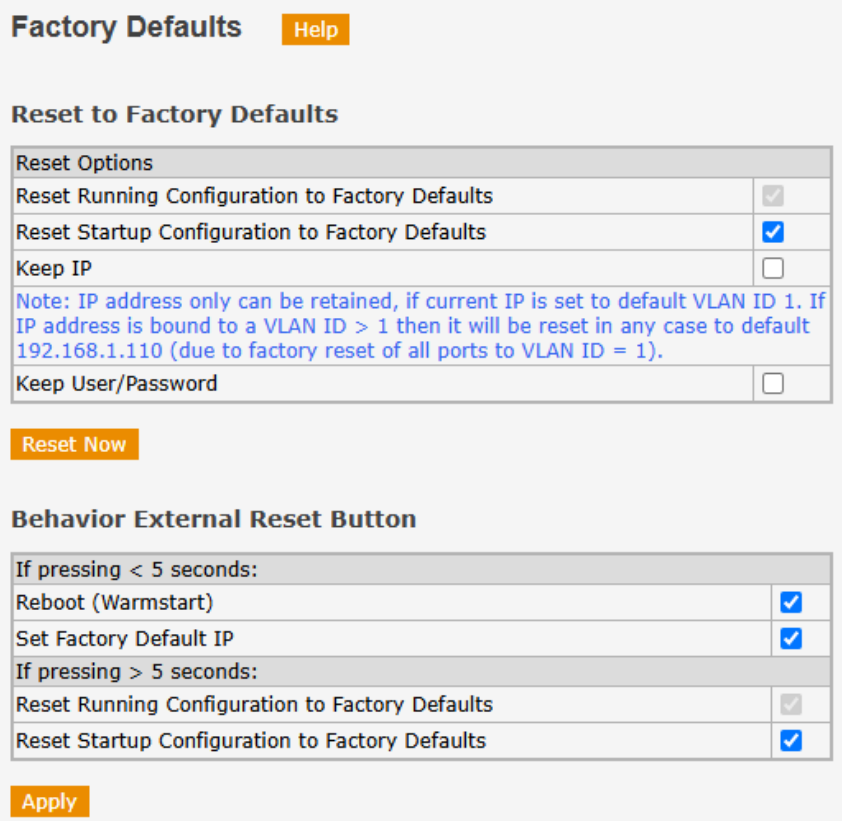


In this web page is also possible to activate the factory default configuration or startup configuration (last saved configuration) to the switch. Select the corresponding configuration file and click the **Activate Configuration** button.

Additionally, it is also possible to delete the startup configuration file by selecting the file and clicking the button **Delete Configuration File**. If the startup configuration file is delete, then the factory default settings will be used at next reboot.

3.17 Factory Defaults

This function provides users with a quick way of restoring the Weidmüller switch's configuration to factory defaults. It is also possible to define different actions for the reset button located in the front of the switch.



Reset to Factory Defaults

The user has the possibility to restore to factory defaults both the running and startup (flash) configuration but keeping the current IP address and username / password settings.

Behavior External Reset Button

Pressing the reset button located in front of the switch for more than five seconds will always restore the running configuration of the switch to factory defaults but the user can also select if the startup configuration is also restored to default values or not by this action.

Additionally, the user has the possibility to decide the effect of pushing the reset button for less than five seconds: no action, reboot the switch, set the IP address factory default or both.

3.18 System Reboot

This function is used to restart the Ethernet Switch.

3.19 Logout

This option can be used for explicit logoff from the web interface.

3.20 License Information

This page shows Weidmüller's declaration for used Open Source Software (GNU General Public License).

A. Downloads (Software and Documentation)

Using below described link you can download following items:

- Firmware Upgrades
- Private MIB files
- EDS file
- GSDML file
- Documentation (User Manual and Hardware Installation Guide)

Download via **Product Catalogue (Online Catalogue)**

- Download latest Firmware version, Private MIB file, PROFINET GSDML file, ICD file or Documentation.

http://www.weidmueller.com

► Select Product Catalogue
⇨ Select „Automation & Software“
⇨ Select „Industrial Ethernet“
⇨ Select „Substation Line Managed Switches”
⇨ Select Product model
⇨ Click and expand section „Downloads“
⇨ Download the needed items

B. Modbus Register Table

Registers can be read via ID = 1 and function code 4 (Input register).

Tag name	Register address (HEX)	Register address (DEC)	Data Type	Max Data Length (Words)	Setting (Description)
System Information					
Vendor	0x0000	0	Word	1	0x6574
Unit ID	0x0001	1	Word	1	Unit ID (Ethernet = 1)
Product Code	0x0002	2	Word	1	The last code of the OID
Switch Port Number	0x0008	8	Word	1	
Vendor Name	0x0010	16	String	16	
Product Name	0x0030	48	String	16	
Version	0x0051	81	Word	2	Firmware version + Kernel version
Firmware Release Date	0x0053	83	Word	2	Firmware was released on 2007-05-06 at 09 o'clock Word 0 = 0 x 0609 Word 1 = 0 x 0705
MAC Address	0x0055	85	Word	3	Eg. 0x001e 0x9412 0x2233
Power 1	0x0058	88	Word	1	0x0000: Off 0x0001: On
Power 2	0x0059	89	Word	1	0x0000: Off 0x0001: On
Fault LED Status	0x005a	90	Word	1	0x0000: Off 0x0001: On
IP Address	0x0090	144	String	16	Eg. 192.168.1.110
System Name	0x0100	256	String	128	
System Description	0x0200	512	String	128	
System Location	0x0300	768	String	128	
System Contact	0x0400	1024	String	128	
Port Information					
Port 1 to 6 Status	0x1000 to 0x1005	4096	Word	1	0x0000: Link down 0x0001: Link up 0x0002: Disable
Port 1 to 6 Speed	0x1100 to 0x1105	4352	Word	1	0x0000: 10M-Half 0x0001: 10M-Full 0x0002: 100M-Half 0x0003: 100M-Full
Port 1 to 6 Flow Ctrl	0x1200 to 0x1205	4608	Word	1	0x0000:Off 0x0001:On
Port Description	0x1400 to 0x1405	5120	String	16	Eg. 100TX
Port PoE Voltage	0x1800~	6144	Word	1	Eg. 0x0005: PoE voltage = 5V
Port PoE Current	0x1830~	6192	Word	1	Eg. 0x000D: PoE current = 13A
Port PoE Power	0x1860~	6240	Word	1	Eg. 0x000A: PoE power = 10W

Packets Information					
Port Tx Packets	0x2000~	8192	Word	2	Eg. 0x44332211: Packet amount = 44332211 Word 0 = 4433 Word 1 = 2211
Port Rx Packets	0x2100~	8448	Word	2	Eg. 0x44332211: Packet amount = 44332211 Word 0 = 4433 Word 1 = 2211
Port Tx Error Packets	0x2200~	8704	Word	2	Eg. 0x44332211: Packet amount = 44332211 Word 0 = 4433 Word 1 = 2211
Port Rx Error Packets	0x2300~	8960	Word	2	Eg. 0x44332211: Packet amount = 44332211 Word 0 = 4433 Word 1 = 2211
Redundancy Information					
Redundancy Protocol	0x3000	12288	Word	1	0x0000: None 0x0001: RSTP 0x0002: O-Ring 0x0003: O-Chain
RSTP Root	0x3100	12544	Word	1	0x0000: Not Root Bridge 0x0001: Root Bridge
RSTP Port 1 to 6 Status	0x3200	12800	Word	1	0x0000: Port Disabled 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: RSTP Not Enable
O-Ring Master / Slave	0x3300	13056	Word	1	0x0000: Slave 0x0001: Master
O-Ring 1st Port Status	0x3301	13057	Word	1	0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding 0xFFFF: Not Enabled
O-Ring 2nd Port Status	0x3302	13058	Word	1	0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding 0xFFFF: Not Enabled
Coupling Ring Enabled	0x3303	13059	Word	1	0x0000: Off 0x0001: On
Coupling Port Status	0x3304	13060	Word	1	0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding 0xFFFF: Not Enabled
O-Chain Edge Switch	0x3700	14080	Word	1	0x0000: Not Edge Switch 0x0001: Edge Switch
O-Chain 1st Port Status	0x3701	14081	Word	1	0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding

					0xFFFF: Not Enabled
O-Chain 2nd Port Status	0x3702	14082	Word	1	0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding 0xFFFF: Not Enabled

C. Supported Logical Nodes (MMS)

LLN0

Category (DO)	Name (DA)	Description	Value	Type	Read / Write
NamPlt	vendor	Vendor Name		Char	RO
	swRev	Software Version		Char	RO
	configRev	Kernel Version		Char	RO
Health	stVal	Switch Status	1: Normal; 3: Fault Alarm Status	Int32	RO

LBRI1

Category (DO)	Name (DA)	Description	Value	Type	Read / Write
NamPlt	vendor	Vendor Name		Char	RO
	swRev	Software Version		Char	RO
	configRev	Kernel Version		Char	RO
MacAddr	stVal	MAC address of switch		Char	RO
RstpRoot	stVal	RSTP root status	True: Enabled False: Disabled	Boolean	RO
RstpPrio	setVal	Priority of STP		Int32	RW
RstpEna	setVal	RSTP admin mode	True: Enabled False: Disabled	Boolean	RW

LPHD1

Category (DO)	Name (DA)	Description	Value	Type	Read / Write
LdpEna	setVal	LLDP admin mode	True: Enabled False: Disabled	Boolean	RW
LocAddrTyp	stVal	Address Subtype of LLDP	1	Int32	RO
LocAddr	stVal	Management IP Address		Char	RO
LocChsldTyp	stVal	Chassis ID Subtype of LLDP	4	Int32	RO
LocChsld	stVal	MAC Address of Switch		Char	RO
PhyHealth	stVal	Switch Status	1: Normal; 3: Fault Alarm Status	Int32	RO

LPCP1-20

Category (DO)	Name (DA)	Description	Value	Type	Read / Write
RxCnt	actVal	Number of Rx packets		Int32	RO
TxCnt	actVal	Number of Tx packets		Int32	RO
NamPlt	vendor	Vendor Name		Char	RO
	swRev	Software Version		Char	RO
	configRev	Kernel Version		Char	RO
AutoNgt	stVal	Auto-nego Ability	True: Enabled	Boolean	RO

			False: Disabled		
AutoNgtCfg	setVal	Auto-nego Status	True: Enabled False: Disabled	Boolean	RW
Mau	stVal	RFC 3636 MAU	See Mau Table below	Int32	RO
AdminCfg	setVal	Admin Status of Port	True: Enabled False: Disabled	Boolean	RW

LBSP1-20

Category (DO)	Name (DA)	Description	Value	Type	Read / Write
RstpSt	stVal	RSTP Port Status	1: disabled / link down / not RSTP port 2: blocking 3: listening 4: learning 5: forwarding 6: unknown	Int32	RO

LCCH1-20

Category (DO)	Name (DA)	Description	Value	Type	Read / Write
ChLiv	stVal	Port Link Status	True: Link Up False: Link Down	Boolean	RO

LPLD1-20

Category (DO)	Name (DA)	Description	Value	Type	Read / Write
LocPortDesc	stVal	LLDP Local Port Description	Port #X, being X port number	Char	RO
LocPortIdTyp	stVal	LLDP Local Port ID Subtype	7	Int32	RO
LocPortId	stVal	LLDP Local Port ID	Port Number	Int32	RO
RemPortDesc	stVal	LLDP Remote Port Description		Char	RO
RemPortIdTyp	stVal	LLDP Remote Port ID Subtype		Char	RO
RemChsIdTyp	stVal	LLDP Remote Chassis ID Subtype		Char	RO
RemPortId	stVal	LLDP Remote Port ID	Port Number	Int32	RO
RemChsId	stVal	LLDP Remote Chassis ID		Char	RO
RemSysDesc	stVal	LLDP Remote System Description		Char	RO
RemAddrTyp	stVal	LLDP Management Address Subtype		Char	RO
RemAddr	stVal	LLDP Management Address		Char	RO

PwrGGIO1

Category (DO)	Name (DA)	Description	Value	Type	Read / Write
Alm1-2	stVal	Power Status	True: Power on False: Power off	Boolean	RO

MAU Table

Code (Value)	Item	Description
0	bOther	Other or Unknown
1	bAUI	AUI
2	b10Base5	10Base-5
3	bFoirl	FOIRL
4	b10base2	10Base-2
5	b10baseT	10Base-T duplex mode unknown
6	b10baseFP	10Base-FP
7	b10baseFB	10Base-FB
8	b10baseFL	10Base-FL duplex mode unknown
9	b10broad36	10BROAD36
10	b10baseTHD	10Base-T half duplex mode
11	b10baseTFD	10Base-T full duplex mode
12	b10baseFLHD	10Base-T half duplex mode
13	b10baseFLFD	10Base-T full duplex mode
14	b100baseT4	100Base-T4
15	b100baseTXHD	100Base-TX half duplex mode
16	b100baseTXFD	100Base-TX full duplex mode
17	b100baseFXHD	100Base-FX half duplex mode
18	b100baseFXFD	100Base-FX full duplex mode
19	b100baseT2HD	100Base-T2 half duplex mode
20	b100baseT2FD	100Base-T2 full duplex mode
21	b1000baseXHD	1000Base-X half duplex mode
22	b1000baseXFD	1000Base-X full duplex mode
23	b1000baseLXHD	1000Base-LX half duplex mode
24	b1000baseLXFD	1000Base-LX full duplex mode
25	b1000baseSXHD	1000Base-SX half duplex mode
26	b1000baseSXFD	1000Base-SX full duplex mode
27	b1000baseCXHD	1000Base-CX half duplex mode
28	b1000baseCXFD	1000Base-CX full duplex mode
29	b1000baseTHD	1000Base-T half duplex mode
30	b1000baseTFD	1000Base-T full duplex mode
31	b10GbaseX	10GBase-X
32	b10GbaseLX4	10GBase-LX4
33	b10GbaseR	10GBase-R
34	b10GbaseER	10GBase-ER
35	b10GbaseLR	10GBase-LR
36	b10GbaseSR	10GBase-SR
37	b10GbaseW	10GBase-W
38	b10GbaseEW	10GBase-EW
39	b10GbaseLW	10GBase-LW
40	b10GbaseSW	10GBase-SW