Industrial Ethernet IEC-61850-3 Switches

Manual

for

IE-SW-SL10M-7TX-3GC

of

SubstationLine

Third Edition, May 2023

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

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-SL10M-7TX-3GC 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.

☐ **Command Line Interface (CLI) Management**

This chapter describes how to configure the Weidmüller switch using the Command Line Interface (CLI) available through the console port or via Telnet.

2. Getting Started

The IE-SW-SL10M-7TX-3GC 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

- 7 x 10/100Base-T(X) ports
- 3 x 10/100/1000Base-T(X) or 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 TFTP-Server
- Network redundancy
  - Spanning Tree Protocol (STP)
  - Rapid Spanning Tree Protocol (RSTP)
  - Multiple Spanning Tree Protocol (MSTP)
  - 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
  - NTP server
  - SNTP client
- Monitoring functions
  - SNMP v1/v2c/v3
  - Link Layer Discovery Protocol (LLDP)
  - Port mirroring
  - Port statistics
  - Port monitoring
  - Syslog
  - Event based warning (via e.mail / via output relay / via SNMP trap)
- Network traffic filter
  - Quality of Service (QoS)
  - Class of Service (CoS) according to IEEE 802.1p
  - Type of Service (ToS) / Differentiated Services Code Point (DSCP)
  - Port / Tag based VLAN
  - IGMP v2/v3
  - Multicast VLAN Registration (MVR)
  - Traffic Rate Limiting
- Security functions
  - VLAN segmentation
  - Enable / Disable ports
  - TACACS+ User Authentication
  - Access Control (port based via IEEE 802.1X)
  - Access Control List (IP based / MAC based)
  - Loop protection
  - Management access security via secure IP list
  - Configuration of allowed access methods (web-interface, telnet, SSH)

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.

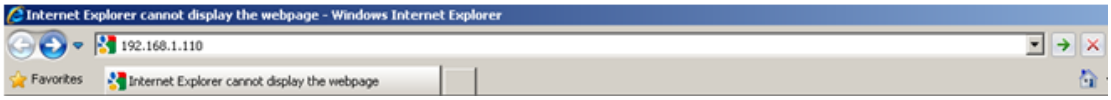
NOTE: If the Weidmüller switch is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

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, Firmware 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.

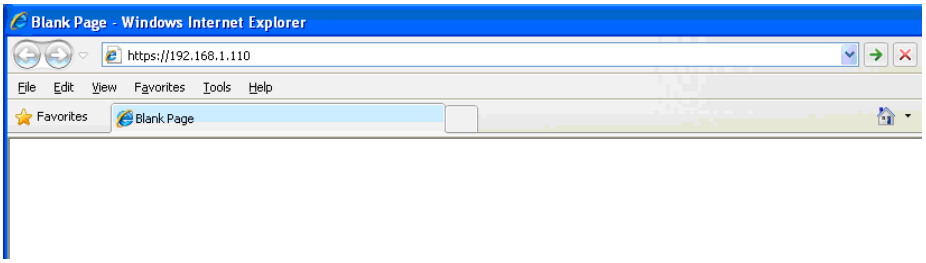
NOTE: The pages of the Web interface include a **Help** button that describes the parameters and functions that can be programmed or monitored in each web page.

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 Configuration** option of the menu.

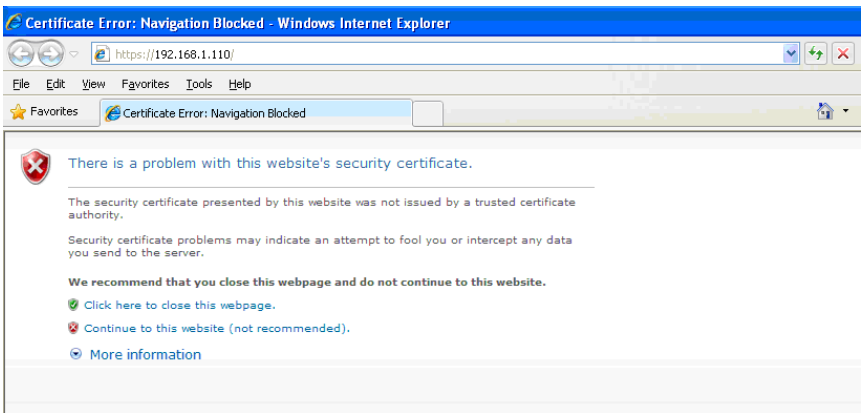
3.2 Accessing the Web interface via HTTPS

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.



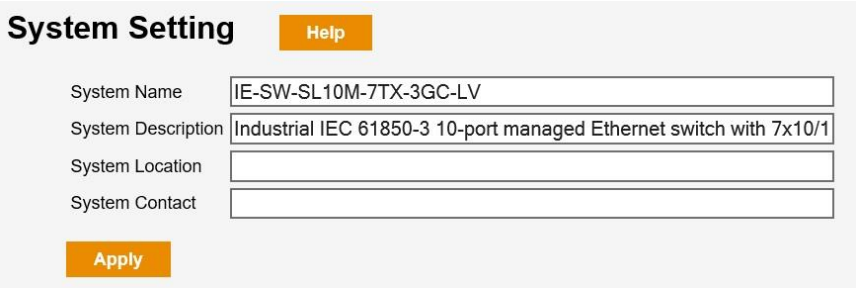
Select "**Continue to this website"** to enter the Weidmüller switch´s web browser interface and access the web browser interface secured via HTTPS.

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 System Setting

The system identification 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. 64 characters	This option is useful for recording a name of the unit.	Name of type

System Description

Setting	Description	Factory Default
Max. 64 characters	This option is useful for recording a more detailed description of the unit.	Description of type

System Location

Setting	Description	Factory Default
Max. 64 characters	This option is useful for differentiating between the locations of different units. Example: Bay 1.	None

System contact

Setting	Description	Factory Default
Max. 64 characters	This option is useful for providing information about who is responsible for maintaining this unit and how to contact this person.	None

3.3.2 Admin Password

The default values of the user name and password used to access to the management options of the Weidmüller switch can be changed.

NOTE: The Switch's default **user name** / **password** are **"admin"** / **"Detmold"**. If these are changed, then you will be required to type the new user name and password when logging into the serial console, Telnet console, or Web console.

The button **Show Passwords/Hide Passwords** can be used to see as readable text or not the introduced password characters.

User Name

Setting	Description	Factory Default
Min / Max length is 5 / 31 characters	Enter the new user name. Allowed characters are: A-Z a-z 0-9 ! @ # $ - _	admin

Confirm Old Password

Setting	Description	Factory Default
Min / Max length is 7 / 31 characters	Enter the old password.	Detmold

New Password

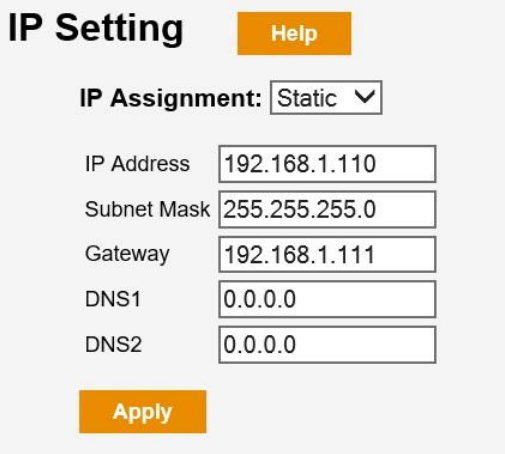
Setting	Description	Factory Default
Min / Max length is 7 / 31 characters	Enter the new password. Allowed characters are: A-Z a-z 0-9 ! @ # $ - _	None

Confirm Password

Setting	Description	Factory Default
Min / Max length is 7 / 31 characters	Enter the new password again. Allowed characters are: A-Z a-z 0-9 ! @ # $ - _	None

3.3.3 IP Setting

The IPv4 settings allow the user to set manually the IP parameters or by means of a DHCP server.



See a brief explanation of each configuration item below.

IP assignment

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

IP Address

Setting	Description	Factory Default
IP address for the Weidmüller Switch	Assigns the Weidmüller Switch´s IP address on a TCP/IP network.	192.168.1.110

Subnet Mask

Setting	Description	Factory Default
Subnet mask for the Weidmüller Switch	Identifies the type of network to which the Switch is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

Gateway

Setting	Description	Factory Default
IP address for the gateway	The IP address of the router that connects the LAN to an outside network.	None

DNS1 and DNS2

Setting	Description	Factory Default
1st DNS Server's IP address	The IP address of the DNS Server used by your network.	None
2nd DNS Server's IP address	The IP address of the secondary DNS Server used by your network. The Switch will use the 2nd DNS Server if the 1st DNS Server fails to connect.	None

3.3.4 IPv6 Setting

IPv6 setting includes two distinct address types—Link-Local Unicast address and "Global" address. A Link-Local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. To connect to a larger network with multiple segments, the switch must be configured with a "Global" address.

Auto Configuration

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.	

Address

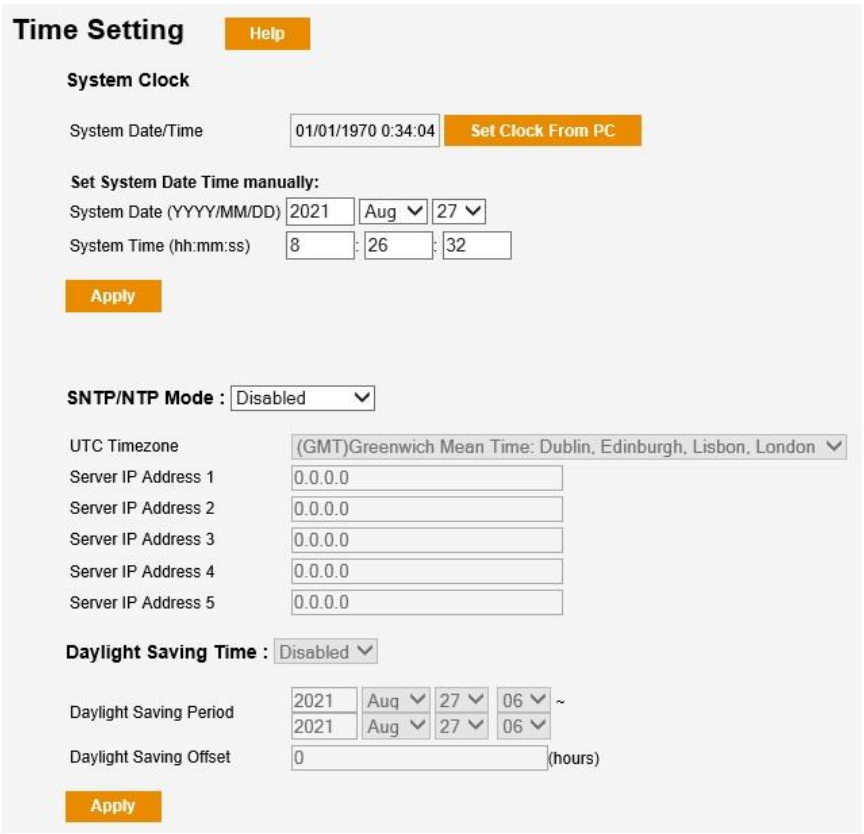
Setting	Description	Factory Default
IP address for the Weidmüller Switch	Assigns the Weidmüller Switch´s IPv6 “Global” address.	None

Link Local Address

Setting	Description	Factory Default
None	The network portion of the Link-Local address is FE80 and the host portion of the Link-Local address is automatically generated using the modified EUI-64 form of the interface identifier (Switch’s MAC address)	FE80 :: (EUI-64 form of the MAC address)

3.3.5 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 NTP server or there is no NTP 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 **Set Clock from PC**.	None

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/NTP mode

Setting	Description	Factory Default
Disabled	No NTP/SNTP used in the switch.	Disabled
Server (NTP)	The Weidmüller switch can synchronize other switches of the network with its programmed time clock.	
Client (SNTP)	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 GMT (Greenwich Mean Time).	GMT (Greenwich Mean Time)

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

Setting	Description	Factory Default
Enabled / Disabled	Automatically set the Weidmüller switch's time forward according to national standards.	Disabled

Daylight Saving Period

Setting	Description	Factory Default
User-specified date.	Specifies the beginning and end date of the Daylight Saving Time.	None

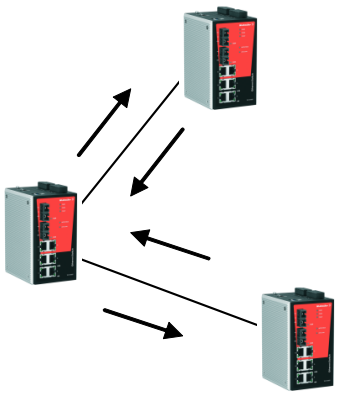
Offset

Setting	Description	Factory Default
User-specified hour.	Specifies the number of hours that the time should be set forward during Daylight Saving Time.	None

3.3.6 LLDP Function

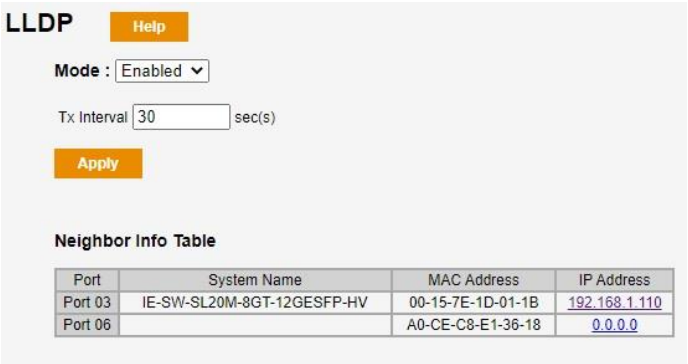
3.3.6.1 Overview

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.

3.3.6.2 Configuring LLDP Settings



General Settings

Mode

Setting	Description	Factory Default
Enable or Disable	Enables or disables the LLDP function.	Enable

Tx Interval

Setting	Description	Factory Default
Numbers from 1 to 9999 sec.	To set the transmit interval of LLDP messages. Unit is in seconds.	30 (sec)

Neighbor Info Table

The LLDP Table displays the following information:

Port	The port number that connects to the neighbor device.
System Name	Hostname of the neighbor device.
MAC Address	The MAC address that identifies a neighbor device.
IP Address	The IP address of a neighbor device. By clicking on this IP address we can reach the web interface of that neighbor.

3.3.7 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

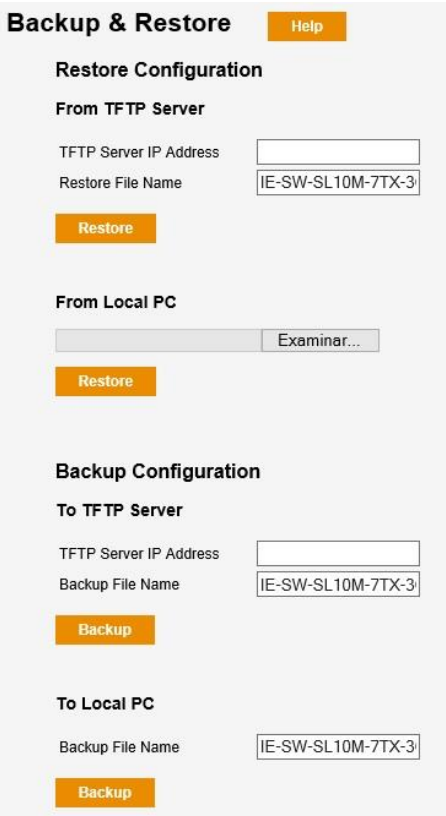
Modbus TCP is disabled by default. To enable Modbus TCP, select **Enable** in **Mode** and then click **Apply**.

In the Appendix B, Modbus Register Table, the user can find all the available registers of the switch.

3.3.8 Backup & Restore

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

- Download a new configuration from remote TFTP server
- Loading a new configuration by importing a file already saved in connected PC
- Upload the current configuration to remote TFTP server
- Save the current configuration in connected PC



TFTP Server IP Address

Setting	Description	Factory Default
IP Address of TFTP Server	Specifies the IP address or name of the remote TFTP server. Must be set up before downloading or uploading files.	None

Restore & Backup File Names

Setting	Description	Factory Default
File name	Specifies the file name of the Weidmüller switch's configuration file.	Name of type

After setting the desired file names, click **Restore** to download the prepared file from the remote TFTP server or to load the configuration file already saved in the computer, or click **Backup** to upload the desired file to the remote TFTP server or to save it to the local host.

3.3.9 Upgrade Firmware

This page lets users upgrade the firmware of the Weidmüller's switches, either from remote TFTP server or from local file.

Upgrade firmware from TFTP server

TFTP Server IP

Setting	Description	Factory Default
IP Address of TFTP Server	Specifies the IP address of the remote TFTP server. Must be set up before downloading the firmware.	None

Firmware File Name

Setting	Description	Factory Default
File name	Specifies the path and file name of the Weidmüller switch's firmware file.	None

After setting the IP address and file names click **Upgrade** to upgrade the firmware of the switch from the remote TFTP server.

Upgrade Firmware from Local PC

To import a new firmware file into the Weidmüller switch, click **Browse** to select the firmware file that is saved on your computer. The upgrade procedure will proceed automatically after clicking **Upgrade**.

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 IP loop guard and Port trunking.

3.4.1 Port control

Port Access, Port Transmission Speed, Flow Control and Security can be programmed from this option.

State

Setting	Description	Factory Default
Enabled	Allows data transmission through the port.	Enabled
Disabled	Immediately shuts off port access.	

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.

Speed/Duplex

Setting	Description	Factory Default
AutoNegotiation	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.	Auto
1000M-Full	Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	
1000M-Half		
100M-Full		
100M-Half		
10M-Full		
10M-Half		

Flow Control

Setting	Description	Factory Default
Disabled	Disables flow control for this port.	Disabled
Symetric	Enables flow control for this port if flow control is enabled in both linked up ports.	
Asymetric	Enables flow control for this port regardless the flow control in the linked port is enabled or not.	

Security

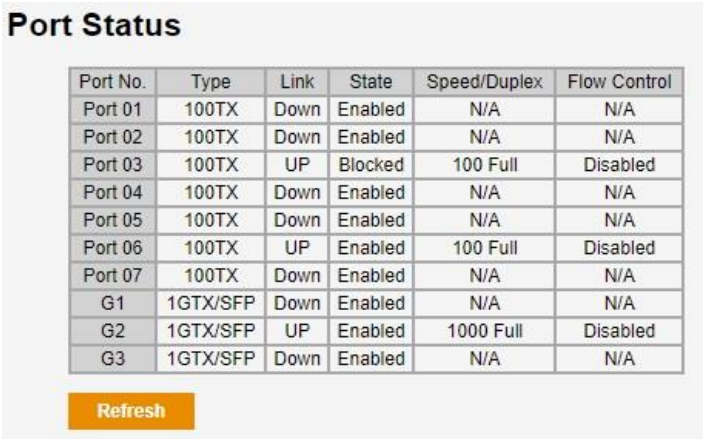
Setting	Description	Factory Default
Enabled	MAC address learning is disabled in this port. Accordingly, only the frames with MAC address in port security list will be forwarded (others will be discarded).	Disabled
Disabled	MAC address learning enabled in this port.	

Auto Detect 100/1000SFP

Setting	Description	Factory Default
Enabled	Allows the automatic speed negotiation for installed SFP transceivers.	Enabled
Disabled	No speed negotiation in SFP transceivers. This option cannot be selected if the speed of the port is set in AutoNegotiation status.	

3.4.2 Port status

From this option the user can easily display the status of the different ports of the switch (Up/Down, Enabled/Blocked/Disabled, Speed and Flow control).



3.4.3 Port Alias

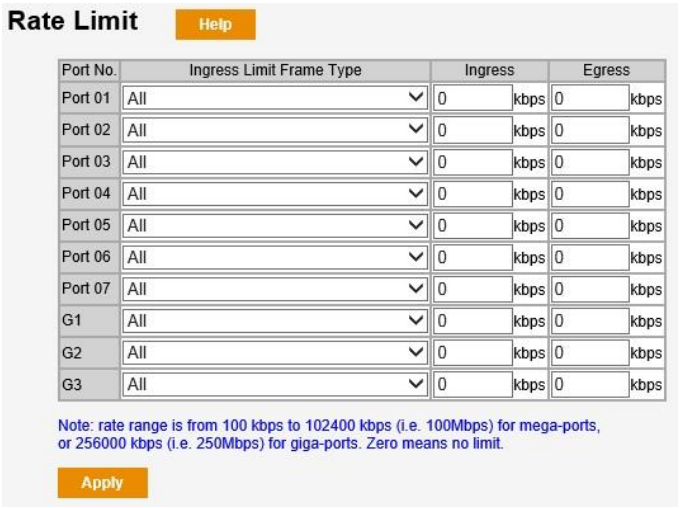
From this option it can be specified an alias (name) for each port to help administrators differentiate between different ports.

Port alias

Setting	Description	Factory Default
Max. 128 characters	Name of the port. Example: Main Busbar Protection Relay	None

3.4.4 Rate Limit

This option allows the user to set for each port the ingress and egress rate limits of different packet types.



Ingress Limit Frame Type	Ingress / Egress rage	Factory Default
All	Select the ingress and egress rate limits in kbps for different packet types. The lowest range is 100 kbps. Value 0 means not limit.	All. 0 (no limit)
Broadcast / Multicast / Flooded Unicast		
Broadcast / Multicast		
Broadcast only		

3.4.5 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 4 ports for each group. If one of the 4 ports fails, the other 3 ports will provide back up and share the traffic automatically.

Port Trunking can be used to combine up to 4 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 800 Mbps.

The Port Trunking Concept

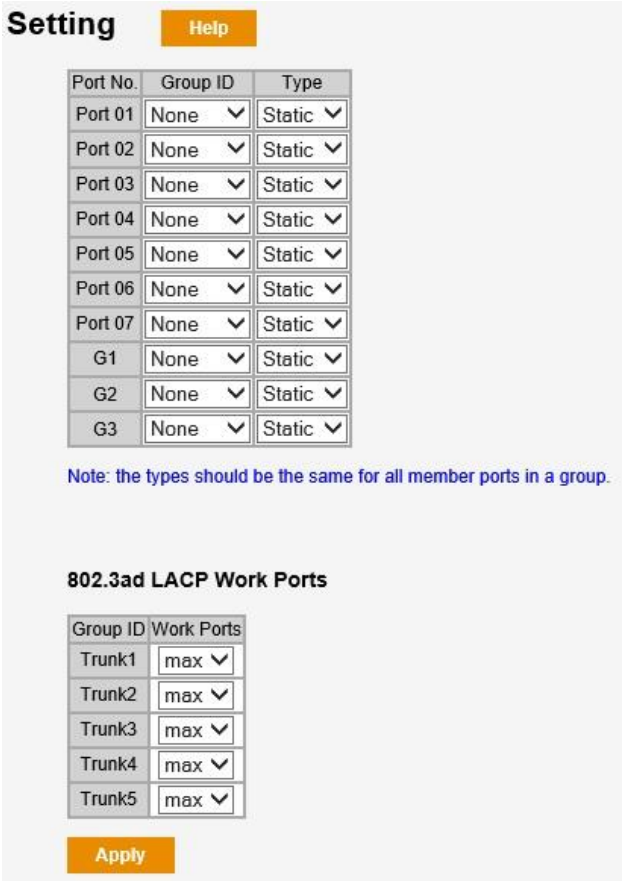
The Port Trunking protocol provides the following benefits:

- 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.

3.4.5.1 Port Trunking Setting

The **Port Trunking Settings** page is used to assign ports to a Trunk Group.



Step 1: For each port select the desired **Trunk Group (1, 2, 3, 4, …)** from the **Group ID** drop-down box.

Step 2: Select Static, or LACP from the **Type** drop-down box.

Step 3: Select the maximum number of working ports for each Trunk Group (only applicable if Trunk Groups are type LACP).

Step 4: Click **Apply** button.

Group ID

Setting	Description	Factory Default
Trk1, Trk2, Trk3, …Trkn	Specifies the current trunk group	None

Type

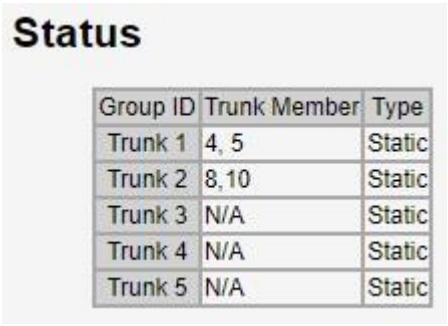
Setting	Description	Factory Default
Static	Selects proprietary trunking protocol	Static
LACP	Selects LACP (IEEE 802.3ad, Link Aggregation Control Protocol).	

802.3ad LACP Work Ports

Setting	Description	Factory Default
Max	Select the number of active ports in Trunk Groups type LACP. If the number is not the maximum number of ports, the other inactive ports will be suspended (no traffic). If the active port is broken, the suspended port will be active automatically.	Max
1		
2		
3		
4		

3.4.5.2 Port Trunking Status

This page shows a table with the status of the different Trunk Groups programmed in the switch.

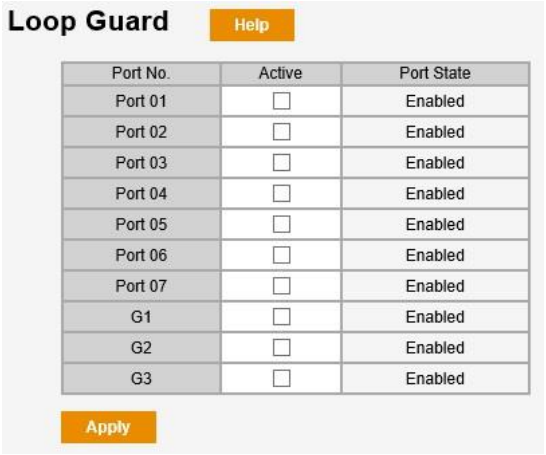


Trunk Table

Setting	Description
Group ID	Displays the Trunk Group.
Trunk Member	Displays which member ports belong to the trunk group.
Type	Displays the Trunk Type

3.4.6 Loop Guard

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



If Loop Guard is **Active** in one port, a loop in that port will be blocked if the loop happens on the switch itself.

3.5 Redundancy

3.5.1 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
- 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 and 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	**O-Chain**	**STP**	**RSTP/MSTP**
Topology	Ring	Chain	Ring, Mesh	Ring, Mesh
Recovery Time	~ 10 ms	~ 10 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.

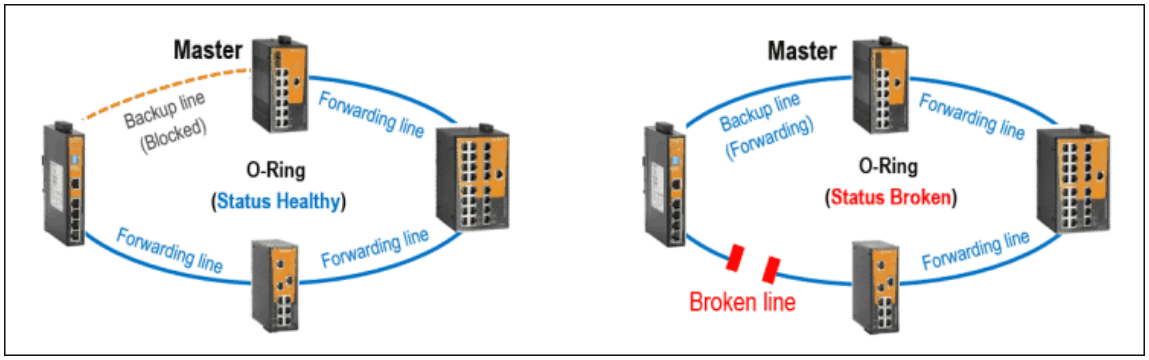
3.5.2 The O-Ring Concept

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.

3.5.2.1 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.



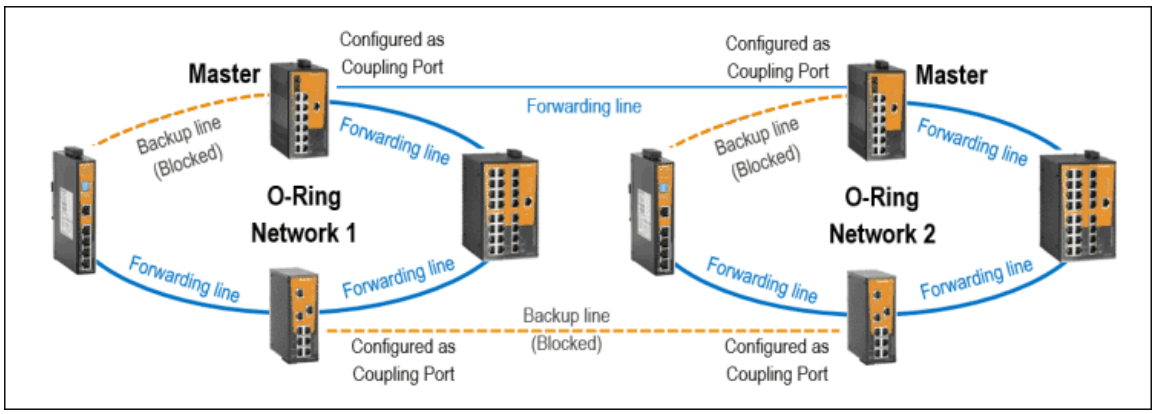
For failure detection the O-Ring protocol uses simultaneously two methods:

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.

3.5.2.2 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.

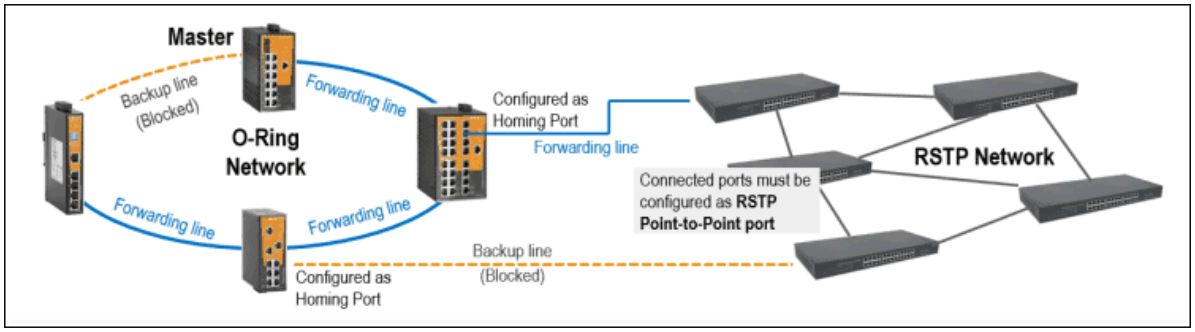
For coupling of two O-Ring networks at both sides the coupling ports must be selected and enabled. Any two switches within an O-Ring network can be selected being a ring coupling switch. The configured coupling switches automatically determine which of the both coupling connections will be the forwarding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

3.5.2.3 Dual Homing Configuration

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

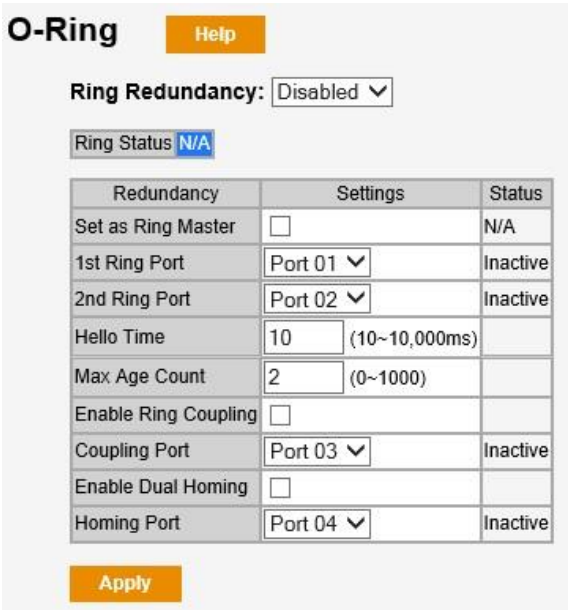


For a Dual Homing connection on any two switches inside of the O-Ring network a Homing port needs to be selected and enabled. Each configured Homing port must be connected to a RSTP enabled port on any switch of the RSTP network. Configure RSTP port being of type Point-to-Point (for switch interconnections). 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.

3.5.3 Configuring “O-Ring”

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



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

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

- Activate checkbox ‘*Set as 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

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

- Activate checkbox ‘*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:

- Activate checkbox ‘*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

Set as Ring Master

Setting	Description	Factory Default
Check	Select this Switch as Master.	Not checked
Uncheck	Do not select this Switch as Master.	
Status	**Description**	**Factory Default**
N/A	O-Ring redundancy disabled.	N/A
Master	Switch programmed as Master.	
Slave	Switch programmed as Slave.	

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 redundancy disabled.	Inactive
Link down	No connection in this port.	
Forwarding	Normal transmission in this port.	
Blocked	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

Enable Ring Coupling

Setting	Description	Factory Default
Check	Enables the Ring Coupling operation in the Switch.	Not checked
Uncheck	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	Ring Coupling is disabled.	Inactive
Link down	No connection in this port.	
Forwarding	Normal transmission in this port.	
Blocked	The port is connected to a backup path and the path is blocked.	

Enable Dual Homing

Setting	Description	Factory Default
Check	Enables the Dual Homing operation in the Switch.	Not checked
Uncheck	Does not enable the Dual Homing operation in the Switch.	

Homing Port

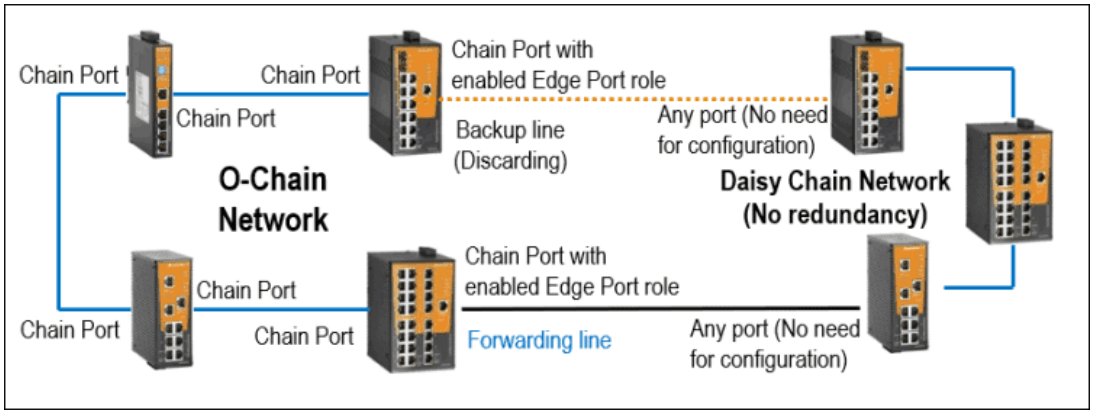
Setting	Description	Factory Default
Homing Port	Select any port of the Switch to be the homing port.	Port 04
Status	**Description**	**Factory Default**
Inactive	Dual Homing is disabled.	Inactive
Link down	No connection in this port.	
Forwarding	Normal transmission in this port.	
Blocked	The port is connected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

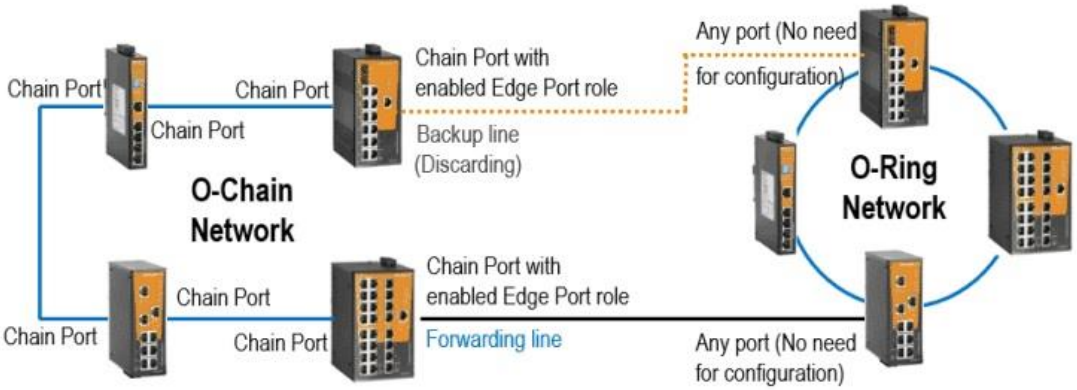
3.5.4 The O-Chain Concept

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.

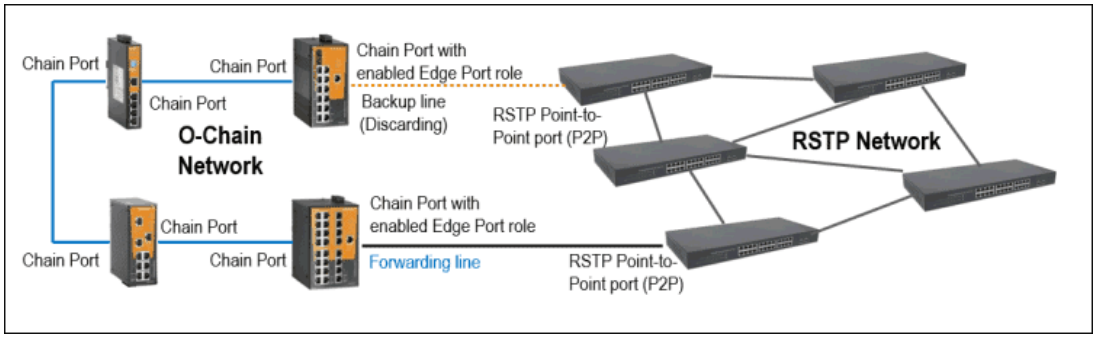
Recovery time for O-Chain connected to Daisy Chain of Weidmüller's Substation/Advanced Line switches OR to an O-Ring network of Substation/Advanced Line switches





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

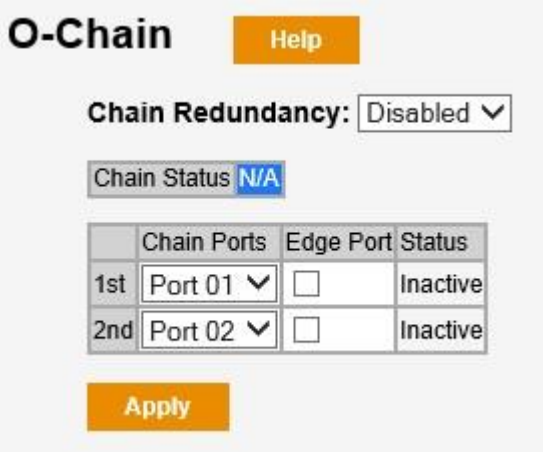
until the MAC address tables of the 3rd party switches will be renewed after the remaining aging-time has been expired.

3.5.5 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**
Enabled	Enable the O-Chain operation.	Disabled
Disabled	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**
Inactive	O-Chain redundancy disabled.	Inactive
Link down	No connection in this port.	
Forwarding	Normal transmission in this port.	
Blocked	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. Only on the two O-Chain Edge port switches **one port** may be selected having the Edge port role. All other ports of the member switches of the chain have to be configured simply as chain ports. The Edge port of the O-Chain Edge switch with lowest MAC address will become the blocking port as long as the chain status is healthy.	Not checked
Uncheck	Does not configure a port of the daisy Chain as edge port.	

3.5.6 STP / RSTP

3.5.6.1 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.

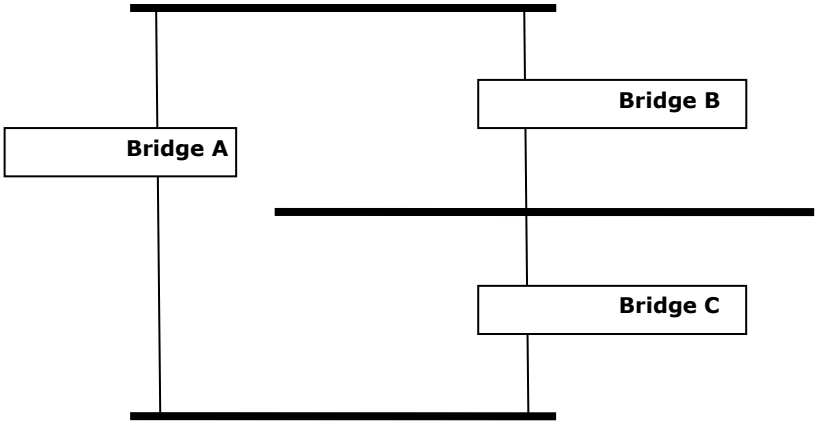
You get essentially the same functionality with RSTP and STP. To see how the two systems differ, see section '*Differences between STP and RSTP*' later in this chapter.

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

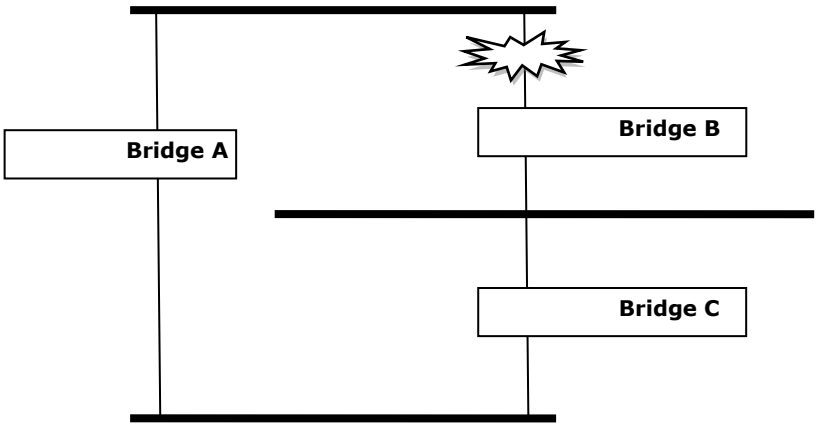
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- 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.

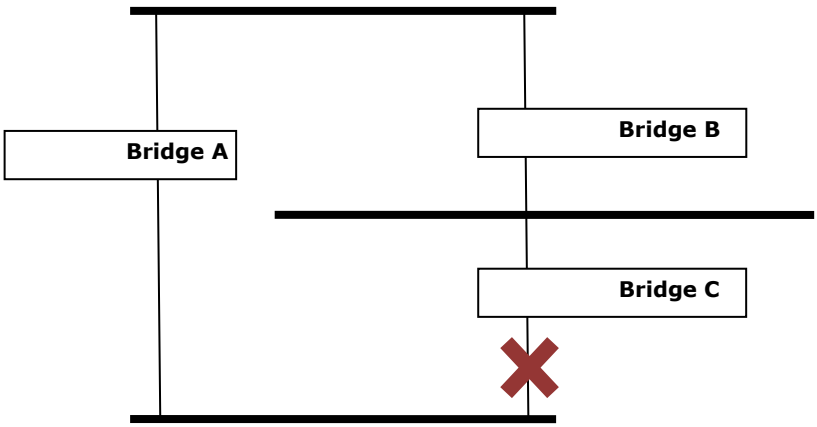
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



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.

3.5.6.2 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

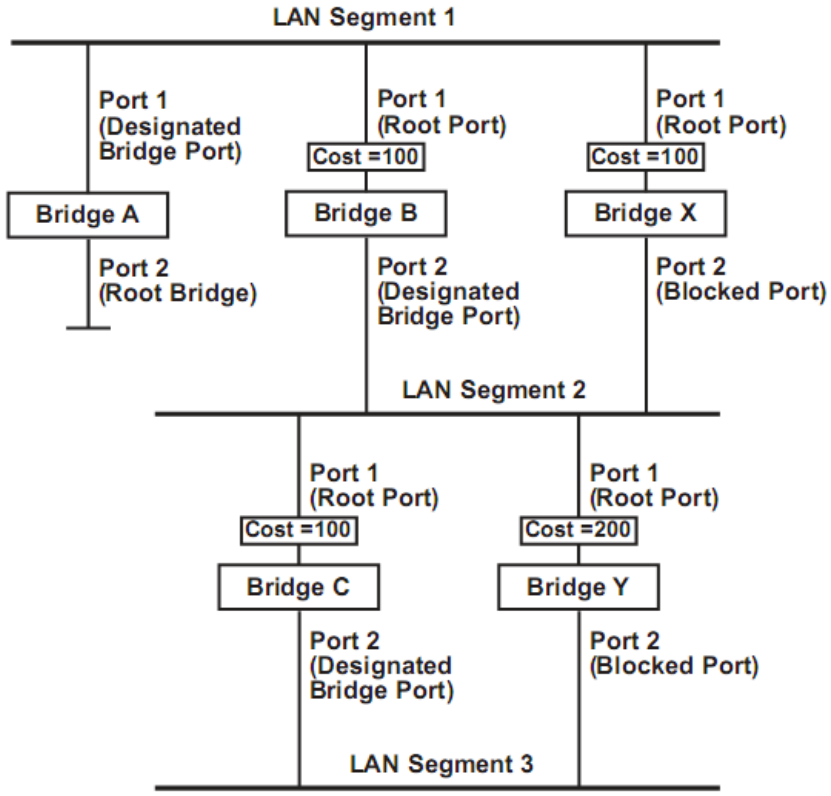
Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, 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.

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.

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.

3.5.6.3 Configuring RSTP

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

Bridge Setting

RSTP mode

Setting	Description	Factory Default
Enable/Disable	Select to enable the RSTP redundancy in the switch.	Disabled

Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Max. Age (sec)

Setting	Description	Factory Default
Numerical value input by user	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

Hello time (sec)

Setting	Description	Factory Default
Numerical value input by user	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

Forwarding Delay Time (sec)

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

Port Setting

Enable RSTP per Port

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as a node on the Spanning Tree topology.	Disabled

NOTE: We suggest not enabling the Spanning Tree Protocol once the port is connected to a device (PLC, RTU, etc.) as opposed to network equipment. The reason is that it will cause unnecessary negotiation.

Path Cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology. The value 0 is for automatic calculation.	0

Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by entering a lower number.	128

Point to Point (P2P)

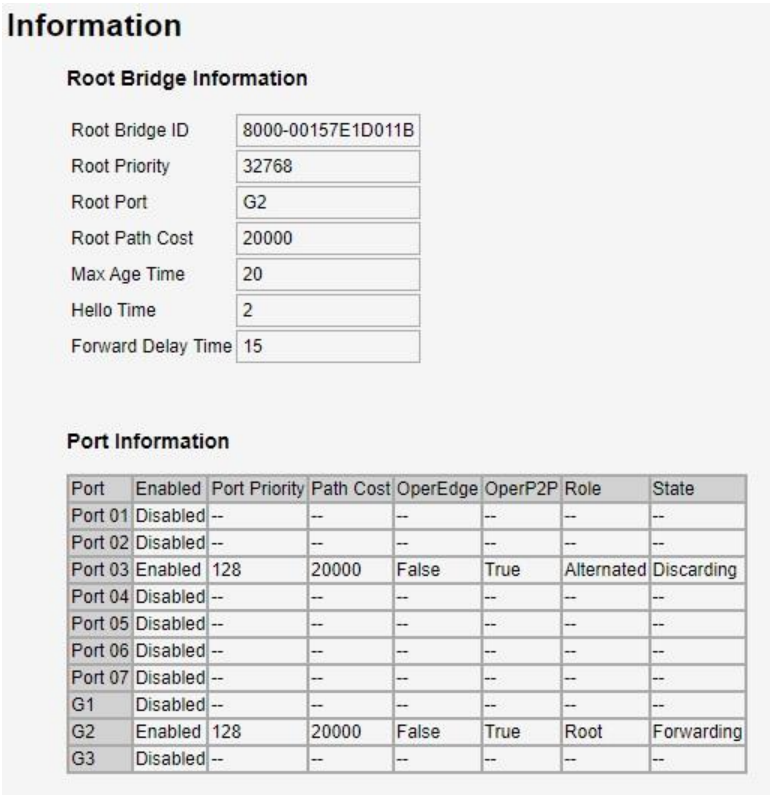
Setting	Description	Factory Default
Auto	Automatic detection if the link port is point to point or not.	Auto
True	The port link is point to point and then is a candidate for rapid transition to the forwarding state.	
False	The port link is not point to point.	

Edge Port

Setting	Description	Factory Default
True	The port is fixed as an edge port and will always be in the forwarding state	True
False	The port is set as the normal RSTP port	

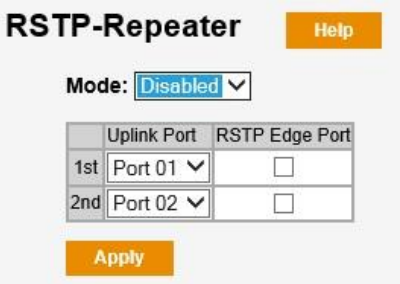
3.5.6.4 Information RSTP

It indicates the current Spanning Tree status of the switch and all the ports. "**Forwarding"** for normal transmission and "**Discarding**" if the port is blocking or not programmed for RSTP.



3.5.6.5 RSTP-Repeater

RSTP-repeater is a simple function to pass a BPDU packet directly from one RSTP device to another as if they were directly connected.



Mode

Setting	Description	Factory Default
Enabled	Enable the RSTP-repeater operation.	Disabled
Disabled	Disable the RSTP-repeater operation.	

Uplink Ports

Setting	Description	Factory Default
1st Uplink Port	Select any port of the Switch according to the topology of the network.	Port 01
2nd Uplink Port	Select any port of the Switch according to the topology of the network.	Port 02

RSTP Edge Port

Setting	Description	Factory Default
Check	The port is directly connected to the RSTP device.	Not checked
Uncheck	The port is not directly connected to the RSTP device.	

3.5.7 MSTP

3.5.7.1 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.

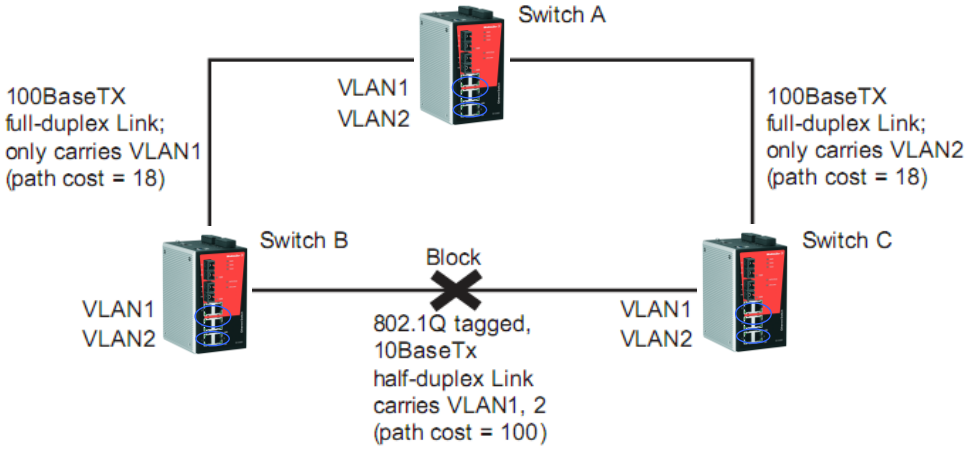
The main concepts that are specific of MSTP when comparing with STP/RSTP are:

- **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.

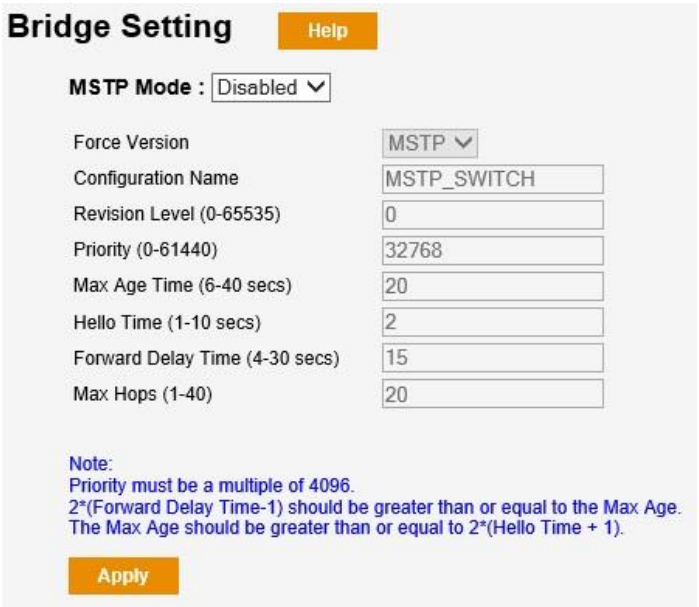


The above situation can be rectified by using MSTP. With MSTP, VLAN 1 and VLAN 2 can be mapped to different MSTIs. Hence, each instance can have a topology independent of other spanning tree instances.

3.5.7.2 Configuring MSTP

Bridge Setting

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



MSTP mode

Setting	Description	Factory Default
Enable/Disable	Select to enable the MSTP redundancy in the switch.	Disabled

Configuration Name

Setting	Description	Factory Default
Name selected by user	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). The name should not exceed 32 characters.	MSTP_SWITCH

Revision Level

Setting	Description	Factory Default
Numerical value selected by user	The revision of the MSTI configuration named above.	32768

Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Max. Age (sec)

Setting	Description	Factory Default
Numerical value input by user	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

Hello time (sec)

Setting	Description	Factory Default
Numerical value input by user	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

Forwarding Delay Time (sec)

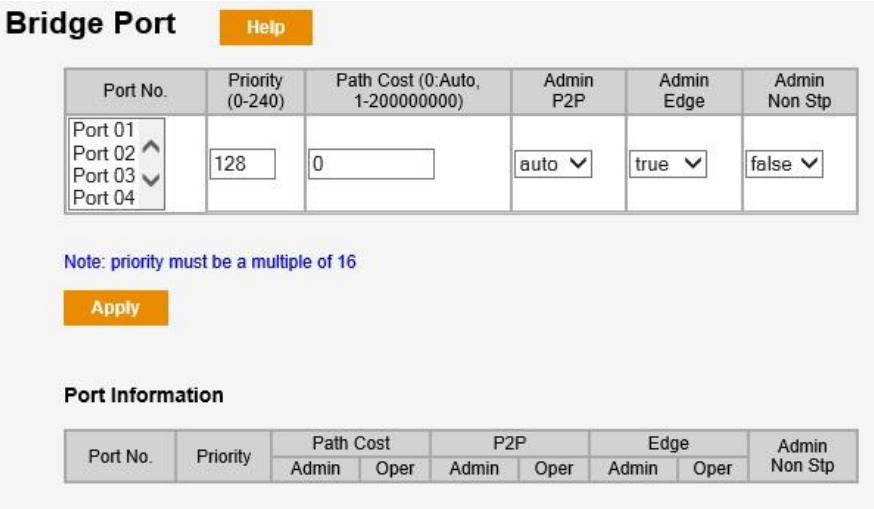
Setting	Description	Factory Default
Numerical value input by user	The amount of time this device waits before checking to see if it should change to a different state.	15

Max Hops

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

Bridge Port

Configuration of MSTP parameters in each port of the switch for the Common and Internal Spanning Tree (CIST).



Port No.

Setting	Description	Factory Default
Port of the Switch	Select the port to be configured.	None

Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by entering a lower number.	128

Path Cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology. The value 0 is for automatic calculation.	0

Admin Point to Point (P2P)

Setting	Description	Factory Default
Auto	Automatic detection if the link port is point to point or not.	Auto
True	The port link is point to point and then is a candidate for rapid transition to the forwarding state.	
False	The port link is not point to point.	

Admin Edge

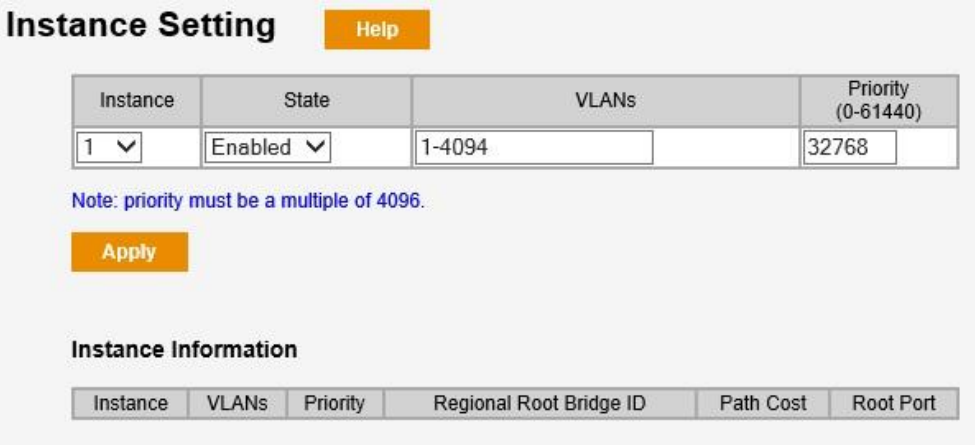
Setting	Description	Factory Default
True	The port is fixed as an edge port and will always be in the forwarding state	True
False	The port is set as the normal RSTP port	

Admin Non STP

Setting	Description	Factory Default
True	The port does not include the mathematic STP calculation and then it does not participate in MSTP.	False
False	The port includes the mathematic STP calculation and participates in MSTP.	

Instance Setting

Configuration of Multiple Spanning Tree Instances (MSTIs).



Instance

Setting	Description	Factory Default
1 to 15	Select the instance number that you want to configure.	1

State

Setting	Description	Factory Default
Enabled/Disabled	Select to enable the specific instant number.	Enabled

VLANs

Setting	Description	Factory Default
Numerical value selected by the user	The list of VLANs mapped to the MSTI. You can use '-' for consecutives VLANs (ex: 1-4) or ',' for non-consecutive VLANs (ex: 5, 8)	1-4094

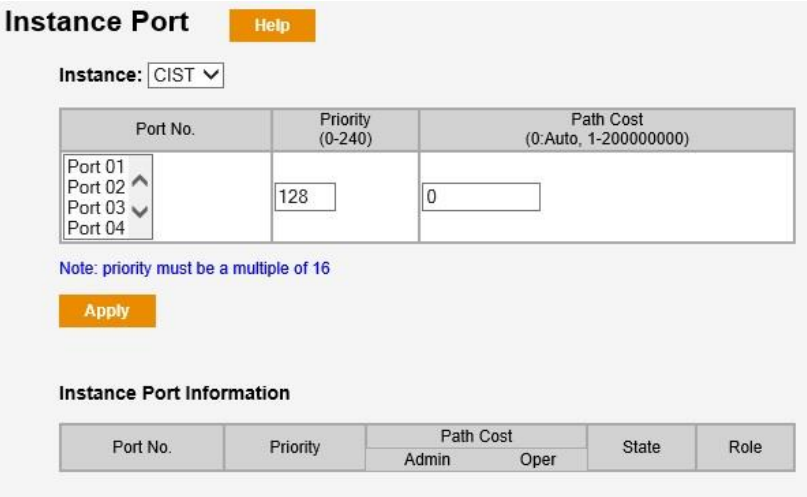
Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Once the Apply button is pressed, in the **Instance Information** table of the page are displayed all the MSTIs created and its mapping with the different VLANs.

Instance Port

Configuration of MSTP parameters of the ports for the different programmed MSTIs.



Instance

Setting	Description	Factory Default
CIST, 1 to 15	Select the instance number for which you want to configure the ports. CIST is the default value (always active) and already programmed at Bridge Port option	CIST

Port No.

Setting	Description	Factory Default
Port of the Switch	Select the port to be configured.	None

Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology of the selected MSTI by entering a lower number.	128

Path Cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology of the selected MSTI. The value 0 is for automatic calculation.	0

In the page is also displayed a Table showing the port information for each instance.

3.5.8 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 10	Select the priority (number from 1 to 10) 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.

3.6 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.

3.6.1 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.

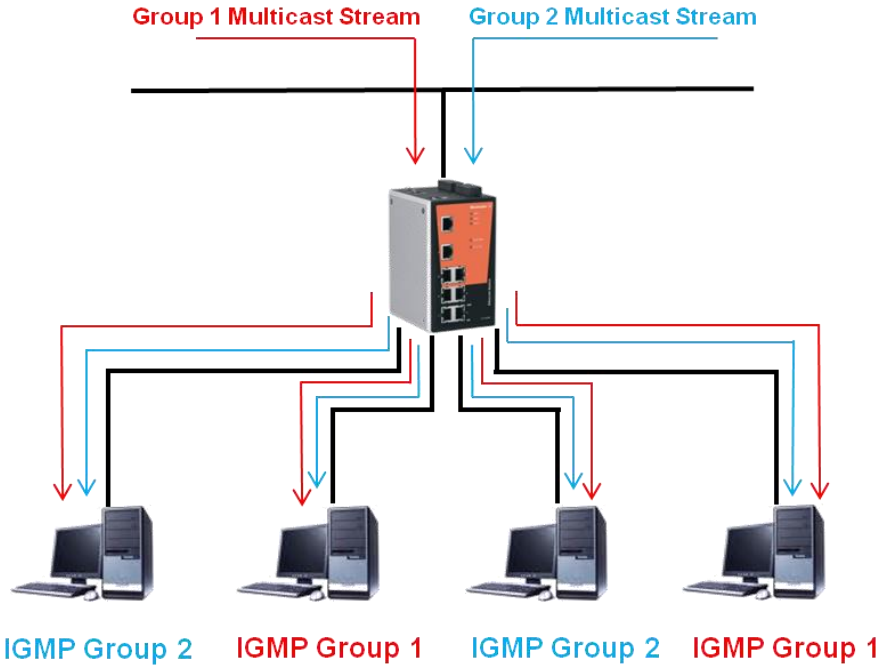
IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

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.

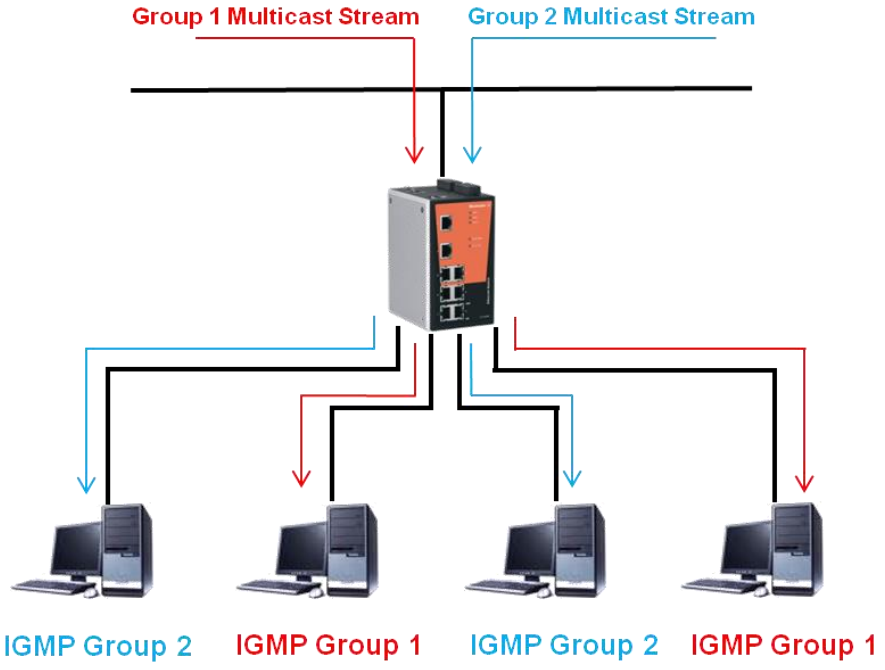
Network without multicast filtering

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 both automatic multicast filtering with IGMP (Internet Group Management Protocol) Snooping and manual multicast filtering by adding static multicast IP addresses.

It additionally supports MVR (Multicast VLAN Registration) to enable Multicast traffic across different VLANs.

IGMP (Internet Group Management Protocol)

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 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 routers (or queriers).

IGMP Multicast Filtering

IGMP 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 querier connected to the LAN or VLAN can become the IGMP 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 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.

Static Multicast

Some devices may only support multicast packets, but may not support IGMP Snooping. The Weidmüller switch supports adding multicast groups manually to enable multicast filtering.

MVR (Multicast VLAN Registration)

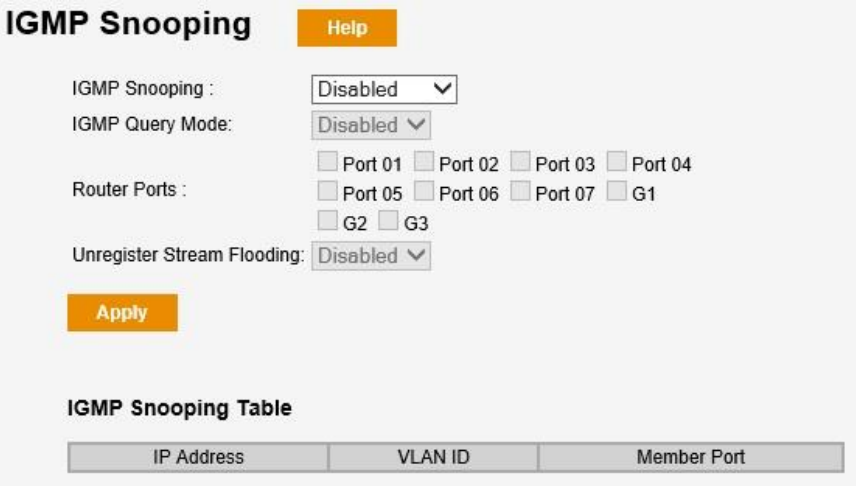
The MVR feature enables more efficient distribution of multicast traffic across an Ethernet Layer-2 network. In standard Layer 2 networks, a multicast stream received on one VLAN is never distributed to interfaces outside that VLAN. If hosts in different VLANs request the same multicast stream, a separate copy of that multicast stream is distributed to each requesting VLAN.

The MVR creates a Multicast VLAN that becomes the only VLAN over which multicast traffic flows through the Layer 2 network. In an Ethernet switch with MVR enabled we can configure both Source ports (connected to a sender of multicast data to the Multicast VLAN) and Receiver ports (connected to subscribers). MVR receiver ports can receive traffic from a port on the Multiple VLAN but cannot send traffic to it.

MVR operates similarly and in conjunction with IGMP Snooping. Whereas IGMP Snooping operates within a given VLAN to regulate multicast traffic, MVR can operate with different VLANs.

3.6.2 Configuring IGMP Snooping

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.



IGMP Snooping

Setting	Description	Factory Default
Enabled/Disabled	Enable the IGMP Snooping (v2 or v3) function globally.	Disabled

IGMP Query Mode

Setting	Description	Factory Default
Enabled/Disabled	The switch may be the IGMP querier. As only one device can be the querier in an IGMP application, the querier role will be taken by the device with the lowest IP address.	Disabled

Router Ports

Setting	Description	Factory Default
Port number	The user can also select/check the ports that will connect to the multicast routers (static router port). These ports will receive all multicast packets from the source. This option is only active when IGMP Snooping is enabled.	Unchecked

Unregister Stream Flooding

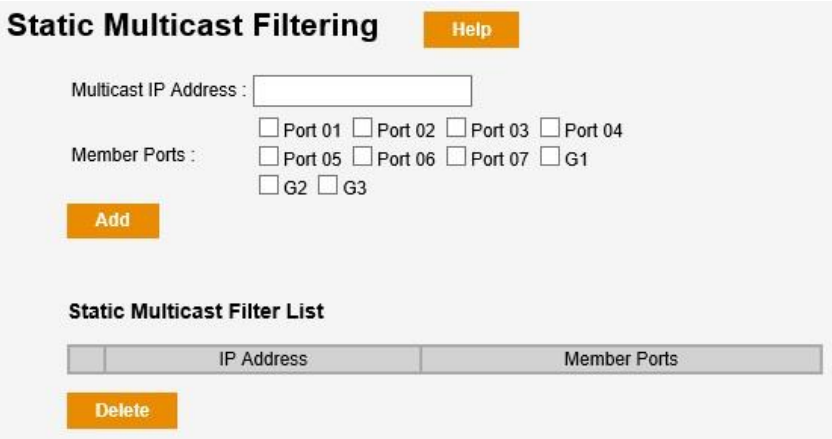
		Factory Default
Enabled/Disabled	Unregistered multicast packets (not learned by IGMP and not configured statically) are handled according to this programming. If Disabled, the unregistered multicast packets will be discarded. If Enabled, the unregistered multicast packets will be forwarded.	Disabled

IGMP snooping table

In the page is also shown a table displaying the current IP multicast link indicating the IP address, the VLAN ID and the Member ports.

3.6.3 Configuring Static Multicast Filtering

If required, the Weidmüller switch also supports adding multicast groups manually. Static multicast filtering provides a method for users to configure multicast group memberships manually. The function enables end devices to receive multicast traffic only if they register to join specific multicast groups. With static multicast filtering, network devices only forward multicast traffic to the ports connected to registered end devices.



Multicast IP Address

Setting	Description	Factory Default
IP Address	Input a multicast group IP address in the range between 224.0.0.0 and 239.255.255.255.	None

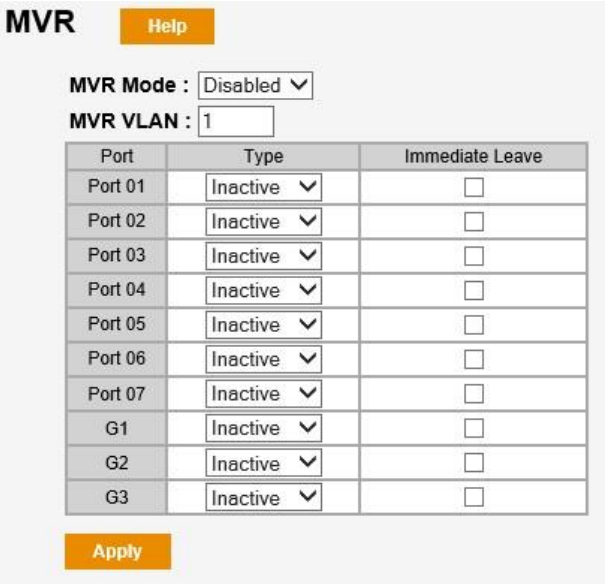
Member Ports

Setting	Description	Factory Default
Check/Unchecked	Checkmark the appropriate check boxes to select the join ports for this multicast group.	None

In the same page is shown a table with the created Static Multicast Filter List indicating the ports of each specific multicast group.

3.6.4 Configuring MVR

MVR is a feature to enable a more efficient distribution of multicast traffic across an Ethernet Layer-2 network.



MVR Mode

Setting	Description	Factory Default
Enabled/Disabled	Enable the MVR function.	Disabled

MVR VLAN

Setting	Description	Factory Default
VLAN number	Specify the VLAN ID of the source group	1

Port Type

Setting	Description	Factory Default
Inactive	MVR not enabled in the port.	Inactive
Receiver	Port acting as Receiver.	
Source	Port acting as Source.	

Immediate leave

Setting	Description	Factory Default
Check/Uncheck	Checkmark this check box to immediately stop forwarding traffic for the multicast group after the host connected to that port leaves the group.	Unchecked

3.7 Virtual LAN

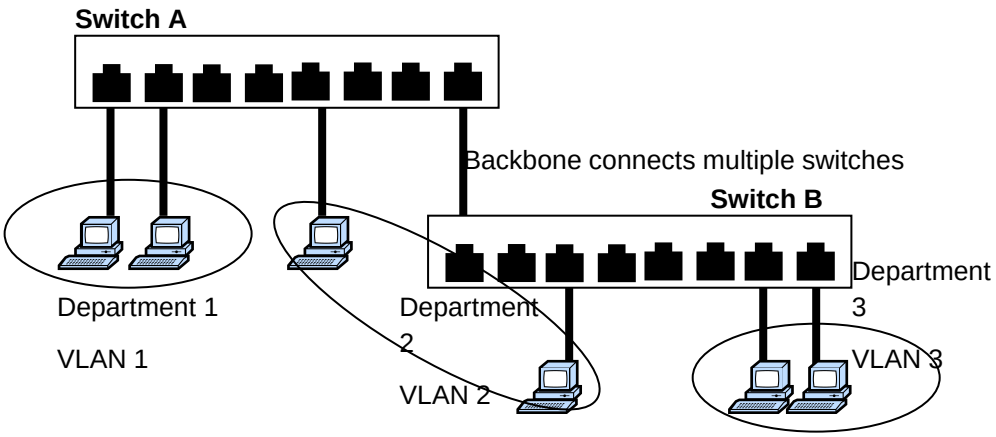
Setting up Virtual LANs (VLANs) on your Weidmüller switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

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*—0 (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.

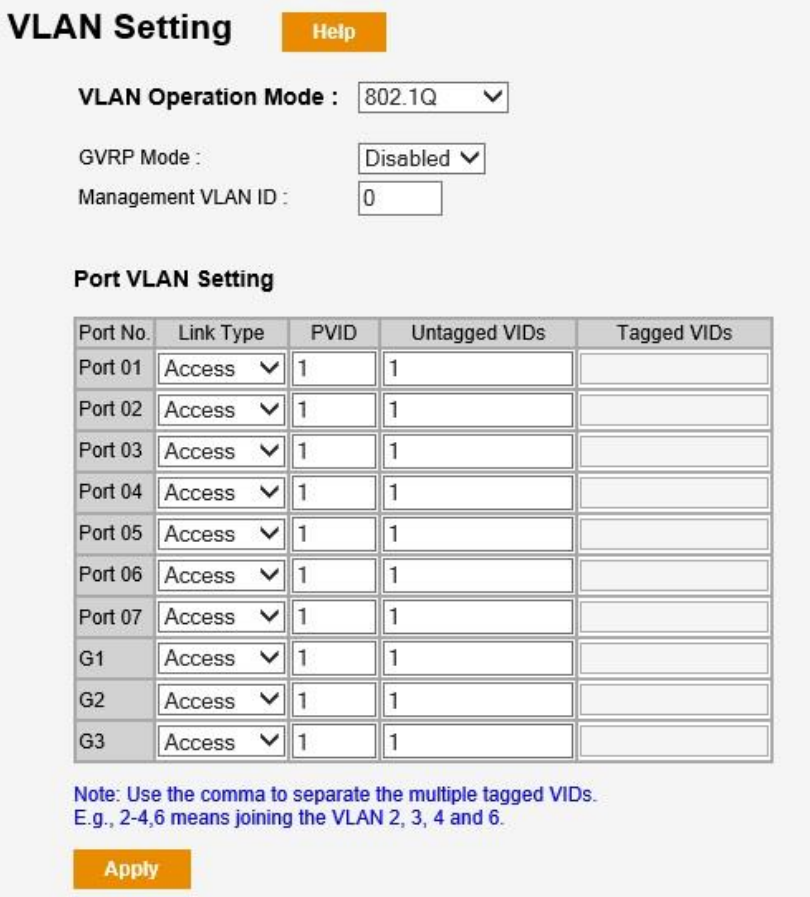
The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs. If a frame is carrying the additional information, it is known as a *tagged* frame.

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 Settings

To configure 802.1Q VLAN and port-based VLANs on the Weidmüller switch, use the **VLAN Settings** page to configure the ports.



VLAN Operation Mode

Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	

GVRP Mode

Setting	Description	Factory Default
Enabled/Disabled	Enable the GVRP function. GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, the switch will automatically add that device to the existing VLAN.	Disabled

Management VLAN ID

Setting	Description	Factory Default
VLAN ID from 0 to 4094	Defines the Management VLAN ID of the CPU Interface of the switch. If changed, only member ports of the Management VLAN can access the device for management via Ethernet (Ping, Web access, SSH, Telnet). Note: Before you change the management VLAN ID, you must add the port, to which the administrator is connected, to the management VLAN. Otherwise the switch no longer is accessible via the network.	0

Link Type

Setting	Description	Factory Default
Access	Access ports are used to connect to end devices which are not VLAN aware. An access port does have the following characteristics: At ingress, accepts frames having no VLAN ID (untagged) which will be tagged by defined parameter PVID to become a member of the PVID-related VLAN group. Note: Already tagged frames having a VLAN ID (which normally is not intended by design) also will be accepted. In this case a tagged packet only will be forwarded to the output queue if it matches to any addressed port of a VLAN group with this ID. Otherwise the frame will be dropped immediately. At egress: • Only frames may leave the port having a VLAN ID configured in parameter Untagged VIDs. • The VLAN ID will be removed (untagged) from all frames which leave the port.	Access
Trunk	Trunk ports are designed to carry traffic of multiple VLANs simultaneously and are normally used for switch interconnections. A Trunk port does have following characteristics: At ingress, accepts and expects frames having a VLAN ID (tagged). Dependent on this ID the packet will be queued if it matches to any addressed port of a VLAN group with this ID. Otherwise the frame will be dropped. Note: Accepts also untagged frames (which normally is not intended by design) which will be tagged by parameter PVID to become a member of the PVID-assigned VLAN group. At egress: • Only frames may leave the port having a VLAN ID	

	configured in parameter Tagged VIDs. • Frames always are transmitted with VLAN ID (tagged).	
Hybrid	Hybrid ports are designed to connect either to switches or hosts. This link type is a combination of Access and Trunk port. A Hybrid port does have following characteristics: At ingress: • Accepts frames having no VLAN ID (untagged) which will be tagged by defined parameter PVID to become a member of the PVID-related VLAN group. • Tagged frames having a VLAN ID will be accepted without any change. A tagged packet only will be forwarded to the output queue if it matches to any addressed port of a VLAN group with this ID. Otherwise the frame will be dropped immediately. At egress: • Only frames may leave the port having a VLAN ID configured in parameter Untagged VIDs or Tagged VIDs. • For all frames, allowed to leave the port by parameter Untagged VIDs the VLAN ID will be removed (untagged). • For all frames, allowed to leave the port by parameter Tagged VIDs, the VLAN ID not will be removed (tagged).	

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.

PVID

Setting	Description	Factory Default
VID ranges from 1 to 4094	Sets the default VLAN ID for untagged devices that connect to the port. Incoming frames (Ingress) that do not have a VLAN ID will be tagged with PVID value. Incoming devices having a VLAN ID will be left unchanged.	1

Untagged VIDs

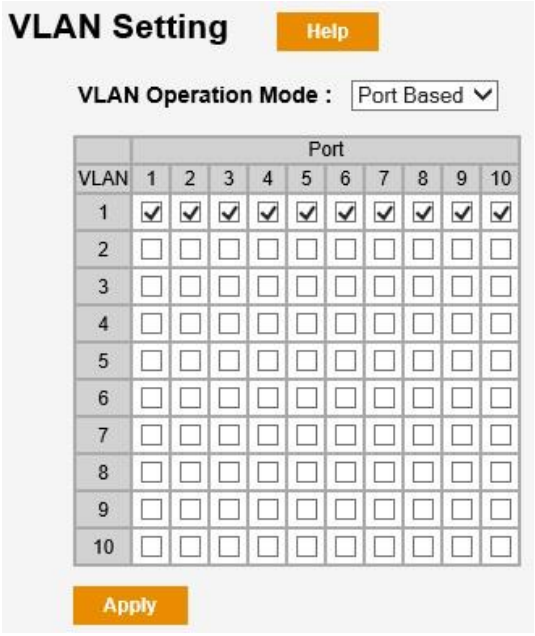
Setting	Description	Factory Default
VID ranges from 1 to 4094	This parameter may be used for link types Access and Hybrid. It is only related to the port's output traffic (Egress) and defines that only frames may leave the port having a VLAN ID configured in Untagged VIDs. The VLAN ID of a frame which may leave the port according to parameter Untagged VIDs always will be removed (untagged). Use commas to separate different VLAN IDs.	None

Tagged VIDs

Setting	Description	Factory Default
VID range from 1 to 4094	This parameter may be used for link types Trunk and Hybrid. It is only related to the port's output traffic (Egress) and defines that only frames may leave the port having a VLAN ID configured in Tagged VIDs. The VLAN ID of a frame which may leave the port according to parameter Tagged VIDs never will be removed (stay tagged). Use commas to separate different VLAN IDs.	None

3.7.2.2 Port-Based VLAN Settings

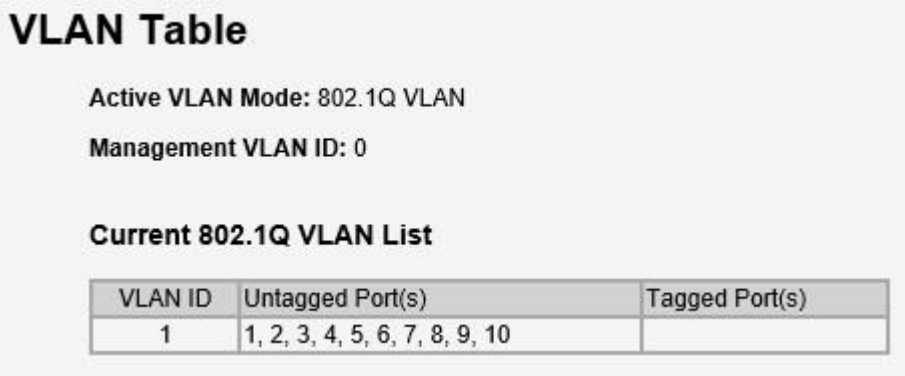
Check each specific port to assign its VLAN ID in the table. The maximum VLAN ID is the same as your number of switch ports.



Port

Setting	Description	Factory Default
Check/Uncheck	Set port to specific VLAN Group by activating checkbox.	All ports belong to VLAN1

3.7.2.3 VLAN Table



In **802.1Q VLAN table**, you can review the VLAN groups that were created, **Untagged Ports** and **Tagged Ports**. In **Port-based VLAN table**, you can review the VLAN group and assigned ports.

3.8 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.

3.8.1 The Traffic Prioritization Concept

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 four 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.

3.8.2 Configuring Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization capability to ensure that important data is delivered consistently and predictably. The Weidmüller switch can inspect IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 ToS information, to provide a consistent classification of the entire network. The implemented QoS capability improves your industrial network's performance and determinism for mission critical applications.

3.8.2.1 Policy

In this page we can enable the QoS in the switch and we can also indicate how is determined the priority of an ingress frame as well as the QoS policy.

QoS Mode

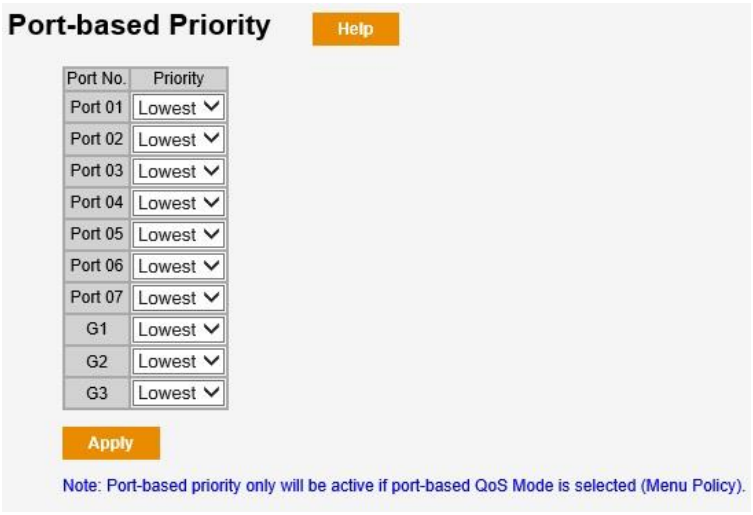
Setting	Description	Factory Default
Disabled	No traffic prioritization of the switch.	Disabled
Port-based	The output priority of the switch is handled according to the ingress port.	
COS only	The output priority of the switch is determined inspecting the 801.1p CoS tag in the MAC frame.	
TOS only	The output priority of the switch is determined inspecting the Type of Service bits in the IPv4 frame.	
COS first	The output priority of the switch is determined inspecting both 802.1p CoS tag and ToS bits in the frame but checking first the priority marking according to IEEE 802.1p.	
TOS first	The output priority of the switch is determined inspecting both 802.1p CoS tag and ToS bits in the frame but checking first the priority bits according to ToS.	

QoS Policy

Setting	Description	Factory Default
Weight Fair	The Weidmüller switch has 4 priority queues. In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Strict
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

3.8.2.2 Port Priority

NOTE: This page has to be programmed if the selected QoS policy of the switch is **Port-based**.

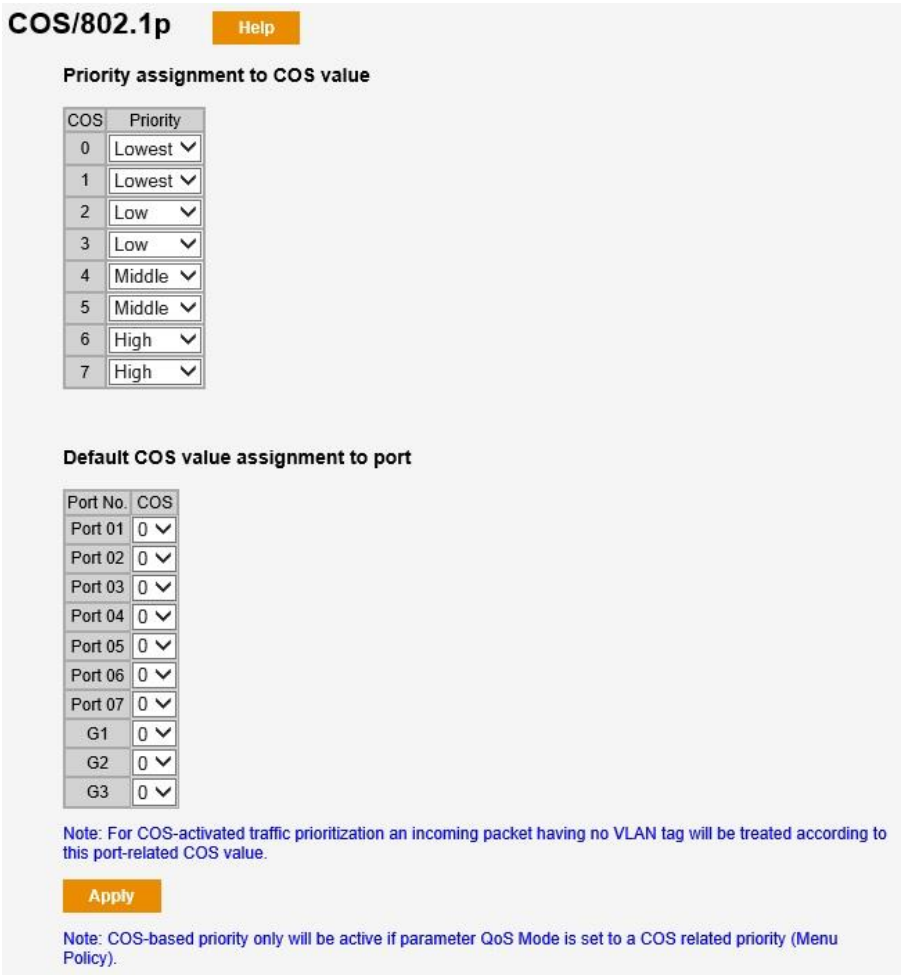


Port-based Priority

Setting	Description	Factory Default
Port priority	The port priority has 4 priority queues. Lowest, Low, Middle, High priority queue option can be applied to each port.	Lowest

3.8.2.3 CoS Priority

NOTE: This page has to be programmed if the selected QoS policy of the switch is based on **CoS** (CoS only, CoS first or ToS first). When CoS enabled, incoming packets without VLAN tag (without IEEE 802.1p priority mark) will be treated according to this programming.



Priority assignment to COS value

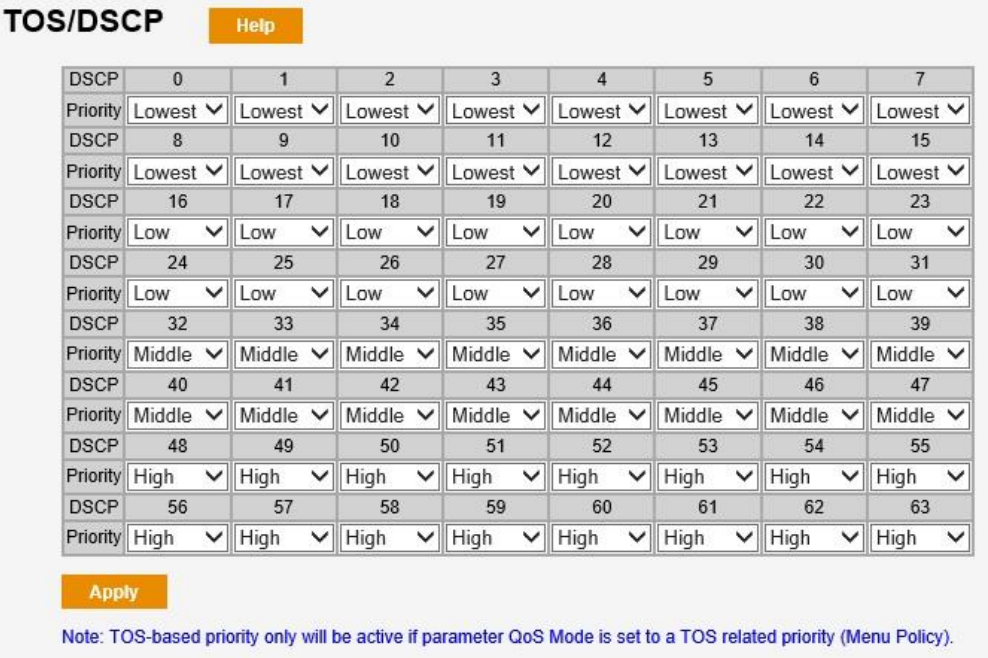
Setting	Description	Factory Default
Lowest / Low / Middle / High	Maps different CoS values to four different egress queues.	0-1 Lowest 2-3 Low 4-5 Middle 6-7 High

Default COS value assignment to port

Setting	Description	Factory Default
0 to 7	For each port we define the priority level from 0 to 7 that will be assigned to one of the priority queues of the switch (according to the mapping programmed). This default CoS value will only be applied to those incoming packets without VLAN tag.	0

3.8.2.4 ToS Priority

NOTE: This page has to be programmed if the selected QoS policy of the switch is based on **ToS** (ToS only, ToS first or CoS first).



TOS/DSCP Value and Priority Queues

Setting	Description	Factory Default
Lowest/Low/ Middle/High	Maps different ToS values to 4 different egress queues.	0 to 15: Lowest 16 to 31: Low 32 to 47: Middle 48 to 63: High

3.9 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.

DHCP Mode

Setting	Description	Factory Default
Disabled	No DHCP Server/Relay.	Disabled
DHCP Server	The switch can assign IP addresses automatically to devices that are equipped with DHCP client.	
DHCP Relay	DHCP clients and server can be located in different subnets.	

3.9.1 Configuring DHCP Server

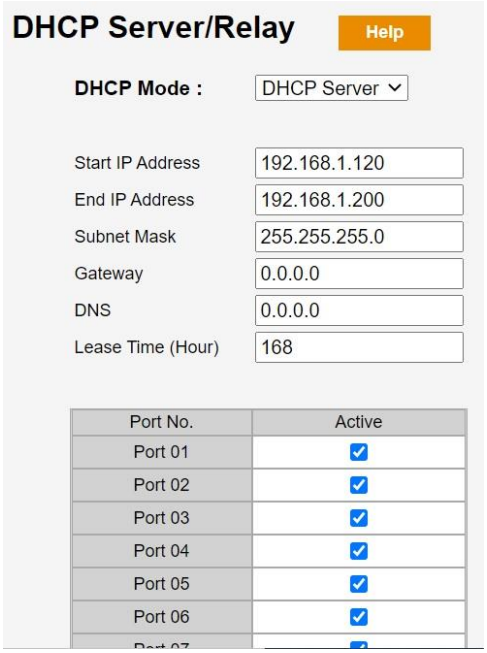
STEP 1 → Set up the connected devices

Set up those Ethernet-enabled devices connected to the Weidmüller switch for which you would like IP addresses to be assigned automatically. The devices must be configured to obtain their IP address automatically.

You also need to decide which of the Weidmüller switch's ports your Ethernet-enabled devices will be connected to.

STEP 2

Configure the Weidmüller switch's **DHCP Server** function. You simply need to enter the range of IP addresses and indicate the ports that will be acting as DHCP servers.



Start IP Address / End IP address

Setting	Description	Factory Default
IP range of the DHCP address pool	Assigns the start and end IP addresses of the pool that will be used to set the IP address of more than one DHCP clients.	192.168.1.120 / 192.168.1.200

Subnet Mask

Setting	Description	Factory Default
IP address of the subnet mask	Subnet mask dynamically assigned to DHCP clients.	255.255.255.0

Gateway

Setting	Description	Factory Default
IP address for the gateway	Gateway IP address dynamically assigned to DHCP clients.	0.0.0.0

DNS

Setting	Description	Factory Default
DNS Server's IP address	The IP address of the DNS Server dynamically assigned to DHCP clients.	0.0.0.0

Lease time

Setting	Description	Factory Default
Lease time of the pool (hours)	Amount of time a network client will be allowed to use a dynamic IP address in the network.	168 hours

3.9.2 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.

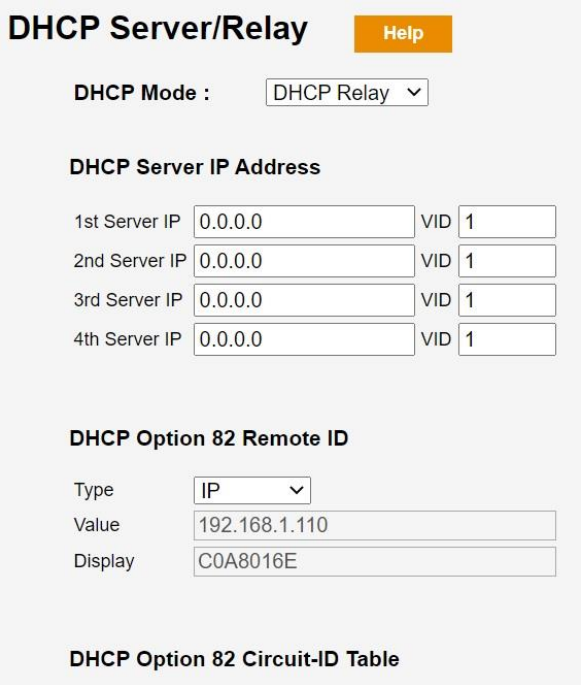
DHCP Option 82 is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and 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.

Configuring DHCP Relay Agent



DHCP Server IP Address

1st Server

Setting	Description	Factory Default
IP address / VID for the 1st DHCP server	Assigns the IP address and VID of the 1st DHCP server that the switch tries to access.	0.0.0.0 / 1

2nd Server

Setting	Description	Factory Default
IP address / VID for the 2nd DHCP server	Assigns the IP address and VID of the 2nd DHCP server that the switch tries to access.	0.0.0.0 / 1

3rd Server

Setting	Description	Factory Default
IP address / VID for the 3rd DHCP server	Assigns the IP address and VID of the 3rd DHCP server that the switch tries to access.	0.0.0.0 / 1

4th Server

Setting	Description	Factory Default
IP address / VID for the 4th DHCP server	Assigns the IP address and VID of the 4th DHCP server that the switch tries to access.	0.0.0.0 / 1

DHCP Option 82 Remote ID

Type

Setting	Description	Factory Default
IP	Uses the switch's IP address as the remote ID sub.	IP
MAC	Uses the switch's MAC address as the remote ID sub.	
Client-ID	Uses a combination of the switch's MAC address and IP address as the remote ID sub.	
Other	Uses the user-designated ID sub.	

Value

Setting	Description	Factory Default
Max. 12 characters	Displays the value that was set. Complete this field if type is set to Other.	Switch IP address

Display

Setting	Description	Factory Default
read-only	The actual hexadecimal value configured in the DHCP server for the Remote-ID. This value is automatically generated according to the Value field. Users cannot modify it.	Depends on switch IP address

DHCP Option 82 Circuit ID Table

Option 82

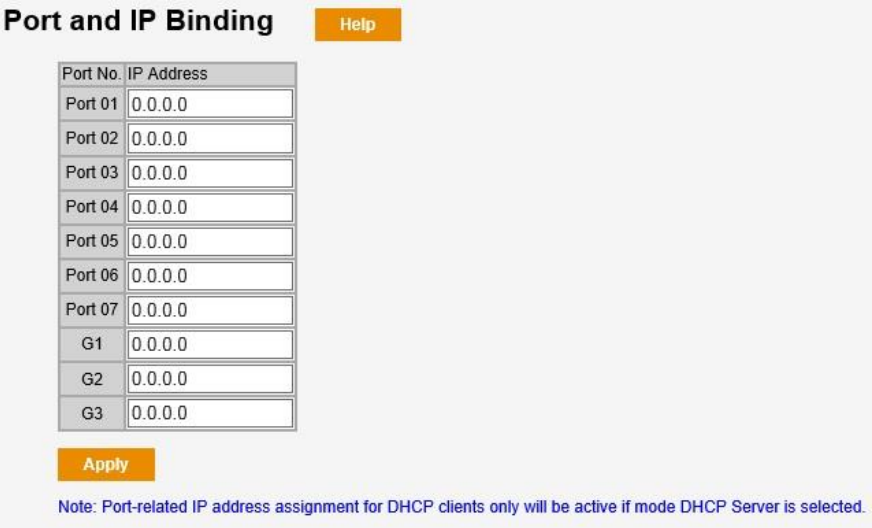
Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function for this port.	Disable

3.9.3 Client List

If the DHCP Server is enabled in the switch, the DHCP clients will be displayed in this page.

3.9.4 Port and IP 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.



NOTE: Port and IP binding will only be active if DHCP Server mode is enabled in the switch.

3.10 SNMP

Weidmüller managed Switches supports 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 below the figure.

3.10.1 SNMP Read/Write Settings

SNMP Agent Versions

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

SNMP V1, V2c Community

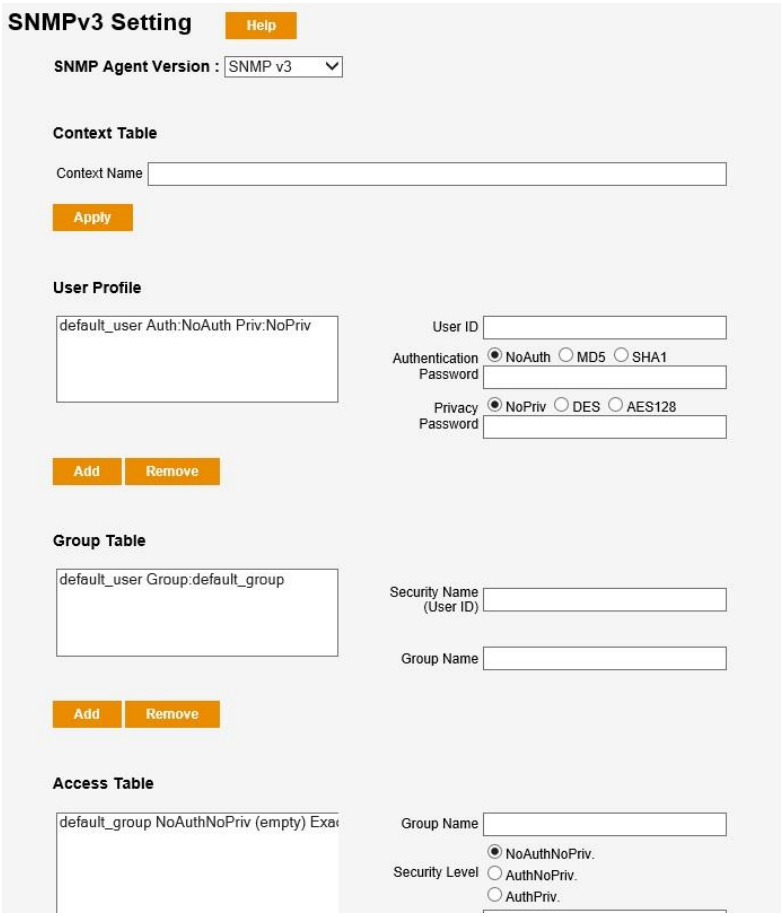
Setting	Description	Factory Default
Max. 32 characters	Specifies the community string to authenticate the SNMP agent for read-only or read/write access. The SNMP agent will access all objects using this community string.	Public Private
Setting	**Description**	**Factory Default**
Read Only / Read and Write	Specifies the privilege of each community string.	Read Only (Public) Read and Write (Private)

Up to four different sets of **Community string / Privilege** are supported in the switch.

SNMP V3 allows the user to create several groups of users and accesses with different levels of security. Object IDs are associated with various levels of permissions and a single view can be assigned to multiple objects. As a summary, in SNMP V3:

- Several users can be created with different security levels.
- Groups of users with the same privilege accesses can be created.
- More than one access to the same Group can be created.
- An access can have more than one MIB view for its read access, write access or notify access.
- A single MIB view can have multiple OIDs associated.

The figure below shows the configuring page when SNMP v3 is selected.



Context Name

Setting	Description	Factory Default
Max. 32 characters	Specifies the name string to authenticate the SNMP V3 agent.	None

User profile – User ID

Setting	Description	Factory Default
Max. 32 characters	A string identifying a user name.	None

User profile – Authentication

Setting	Description	Factory Default
Max. 32 characters	A string identifying the authentication pass phrase of the created user.	None
No-Auth	Allows the user to access objects without authentication.	No-Auth
MD5	Authentication will be based on the MD5 algorithms.	
SHA1	Authentication will be based on the SHA1	

	algorithms.	

User profile – Privacy

Setting	Description	Factory Default
Max. 32 characters	A string identifying the privacy pass phrase of the created user.	None
No-Priv	Allows the user to access objects without encryption.	No-Priv
DES	Encryption will be based on DES protocol.	
AES128	Encryption will be based on AES128 protocol.	

The buttons **Add** / **Remove** have to be used to create / delete Users.

Group Table – Security Name

Setting	Description	Factory Default
Max. 32 characters	A string identifying the user name belonging to the created Group.	None

Group Table – Group Name

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

The buttons **Add** / **Remove** have to be used to create / delete Groups.

Access Table – Group Name

Setting	Description	Factory Default
Max. 32 characters	A string identifying the Group name belonging to the created Access Table.	None

Access Table – Security Level

Setting	Description	Factory Default
NoAuthNoPriv	No authentication and no encryption required. Security configuration of group of users belonging to this access must be None.	NoAuthNoPriv
AuthNoPriv	Authentication is required but no encryption. Security configuration of group of users belonging to this access must be in accordance.	
AuthPriv	Authentication and encryption required. Security configuration of group of users belonging to this access must be in accordance.	

Access Table – Context Prefix

Setting	Description	Factory Default
Max. 32 characters	The context name as defined in the context table. The context name can be treated differently depending on the setting of the Content Match Rule.	None

Access Table – Context Match Rule

Setting	Description	Factory Default
Exact	The context name is treated as a full-context name string and must match exactly	Exact
Prefix	Only a match between the prefix and the starting portion of context name is required	

Access Table – 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.	None

Access Table – 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.	None

Access Table – Notify View Name

Setting	Description	Factory Default
Max. 32 characters	The name of the MIB View defining the MIB objects which may be included in notification requests.	None

The buttons **Add** / **Remove** have to be used to create / delete Access Tables.

MIBView Table – View Name

Setting	Description	Factory Default
Max. 32 characters	A string identifying the View name that will be used in the Access Table.	None

MIBView Table – SubOid-Tree

Setting	Description	Factory Default
Number (OID)	The object identifier (OID) value for the created view table.	None
Included / Excluded	We can indicate if the subtree indicated by the OID should be included or excluded in the created view.	Included

The buttons **Add** / **Remove** have to be used to create / delete MIB Views.

NOTE: At the end of this programming page is shown the Private MIB Information of the switch as well as the Engine ID (if SNMP V3 is used).

3.10.2 Trap Settings

SNMP traps allow an SNMP agent to notify a Network Management System (NMS) of a significant event.

Server IP

Setting	Description	Factory Default
IP address	Specifies the IP address of the trap server used by your network.	None

Community or V3 Security Name

Setting	Description	Factory Default
Character string	Specifies the community string to use for authentication (maximum of 32 characters).	None

Trap Version

Setting	Description	Factory Default
V1 / V2C / V3	Specifies the SNMP trap supported version.	V1

After indicating the IP address of the trap server, the community name for authentication and the SNMP trap version, we press the **Add** button.

All the configured trap servers are shown in the table **Trap Server Profile** of the web page.

3.11 Security

Security can be categorized in two levels: the user name/password level, and the port access level. 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+). The TACACS+ mechanism is a centralized “AAA” (Authentication, Authorization and Accounting) system for connecting to network services.

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

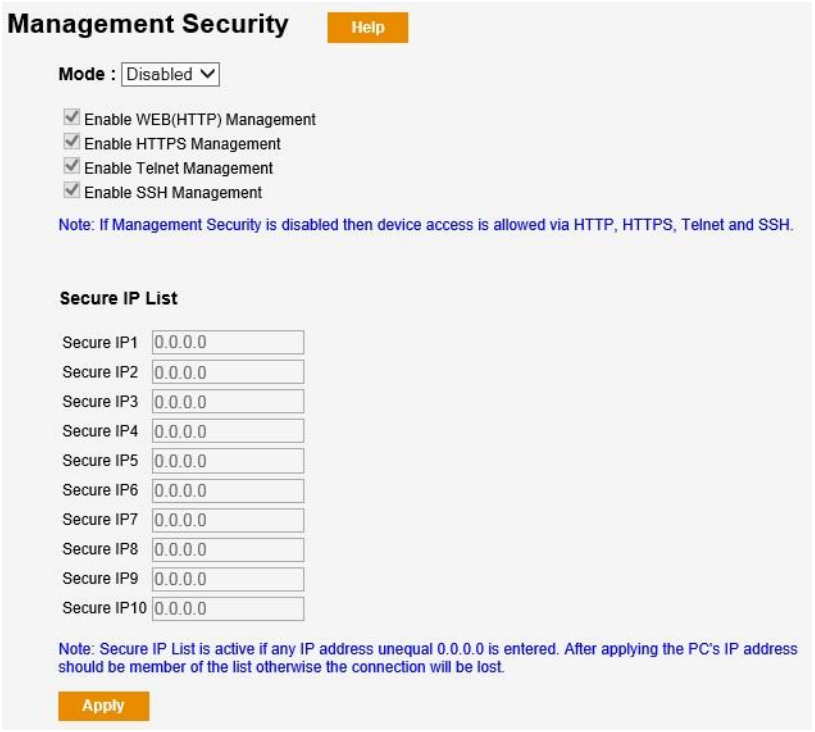
- **Static Port Lock, either using MAC or IP addresses**
- **IEEE 802.1X**

A more detailed description about all the security options is provided in the following sections.

3.11.1 User Login Authentication

3.11.1.1 Management Security

The Management Security 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) and is also possible to restrict it to specific IP addresses. When the Secure IP list is enabled, only addresses on the list will be allowed to access to the Weidmüller switch.



Management Security Mode

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the control access to the management of the switch. When disabled, the access to the switch is allowed via HTTP, HTTPS, TELNET and SSH. When enabled, it is possible to restrict this access.	Disabled

Enable WEB(HTTP) Management

Setting	Description	Factory Default
Check	Web management through HTTP is allowed	Check
Uncheck	Web management through HTTP is not allowed	

Enable HTTPS Management

Setting	Description	Factory Default
Check	Web management through HTTPS is allowed	Check
Uncheck	Web management through HTTPS is not allowed	

Enable Telnet Management

Setting	Description	Factory Default
Check	Access through Telnet is allowed	Check
Uncheck	Access through Telnet is not allowed	

Enable SSH Management

Setting	Description	Factory Default
Check	Access through SSH is allowed	Check
Uncheck	Access through SSH is not allowed	

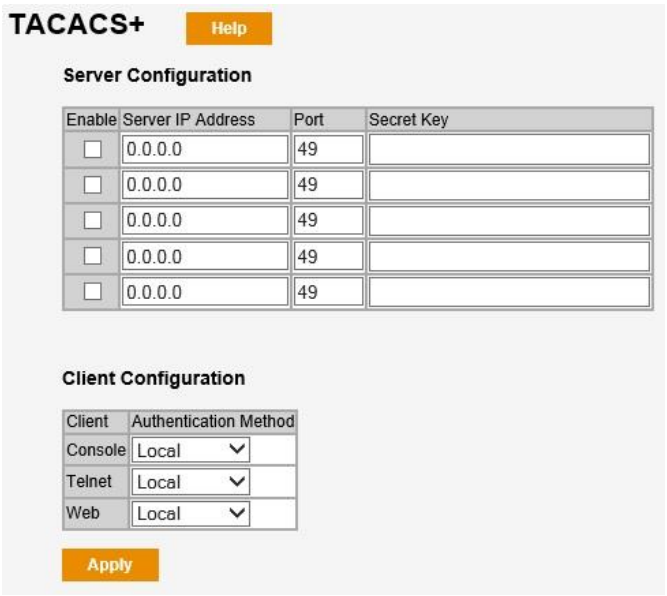
Secure IP List

Setting	Description	Factory Default
IP address (up to 10)	Defines an IP address that is allowed to access to the management of the switch. It is active whenever any IP address different from 0.0.0.0 is entered.	0.0.0.0

NOTE: After programming IP addresses in the Secure IP List and before applying, be sure that the IP address of the management PC is in the list. Otherwise the connection will be lost.

3.11.1.2 TACACS+

The detailed configuration settings of TACACS+ are displayed in the table below. As it can be seen in the page below, up to five different TACACS+ servers can be configured in the switch.



Server Configuration

Setting	Description	Factory Default
Enable	Check or uncheck the access through TACACS`server.	Unchecked
Server IP Address	Set IP address of the external TACACS+ server as the authentication database.	0.0.0.0
Port	Set communication port of the external TACACS+ server as the authentication database.	49
Secret Key	Set specific characters for server authentication	None

	verification.	

Client Configuration

Setting	Description	Factory Default
Local / TACACS+	Indicate if the authentication verification to access through Console / Telnet / Web is made using the local database of the switch or a remote TACACS+ server.	Local

3.11.2 Using Port Access Control

The Weidmüller switches provide two kinds of Port-Based Access Control:

- **Static Port Lock**
- **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 Port Lock function, these locked ports will not learn any additional MAC addresses, but only allow traffic from preset static MAC/IP addresses, helping to block hackers and careless usage.

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.

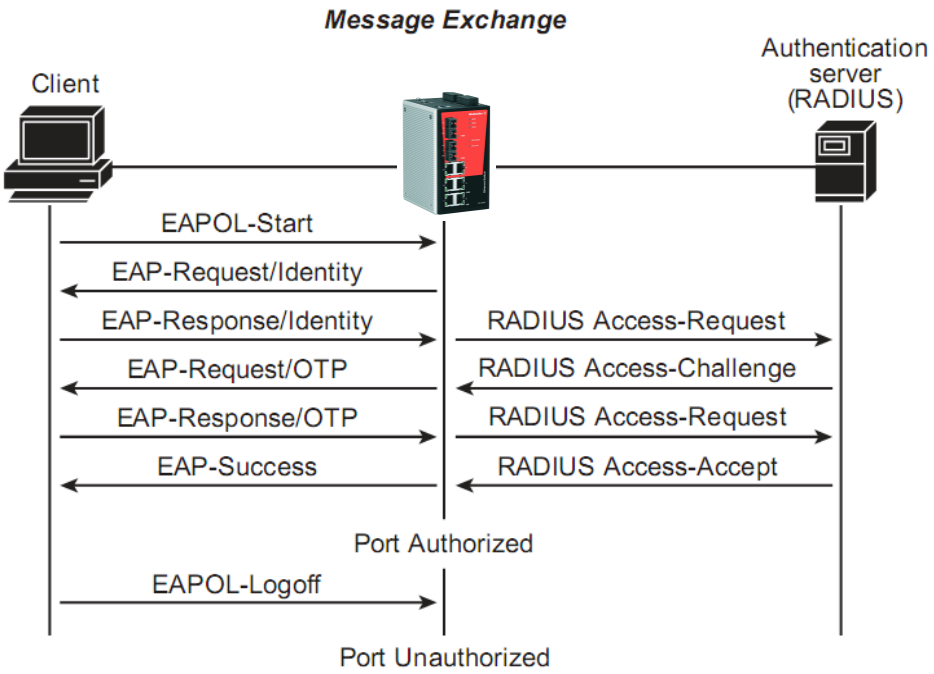
Client/Supplicant: The end station that requests access to the LAN and switch services and responds to the requests from the switch.

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.

3.11.2.1 Static MAC Forwarding

If port security is enabled in the option **Port Control** (menu **Port Settings**), this page has to be used to indicate the list of MAC addresses that will not be discarded.

Setting	Description	Factory Default
MAC Address	Add the static unicast MAC address.	None
Port	Associates the static address with a dedicated port.	1

3.11.2.2 MAC Blacklist

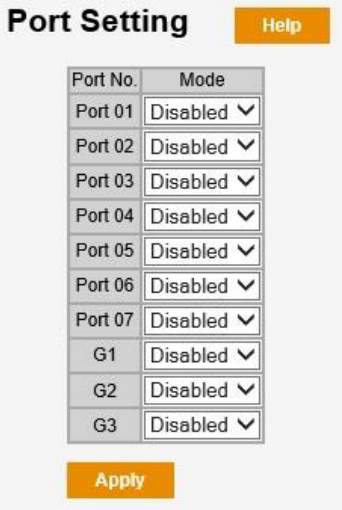
This option can be used to block any traffic to some specific device. Any frame forwarding to MAC addresses of this blacklist will be discarded.

Setting	Description	Factory Default
MAC Address	Add the static unicast MAC address.	None

3.11.2.3 IP Guard

IP Guard is a simple security option that consists in defining an IP allowed list. Any traffic from IP addresses not belonging to this list will be discarded.

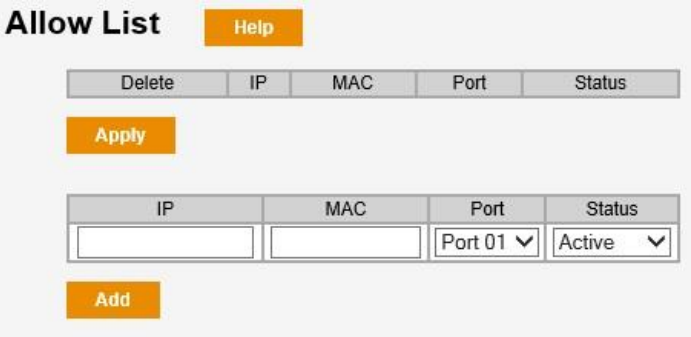
Port Setting



The IP Guard function can be applied to each port of the switch through this **Port Setting** option.

Setting	Description	Factory Default
Disabled	IP Guard function disabled in the port.	Disabled
Monitor	IP monitoring in the port but no traffic discarding.	
Security	IP Guard function fully enabled. Illegal IP traffic will be blocked.	

Allow list



In the option **Allow list** the user can create the list of allowed IP addresses of a port applicable when the IP Guard feature is enabled.

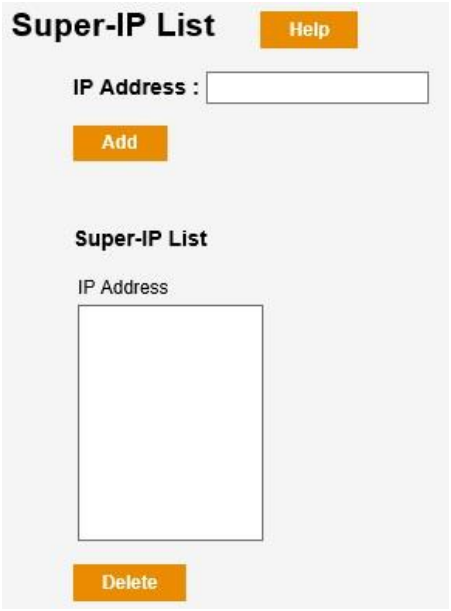
Setting	Description	Factory Default
IP	IP address of the allowed entry.	None
MAC	MAC address of the allowed entry.	None
Port	Port number for the allowed IP/MAC address	1
Status	Active or Suspend. Active allows the IP traffic whilst Suspend blocks it. If there are doubts about some IP allowed traffic, it can be suspended.	Active

The user can **Add** and **Delete** rows of the allow list by using the corresponding buttons.

Super-IP list

As it has been seen in the previous section, the IP addresses of the option **Allow list** have to match the programmed MAC address and ingress port to be allowed by the IP Guard function.

The option **Super-IP list** allows the user to define IP addresses with special priority. Any IP traffic of the Super-IP list is allowed regardless the MAC address and ingress port.



Setting	Description	Factory Default
IP	IP address of the Super-IP list.	None

The user can **Add** and **Delete** IP addresses of the Super-IP list by using the corresponding buttons.

Monitor List

In this option is displayed a log of all the traffic blocked by the IP Guard function. The user can display the IP address / MAC address / Port of the entry as well as the time when the entry was logged.

The user also has the possibility to add to the allow list any entry of the blocked traffic by checking **Add to allow list**.

3.11.2.4 802.1x

Radius Server

Radius Server Setting

Setting	Description	Factory Default
802.1x Protocol	Enables or Disables the use of an external RADIUS server as the authentication database.	Disabled
Radius Server IP	The IP address of the RADIUS server	0.0.0.0
Server Port	The UDP authentication port of the RADIUS server.	1812
Accounting Port	The UDP accounting port of the RADIUS server.	1813
Shared Key	A key to be shared between the external RADIUS server and the Weidmüller switch. Both ends must be configured to use the same key.	12345678
NAS, identifier	String used to identify the switch.	NAS_L2_Switch

Advanced Setting

Setting	Description	Factory Default
Quiet Period	Time interval (in sec) between an authentication failure from a supplicant and the start of a new authentication attempt.	60
TX Period	Time (in sec) that the switch can wait for a response from the client of an EAP request/identify frame. If no response after this time, the request is re-sent.	30
Supplicant Timeout	Time (in sec) that the switch can wait for a supplicant response to an EAP request.	30
Server Timeout	Time (in sec) that the switch can wait for a Radius	30

	server response to an authentication request.	
Max Requets	Maximum number of authentication attempts that must time-out before authentication fails.	2
Re-Auth Period	Specify how frequently (in sec) the end stations need to reenter usernames and passwords in order to stay connected.	3600

Port Authorize Setting

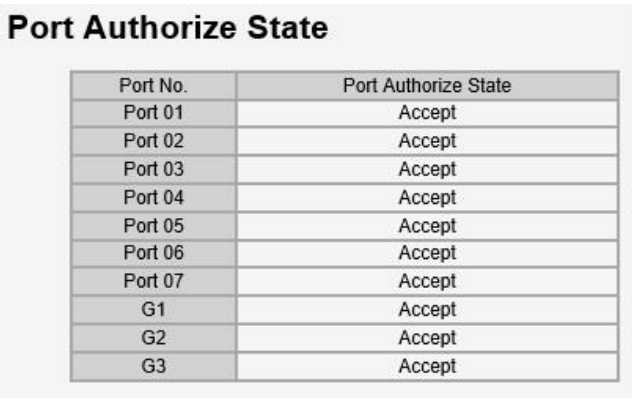
The user can define the behavior of each port of the switch according to the 802.1x programming.

Port Authorize Setting

Setting	Description	Factory Default
Reject	The port is forced to be unauthorized.	Accept
Accept	The port is forced to be authorized.	
Authorize	The authorize status of the port depends on the 802.1x authentication.	
Disabled	The port is not participating in 802.1x authentication.	

Port Authorize State

This option shows the 802.1x authorize setting of each port.



3.12 Warnings

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.

3.12.1 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).

3.12.2 Configuring Email Warning

The Auto Email Warning 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:

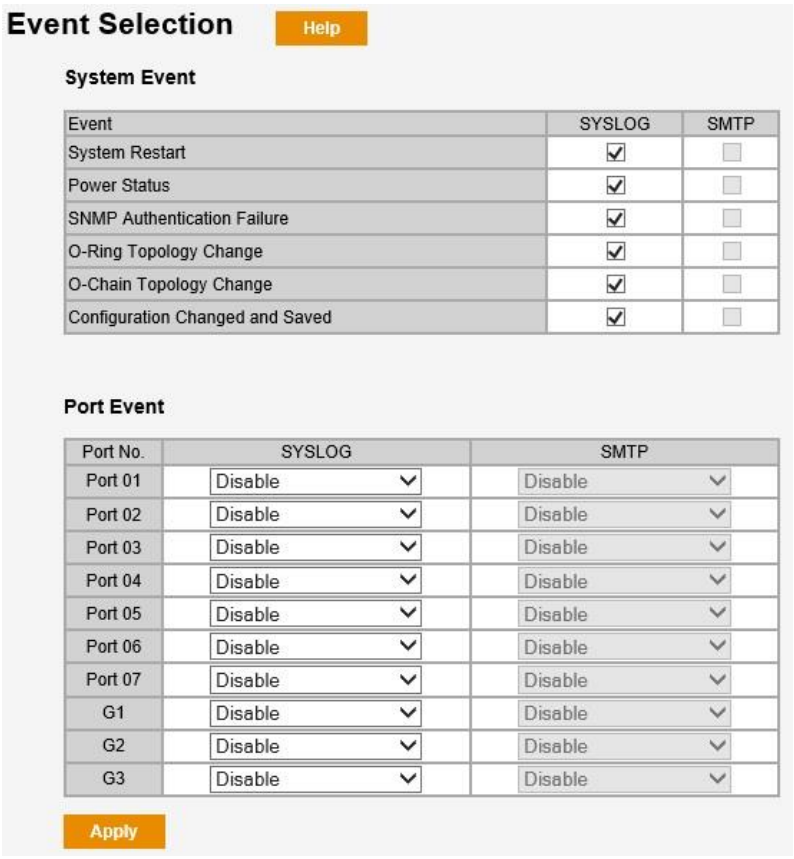
Configure Email Event Types

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.

3.12.2.1 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). It is necessary to Enable Syslog and/or SMTP in the switch to have the possibility to select events in the Event selection 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.

3.12.2.2 Email Settings

Mode

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	None

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.	Check
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

3.12.3 SYSLOG Setting

Mode

Setting	Description	Factory Default
Disabled	No registration of event logs.	Client Only
Client Only	Events are logged only in the switch.	
Server Only	Events are logged only in a remote SYSLOG server.	
Both	Events are logged both locally (switch) and in a remote SYSLOG server.	

Server IP Address

Setting	Description	Factory Default
IP address	The IP address of Syslog Server used by your network.	0.0.0.0

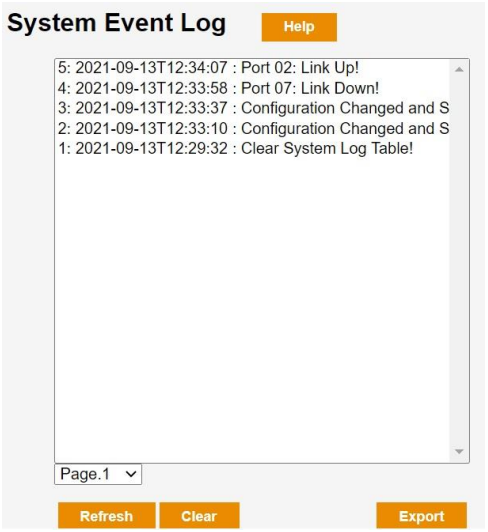
3.13 Monitoring/Diagnosis

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.

3.13.1 System Event Log

If the local SYSLOG setting is enabled (menu Warnings), in this page will be shown the Event Log Table stored in the switch.



The Event Log Table displays the following information:

Date	The date is updated based on how the current date is set in the Basic Setting menu (Time Setting page).
Time	The time is updated based on how the current time is set in the Basic Setting menu (Time Setting page).
Events	Events that have occurred.

The user can press any or the following buttons:

Refresh	Reload the page to get the latest events.
Clear	Delete all the events stored in the switch.
Export	Save the Event Log in a file (.txt format).

NOTE: The local Event Log Table is not stored in flash memory so is deleted when the switch is rebooted. As explained, the user can save it as a .txt file using the Export button.

3.13.2 MAC Address Table

This section explains the information provided by the Weidmüller switch's MAC address table.

The MAC Address table can be configured to display the following Weidmüller switch MAC address groups, which are selected from the drop-down list **Port No.**:

ALL	Select this item to show all of the Weidmüller switch's MAC addresses.
Port n	Select this item to show all of the MAC addresses dedicated ports.

The table displays the following information:

Type	This field shows the type of this MAC address.
MAC	This field shows the MAC address.
Port	This field shows the port that this MAC address belongs to.

Below the table is also shown the number of Static and Dynamic MAC Addresses. The button **Flush Table** deletes all the MAC addresses shown in the table.

In this page the user can also configure the **MAC Address Aging Setting**:

MAC Address Aging Time

Setting	Description	Factory Default
Time (30 sec to 1 hour)	The time before an entry ages and is discarded from the MAC address table.	5 min

Auto Flush Table When Ports Link Down

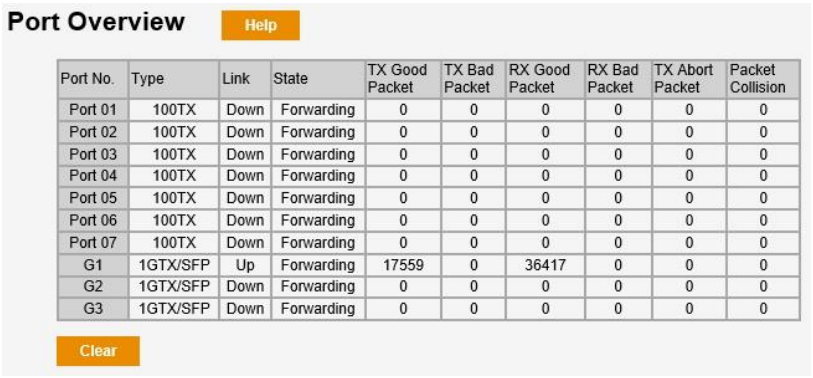
Setting	Description	Factory Default
Enabled / Disabled	When enabled, the switch will delete the MAC address table if a port link gets down.	Disabled

MAC Address Auto Learning

Setting	Description	Factory Default
Enabled / Disabled	Enable or disable the MAC learning function of the switch.	Enabled

3.13.3 Port Overview

This pages provides several traffic statistics for all the ports of the switch.



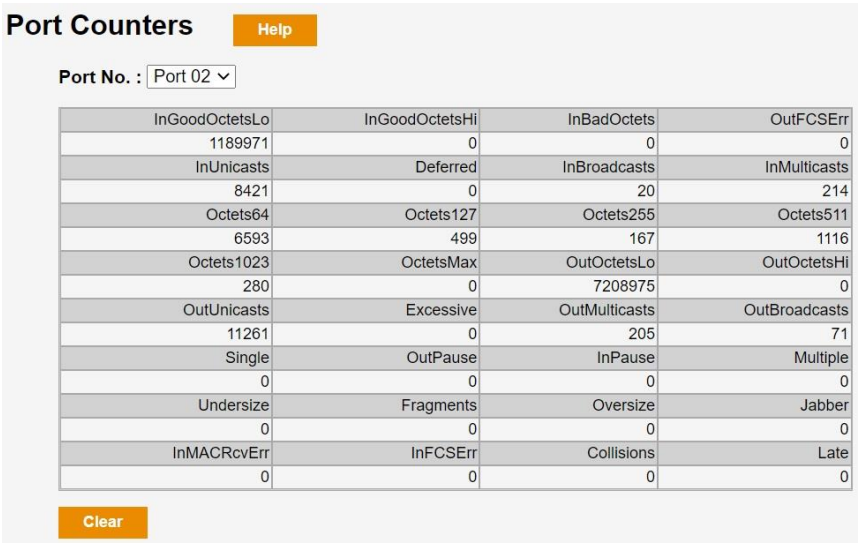
Users can display the following information for each port:

Type	Port speed and media type.
Link	Link status (up or down).
State	Port enabled (forwarding) or disabled.
TX Packets	Packets sent out from the port of the Weidmüller switch. It is distinguished between good packets and bad packets. Bad packets are packets that did not pass TCP/IP's error checking algorithm.
RX Packets	Packets received in the port of the Weidmüller switch from connected devices. It is distinguished between good packets and bad packets. Bad packets are packets that did not pass TCP/IP's error checking algorithm.
Packets collision	The number of times a collision is detected in the port.

The **Clear** button allows the user to reset all the port counters.

3.13.4 Port Counters

This page provides more detailed statistic counters than Port Overview option. Use the port select box to select which switch port details to display.



Users can display the following information for each port:

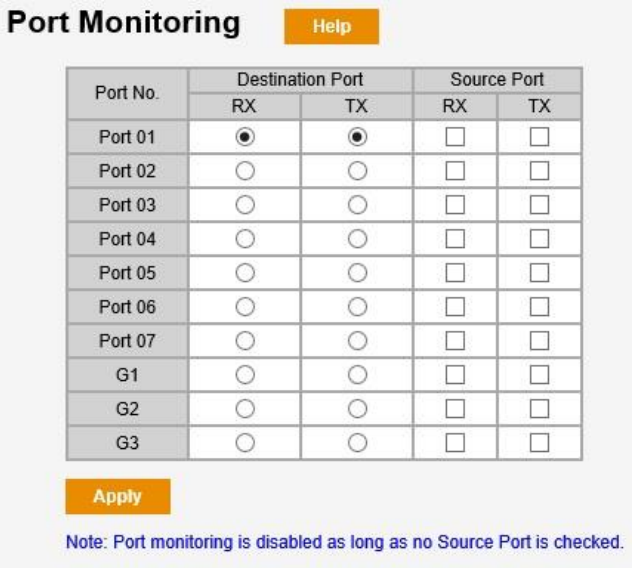
InGoodOctetsLo	The lower 32-bits of the 64-bit InGoodOctets counter.
InGoodOctetsHi	The upper 32-bits of the 64-bit InGoodOctets counter.
InBadOctets	The sum of lengths of all bad Ethernet frames received.
OutFCSErr	The number of frames transmitted with an invalid FCS/CRC.
InUnicasts	The number of good frames received that have a Unicast destination MAC address.
Deferred	The total number of successfully transmitted frames that experienced no collisions but are delayed because the medium is busy during the first attempt.
InBroadcasts	The number of good frames received that have a Broadcast destination MAC address.
InMulticasts	The number of good frames received that have a Multicast destination MAC address.
Octets64	Total frames received (and/or transmitted) with a length of exactly 64 octets.
Octets127	Total frames received (and/or transmitted) with a length between 65 and 127 octets.
Octets255	Total frames received (and/or transmitted) with a length between 128 and 255 octets.
Octets511	Total frames received (and/or transmitted) with a length between 256 and 511 octets.
Octets1023	Total frames received (and/or transmitted) with a length between 512 and 1023 octets.
OctetsMax	Total frames received (and/or transmitted) with a length between 1024 and MaxSize octets.

OutOctetsLo	The lower 32-bit of the 64-bit OutOctets counter.
OutOctetsHi	The upper 32-bit of the 64-bit OutOctets counter.
OutUnicasts	The number of frames sent that have an Unicast destination MAC address.
Excessive	The number frames dropped in the transmit MAC because the frame experienced 16 consecutive collisions. This counter is applicable in half-duplex only.
OutMulticasts	The number of good frames sent that have a Multicast destination MAC address.
OutBroadcasts	The number of good frames sent that have a Broadcast destination MAC address.
Single	The total number of successfully transmitted frames that experienced exactly one collision. This counter is applicable in half-duplex only.
OutPause	The number of good Flow Control frames sent.
InPause	The number of good Flow Control frames received.
Multiple	The total number of successfully transmitted frames that experienced more than one collision. This counter is applicable in half-duplex only.
Undersize	Total frames received with a length of less than 64 octets but with a valid FCS/CRC.
Fragments	Total frames received with a length of more than 64 octets and with an invalid FCS/CRC.
Oversize	Total frames received with a length of more than MaxSize octets but with a valid FCS/CRC.
Jabber	Total frames received with a length of more than MaxSize octets but with an invalid FCS/CRC.
InMACRcvErr	Total frames received with an RxErr signal from the physical interface.
InFCSErr	Total frames received with an FCS/CRC error not counted in Fragments, Jabber or RxErr.
Collisions	The number of collision events seen by MAC not including those counted in Single, Multiple, Excessive or Late. This counter is applicable in half-duplex only.
Late	The number of times a collision is detected later than 512 bit-times into the transmission of a frame. This counter is applicable in half-duplex only.

The **Clear** button allows the user to reset all the port counters.

3.13.5 Port Monitoring (Mirror port)

The **Port Monitoring (Mirror port)** function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the *monitored / mirror port*) to receive the same data being transmitted from, or both to and from, the port under observation. This allows the network administrator to **sniff** the observed port and thus keep tabs on network activity.



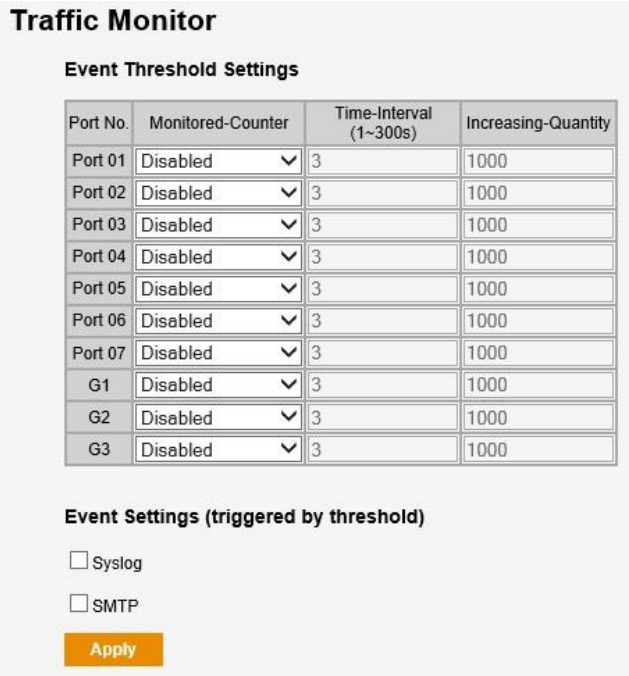
Port Monitoring Settings

Setting	Description
Source Port	Select one or several ports whose network activity will be monitored. It is possible to select RX, TX or both. • **RX** Select this option to monitor only those data packets coming in through the monitored port. • **TX** Select this option to monitor only those data packets being sent out through the monitored port. Select both RX and TX to monitor data packets both coming into, and being sent out through, the monitored port.
Destination Port	Select one port that will be used to monitor the activity of the monitored port. It is possible to use different monitored / mirror ports for TX and RX data.

NOTE: Port Monitoring is enabled by selecting at least one source port and pressing the button Apply.

3.13.6 Traffic Monitor

This page allows the user to set up an event when high volume of traffic is received during a short period of time through any of the ports of the switch. This event can be either logged in the Syslog or sent by email as a warning.



The parameters that can be programmed in each port to set up this excessive traffic event are:

Monitored-Counter

Setting	Description	Factory Default
Disabled / “Traffic type”	To enable the traffic monitoring in the port of the switch we have to select the type of traffic we want to monitor: • RX Octet **(**all received frames) • RX Broadcast (broadcast received frames) • RX Multicast (multicast received frames) • RX Unicast (unicast received frames) • RX Non-Unicast (broadcast and unicast received frames)	Disabled

Time Interval

Setting	Description	Factory Default
Time between 1 and 300 sec	Define the time that the switch will be monitoring/counting the number of received frames.	3 sec

Increasing Quantity

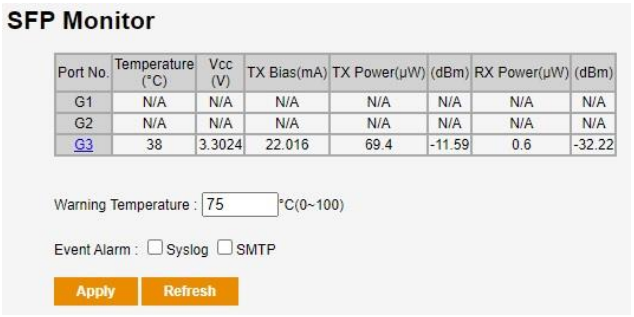
Setting	Description	Factory Default
Number between 1 and 999999999	Threshold to define the minimum number of frames that have to be received during the time interval to consider that excessive traffic is being received.	1000

Event Settings (triggered by threshold)

Setting	Description	Factory Default
Syslog	Check to register the event in Syslog.	Unchecked
SMTP	Check to send an email event.	Unchecked

3.13.7 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 (uW)	The amount of light being transmitted into the fiber optic cable in uW
(dBm)	The amount of light being transmitted into the fiber optic cable in dBm
Rx power (uW)	The amount of light being received from the fiber optic cable in uW
(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 either logged in Syslog or sent as event by email.

Warning Temperature

Setting	Description	Factory Default
Number between 0 and 100 ºC	Temperature threshold for warning event.	75 ºC

Event Alarm

Setting	Description	Factory Default
Syslog	Check to register the event in Syslog.	Unchecked
SMTP	Check to send an email event.	Unchecked

3.13.8 Ping

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, and then click **Send Ping**.

3.14 Save Configuration

After changing any parameter / function in a web page the button **Apply** activates the change but **does not save it**. The text "*Configuration changed and applied but not saved!*" is shown in all the pages of the web interface. It means the changes would be lost after restarting the switch.

The Save Configuration option permanently saves the applied changes to flash memory.

In the page is always indicated if the current configuration is saved to flash memory or not.

3.15 Factory Default

This function provides users with a quick way of restoring the Weidmüller switch's configuration to factory defaults.

The user has the possibility to restore to factory defaults but keeping the current IP address and username / password settings.

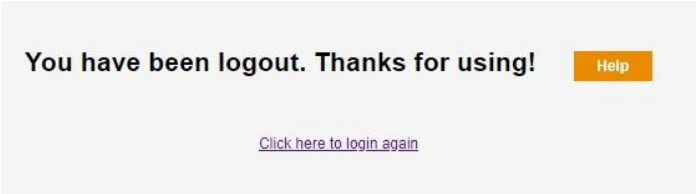
3.16 System Reboot

This function is used to restart the Ethernet Switch.

In the page are shown the active (running) and alternate firmware images and the user can decide which one should be taken for the reboot.

3.17 Logout

This option can be used to leave the Web Management of the switch.



4. Command Line Interface (CLI) Management

Besides Web Management, the IE-SW-SL10M-7TX-3GC also supports CLI Management either from console port or Telnet.

4.1 CLI Management by Console port

Using the provided accessory cable, connect the “CONSOLE” port (RJ-45) to the PC terminal communication port (DB9). Run any terminal emulation program (HyperTerminal, PuTTY, TeraTermPro, etc.) and configure the communication parameters as follows:

- Speed: 9600
- Data: 8 bits
- Parity: None
- Stop bits: 1
- Flow Control: None

The console login screen will appear. Use the keyboard to introduce the “Username” and “Password”.

NOTE: The same Username and password used to access to the Web Management have to be used for the Console port.

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

4.2 CLI Management by Telnet

Opening the Weidmüller switch’s Telnet over a network requires that the PC host and Weidmüller switch are on the same logical subnet (same as with Web Management). You may need to adjust your PC host’s IP address and subnet mask. By default, the Weidmüller switch’s IP address is 192.168.1.110 and the switch’s subnet mask is 255.255.255.0 (for a Class C network). If you do not change these values, and your PC host's subnet mask is 255.255.255.0, then its IP address must have the form 192.168.1.xxx

NOTE: When connecting to the switch’s Telnet ensure that your PC host and the switch are on the same logical subnet.

NOTE: When connecting to the switch’s Telnet, first connect one of the switch’s Ethernet ports to your Ethernet LAN or directly to your PC’s Ethernet port. You may use 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 Weidmüller switch's Telnet console using any Telnet client (Windows Telnet Client, PuTTY, TeraTermPro, etc.).

4.3 CLI Modes

The Command Line Interface (CLI) of Substation Line series is mainly divided into five basic modes; these are User mode, EXEC mode, Configuration mode, VLAN database and Configuration Interface mode. The commands available in User mode and EXEC mode are limited. For more advanced configurations, you must enter Config mode, VLAN database or Config Interface mode. In each mode, a question mark (?) at the system prompt can be issued to obtain a list of commands available for each command mode. The following table provides a brief overview of modes available in this device.

Mode	Prompt	Enter Method	Exit Method
User mode	>	enable	disable
EXEC mode	#	Enter authorized username and password	Exit, logout
Global Config Mode	(config)#	Enter "configure terminal" after "#"	End, exit, do logout
VLAN Database	(vlan)#	Enter "vlan database" after "#"	Exit, do logout
Config Interface Mode	(config-if)#	Specify interface, interface type and number after (config)#	End, exit, do logout

4.4 Quick keys

There are several useful quick keys you can use when editing command lines.

Keyboard	Action
?	Issue "?" to get a list of commands available in the current mode.
Up arrow key	To view the previous entered commands.
Down arrow key	To view the previous entered commands.
Tab key	To complete an unfinished command.

4.5 System commands

Command	Mode	Description	Example
show config	User	Show switch configuration	>show config
show terminal	EXEC	Show console information	#show terminal
write memory	EXEC	Save your configuration into permanent memory (flash rom)	#write memory
system name [System Name]	Global Config	Configure system name	(config)#system name xxx
system location [System Location]	Global Config	Set switch system location string	(config)#system location xxx
system description [System Description]	Global Config	Set switch system description string	(config)#system description xxx
system contact [System Contact]	Global Config	Set switch system contact window string	(config)#system contact xxx
show system-info	User	Show system information	>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	Global Config	Configure the IP address of switch	(config)#ip address 192.168.1.110 255.255.255.0 192.168.1.254
ip dhcp	Global Config	Enable DHCP client function of switch	(config)#ip dhcp
show ip	EXEC	Show IP information of switch	#show ip
no ip dhcp	Global Config	Disable DHCP client function of switch	(config)#no ip dhcp
reload	Global Config	Halt and perform a cold restart	(config)#reload
default	Global Config	Restore to default	(config)#default

admin username [Username]	Global Config	Changes a login username.(maximum 10 words)	(config)#admin username xxxxxx
admin password [Password]	Global Config	Specifies a password (maximum 10 words)	(config)#admin password xxxxxx
show admin	EXEC	Show administrator information	#show admin
dhcpserver enable	Global Config	Enable DHCP Server	(config)#dhcpserver enable
dhcpserver lowip [Low IP]	Global Config	Configure low IP address for IP pool	(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip [High IP]	Global Config	Configure high IP address for IP pool	(config)# dhcpserver highip 192.168.1.50
dhcpserver subnetmask [Subnet mask]	Global Config	Configure subnet mask for DHCP clients	(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	Global Config	Configure gateway for DHCP clients	(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	Global Config	Configure DNS IP for DHCP clients	(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [Hours]	Global Config	Configure lease time (in hour)	(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	Interface Config	Set static IP for DHCP clients by port	(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	EXEC	Show configuration of DHCP server	#show dhcpserver configuration
show dhcpserver clients	EXEC	Show client entries of DHCP server	#show dhcpserver clinets
show dhcpserver ip-binding	EXEC	Show IP-Binding information of DHCP server	#show dhcpserver ip-binding

no dhcpserver	Global Config	Disable DHCP server function	(config)#no dhcpserver
security enable	Global Config	Enable IP security function	(config)#security enable
security http	Global Config	Enable IP security of HTTP server	(config)#security http
security telnet	Global Config	Enable IP security of telnet server	(config)#security telnet
security ip [Index(1..10)] [IP Address]	Global Config	Set the IP security list	(config)#security ip 1 192.168.1.55
show security	EXEC	Show the information of IP security	#show security
no security	Global Config	Disable IP security function	(config)#no security
no security http	Global Config	Disable IP security of HTTP server	(config)#no security http
no security telnet	Global Config	Disable IP security of telnet server	(config)#no security telnet

4.6 Port commands

Command	Mode	Description	Example
interface fastEthernet [Portid]	Global Config	Choose the port for modification.	(config)#interface fastEthernet 2
duplex [full | half]	Interface Config	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	(config)#interface fastEthernet 2 (config-if)#duplex full
speed [10|100|1000|auto]	Interface Config	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	(config)#interface fastEthernet 2 (config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	Interface Config	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	(config)#interface fastEthernet 2 (config-if)#flowcontrol mode Asymmetric
no flowcontrol	Interface Config	Disable flow control of interface	(config-if)#no flowcontrol
security enable	Interface Config	Enable security of interface	(config)#interface fastEthernet 2 (config-if)#security enable
no security	Interface Config	Disable security of interface	(config)#interface fastEthernet 2 (config-if)#no security
bandwidth type all	Interface Config	Set interface ingress limit frame type to "accept all frame"	(config)#interface fastEthernet 2 (config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	Interface Config	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	(config)#interface fastEthernet 2 (config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	Interface Config	Set interface ingress limit frame type to "accept broadcast and multicast frame"	(config)#interface fastEthernet 2 (config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	Interface Config	Set interface ingress limit frame type to "only accept broadcast frame"	(config)#interface fastEthernet 2 (config-if)#bandwidth type broadcast-only
bandwidth in [Value]	Interface Config	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	(config)#interface fastEthernet 2 (config-if)#bandwidth in 100

bandwidth out [Value]	Interface Config	Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	(config)#interface fastEthernet 2 (config-if)#bandwidth out 100
show bandwidth	Interface Config	Show interfaces bandwidth control	(config)#interface fastEthernet 2 (config-if)#show bandwidth
state [Enable | Disable]	Interface Config	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	(config)#interface fastEthernet 2 (config-if)#state Disable
show interface configuration	Interface Config	show interface configuration status	(config)#interface fastEthernet 2 (config-if)#show interface configuration
show interface status	Interface Config	show interface actual status	(config)#interface fastEthernet 2 (config-if)#show interface status
show interface accounting	Interface Config	show interface statistic counter	(config)#interface fastEthernet 2 (config-if)#show interface accounting
no accounting	Interface Config	Clear interface accounting information	(config)#interface fastEthernet 2 (config-if)#no accounting

4.7 Port trunking commands

Command	Mode	Description	Example
aggregator priority [1to65535]	Global Config	Set port group system priority	(config)#aggregator priority 22
aggregator activityport [Port Numbers]	Global Config	Set activity port	(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] lacp workp [Workport]	Global Config	Assign a trunk group with LACP active. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	(config)#aggregator group 1 1-4 lacp workp 2 or (config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group [GroupID] [Port-list] nolacp	Global Config	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	(config)#aggregator group 1 2-4 nolacp or (config)#aggreator group 1 3,1,2 nolacp
show aggregator	EXEC	Show the information of trunk group	#show aggregator
no aggregator lacp [GroupID]	Global Config	Disable the LACP function of trunk group	(config)#no aggreator lacp 1
no aggregator group [GroupID]	Global Config	Remove a trunk group	(config)#no aggreator group 2

4.8 VLAN commands

Command	Mode	Description	Example
vlan database	EXEC	Enter VLAN configure mode	#vlan database
vlan [8021q | portbase | gvrp]	VLAN Database	To set switch VLAN mode.	(vlan)# vlanmode 802.1q or (vlan)# vlanmode port or (vlan)# vlanmode gvrp
no vlan [VID]	VLAN Database	Disable vlan group(by VID)	(vlan)#no vlan 2
no gvrp	VLAN Database	Disable GVRP	(vlan)#no gvrp
vlan port-based grpname [GroupName] grpid [VLANID] port [PortMembers]	VLAN Database	Set VLAN ID and port members in Port based VLAN operation	(vlan)# vlan port-based grpname 1 grpid 1 port 1-3
no vlan [VID]	VLAN Database	Remove created port-based VLAN	no vlan 1
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	VLAN Database	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	(vlan)#vlan 802.1q port 3 access-link untag 33
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	VLAN Database	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or (vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	VLAN Database	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or (vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggreator [TrunkID] access-link untag [UntaggedVID]	VLAN Database	Assign a access link for VLAN by trunk group	(vlan)#vlan 8021q aggreator 3 access-link untag 33
vlan 8021q aggreator [TrunkID] trunk-link tag [TaggedVID List]	VLAN Database	Assign a trunk link for VLAN by trunk group	(vlan)#vlan 8021q aggreator 3 trunk-link tag 2,3,6,99 or (vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator [PortNumber] hybrid-link	VLAN Database	Assign a hybrid link for VLAN by trunk group	(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8

untag [UntaggedVID] tag [TaggedVID List]			or (vlan)# vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or show vlan	VLAN Database	Show VLAN information	(vlan)#show vlan 23

4.9 Spanning Tree commands

Command	Mode	Description	Example
spanning-tree enable	Global Config	Enable spanning tree	(config)#spanning-tree enable
spanning-tree priority [0to61440]	Global Config	Configure spanning tree priority parameter	(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	Global Config	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	(config)#spanning-tree max-age 15
spanning-tree hello-time [seconds]	Global Config	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	Global Config	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	(config)#spanning-tree forward-time 20

stp-path-cost [1to200000000]	Interface Config	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	(config)#interface fastEthernet 2 (config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	Interface Config	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	(config)#interface fastEthernet 2 (config-if)# stp-path-priority 127
stp-admin-p2p [Auto|True|False]	Interface Config	Admin P2P of STP priority on this interface.	(config)#interface fastEthernet 2 (config-if)# stp-admin-p2p Auto
stp-admin-edge [True|False]	Interface Config	Admin Edge of STP priority on this interface.	(config)#interface fastEthernet 2 (config-if)# stp-admin-edge True
stp-admin-non-stp [True|False]	Interface Config	Admin NonSTP of STP priority on this interface.	(config)#interface fastEthernet 2 (config-if)# stp-admin-non-stp False
Show spanning-tree	User	Display a summary of the spanning-tree states.	>show spanning-tree
no spanning-tree	Global Config	Disable spanning-tree.	(config)#no spanning-tree

4.10 O-Ring Redundancy commands

Command	Mode	Description	Example
Ring enable	Global Config	Enable O-Ring	(config)# ring enable
Ring master	Global Config	Enable ring master	(config)# ring master
Ring couplering	Global Config	Enable couple ring	(config)# ring couplering
Ring dualhoming	Global Config	Enable dual homing	(config)# ring dualhoming
Ring ringport [1st Ring Port] [2nd Ring Port]	Global Config	Configure 1st/2nd Ring Port	(config)# ring ringport 7 8
Ring couplingport [Coupling Port]	Global Config	Configure Coupling Port	(config)# ring couplingport 1
Ring controlport [Control Port]	Global Config	Configure Control Port	(config)# ring controlport 2
Ring homingport [Dual Homing Port]	Global Config	Configure Dual Homing Port	(config)# ring homingport 3
show Ring	EXEC	Show the information of O-Ring	#show ring
no Ring	Global Config	Disable O-Ring	(config)#no ring
no Ring master	Global Config	Disable ring master	(config)# no ring master
no Ring couplering	Global Config	Disable couple ring	(config)# no ring couplering
no Ring dualhoming	Global Config	Disable dual homing	(config)# no ring dualhoming

4.11 QoS commands

Command	Mode	Description	Example
qos policy [weighted-fair|strict]	Global Config	Select QOS policy scheduling	(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	Global Config	Setting of QOS priority type	(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	Global Config	Configure Port-based Priority	(config)#qos priority portbased 1 low
qos priority cos [Priority][lowest|low|middle|high]	Global Config	Configure CoS Priority	(config)#qos priority cos 22 middle
qos priority tos [Priority][lowest|low|middle|high]	Global Config	Configure ToS Priority	(config)#qos priority tos 3 high
show qos	User	Display the information of QoS configuration	>show qos
no qos	Global Config	Disable QoS function	(config)#no qos

4.12 IGMP commands

Command	Mode	Description	Example
igmp enable	Global Config	Enable IGMP snooping function	(config)#igmp enable
Igmp-query auto	Global Config	Set IGMP query to auto mode	(config)#Igmp-query auto
Igmp-query force	Global Config	Set IGMP query to force mode	(config)#Igmp-query force
show igmp configuration	EXEC	Displays the details of an IGMP configuration.	#show igmp configuration
show igmp multi	EXEC	Displays the details of an IGMP snooping entries.	#show igmp multi
no igmp	Global Config	Disable IGMP snooping function	(config)#no igmp
no igmp-query	Global Config	Disable IGMP query	#no igmp-query

4.13 Static filtering commands

Command	Mode	Description	Example
mac-address-table static hwaddr [MAC]	Interface Config	Configure MAC address table of interface (static).	(config)#interface fastEthernet 2 (config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	Global Config	Configure MAC address table(filter)	(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	EXEC	Show all MAC address table	#show mac-address-table
show mac-address-table static	EXEC	Show static MAC address table	#show mac-address-table static
show mac-address-table filter	EXEC	Show filter MAC address table.	#show mac-address-table filter
no mac-address-table static hwaddr [MAC]	Interface Config	Remove an entry of MAC address table of interface (static)	(config)#interface fastEthernet 2 (config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	Global Config	Remove an entry of MAC address table (filter)	(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	Global Config	Remove dynamic entry of MAC address table	(config)#no mac-address-table

4.14 SNMP commands

Command	Mode	Description	Example
snmp agent-mode [v1v2c | v3]	Global Config	Select the agent mode of SNMP	(config)#snmp agent-mode v1v2c
snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]	Global Config	Configure SNMP server host information and community string	(config)#snmp-server host 192.168.10.50 community public trap-version v1 (remove) (config)# no snmp-server host 192.168.10.50
snmp community-strings [Community-string] right [RO|RW]	Global Config	Configure the community string right	(config)#snmp community-strings public right RO or (config)#snmp community-strings public right RW
snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	Global Config	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	EXEC	Show SNMP configuration	#show snmp
show snmp-server	EXEC	Show specified trap server information	#show snmp-server
no snmp community-strings [Community]	Global Config	Remove the specified community.	(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	Global Config	Remove specified user of SNMPv3 agent. Privacy password could be empty.	(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host [Host-address]	Global Config	Remove the SNMP server host.	(config)#no snmp-server 192.168.10.50

4.15 Port Mirroring commands

Command	Mode	Description	Example
monitor rx	Global Config	Set RX destination port of monitor function	(config)#monitor rx
monitor tx	Global Config	Set TX destination port of monitor function	(config)#monitor tx
show monitor	EXEC	Show port monitor information	#show monitor
monitor [RX|TX|Both]	Interface Config	Configure source port of monitor function	(config)#interface fastEthernet 2 (config-if)#monitor RX
show monitor	Interface Config	Show port monitor information	(config)#interface fastEthernet 2 (config-if)#show monitor
no monitor	Interface Config	Disable source port of monitor function	(config)#interface fastEthernet 2 (config-if)#no monitor

4.16 802.1x commands

Command	Mode	Description	Example
8021x enable	Global Config	Use the 802.1x global configuration command to enable 802.1x protocols.	(config)# 8021x enable
8021x system radiousip [IP address]	Global Config	Use the 802.1x system radious IP global configuration command to change the radious server IP.	(config)# 8021x system radiousip 192.168.1.1
8021x system serverport [port ID]	Global Config	Use the 802.1x system server port global configuration command to change the radious server port	(config)# 8021x system serverport 1815
8021x system accountport [port ID]	Global Config	Use the 802.1x system account port global configuration command to change the accounting port	(config)# 8021x system accountport 1816
8021x system sharekey [ID]	Global Config	Use the 802.1x system share key global configuration command to change the shared key value.	(config)# 8021x system sharekey 123456
8021x system nasid [words]	Global Config	Use the 802.1x system nasid global configuration command to change the NAS ID	(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	Global Config	Use the 802.1x misc quiet period global configuration command to specify	(config)# 8021x misc quietperiod 10

		the quiet period value of the switch.	
8021x misc txperiod [sec.]	Global Config	Use the 802.1x misc TX period global configuration command to set the TX period.	(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	Global Config	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	Global Config	Use the 802.1x misc server timeout global configuration command to set the server timeout.	(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	Global Config	Use the 802.1x misc max request global configuration command to set the MAX requests.	(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	Global Config	Use the 802.1x misc reauth period global configuration command to set the reauth period.	(config)# 8021x misc reauthperiod 3000
8021x portstate [disable | reject | accept | authorize]	Interface Config	Use the 802.1x port state interface configuration command to set the state of the selected port.	(config)#interface fastethernet 3 switch(config-if)#802 1x portstate accept
show 8021x	User	Display a summary of the 802.1x properties and also the port sates.	>show 8021x
no 8021x	Global Config	Disable 802.1x function	(config)#no 8021x

4.17 TFTP commands

Command	Mode	Description	Example
backup flash:backup_cfg	Global Config	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	(config)#backup flash:backup_cfg
restore flash:restore_cfg	Global Config	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	Global Config	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	(config)#upgrade flash:upgrade_fw

4.18 Syslog / SMTP / Event commands

Command	Mode	Description	Example
systemlog ip [IP address]	Global Config	Set System log server IP address.	(config)# systemlog ip 192.168.1.100
systemlog mode [client|server|both]	Global Config	Specified the log mode	(config)# systemlog mode both
show systemlog	User	Display system log.	>show systemlog
show systemlog	EXEC	Show system log client & server information	#show systemlog
no systemlog	Global Config	Disable systemlog functon	(config)#no systemlog
smtp enable	Global Config	Enable SMTP function	(config)#smtp enable
smtp serverip [IP address]	Global Config	Configure SMTP server IP	(config)#smtp serverip 192.168.1.5
smtp authentication	Global Config	Enable SMTP authentication	(config)#smtp authentication
smtp account [account]	Global Config	Configure authentication account	(config)#smtp account User
smtp password [password]	Global Config	Configure authentication password	(config)#smtp password
smtp rcptemail [Index] [Email address]	Global Config	Configure Rcpt e-mail Address	(config)#smtp rcptemail 1 Alert@test.com
show smtp	EXEC	Show the information of SMTP	#show smtp
no smtp	Global Config	Disable SMTP function	(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	Global Config	Set cold start event type	(config)#event device-cold-start both
event authentication-failure [Systemlog|SMTP|Both]	Global Config	Set Authentication failure event type	(config)#event authentication-failure both
event O-Ring-topology-change [Systemlog|SMTP|Both]	Global Config	Set s ring topology changed event type	(config)#event ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	Interface Config	Set port event for system log	(config)#interface fastethernet 3 (config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	Interface Config	Set port event for SMTP	(config)#interface fastethernet 3 (config-if)#event smtp both
show event	EXEC	Show event selection	#show event

no event device-cold-start	Global Config	Disable cold start event type	(config)#no event device-cold-start
no event authentication-failure	Global Config	Disable Authentication failure event typ	(config)#no event authentication-failure
no event O-Ring-topology-change	Global Config	Disable O-Ring topology changed event type	(config)#no event ring-topology-change
no event systemlog	Interface Config	Disable port event for system log	(config)#interface fastethernet 3 (config-if)#no event systemlog
no event smpt	Interface Config	Disable port event for SMTP	(config)#interface fastethernet 3 (config-if)#no event smtp
show systemlog	EXEC	Show system log client & server information	#show systemlog

4.19 SNTP commands

Command	Mode	Description	Example
sntp enable	Global Config	Enable SNTP function	(config)#sntp enable
sntp daylight	Global Config	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	(config)#sntp daylight
sntp daylight-period [Start time] [End time]	Global Config	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	Global Config	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	(config)#sntp daylight-offset 3
sntp ip [IP]	Global Config	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	Global Config	Set timezone index, use "show sntp timzezone" command to get more information of index number	(config)#sntp timezone 22
show sntp	EXEC	Show SNTP information	#show sntp
show sntp timezone	EXEC	Show index number of time zone list	#show sntp timezone
no sntp	Global Config	Disable SNTP function	(config)#no sntp
no sntp daylight	Global Config	Disable daylight saving time	(config)#no sntp daylight

A. Downloads (Software and Documentation)

Using below described link you can download following items:

- Firmware Upgrades
- Private MIB files
- Documentation (User Manual and Hardware Installation Guide)

Download via **Product Catalogue (Online Catalogue)**

- Download latest Firmware version, Private MIB 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