

# Industrial Ethernet managed Switches

---

## Manual for Lite Advanced Line Switches

IE-SW-AL05M-5TX (2682250000)

IE-SW-AL06M-4TX-2SC (2682260000)

IE-SW-AL06M-4TX-2SCS (2682270000)



Second Edition, July 2022

**Weidmüller** 

# Industrial Ethernet managed Switches

## Manual

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

### Copyright Notice

Copyright ©2016 Weidmüller Interface GmbH & Co. KG

All rights reserved.

Reproduction without permission is prohibited.

### Disclaimer

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

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

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

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

### Contact Information

Weidmüller Interface GmbH & Co. KG

Postfach 3030

32760 Detmold

Klingenbergstraße 26

32758 Detmold

Germany

Phone +49 (0) 5231 14-0

Fax +49 (0) 5231 14-2083

E-Mail [info@weidmueller.com](mailto:info@weidmueller.com)

Internet [www.weidmueller.com](http://www.weidmueller.com)

# Table of Contents

<b>1. About this Manual .....</b>	<b>3</b>
<b>2. Getting Started .....</b>	<b>3</b>
2.1 Hardware features .....	3
2.2 Software features .....	3
<b>3. Web Management.....</b>	<b>4</b>
3.1 Accessing the Web interface via HTTP .....	4
3.2 Accessing the Web interface via HTTPS .....	6
3.3 Basic Settings .....	6
3.3.1 System Setting .....	7
3.3.2 Admin Password .....	7
3.3.3 IP Setting.....	8
3.3.4 IPv6 Setting.....	10
3.3.5 Time Setting .....	10
3.3.6 LLDP Function .....	12
3.3.6.1 Overview .....	12
3.3.6.2 Configuring LLDP Settings .....	13
3.3.7 Modbus TCP .....	14
3.3.8 DIP Switch.....	14
3.3.9 Backup & Restore .....	15
3.3.10 Upgrade Firmware .....	16
3.4 Port Settings .....	17
3.4.1 Port control.....	17
3.4.2 Port status .....	18
3.4.3 Port Alias.....	18
3.4.4 Loop Guard .....	18
3.5 Redundancy .....	19
3.5.1 Introduction to Communication Redundancy .....	19
3.5.2 The O-Ring Concept .....	20
3.5.2.1 Topology Setup for “O-Ring” .....	20
3.5.2.2 Ring Coupling Configuration.....	21
3.5.2.3 Dual Homing Configuration.....	21
3.5.3 Configuring “O-Ring” .....	22
3.5.4 The O-Chain Concept .....	24
3.5.5 Configuring O-Chain .....	26
3.5.6 STP / RSTP.....	27
3.5.6.1 The STP / RSTP Concept.....	27
3.5.6.2 How STP Works.....	29
3.5.6.3 Configuring RSTP .....	31

3.5.6.4 Information RSTP .....	33
3.5.6.5 RSTP-Repeater .....	34
3.5.7 Fast Recovery .....	34
<b>3.6 Virtual LAN.....</b>	<b>35</b>
3.6.1 The Virtual LAN (VLAN) Concept .....	35
3.6.2 Configuring port-based Virtual LAN .....	36
<b>3.7 DHCP Server/Relay .....</b>	<b>36</b>
3.7.1 Configuring DHCP Server .....	37
3.7.2 DHCP Relay Agent (Option 82) .....	39
3.7.3 Client List .....	41
3.7.4 Port and IP binding .....	41
<b>3.8 SNMP .....</b>	<b>41</b>
3.8.1 SNMP Read/Write Settings .....	42
3.8.2 Trap Settings .....	47
<b>3.9 Security .....</b>	<b>48</b>
3.9.1 Management Security .....	48
3.9.2 TACACS+ .....	49
<b>3.10 Warnings .....</b>	<b>50</b>
3.10.1 Configuring Relay Warnings .....	50
3.10.2 Configuring Email Warning .....	51
3.10.2.1 Event Selection .....	51
3.10.2.2 Email Settings .....	52
3.10.3 SYSLOG Setting .....	53
<b>3.11 Monitoring/Diagnosis .....</b>	<b>54</b>
3.11.1 System Event Log .....	54
3.11.2 Ping .....	55
<b>3.12 Save Configuration .....</b>	<b>55</b>
<b>3.13 Factory Default .....</b>	<b>56</b>
<b>3.14 System Reboot .....</b>	<b>56</b>
<b>3.15 Logout .....</b>	<b>56</b>
<b>A. Downloads (Software and Documentation).....</b>	<b>57</b>
<b>B. Modbus Register Table .....</b>	<b>58</b>

# 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 Lite Advanced Line Switches. The information related with the Installation of each 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

The Lite Advanced Line Switches are configured and monitored through its web interface. This web interface is fully described in this chapter.

# 2. Getting Started

The Lite Advanced Line Switches are cost-effective products specially designed to operate in harsh industrial environments thanks to rugged design. The products come with an IP30 rugged case, redundant power input, alarm relay and wide operating temperature range from -40 to 75°C.

## 2.1 Hardware features

- IE-SW-AL05M-5TX: 5 x 10/100Base-T(X) ports
- IE-SW-AL06M-4TX-2SC
  - 4 x 10/100Base-T(X) ports
  - 2 x 100Base-FX ports (SC connector), multimode
- IE-SW-AL06M-4TX-2SCS
  - 4 x 10/100Base-T(X) ports
  - 2 x 100Base-FX ports (SC connector), singlemode
- Redundant power input: 12 to 48Vdc
- Alarm relay contact
- Operating temperature from -40 to 75°C

## 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)

- O-Ring (optimized protocol for ring topologies; recovery time < 10ms)
  - O-Chain (allows multiple redundant network topologies; recovery time < 10ms)
  - 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)
  - Syslog
  - Event based warning (via e.mail / via output relay / via SNMP trap)
- Network traffic filter
  - Port based VLAN
- Security functions
  - VLAN segmentation
  - Enable / Disable ports
  - TACACS+ User Authentication
  - 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 recommended web browser is Microsoft Internet Explorer 8.0 or higher with JVM (Java Virtual Machine) installed.



**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.



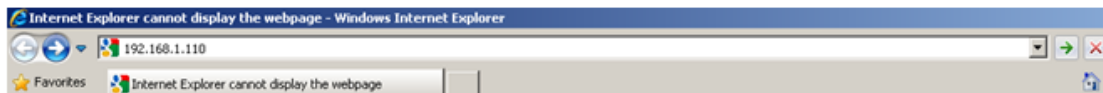
**NOTE:** Before accessing the Switch's web browser interface, first connect one of its RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can establish a connection with either a straight-through or cross-over Ethernet cable.



**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.

System Information

Help

System Name	IE-SW-AL05LM-5TX
System Description	Industrial 5-port slim type lite-managed Ethernet switch with 5x10/100Base-T(X)
System Location	
System Contact	
SNMP OID	1.3.6.1.4.1.38187.4.56
Firmware Version	v1.12
Kernel Version	v3.54
MAC Address	00-15-7E-1D-00-07
Serial Number	02009DB00011
System Uptime	60 Day(s) 5 Hour(s) 51 Min(s) 17 Sec(s)
Redundancy Setting	Not activated

Enable Location Alert



**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.

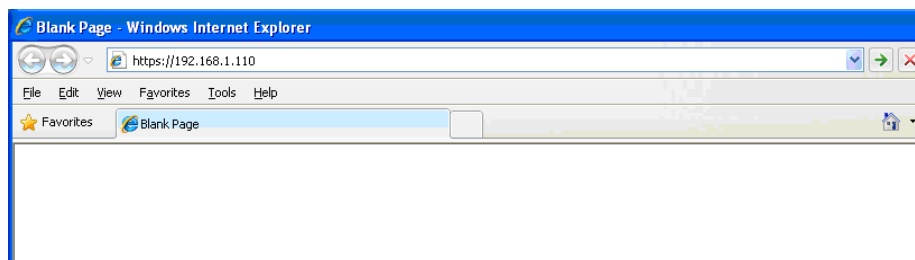


**NOTE:** After changing any parameter / function in a web page the button **Apply** activates the change but **does not save it**. The changes have to be saved using the **Save Configuration** option of the menu.

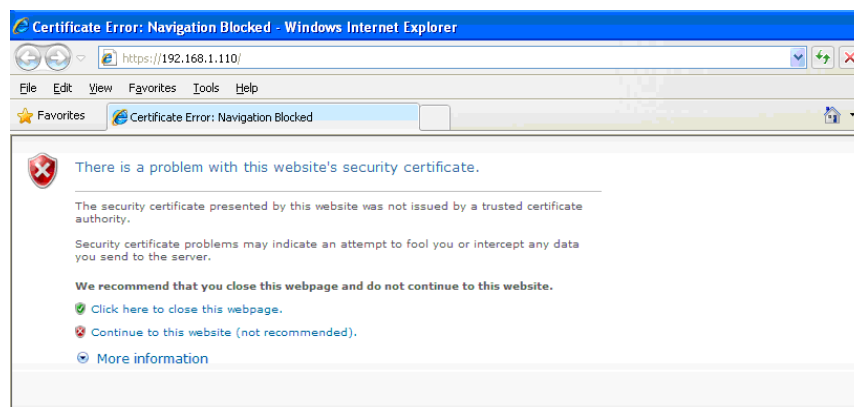
## 3.2 Accessing the Web interface via HTTPS

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 Setting**
Help

System Name 
System Description 
System Location 
System Contact

Apply

#### 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: Production Line 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.

### Admin Password

User Name

Confirm Old Password

New Password

Confirm Password



**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.

#### User Name

Setting	Description	Factory Default
Max. 31 characters	Enter the new user name.	admin

#### Confirm Old Password

Setting	Description	Factory Default
Max. 24 characters	Enter the old password.	Detmold

#### New Password

Setting	Description	Factory Default
Max. 24 characters	Enter the new password.	None

#### Confirm Password

Setting	Description	Factory Default
Max. 24 characters	Enter the new password again.	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.

**IP Setting**
Help

**IP Assignment:** Static ▼

IP Address   
Subnet Mask   
Gateway   
DNS1   
DNS2

Apply

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	The IP address of the secondary DNS Server used by	None

IP address	your network. The Switch will use the 2nd DNS Server if the 1st DNS Server fails to connect.	
------------	--	--

### 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.

#### IPv6 Setting

**Auto Configuration :** Disabled ▼

Address

Link Local Address

Apply

#### 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.

## Time Setting

Help

### System Clock

System Date/Time 

Set Clock From PC

Set System Date Time manually:

System Date (YYYY/MM/DD)

System Time (hh:mm:ss)

Apply

### SNTP/NTP Mode

SNTP/NTP Mode :

UTC Timezone

Server IP Address 1

Server IP Address 2

Server IP Address 3

Server IP Address 4

Server IP Address 5

### Daylight Saving Time

Daylight Saving Time :

Daylight Saving Period     ~

Daylight Saving Offset  (hours)

Apply



**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 <b>Set Clock from PC</b> .	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.	

Server (NTP)	The Weidmüller switch can synchronize other switches of the network with its programmed time clock.	Disabled
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

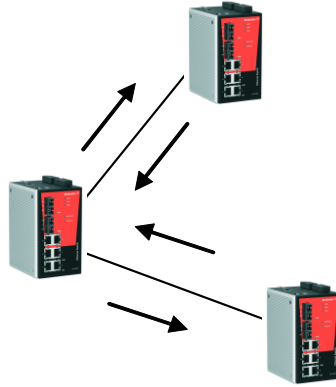
**Daylight Saving Offset**

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

**LLDP**
Help

**Mode :** Enabled ▾

**Tx Interval** 30 sec(s)

Apply

**Neighbor Info Table**

Port	System Name	MAC Address	IP Address
Port 02	IE-SW-AL06LM-4TX-2SC	00-15-7E-1D-00-35	<a href="#">192.168.50.70</a>
Port 05	IE-SW-AL24M-24TX	00-15-7E-1D-00-66	<a href="#">192.168.50.31</a>

## 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:

<b>Port</b>	The port number that connects to the neighbor device.
<b>System Name</b>	Hostname of the neighbor device.
<b>MAC Address</b>	The MAC address that identifies a neighbor device.
<b>IP Address</b>	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 DIP Switch



This option is available only in the IE-SW-AL05M-5TX model. It allows the user to enable or disable the settings of the 4 DIP switches located on the front of the switch housing.



If **Mode** is **Enabled** (and **Apply** is pressed), DIP switch SW1 defines the behavior of fault relay in terms of power failure and DIP switches SW2, SW3 and SW4 define the settings for O-Ring redundancy.



If **Mode** is **Disabled**, the settings of the front DIP switches SW1/2/3/4 have no function. The behavior of the fault relay and the settings of O-Ring redundancy mode have to be configured through the web interface (Menu Warnings and Redundancy, respectively).

#### Configuring alarm relay by external DIP switch

- SW 1 ON: Relay contact is closed if the device is powered-off. Relay contact is open if the device is powered by PWR1 and PWR2. Relay contact is closed if device is powered either by PWR1 or PWR2 (supplied by only 1 power input).
- SW 2 OFF: Relay does not have any power-related function.

#### Configuring O-Ring redundancy by external DIP switches

- SW 2 ON: Enables O-Ring redundancy function.
- SW 2 OFF: Disables O-Ring redundancy function.
- SW 3 ON: Sets device as Ring-master.
- SW 3 OFF: Device is not the Ring-master.
- SW 4 ON: Ports 1 and 2 are used as redundancy ports.
- SW 4 OFF: Ports 1 and 5 are used as redundancy ports.

If DIP Switch Mode is enabled the Web interface menu Redundancy->O-Ring is locked and can only be used for displaying O-Ring redundancy settings and the status.



By default **Mode** is **Disabled** so DIP switches SW1/2/3/4 located on the front of the switch housing have no function.

### 3.3.9 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

### Backup & Restore

Help

#### Restore Configuration

##### From TFTP Server

TFTP Server IP Address

Restore File Name

Restore

##### From Local PC

Seleccionar archivo

Restore

#### Backup Configuration

##### To TFTP Server

**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.

**3.3.10 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.

### 3.4.1 Port control

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

**Port Control**
Help

Port No.	State	Speed/Duplex	Flow Control
Port 01	Enabled ▾	AutoNegotiation ▾	Disabled ▾
Port 02	Enabled ▾	AutoNegotiation ▾	Disabled ▾
Port 03	Enabled ▾	AutoNegotiation ▾	Disabled ▾
Port 04	Enabled ▾	AutoNegotiation ▾	Disabled ▾
Port 05	Enabled ▾	AutoNegotiation ▾	Disabled ▾

Apply

#### 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
100M-Full	Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	
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.	

**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).

Port Status					
Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port 01	100TX	Down	Enabled	N/A	N/A
Port 02	100TX	UP	Enabled	100 Full	Disabled
Port 03	100TX	Down	Enabled	N/A	N/A
Port 04	100TX	Down	Enabled	N/A	N/A
Port 05	100TX	UP	Enabled	100 Full	Disabled

**Refresh**

**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	
	<b>Help</b>
Port No.	Port Alias
Port 01	<input type="text"/>
Port 02	<input type="text"/>
Port 03	<input type="text"/>
Port 04	<input type="text"/>
Port 05	<input type="text"/>

**Apply**

**Port alias**

Setting	Description	Factory Default
Max. 128 characters	Name of the port. Example: PLC 1	None

**3.4.4 Loop Guard**

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

**Loop Guard**
Help

Port No.	Active	Port State
Port 01	<input type="checkbox"/>	Enabled
Port 02	<input type="checkbox"/>	Enabled
Port 03	<input type="checkbox"/>	Enabled
Port 04	<input type="checkbox"/>	Enabled
Port 05	<input type="checkbox"/>	Enabled

Apply

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 industrial 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 a production line, 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), and STP (Spanning Tree Protocols) according to IEEE 802.1W/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 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
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.**

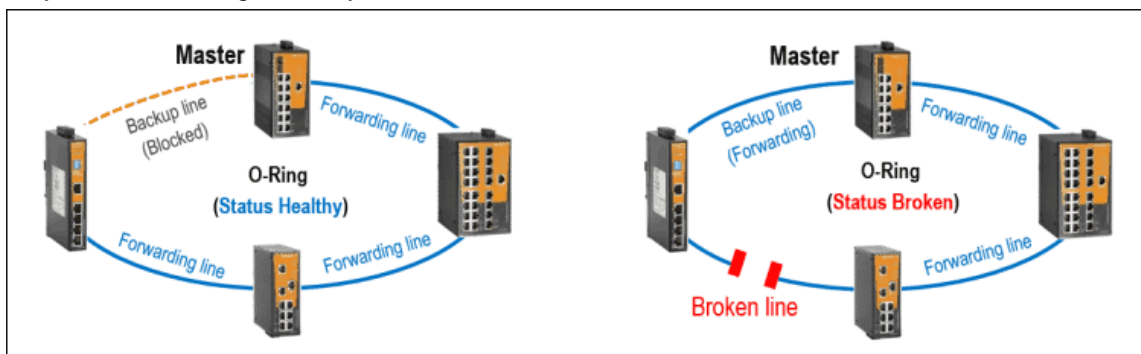
## 3.5.2 The O-Ring Concept

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.



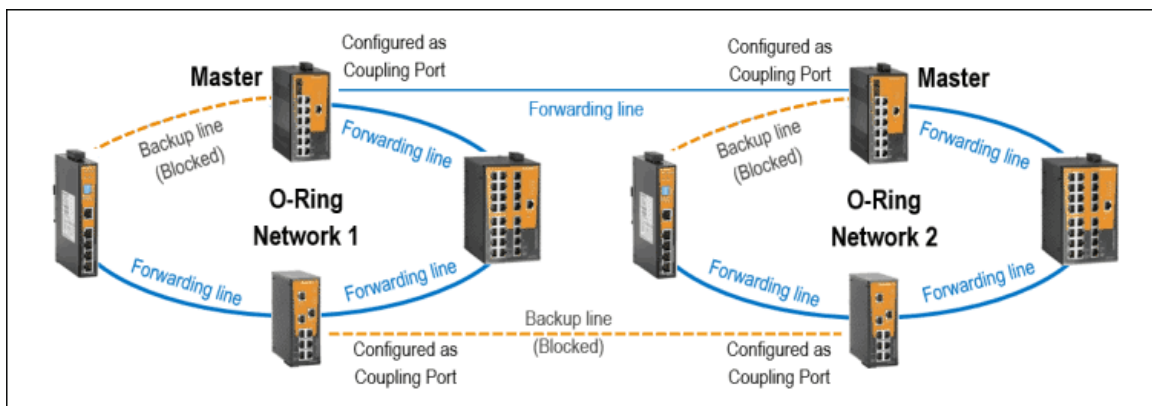
For failure detection the O-Ring protocol uses simultaneously two methods:

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.

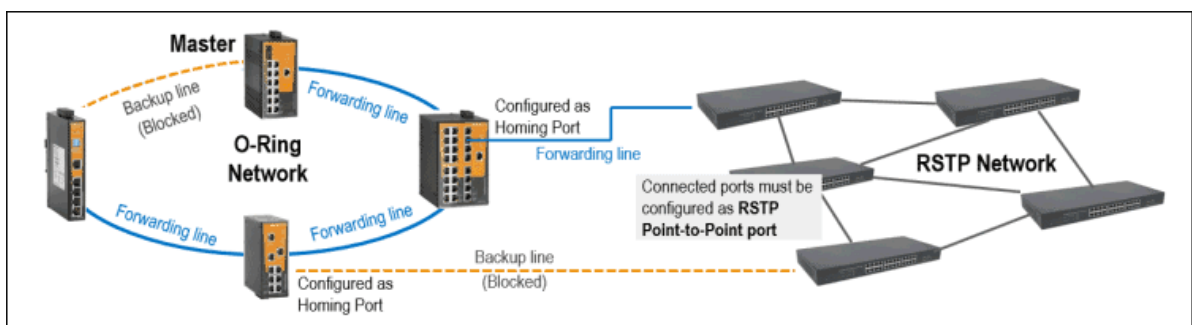
For failure detection of the coupling connection the same checking mechanisms are used as applied for the O-Ring protocol (Refer to section “*Topology setup for O-Ring*” above). Based on the used methods (Physical link change detection and/or Cyclic sending of control packets every 10ms) the coupling 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.



Redundancy	Settings	Status
Set as Ring Master	<input type="checkbox"/>	N/A
1st Ring Port	Port 01	Inactive
2nd Ring Port	Port 02	Inactive
Hello Time	10 (10~10,000ms)	
Max Age Count	2 (0~1000)	
Enable Ring Coupling	<input type="checkbox"/>	
Coupling Port	Port 03	Inactive
Enable Dual Homing	<input type="checkbox"/>	
Homing Port	Port 04	Inactive

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 2 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 1 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 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**

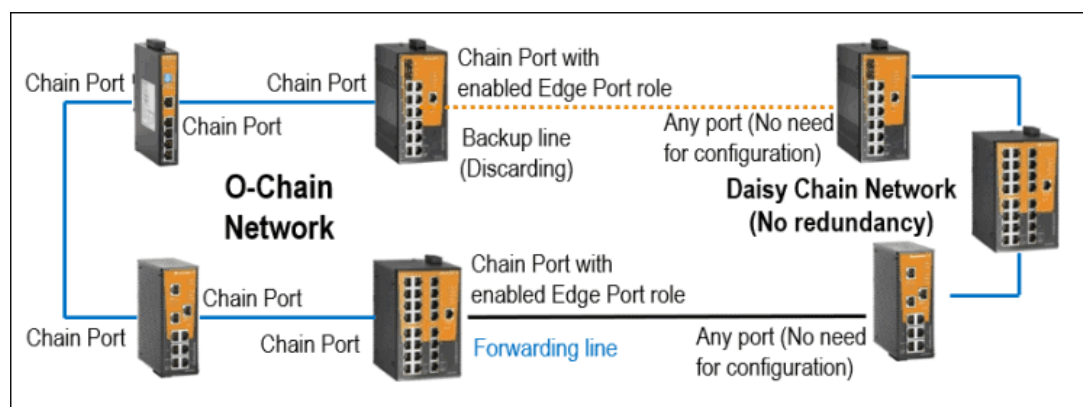
Setting	Description	Factory Default
Homing Port	Select any port of the Switch to be the homing port.	Port 04
Status	Description	Factory Default
Inactive	Dual Homing is disabled.	Inactive
Link down	No connection in this port.	
Forwarding	Normal transmission in this port.	
Blocked	The port is connected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

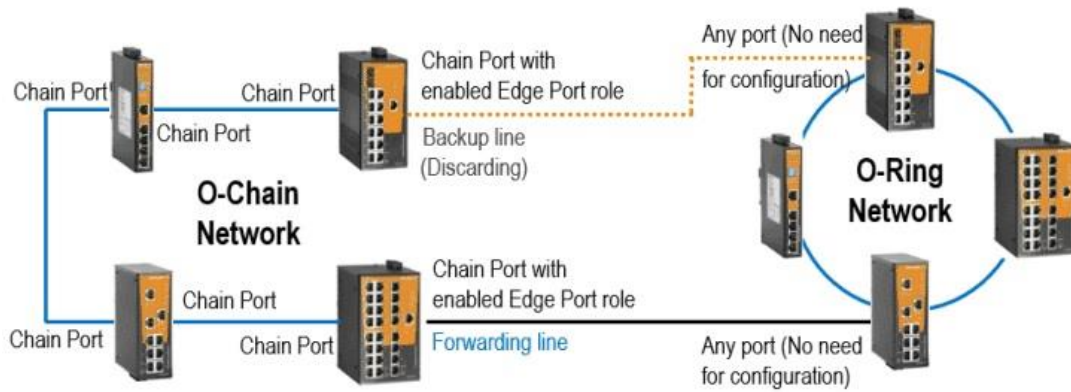
**3.5.4 The O-Chain Concept**

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.

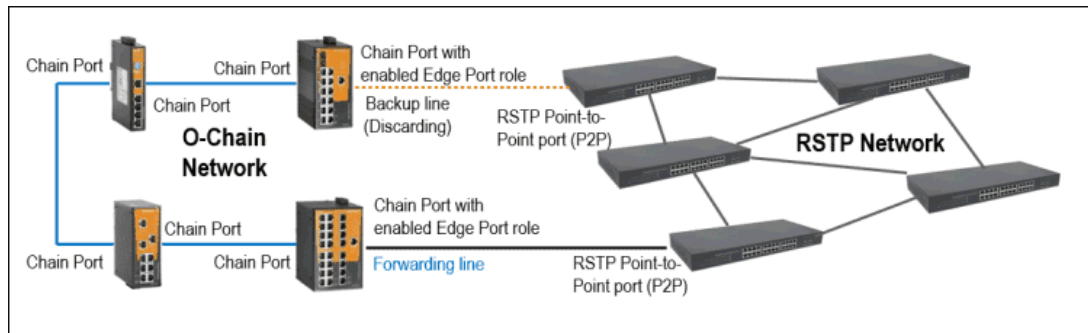
**Recovery time for O-Chain connected to Daisy Chain of Weidmüller's Substation/Advanced Line switches OR to an O-Ring network of Substation/Advanced Line switches**





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 3<sup>rd</sup> party network

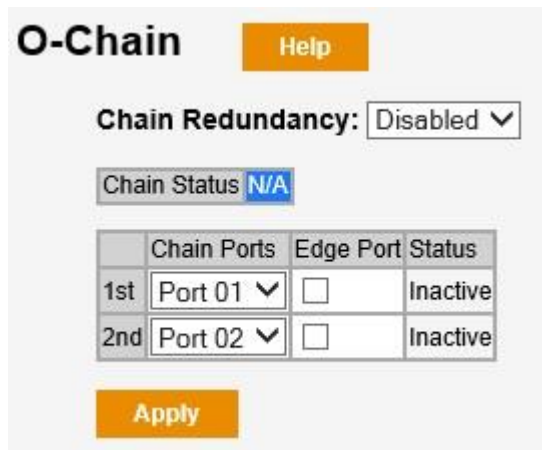
For connections to unmanaged switches, to a non-redundant daisy chain network or to a redundant proprietary 3<sup>rd</sup> party network the overall network topology recreation time depends worst case on the remaining MAC address aging time of the 3<sup>rd</sup> party switches (when the chain becomes 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 3<sup>rd</sup> party network devices to O-Chain connected devices, do not longer work until the MAC address tables of the 3<sup>rd</sup> 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.



**O-Chain** Help

**Chain Redundancy:** Disabled ▼

Chain Status N/A

	Chain Ports	Edge Port	Status
1st	Port 01 ▼	<input type="checkbox"/>	Inactive
2nd	Port 02 ▼	<input type="checkbox"/>	Inactive

Apply

### 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 <b>one port</b> 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.

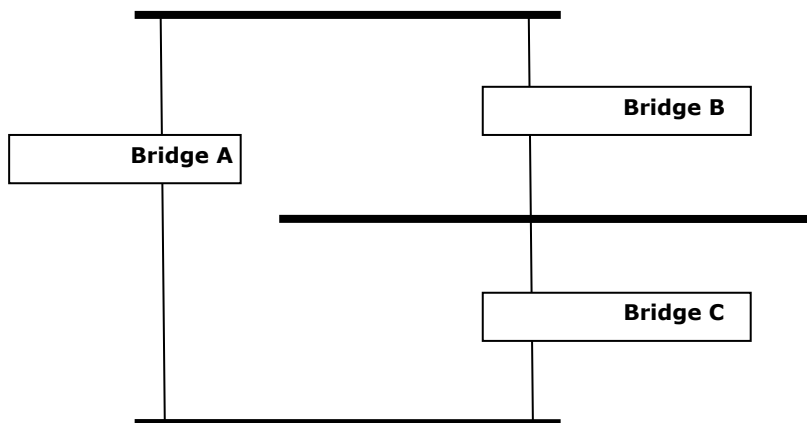


**NOTE:** The STP protocol is part of the IEEE Std 802.1D, 2004 Edition bridge specification. The following explanation uses “bridge” instead of “switch.”

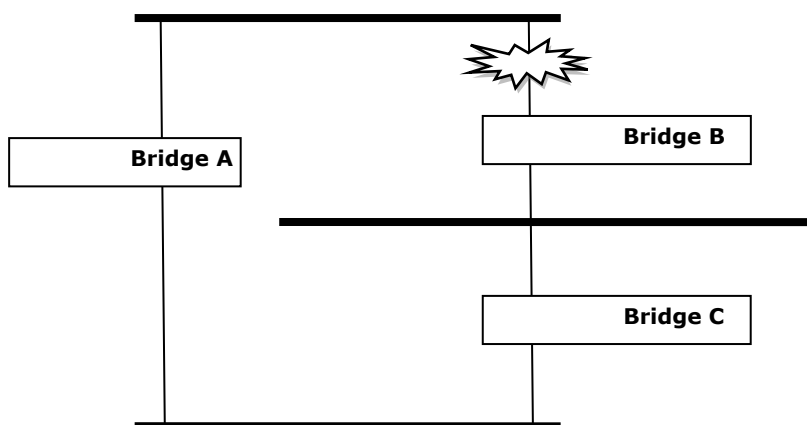
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- 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.

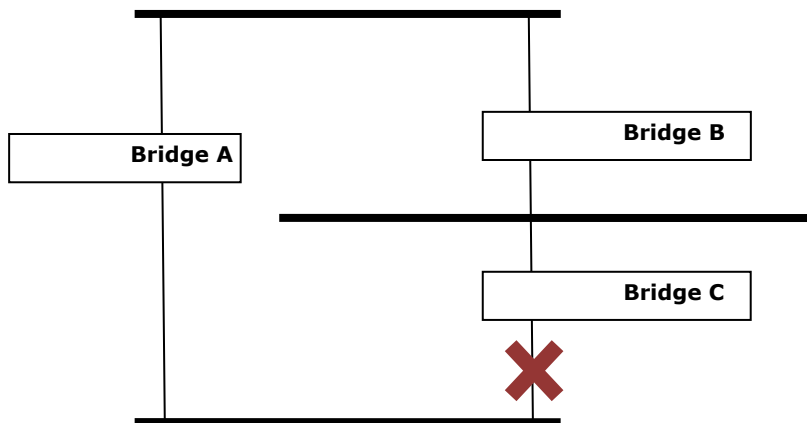
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



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.

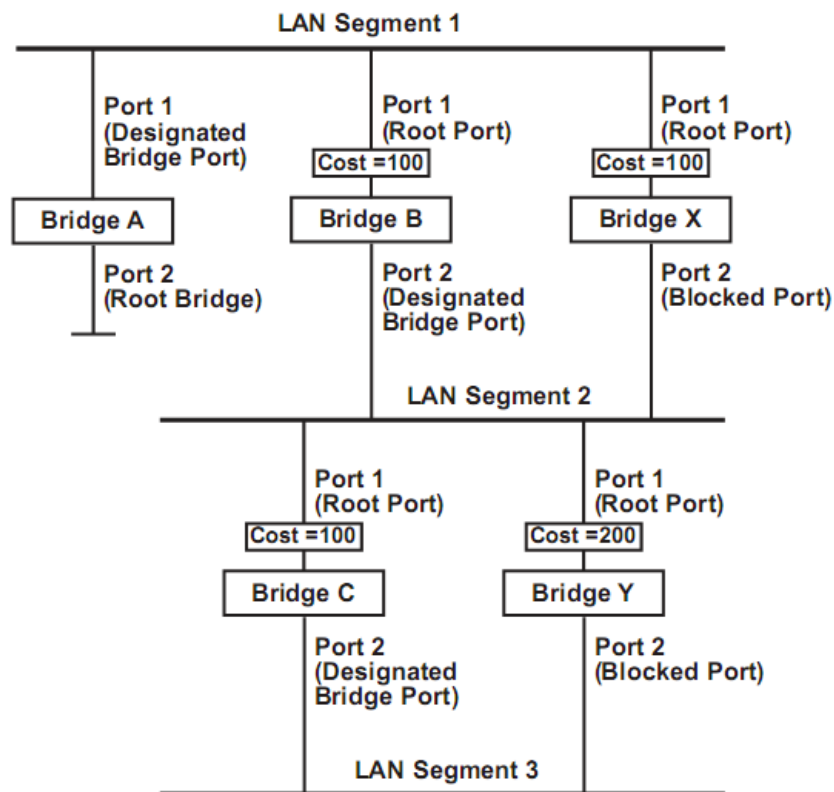
## Differences between STP and RSTP

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.

**Setting**
Help

**RSTP Mode :** Disabled ▾

**Bridge Setting**

Priority (0-61440) 32768

Max Age Time (6-40 secs) 20

Hello Time (1-10 secs) 2

Forward Delay Time (4-30 secs) 15

**Port Setting**

Port No.	Enable	Path Cost (0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port 01	<span>enabled ▾</span>	0	128	<span>auto ▾</span>	<span>true ▾</span>
Port 02	<span>enabled ▾</span>	0	128	<span>auto ▾</span>	<span>true ▾</span>
Port 03	<span>enabled ▾</span>	0	128	<span>auto ▾</span>	<span>true ▾</span>
Port 04	<span>enabled ▾</span>	0	128	<span>auto ▾</span>	<span>true ▾</span>
Port 05	<span>enabled ▾</span>	0	128	<span>auto ▾</span>	<span>true ▾</span>

## 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.

### Information

#### Root Bridge Information

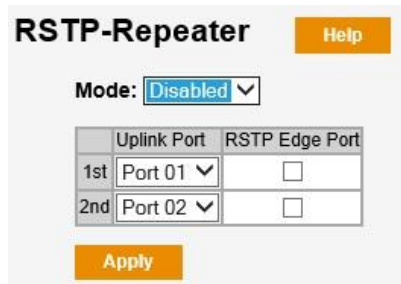
Root Bridge ID	N/A
Root Priority	N/A
Root Port	N/A
Root Path Cost	N/A
Max Age Time	N/A
Hello Time	N/A
Forward Delay Time	N/A

#### Port Information

Port	Enabled	Port Priority	Path Cost	OperEdge	OperP2P	Role	State
------	---------	---------------	-----------	----------	---------	------	-------

### 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.



**RSTP-Repeater** Help

Mode: Disabled ▼

	Uplink Port	RSTP Edge Port
1st	<span>Port 01</span> ▼	<input type="checkbox"/>
2nd	<span>Port 02</span> ▼	<input type="checkbox"/>

Apply

#### 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 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.



**Fast Recovery** Help

Mode: Disabled ▼

Port No.	Recovery Priority
Port 01	<span>Not included</span> ▼
Port 02	<span>Not included</span> ▼
Port 03	<span>Not included</span> ▼
Port 04	<span>Not included</span> ▼
Port 05	<span>Not included</span> ▼

Apply

#### 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 total number of ports	Select the priority (number from 1 to total number of ports) 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 Virtual LAN

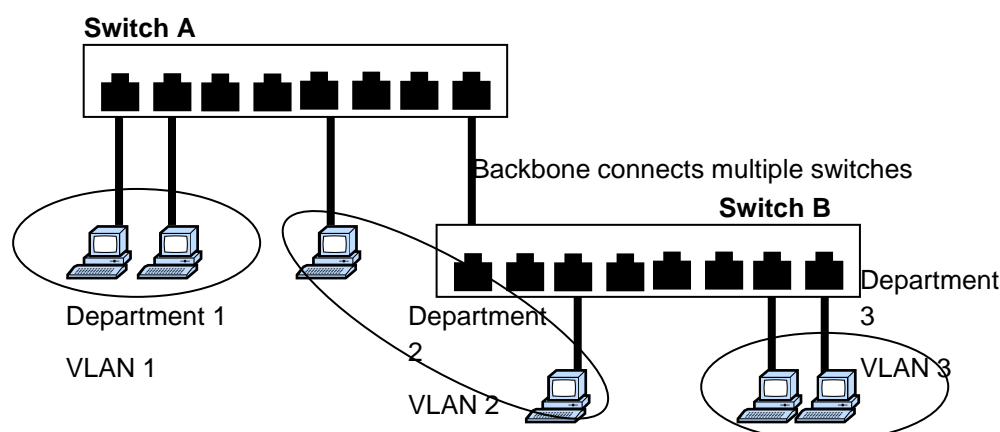
Setting up Virtual LANs (VLANs) on your Weidmüller switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

### 3.6.1 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

Lite Advanced Line switches support port-based VLANs, what means that the user can define a single VLAN for each available port on the switch.

### 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.

### 3.6.2 Configuring port-based Virtual LAN

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-Based VLAN**

VLAN	Port				
	1	2	3	4	5
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Apply**

#### Port

Setting	Description	Factory Default
Enable/Disable	Set port to specific VLAN Group by activating checkbox.	Enable  (all ports belong to VLAN1)

## 3.7 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.	

### 3.7.1 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.

### DHCP Server/Relay Help

**DHCP Mode :** DHCP Server ▾

Start IP Address 192.168.1.120

End IP Address 192.168.1.200

Subnet Mask 255.255.255.0

Gateway 0.0.0.0

DNS 0.0.0.0

Lease Time (Hour) 168

Port No.	Active
Port 01	<input checked="" type="checkbox"/>
Port 02	<input checked="" type="checkbox"/>
Port 03	<input checked="" type="checkbox"/>
Port 04	<input checked="" type="checkbox"/>
Port 05	<input checked="" type="checkbox"/>

**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



### 3.7.2 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/Relay**
Help

**DHCP Mode :**
DHCP Relay

**DHCP Server IP Address**

1st Server IP  VID   
2nd Server IP  VID   
3rd Server IP  VID   
4th Server IP  VID

**DHCP Option 82 Remote ID**

Type IP  
Value   
Display

**DHCP Option 82 Circuit-ID Table**

### 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

### 3.7.3 Client List

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

**Client List**
Help

IP Address	MAC Address	Type	Status	Lease
------------	-------------	------	--------	-------

### 3.7.4 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.

**Port and IP Binding**
Help

Port No.	IP Address
Port 01	<input type="text" value="0.0.0.0"/>
Port 02	<input type="text" value="0.0.0.0"/>
Port 03	<input type="text" value="0.0.0.0"/>
Port 04	<input type="text" value="0.0.0.0"/>
Port 05	<input type="text" value="0.0.0.0"/>

Apply

Note: Port-related IP address assignment for DHCP clients only will be active if mode DHCP Server is selected.



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

## 3.8 SNMP

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

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

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

These parameters are configured on the SNMP page. A more detailed explanation of each parameter is given below the figure.



### 3.8.1 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.

**SNMPv3 Setting**
Help

SNMP Agent Version : SNMP v3

**Context Table**

Context Name

Apply

**User Profile**

default\_user Auth:NoAuth Priv:NoPriv

User ID

Authentication
☒ NoAuth
☐ MD5
☐ SHA1

Password

Privacy
☒ NoPriv
☐ DES
☐ AES128

Password

Add Remove

**Group Table**

default\_user Group:default\_group

Security Name (User ID)

Group Name

Add Remove

**Access Table**

default\_group NoAuthNoPriv (empty) Exa

Group Name

☒ NoAuthNoPriv.
☐ AuthNoPriv.
☐ AuthPriv.

Security Level

**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.

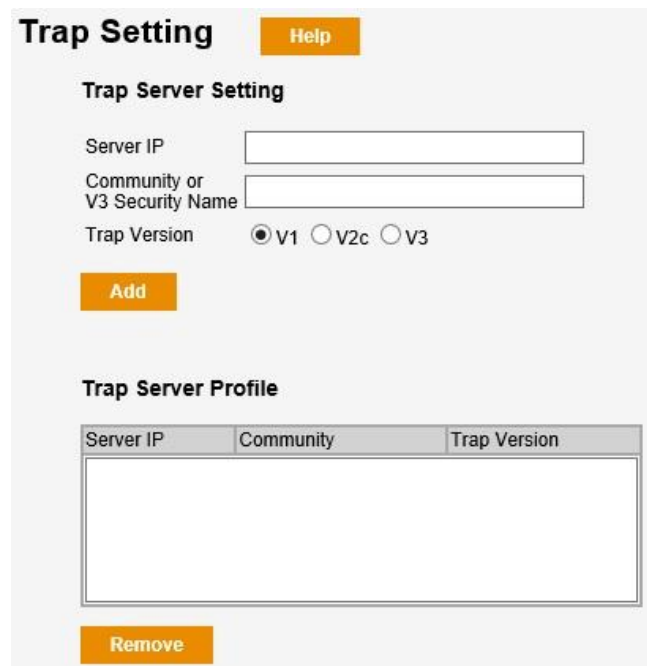


**NOTE:** At the end of this programming page is shown the Private MIB Information of the switch as well as the Engine ID (if SNMP V3 is used).



## 3.8.2 Trap Settings

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



**Trap Setting** [Help](#)

**Trap Server Setting**

Server IP

Community or V3 Security Name

Trap Version ☒ V1 ☐ V2c ☐ V3

[Add](#)

**Trap Server Profile**

Server IP	Community	Trap Version

[Remove](#)

### 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.

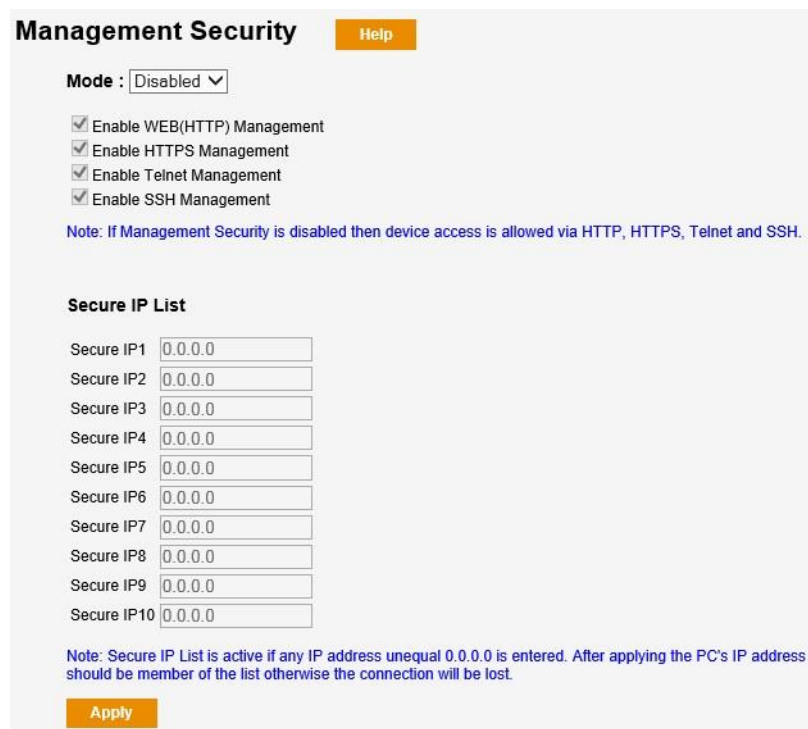
All the configured trap servers are shown in the table **Trap Server Profile** of the web page.

## 3.9 Security

Weidmüller Lite 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.

### 3.9.1 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.

## 3.9.2 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.

**TACACS+**
Help

**Server Configuration**

Enable	Server IP Address	Port	Secret Key
<input type="checkbox"/>	0.0.0.0	49	
<input type="checkbox"/>	0.0.0.0	49	
<input type="checkbox"/>	0.0.0.0	49	
<input type="checkbox"/>	0.0.0.0	49	
<input type="checkbox"/>	0.0.0.0	49	

**Client Configuration**

Client	Authentication Method
Console	Local <span>▼</span>
Telnet	Local <span>▼</span>
Web	Local <span>▼</span>

Apply

**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 verification.	None

**Client Configuration**

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

## 3.10 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.

### 3.10.1 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

**Fault Relay Alarm**
Help

**Power Failure**
  
☐ PWR 1    ☐ PWR 2

**Port Link Down/Broken**
  
☐ Port 01    ☐ Port 02    ☐ Port 03    ☐ Port 04

☐ Port 05

Apply

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).

## 3.10.2 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.

#### 3.10.2.1 Event Selection

**Event Selection**
Help

**System Event**

Event	SYSLOG	SMTP
System Restart	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Power Status	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SNMP Authentication Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>
O-Ring Topology Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>
O-Chain Topology Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Configuration Changed and Saved	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Port Event**

Port No.	SYSLOG	SMTP
Port 01	Disable ▾	Disable ▾
Port 02	Disable ▾	Disable ▾
Port 03	Disable ▾	Disable ▾
Port 04	Disable ▾	Disable ▾
Port 05	Disable ▾	Disable ▾

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.

### 3.10.2.2 Email Settings

**SMTP Setting**
Help

**Mode :** Disabled ▼

SMTP Server Address

Sender E-mail Address

Mail Subject

☒ Authentication
 

Username

Password

Confirm Password

Recipient E-mail Address 1

Recipient E-mail Address 2

Recipient E-mail Address 3

Recipient E-mail Address 4

Recipient E-mail Address 5

Recipient E-mail Address 6

Apply

**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

**3.10.3 SYSLOG Setting**

**SYSLOG Setting**
Help

Mode :

Server IP Address :

Apply

**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**

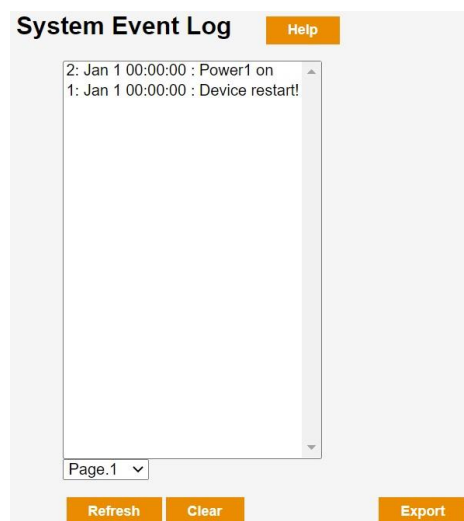
Setting	Description	Factory Default
IP address	The IP address of Syslog Server used by your network.	0.0.0.0

## 3.11 Monitoring/Diagnosis

You can check the log register of the Weidmüller switch as well as troubleshoot network problems with the Ping function.

### 3.11.1 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:

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



The user can press any or the following buttons:

<b>Refresh</b>	Reload the page to get the latest events.
<b>Clear</b>	Delete all the events stored in the switch.
<b>Export</b>	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.

### 3.11.2 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**.



### 3.12 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.

## 3.13 Factory Default

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

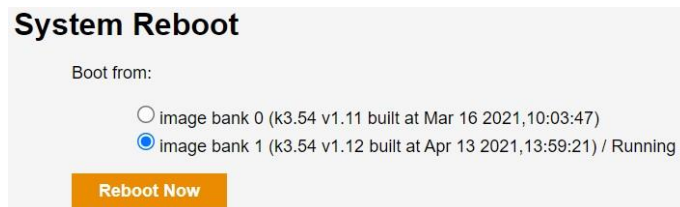


The screenshot shows a web interface titled "Factory Default" with a "Help" button. Below the title, there are two checked checkboxes: "Keep current IP address setting?" and "Keep current username & password?". At the bottom, there is a "Reset" button.

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

## 3.14 System Reboot

This function is used to restart the Ethernet Switch.

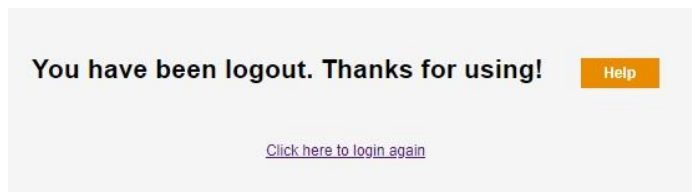


The screenshot shows a web interface titled "System Reboot". Under the heading "Boot from:", there are two radio button options. The first option is "image bank 0 (k3.54 v1.11 built at Mar 16 2021,10:03:47)". The second option is "image bank 1 (k3.54 v1.12 built at Apr 13 2021,13:59:21) / Running", which is selected. At the bottom, there is a "Reboot Now" button.

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.

## 3.15 Logout

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



The screenshot shows a web interface with the message "You have been logout. Thanks for using!". There is a "Help" button. Below the message, there is a link that says "Click here to login again".

## 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 „Advanced 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)
<b>System Information</b>					
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	
<b>Port Information</b>					
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 1 <sup>st</sup> 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 1 <sup>st</sup> Port Status	0x3701	14081	Word	1	0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding

					0xFFFF: Not Enabled
O-Chain 2 <sup>nd</sup> Port Status	0x3702	14082	Word	1	0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding 0xFFFF: Not Enabled