

Industrial Full Gigabit Ethernet Switch

User Manual IE-SW-PL09M-4GC-5GT

First Edition, January 2011
1243240000/00/01.11

Weidmüller 

© 2011 Weidmueller Interface. All rights reserved.
Reproduction without permission is prohibited.

Industrial Full Gigabit Ethernet Switch User Manual IE-SW-PL09M-5GC-4GT

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 © 2011 Weidmueller
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 Weidmueller.

Weidmueller provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Weidmueller 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, Weidmueller 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
Postbox 3030
32760 Detmold
Klingenbergstraße 16
32758 Detmold
Germany

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

Table of Contents

| | |
|---|-----|
| Overview | 5 |
| Features | 5 |
| Industrial Networking Capability..... | 5 |
| Designed for Industrial Applications..... | 5 |
| Useful Utility and Remote Configuration..... | 6 |
| RS-232 Console Configuration (115200, None, 8, 1, VT100)..... | 8 |
| Configuration using a Telnet Console | 10 |
| Configuration using a Web Browser..... | 12 |
| Disabling Telnet and Browser Access | 14 |
| Configuring Basic Settings | 16 |
| Using Port Trunking..... | 32 |
| Configuring SNMP..... | 35 |
| Using Communication Redundancy..... | 39 |
| The Turbo Ring Concept..... | 41 |
| Configuring “Turbo Ring” and “Turbo Ring V2”..... | 45 |
| The Turbo Chain Concept..... | 49 |
| Configuring “Turbo Chain” | 50 |
| Using Traffic Prioritization..... | 60 |
| The Traffic Prioritization Concept..... | 60 |
| Configuring Traffic Prioritization..... | 63 |
| Using Virtual LAN | 65 |
| The Virtual LAN (VLAN) Concept | 65 |
| Sample Applications of VLANs using Weidmüller IE-SW-PL09M-GB..... | 68 |
| Configuring Virtual LAN | 69 |
| Using Multicast Filtering..... | 71 |
| The Concept of Multicast Filtering | 72 |
| Configuring IGMP Snooping | 75 |
| Using Bandwidth Management | 78 |
| Using Port Access Control | 79 |
| Using Auto Warning..... | 84 |
| Configuring Email Warning | 84 |
| Configuring Relay Warning..... | 87 |
| Using Line-Swap-Fast-Recovery | 89 |
| Using Set Device IP | 90 |
| Using Diagnosis | 93 |
| Using Monitor | 96 |
| Using the MAC Address Table..... | 97 |
| Using Event Log..... | 98 |
| Using Syslog | 99 |
| Using HTTPS/SSL..... | 100 |
| Starting Weidmüller SWITCH Configuration Utility..... | 103 |
| Broadcast Search..... | 103 |
| Search by IP address | 104 |
| Upgrade Firmware..... | 105 |
| Modify IP Address | 106 |
| Export Configuration..... | 106 |
| Import Configuration..... | 107 |
| Unlock the Ethernet Switch | 109 |
| Modbus information v1.0..... | 114 |

Welcome to the Weidmueller IE-SW-PL09M-5GC-4GT Full Gigabit Ethernet Switch. This Managed Redundant Ethernet Switch is designed specially for connecting Ethernet-enabled devices in industrial field applications with high network performance requirements.

The following topics are covered in this chapter:

Overview

Package Checklist

Features

- Industrial Networking Capability
- Designed for Industrial Applications
- Useful Utility and Remote Configuration

Overview

As the world's network and information technology becomes more mature, the trend is to use Ethernet as the major communications interface in many industrial communications and automation applications. In fact, a whole new industry has sprung up to provide Ethernet products that comply with the requirements of demanding industrial applications.

The IE-SW-PL09M-GB Switch is equipped with 9 Gigabit Ethernet ports and up to 5 combo (10/100/1000BaseTX) or 100/1000BaseSFP slot) Gigabit ports, making it ideal for upgrading an existing network to Gigabit speeds or building a new Gigabit backbone. Gigabit transmission increases bandwidth for higher performance and transfers large amounts of video, voice, and data across a network quickly.

This Ethernet Switch has passed a 100% burn-in test to ensure that they fulfill the special needs of industrial automation control.

Package Checklist

The IE-SW-PL09M-GB is shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative for assistance.

- 1 Ethernet Switch IE-SW-PL09M-5GC-4GT
- Hardware Installation Guide
- CD-ROM with User's Manual and Windows Utility
- RJ45 to DB9 console port cable
- Protective caps for unused ports

Features

Industrial Networking Capability

- Gigabit Ethernet Turbo Ring, Turbo Chain (<20ms recovery time at full load) and STP/RSTP (IEEE 802.1w/D)
- IPv6 ready (IPv6 Logo Committee certified)
- IEEE 1588 PTP (Precision Time Protocol) for precise time synchronization of networks
- DHCP Option 82 for IP address assignment for different policies.
- Supports Modbus TCP
- Supports LLDP (Link Layer Discovery Protocol)

Designed for Industrial Applications

- Bandwidth management prevents unpredictable network status
- Support ABC-01 (Automatic Backup Configurator) for system configuration backup
- Long-haul transmission distance up to 80 km (with optional mini-GBIC)
- Redundant, dual 12 to 48 VDC power inputs
- IP30, rugged high-strength metal case
- DIN-Rail or panel mounting ability
- Bandwidth management to prevent unpredictable network status
- Lock port for allowing access to authorized MAC addresses only
- Port mirroring for online debugging
- Automatic warning by exception through email, relay output

- Digital inputs to integrate a sensor and alarm with an IP network
- Automatic recovery of connected device IP addresses
- Line-swap fast recovery

Useful Utility and Remote Configuration

- Configurable using a Web browser, Telnet/Serial console, or Windows utility
- Send ping commands to identify network segment integrity

2

Getting Started

This chapter explains how to access the IE-SW-PL09M-GB for the first time. There are three ways to access the switch: serial console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect the IE-SW-PL09M-GB to a PC's COM port, can be used if you do not know the switch's IP address. The Telnet console and web browser connection methods can be used to access the switch over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

RS-232 Console Configuration (115200, None, 8, 1, VT100)

Configuration using a Telnet Console

Configuration using a Web Browser

Disabling Telnet and Browser Access

RS-232 Console Configuration (115200, None, 8, 1, VT100)

NOTE

Connection Caution!

1. You **cannot** connect to the IE-SW-PL09M-GB simultaneously by serial console and Telnet.
2. You **can** connect to the IE-SW-PL09M-GB simultaneously by web browser and serial console, or by web browser and Telnet. However, we strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your IE-SW-PL09M-GB.

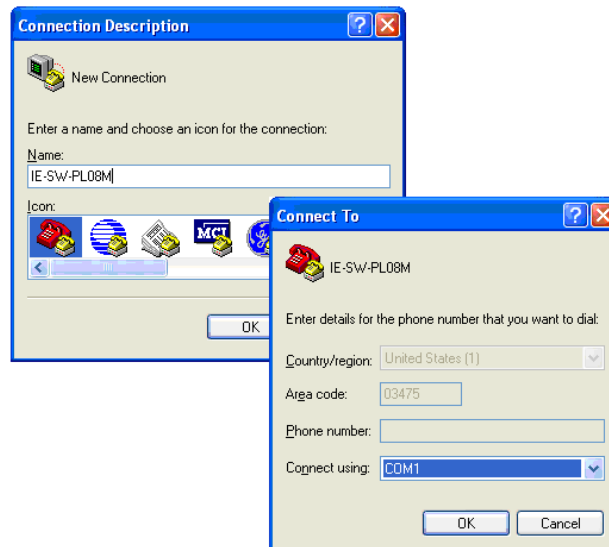
NOTE

We recommend using Hyper Terminal, which is part of Windows operation system..

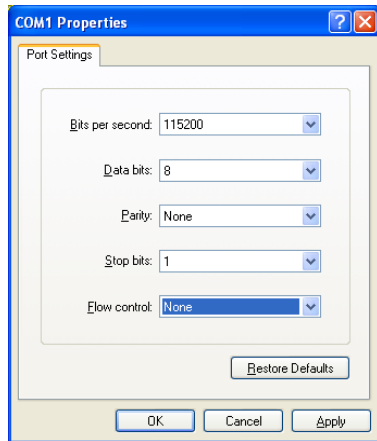
Before running Hyper Terminal Program, uses an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the Ethernet Switch's RS-232 Console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

After starting Hyper Terminal Program, perform the following steps to access the RS-232 Console utility.

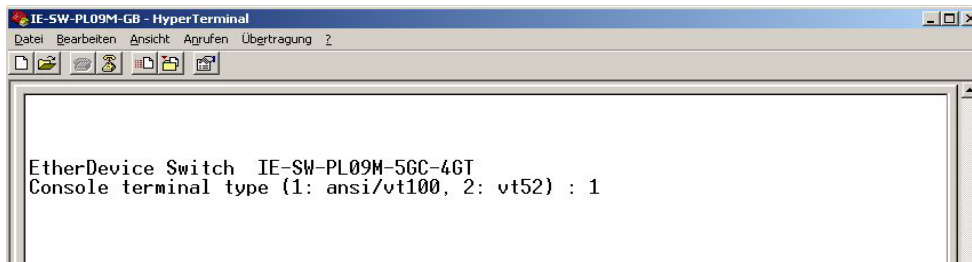
1. From the Windows desktop, click **Start → Programs → Accessories → Communications → Hyper Terminal**.
2. Start Hyper Terminal and enter a name of your choice for the new connection. Select the appropriate COM port for console connection in the "New Connection" window.



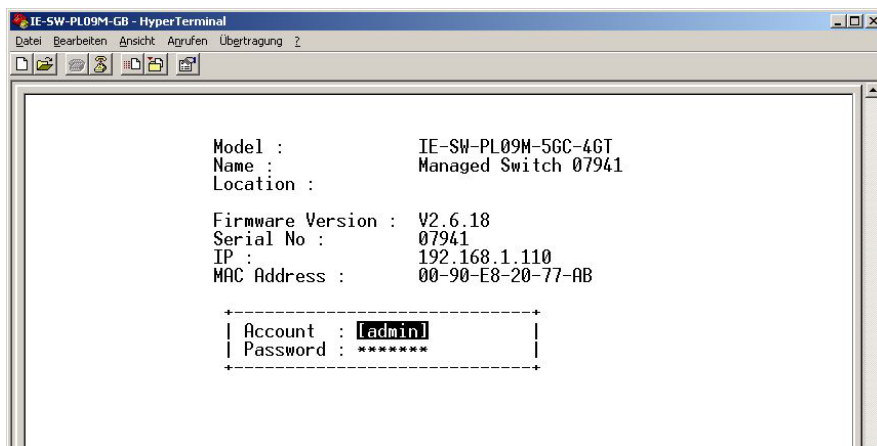
3. The Communication Parameter for console connection are: 115200 for Baud Rate, 8 for Data Bits, None for Parity, 1 for Stop Bits, and None for Flow control. Click OK to continue.

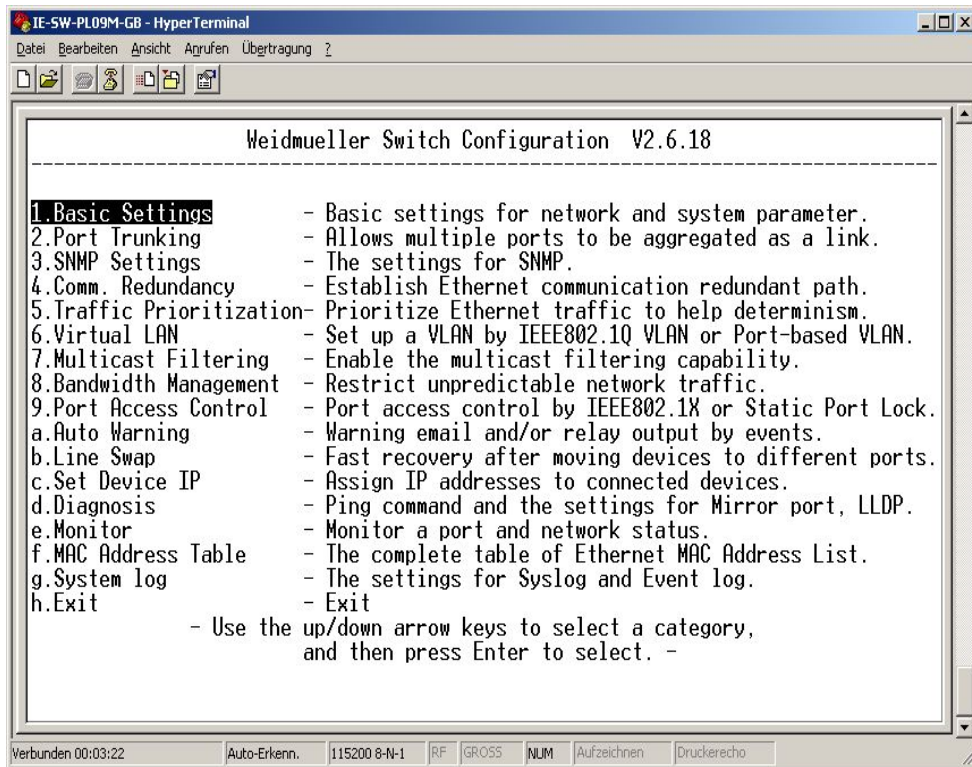


- 4. Type **1** to select **ansi/VT100** terminal type, and then press **Enter**
- 5. The Console login screen will appear. Press **Enter** to open the Account pop-up selector and then select either **admin** or **user**. Use the keyboard's down arrow to move the cursor to the Password field, enter the default **Console Password "Detmold"** (this is the same as the Web Browser password; leave the **Password** field blank if a console password has not been set), and then press **Enter**.



- 6. The IE-SW-PL09M-GB **Main Menu** will be displayed. (NOTE: To modify the appearance of the Hyper Terminal window, select **Font...** under the **Edit** menu, and then choose the desired formatting options.)





7. After entering the **Main Menu**, use the following keys to move the cursor, and to select options.

| Key | Function |
|-----------------------------------|--------------------------|
| Up/Down/Left/Right arrows, or Tab | Move the onscreen cursor |
| Enter | Display & select options |
| Space | Toggle options |
| Esc | Previous Menu |

Configuration using a Telnet Console

You may use Telnet to access the console utility over a network. To be able to access the switch's functions over the network (by Telnet or web browser) from a PC host that is connected to the same LAN as the IE-SW-PL09M-GB, you need to make sure that the PC host and the Ethernet Switch are on the same logical subnet. To do this, check your PC host's IP address and subnet mask. By default, the IP address is 192.168.1.110 and the subnet mask is 255.255.255.0 (for a Class C network). If you do not change these values, and your PC host's subnet mask is 255.255.0.0, then its IP address must have the form 192.168.xxx.xxx. On the other hand, if your PC host's subnet mask is 255.255.255.0, then its IP address must have the form 192.168.1.xxx.

NOTE To use the management and monitoring functions from a PC host connected to the same LAN as the IE-SW-PL09M-GB, you must make sure that the PC host and the

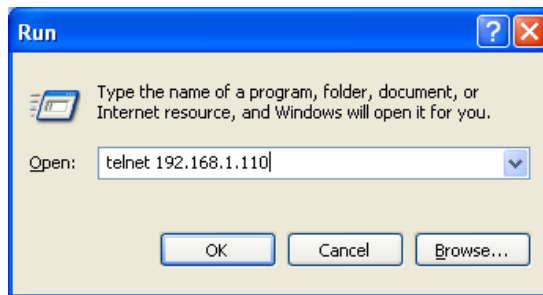
Ethernet Switch are connected to the same logical subnet.

NOTE Before accessing the console utility via Telnet, first connect one of the IE-SW-PL09M-GB's RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can use either a straight-through or cross-over Ethernet cable.

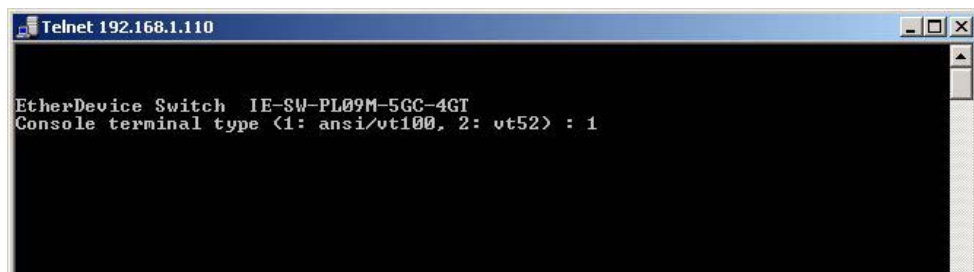
NOTE The IE-SW-PL09M-GB's default IP address is **192.168.1.110**.

Perform the following steps to access the console utility via Telnet.

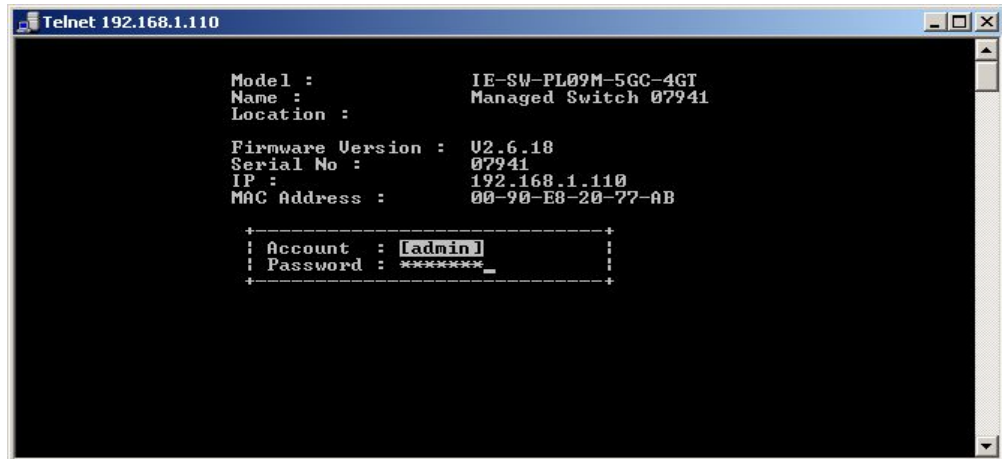
1. Click **Start** → **Run**, and then telnet to the IE-SW-PL09M-GB's IP address from the Windows **Run** window. (You may also issue the telnet command from the MS-DOS prompt.)



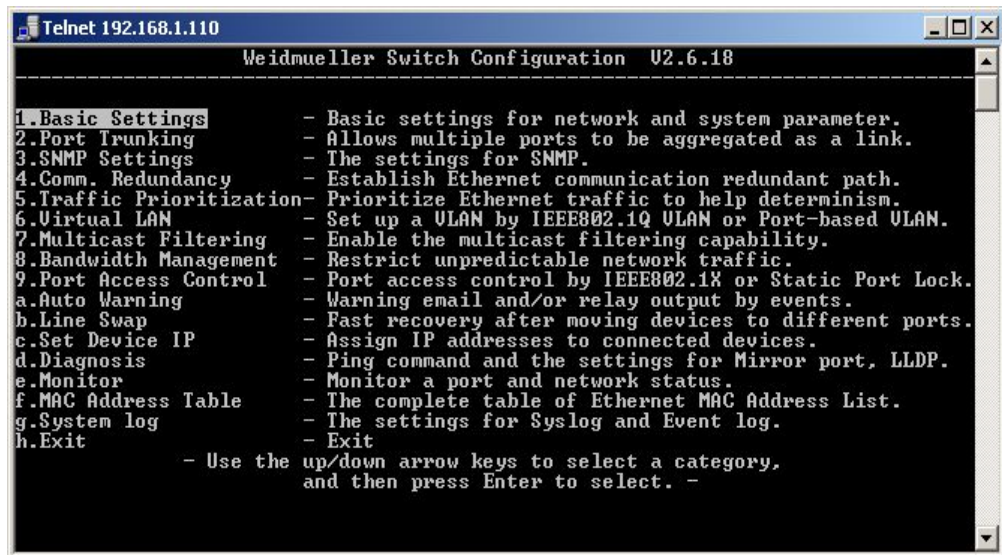
2. Press **OK**.



3. The Console login screen will appear. Press **Enter** to open the Account pop-up selector and then select either **admin** or **user**. Use the keyboard's down arrow to move the cursor to the Password field, enter the **Console Password** (this is the same as the Web Browser password; edit the **Password** default is "Detmold"), and then press **Enter**.



4. When the **Main Menu** of the IE-SW-PL09M-GB's console utility opens, click Enter.
5. Now the Switch's Main Menu is displayed.



NOTE The Telnet Console looks and operates in precisely the same manner as the RS-232 Console.

Configuration using a Web Browser

The 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 5.5 or higher with JVM (Java Virtual Machine) installed, also Mozilla Firefox is usable.

NOTE To use the management and monitoring functions from a PC host connected to the same LAN as the IE-SW-PL09M-GB, you must make sure that the PC host and the IE-SW-PL09M-GB are on the same logical subnet.

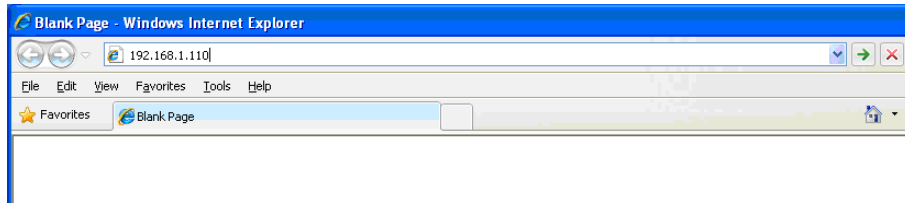
NOTE If the IE-SW-PL09M-GB is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

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

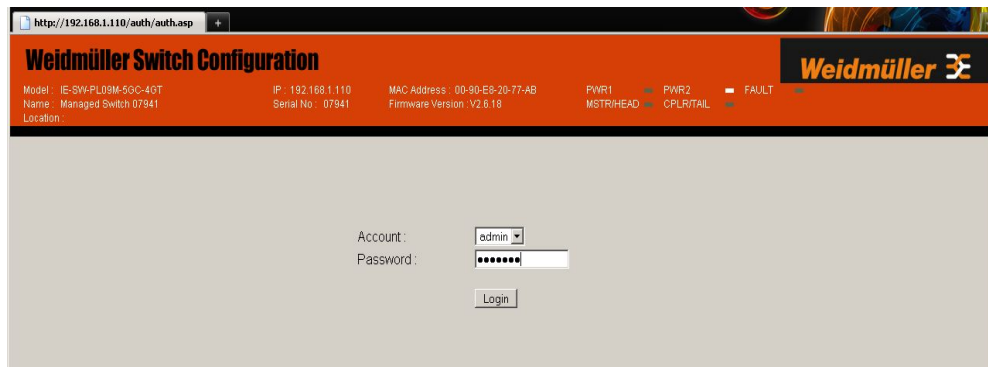
NOTE The IE-SW-PL09M-GB's default IP is **192.168.1.110**.

Perform the following steps to access the IE-SW-PL09M-GB's web browser interface.

1. Open Internet Explorer and type IE-SW-PL09M-GB's IP address in the **Address** field. Press **Enter** to establish the connection.

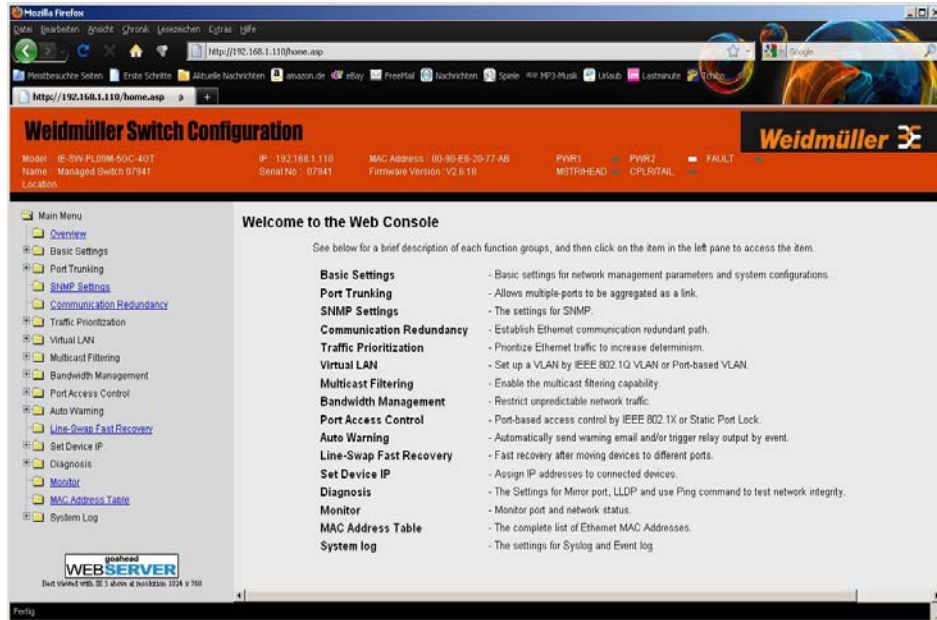


2. The web login page will open. Select the login account (Admin or User) and enter the **Password** (this is the same as the Console password), and then click **Login** to continue. Leave the **Password** field blank if a password has not been set.



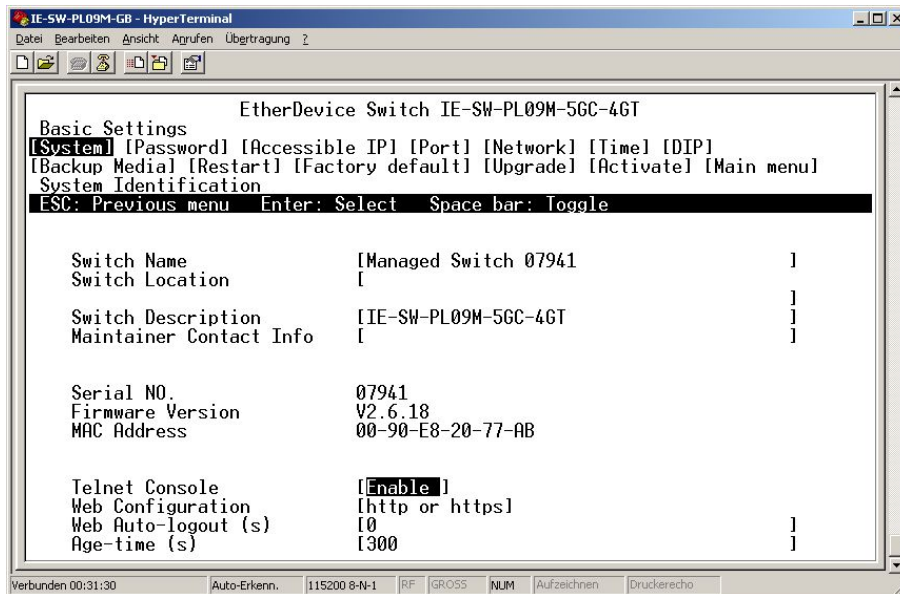
NOTE By default, the IE-SW-PL09M-GB's password is **Detmold**.

- You may need to wait a few moments for the web page to be downloaded to your computer. Use the menu tree on the left side of the window to open the function pages to access each of the switch's functions.



Disabling Telnet and Browser Access

If you are connecting the IE-SW-PL09M-GB to a public network, but do not intend to use its management functions over the network, we suggest using the RS-232 console's **Basic Settings** → **System Info** page to disable both **Telnet Console** and **Web Configuration**, as shown in the following figure.



3

Featured Functions

In this chapter, we explain how to access the IE-SW-PL09M-GB's configuration options, perform monitoring, and use administration functions. There are three ways to access these functions: RS-232 console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect the IE-SW-PL09M-GB to a PC's COM port, can be used if you do not know the IP address of the Ethernet Switch. The Telnet console and web browser connection methods can be used to access the IE-SW-PL09M-GB over an Ethernet LAN, or over the Internet.

The web console is the most user-friendly way to configure the IE-SW-PL09M-GB. In this chapter, we use the web console interface to introduce the functions. There are only a few differences between the web console, serial console, and Telnet console.

The following topics are covered in this chapter:

- Configuring Basic Settings
- Using Port Trunking
- Configuring SNMP
- Using Communication Redundancy
- Using Traffic Prioritization
- Using Virtual LAN
- Using Multicast Filtering
- Using Bandwidth Management
- Using Port Access Control
- Using Auto Warning
- Using Line-Swap-Fast-Recovery
- Using Set Device IP
- Using Diagnosis
- Using Monitor
- Using the MAC Address Table
- Using Event Log

Configuring Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control IE-SW-PL09M-GB.

System Identification

The system identification items are displayed at the top of the web page, and will be included in alarm emails. Entering the system identification information makes it easier to identify the different switches connected to your network.

System Identification

| | |
|-------------------------|---|
| Switch Name | <input type="text" value="Managed Switch 07941"/> |
| Switch Location | <input type="text"/> |
| Switch Description | <input type="text" value="IE-SW-PL09M-5GC-4GT"/> |
| Maintainer Contact Info | <input type="text"/> |
| Web Configuration | <input type="text" value="http or https"/> |
| Web Auto-logout (s) | <input type="text" value="0"/> |
| Age Time (s) | <input type="text" value="300"/> |

Switch Name

| Setting | Description | Factory Default |
|--------------------|---|---|
| Max. 30 Characters | This option is useful for specifying the role or application of different IE-SW-PL09M-GB units. E.g., Factory Switch 1. | Managed Redundant Switch [<i>Serial No. of this switch</i>] |

Switch Location

| Setting | Description | Factory Default |
|--------------------|---|-----------------|
| Max. 80 Characters | To specify the location of different IE-SW-PL09M-GB units. E.g., production line 1. | Switch Location |

Switch Description

| Setting | Description | Factory Default |
|--------------------|---|-----------------|
| Max. 30 Characters | Use this to enter a more detailed description of the IE-SW-PL09M-GB unit. | None |

Maintainer Contact Info

| Setting | Description | Factory Default |
|--------------------|--|-----------------|
| Max. 30 Characters | To provide information about whom to contact in order to resolve problems. Use | None |

| | | |
|--|--|--|
| | this to enter contact information of the person responsible for maintaining this IE-SW-PL09M-GB. | |
|--|--|--|

Password

The IE-SW-PL09M-GB provides two levels of access privilege: **admin** privilege gives read/write access to all IE-SW-PL09M-GB configuration parameters, and **user** privilege provides read access only. You will be able to view the configuration, but will not be able to make modifications.

Password Setting

Account Name :

Old Password :

Type Old Password :

New Password :

Retype Password :



ATTENTION

The IE-SW-PL09M-GB's default Password is "Detmold". If this Password is changed, then you will be required to type the new Password when logging into the RS-232 Console, Telnet Console, or Web Browser interface.

Account

| Setting | Description | Factory Default |
|---------|---|-----------------|
| admin | "admin" privilege allows the user to <i>modify</i> all IE-SW-PL09M-GB configurations. | admin |
| user | "user" privilege only allows <i>viewing</i> IE-SW-PL09M-GB configurations. | |

Password

| Setting | Description | Factory Default |
|-----------------------------------|--|-----------------|
| Old Password (Max. 16 Characters) | Type current password when changing the password | None |
| New Password (Max. 16 Characters) | Type new password when changing the password | None |
| Retype Password (Max. 16) | If you type a new password in the Password field, you will be required to retype the | None |

| | | |
|-------------|---|--|
| Characters) | password in the Retype new password field before updating the new password. | |
|-------------|---|--|

Accessible IP

The IE-SW-PL09M-GB uses an IP address-based filtering method to control access to the IE-SW-PL09M-GB units.

Accessible IP List

Enable the accessible IP list ("Disable" will allow all IP's connection)

| Index | IP | NetMask |
|-------|----|---------|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

Accessible IP Settings allows you to add or remove "Legal" remote host IP addresses to prevent unauthorized access. Access to the IE-SW-PL09M-GB is controlled by IP address. If a host's IP address is in the accessible IP table, then the host will be allowed access to the IE-SW-PL09M-GB. You can allow one of the following cases by setting this parameter:

- **Only one host with the specified IP address can access the IE-SW-PL09M-GB**
E.g., enter "192.168.1.1/255.255.255.255" to allow access to *just* the IP address 192.168.1.1.
- **Any host on a specific subnetwork can access the IE-SW-PL09M-GB**
E.g., enter "192.168.1.0/255.255.255.0" to allow access to all IPs on the subnet defined by this IP address/subnet mask combination.
- **Any host can access the IE-SW-PL09M-GB**
Disable this function by deselecting the **Enable the accessible IP list** option.

The following table shows additional configuration examples:

| Allowable Hosts | Input format |
|--------------------------------|---------------------------------|
| Any host | Disable |
| 192.168.1.120 | 192.168.1.120 / 255.255.255.255 |
| 192.168.1.1 to 192.168.1.254 | 192.168.1.0 / 255.255.255.0 |
| 192.168.0.1 to 192.168.255.254 | 192.168.0.0 / 255.255.0.0 |
| 192.168.1.1 to 192.168.1.126 | 192.168.1.0 / 255.255.255.128 |
| 192.168.1.129 to 192.168.1.254 | 192.168.1.128 / 255.255.255.128 |

Port

Port settings are included to give the user control over Port Access, Port Transmission Speed, Flow Control, and Port Type (MDI or MDIX). An explanation of each configuration item follows:

Port Settings

| Port | Enable | Description | Name | Speed | FDX Flow Ctrl | MDI/MDIX |
|------|-------------------------------------|--------------|----------------------|---|--|---|
| G1 | <input checked="" type="checkbox"/> | 1000TX,RJ45. | <input type="text"/> | Auto ▼ | Disable ▼ | Auto ▼ |
| G2 | <input checked="" type="checkbox"/> | 1000TX,RJ45. | <input type="text"/> | Auto ▼ | Disable ▼ | Auto ▼ |
| G3 | <input checked="" type="checkbox"/> | 1000TX,RJ45. | <input type="text"/> | Auto ▼ | Disable ▼ | Auto ▼ |
| G4 | <input checked="" type="checkbox"/> | 1000TX,RJ45. | <input type="text"/> | Auto ▼ | Disable ▼ | Auto ▼ |
| G5 | <input checked="" type="checkbox"/> | 1000TX,RJ45. | <input type="text"/> | Auto ▼ | Disable ▼ | Auto ▼ |
| G6 | <input checked="" type="checkbox"/> | 1000TX,RJ45. | <input type="text"/> | Auto ▼ | Disable ▼ | Auto ▼ |
| G7 | <input checked="" type="checkbox"/> | 1000TX,RJ45. | <input type="text"/> | Auto ▼ | Disable ▼ | Auto ▼ |
| G8 | <input checked="" type="checkbox"/> | 1000TX,RJ45. | <input type="text"/> | Auto ▼ | Disable ▼ | Auto ▼ |
| G9 | <input checked="" type="checkbox"/> | 1000TX,RJ45. | <input type="text"/> | Auto ▼ | Disable ▼ | Auto ▼ |

Enable

| Setting | Description | Factory Default |
|-----------|--|-----------------|
| checked | Allows data transmission through the port. | enabled |
| unchecked | Immediately shuts off port access. | |

Description

| Setting | Description | Factory Default |
|------------|--|-----------------|
| Media type | Displays the media type for each module's port | N/A |

Name

| Setting | Description | Factory Default |
|--------------------|--|-----------------|
| Max. 63 Characters | Specify an alias for each port, and assist the administrator in remembering important information about the port. E.g., PLC 1 | None |

Speed

| Setting | Description | Factory Default |
|-----------|--|-----------------|
| Auto | Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection. | Auto |
| 1G-Full | Choose one of these fixed speed options if the opposing Ethernet device has trouble auto-negotiating line speed. | |
| 100M-Full | | |
| 100M-Half | | |
| 10M-Full | | |

| | | |
|----------|--|--|
| 10M-Half | | |
|----------|--|--|

FDX Flow Ctrl

This setting enables or disables the flow control capability of this port when the “port transmission speed” setting is in “auto” mode. The final result will be determined by the “auto” process between the IE-SW-PL09M-GB and connected devices.

| Setting | Description | Factory Default |
|---------|--|-----------------|
| Enable | Enables flow control for this port when in auto-negotiate mode. | Disable |
| Disable | Disables flow control for this port when in auto-negotiate mode. | |

MDI/MDIX

| Setting | Description | Factory Default |
|---------|--|-----------------|
| Auto | Allows the port to auto detect the port type of the opposing Ethernet device and change the port type accordingly. | Auto |
| MDI | Choose the MDI or MDIX option if the opposing Ethernet device has trouble auto-negotiating port type. | |
| MDIX | | |

Network

The **Network** configuration allows users to modify the usual TCP/IP network parameters. An explanation of each configuration item follows.

Network Parameters

General Settings

IPv4

Auto IP Configuration:

Switch IP Address:

Switch Subnet Mask:

Default Gateway:

1st DNS Server IP Address:

2nd DNS Server IP Address:

IPv6

Global Unicast Address Prefix:

Global Unicast Address:

Link-Local Address:

Auto IP Configuration

| Setting | Description | Factory Default |
|----------|---|-----------------|
| Disable | Set up the IE-SW-PL09M-GB's IP address manually. | Disable |
| By DHCP | The IE-SW-PL09M-GB's IP address will be assigned automatically by the network's DHCP server. | |
| By BOOTP | The IE-SW-PL09M-GB's IP address will be assigned automatically by the network's BOOTP server. | |

Switch IP Address

| Setting | Description | Factory Default |
|----------------------------------|--|-----------------|
| IP Address of the IE-SW-PL09M-GB | Identifies the IE-SW-PL09M-GB on a TCP/IP network. | 192.168.1.110 |

Switch Subnet Mask

| Setting | Description | Factory Default |
|-----------------------------------|--|-----------------|
| Subnet mask of the IE-SW-PL09M-GB | Identifies the type of network to which the IE-SW-PL09M-GB 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 |

Default Gateway

| Setting | Description | Factory Default |
|-------------------------------|---|-----------------|
| Default Gateway of the Switch | The IP address of the router that connects the LAN to an outside network. | None |

DNS IP Address

| Setting | Description | Factory Default |
|-----------------------------|---|-----------------|
| 1st DNS Server's IP Address | The IP address of the DNS Server used by your network. | None |
| 2nd DNS Server's IP Address | The IP address of the DNS Server used by your network. The IE-SW-PL09M-GB will try to locate the 2nd DNS Server if the 1st DNS Server fails to connect. | None |

Global Unicast Address Prefix (Prefix Length: 64 bits)

| Setting | Description | Factory Default |
|-------------------------------|---|-----------------|
| Global Unicast Address Prefix | The prefix value must be formatted according to RFC 2373 "IPv6 Addressing Architecture" using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. | None |

Global Unicast Address

| Setting | Description | Factory Default |
|---------|---|-----------------|
| None | Displays the IPv6 Global Unicast address. The network portion of the Global Unicast address can be configured by specifying the Global Unicast Prefix and using a EUI-64 interface ID in the low order 64 bits. The host portion of the Global Unicast address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC 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 Link-Local address is automatically generated using the modified EUI-64 from of the interface identifier (Switch's MAC address) | FE80: (EUI-64 form of the MAC address) |

Neighbor Cache

| IPv6 Address | Link Layer (MAC) Address | State |
|--------------------------|--------------------------|-----------|
| fe80::290:e8ff:fe16:3665 | 00-90-e8-16-36-65 | Reachable |

Neighbor Cache

| Setting | Description | Factory Default |
|---------|--|-----------------|
| None | The information in the neighbor cache that includes the neighboring node's IPv6 address, the corresponding Link-Layer address, and the current state of the entry. | None |

Time

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

System Time Settings

Current Time: : : (ex: 04:00:04)

Current Date: / / (ex: 2002/11/13)

Daylight Saving Time

Start Date: Month Week Day Hour

End Date: Month Week Day Hour

Offset: hour(s)

System Up Time: 4d23h3m29s

Time Zone: (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

1st Time Server IP/Name:

2nd Time Server IP/Name:

Time Server Query Period: sec

The IE-SW-PL09M-GB has a time calibration function based on information from an NTP server or user specified Time and Date information. Functions such as Auto warning “Email” can add real-time information to the message.

NOTE The IE-SW-PL09M-GB does not have a real time clock. The user must update the **Current Time** and **Current Date** to set the initial time for the IE-SW-PL09M-GB 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.

Current Time

| Setting | Description | Factory Default |
|-----------------------|--|-----------------|
| User adjustable time. | The time parameter allows configuration of the local time in local 24-hour format. | None (hh:mm:ss) |

Current Date

| Setting | Description | Factory Default |
|-----------------------|---|-------------------|
| User adjustable date. | The date parameter allows configuration of the local date in yyyy/mm/dd format. | None (yyyy/mm/dd) |

Daylight Saving Time

Daylight saving time (also know as **DST** or **summer time**) involves advancing clocks (usually 1 hour) during the summer time to provide an extra hour of daylight in the afternoon.

Start Date

| Setting | Description | Factory Default |
|-----------------------|---|-----------------|
| User adjustable date. | The Start Date parameter allows users to enter the date that daylight saving time begins. | None |

End Date

| Setting | Description | Factory Default |
|-----------------------|---|-----------------|
| User adjustable date. | The End Date parameter allows users to enter the date that daylight saving time ends. | None |

Offset

| Setting | Description | Factory Default |
|-----------------------|---|-----------------|
| User adjustable hour. | The offset parameter indicates how many hours forward the clock should be advanced. | None |

System Up Time

Indicates the IE-SW-PL09M-GB's up time from the last cold start. The unit is seconds.

Time Zone

| Setting | Description | Factory Default |
|---------------------------|---|---------------------------|
| User selectable time zone | The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time. | GMT (Greenwich Mean Time) |

NOTE Changing the time zone will automatically correct the current time. You should **configure the time zone before setting the time.**

Time Server IP/Name

| Setting | Description | Factory Default |
|-------------------------|--|-----------------|
| 1st Time Server IP/Name | IP or Domain address (e.g., 192.168.1.1 or time.nist.gov). | None |
| 2nd Time Server IP/Name | The IE-SW-PL09M-GB will try to locate the 2nd NTP Server if the 1st NTP Server fails to connect. | |

Time Server Query Period

| Setting | Description | Factory Default |
|--------------|---|-----------------|
| Query Period | This parameter determines how frequently the time is updated from the NTP server. | 600 seconds |

IEEE 1588 PTP

The following information is taken from the NIST website at <http://ieee1588.nist.gov/intro.htm>:

Time measurement can be accomplished using the IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems (IEEE 1588-2008) to synchronize real-time clocks incorporated within each component of the electrical power system for power automation applications.

IEEE 1588, which was published in November 2002, expands the performance

capabilities of Ethernet networks to control systems that operate over a communication network. In recent years an increasing number of electrical power systems have been using a more distributed architecture with network technologies that have less stringent timing specifications. IEEE 1588 generates a master-slave relationship between the clocks, and enforces the specific timing requirements in such power systems. All devices ultimately get their time from a clock known as the grandmaster clock. In its basic form, the protocol is intended to be administration free.

How does an Ethernet Switch Affect 1588 Synchronization?

The following content is taken from the NIST website at <http://ieee1588.nist.gov/switch.htm>:

An Ethernet switch potentially introduces multi-microsecond fluctuations in the latency between the 1588 grandmaster clock and a 1588 slave clock. Uncorrected these fluctuations will cause synchronization errors. The magnitude of these fluctuations depends on the design of the Ethernet switch and the details of the communication traffic. Experiments with prototype implementations of IEEE 1588 indicate that with suitable care the effect of these fluctuations can be successfully managed. For example, use of appropriate statistics in the 1588 devices to recognized significant fluctuations and use suitable averaging techniques in the algorithms controlling the correction of the local 1588 clock will be the good design means to achieve the highest time accuracy.

PTP Setting

PTP Setting

Operation IEEE 1588/PTP
 Operation Enable PTP

Configuration IEEE 1588/PTP
 Clock Mode
 Sync Interval
 Subdomain Name _DFLT

Status
 Offset To Master(nsec)
 Grandmaster UUID
 Parent UUID
 Clock Stratum
 Clock Identifier

PTP Port Settings

| Port | Port Enable | Port Status |
|------|---------------------------------|--------------|
| G1 | <input type="checkbox"/> Enable | PTP_DISABLED |
| G2 | <input type="checkbox"/> Enable | PTP_DISABLED |
| G3 | <input type="checkbox"/> Enable | PTP_DISABLED |
| G4 | <input type="checkbox"/> Enable | PTP_DISABLED |
| G5 | <input type="checkbox"/> Enable | PTP_DISABLED |

Operation IEEE 1588/PTP

| Setting | Description | Factory Default |
|-----------|--|-----------------|
| Operation | Disable or enable IEEE 1588(PTP) operation | Disable |

Configuration IEEE 1588/PTP

| Setting | Description | Factory Default |
|-----------------|---|-----------------|
| Clock Mode | Support software-based IEEE 1588(PTP) mode | <i>Disable</i> |
| Sync Interval | Period for sending synchronization message (in seconds) | <i>Disable</i> |
| Sub-domain Name | Support <i>_DFLT</i> (Default) domain only | <i>_DFLT</i> |

Status

| Setting | Description | Factory Default |
|-------------------------|--|-----------------|
| Offset To Master (nsec) | Deviation between local time and the reference clock (in nanoseconds). | |
| Grandmaster UUID | When the clock has a port in PTP_SLAVE state, this member's value is the value of the grand master Clock's Uuid field of the last Sync message received from the parent of the slave port. | |
| Parent UUID | When the clock has a port in PTP_SLAVE state, this member's value is the value of the source-Uuid field of the last Sync message received from the parent of the slave port. | |
| Clock Stratum | The stratum number describes one measure of the quality of a clock. Each clock is characterized by a stratum number used by the best master clock algorithm as one parameter of clock quality. | 4 |
| Clock Identifier | Properties of the clock. | <i>DFLT</i> |

PTP Port Settings

| Setting | Description | Factory Default |
|-------------|---------------------------------------|---------------------|
| Port Enable | Enable or disable PTP port operation. | <i>None</i> |
| Port Status | Display PTP port real status. | <i>PTP_DISABLED</i> |

Turbo Ring DIP Switch

The **Turbo Ring DIP Switch** page allows users to disable the four DIP switches located on the Switch's outer casing. When enabled, the DIP switches can be used to configure basic settings for either the "**Turbo Ring**" protocol or "**Turbo Ring V2**" protocol. A complete description of the settings is given below.

NOTE The "**Turbo Ring**" protocol (recovery time < 300 ms) provides a better network reliability and faster recovery time for redundant ring topologies. The "**Turbo Ring V2**" protocol (recovery time < 20 ms), supports additional redundant ring architectures.

In this manual, we use the terminology "**Turbo Ring**" ring and "**Turbo Ring V2**" ring to

differentiate between rings configured for one or the other of these protocols.

For a detailed description of “Turbo Ring” and “Turbo Ring V2” please refer to the **Using Communication Redundancy** section later in this chapter.

How to Enable or Disable the Turbo Ring DIP Switches

Turbo Ring DIP Switch

Disable the Turbo Ring DIP Switch

1. To enable the entire set of Hardware DIP switches, uncheck the "Disable the Turbo Ring DIP Switch" option.
 2. To disable the entire set of Hardware DIP switches, check the "Disable the Turbo Ring DIP Switch" option.

Set DIP switch as Turbo Ring
 Set DIP switch as Turbo Ring V2

Disable the Turbo Ring DIP Switch

| Setting | Description | Factory Default |
|-------------------------------------|---|--|
| Enable the Turbo Ring DIP Switches | The four DIP switches are <i>enabled</i> when the “Disable the Turbo Ring DIP Switch” box is not checked. | Not checked (i.e., the Turbo Ring DIP Switches are enabled by default) |
| Disable the Turbo Ring DIP Switches | The four DIP switches are <i>disabled</i> when the “Disable the Turbo Ring DIP Switch” box is checked. | |

Set DIP switch as Turbo Ring / Set DIP switch as Turbo Ring V2

| Setting | Description | Factory Default |
|---------------------------------|--|--|
| Set DIP switch as Turbo Ring | Select this option to enable the Turbo Ring DIP switches to configure the SWITCH for a “Turbo Ring” ring. | This is the default if you do NOT reset the switch to factory default settings (provided you upgraded the firmware for Turbo Ring V2). |
| Set DIP switch as Turbo Ring V2 | Select this option to enable the Turbo Ring DIP switches to configure the SWITCH for a “Turbo Ring V2” ring. | This is the default if you DO reset the switch to factory default settings (provided you upgraded the firmware for Turbo Ring V2). |

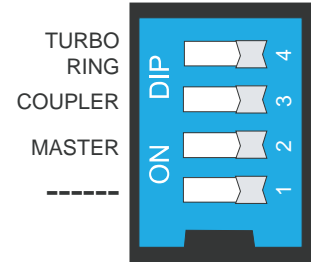
NOTE If you upgrade the firmware of your SWITCH from Turbo Ring to Turbo Ring V2, but do not reset the switch to factory defaults, the DIP switches will be set to configure the SWITCH for a “Turbo Ring” ring. If you reset the switch to factory defaults, the DIP

switches will be set to configure the SWITCH for a “Turbo Ring V2” ring.

How to Configure the Turbo Ring DIP Switches

The Turbo Ring DIP Switches are set to the OFF position at the factory.

NOTE The four DIP Switches are used to configure both the “**Turbo Ring**” and “**Turbo Ring V2**” protocols, depending on which protocol is active. To select which protocol the SWITCH will use, start the user interface software, and then use the left menu to navigate to the **Communication Redundancy** page. To use one of the Turbo Ring protocols for the Switch, select either “**Turbo Ring**” or “**Turbo Ring V2**” in the **Redundancy Protocol** drop-down box. See the **Configuring “Turbo Ring” and “Turbo Ring V2”** section in this chapter for details.



The following tables show how to use the DIP switches to configure the SWITCH for “Turbo Ring” or “Turbo Ring V2”.

NOTE DIP switch 4 must be set to the ON position to enable DIP switches 1, 2, and 3. If DIP switch 4 is set to the “OFF” position, then DIP switches 1, 2, and 3 will all be disabled.

“Turbo Ring” DIP Switch Settings

| DIP 1 | DIP 2 | DIP 3 | DIP 4 |
|--------------------------|---|--|--|
| Reserved for future use. | <u>ON</u> : Enables this SWITCH as the Ring Master. | <u>ON</u> : Enables the default “Ring Coupling” ports. | <u>ON</u> : Activates DIP switches 1, 2, 3 to configure “Turbo Ring” settings. |
| | <u>OFF</u> : This SWITCH will not be the Ring Master. | <u>OFF</u> : Do not use this SWITCH as the ring coupler. | <u>OFF</u> : DIP switches 1, 2, 3 will be disabled. |

“Turbo Ring V2” DIP Switch Settings

| DIP 1 | DIP 2 | DIP 3 | DIP 4 |
|--|---|--|---|
| <u>ON</u> : Enables the default “Ring Coupling (backup)” port. | <u>ON</u> : Enables this SWITCH as the Ring Master. | <u>ON</u> : Enables the default “Ring Coupling” port. | <u>ON</u> : Activates DIP switches 1, 2, 3 to configure “Turbo Ring V2” settings. |
| <u>OFF</u> : Enables the default “Ring Coupling (primary)” port. | <u>OFF</u> : This SWITCH will not be the Ring Master. | <u>OFF</u> : Do not use this SWITCH as a ring coupler. | <u>OFF</u> : DIP switches 1, 2, 3 will be disabled. |

NOTE The DIP 1 setting will only be active if DIP 3 is in the ON position. If you set DIP 3 to OFF, then the default Ring Coupling port will NOT be enabled, even if DIP 1 is ON.

| Protocol | Default Turbo Ring Ports | Default Ring Coupling Port(s) |
|---------------|--------------------------|-------------------------------|
| Turbo Ring | ports G2 and G3 | Port 7 |
| Turbo Ring V2 | ports G2 and G3 | Port G1 |

NOTE The Turbo Ring Ports and Coupling Ports will be added automatically to all VLANs if you set DIP Switch 4 to the "ON" position.

NOTE If you do not enable any of the managed Weidmüller Ethernet Switches to be the Ring Master, the Turbo Ring protocol will automatically choose the Ethernet Switch with the smallest MAC address range to be the Ring Master. If you accidentally enable more than one Ethernet Switch to be the Ring Master, these IE-SW-PL09M-GB switches will auto-negotiate to determine which one will be the Ring Master.

NOTE If you use the browser interface to enable the DIP switches (by un-checking the "Disable the Turbo Ring DIP switch" checkbox), and then flip DIP switch 4 from **ON** to **OFF**, the Ring Ports and Coupling Ports that were added to all VLANs will be restored to their previous software settings. (For details, please refer to the "Using Virtual LANs" section of this manual).

System File Update: By Remote TFTP

The IE-SW-PL09M-GB supports saving your configuration file to a remote TFTP server or local host to allow other IE-SW-PL09M-GB switches to use the same configuration at a later time, or saving the Log file for future reference. Loading pre-saved firmware or a configuration file from the TFTP server or local host is also supported for easy upgrading or configuration of the IE-SW-PL09M-GB.

Update System Files by TFTP

| | | | |
|-----------------------------------|----------------------|---|---------------------------------------|
| TFTP Server IP/Name | <input type="text"/> | | |
| Configuration Files Path and Name | <input type="text"/> | <input type="button" value="Download"/> | <input type="button" value="Upload"/> |
| Firmware Files Path and Name | <input type="text"/> | <input type="button" value="Download"/> | |
| Log Files Path and Name | <input type="text"/> | | <input type="button" value="Upload"/> |

TFTP Server IP/Name

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

Configuration Files Path and Name

| Setting | Description | Factory Default |
|--------------------|---|-----------------|
| Max. 40 Characters | The path and file name of the IE-SW-PL09M-GB's configuration file in the TFTP server. | None |

Firmware Files Path and Name

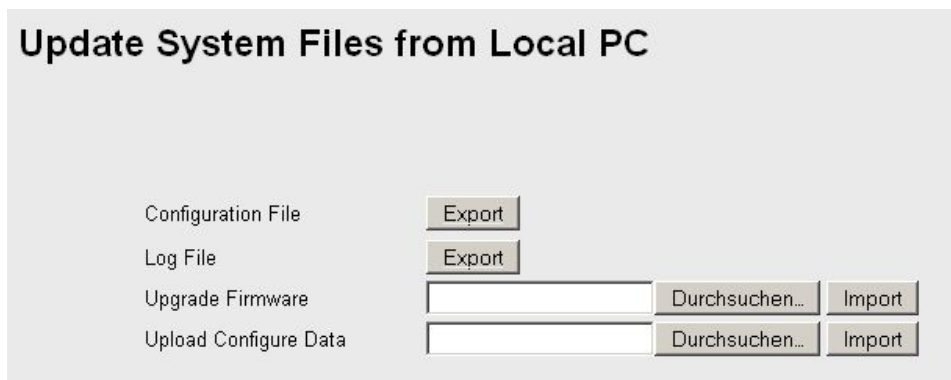
| Setting | Description | Factory Default |
|--------------------|---|-----------------|
| Max. 40 Characters | The path and file name of the IE-SW-PL09M-GB's firmware file. | None |

Log Files Path and Name

| Setting | Description | Factory Default |
|--------------------|---|-----------------|
| Max. 40 Characters | The path and file name of the IE-SW-PL09M-GB's log file | None |

After setting up the desired path and file name, click **Activate** to save the setting, and then click **Download** to download the prepared file from the remote TFTP server, or click **Upload** to upload the desired file to the remote TFTP server.

System File Update: By Local Import/Export



Configuration File

To export the configuration file of this IE-SW-PL09M-GB, click **Export** to save it to the local host.

Log File

To export the Log file of this IE-SW-PL09M-GB, click **Export** and save it to the local host.

NOTE Some operating systems will open the configuration file and log file directly in the web page. In such cases, right click **Export** to save as a file.

Upgrade Firmware

To import the firmware file of this IE-SW-PL09M-GB, click **Browse** to select the firmware file already saved on your computer. The upgrade procedure will proceed automatically after clicking **Import**.

Upload Configuration Data

To import the configuration file of this IE-SW-PL09M-GB, click **Browse** to select the configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking **Import**.

System File Update: By Backup Media

EBR-Module (External Backup and Restore Module)

Auto load EBR-Module's system configurations when system boots up Activate

Save the current configurations to EBR-Module Save

Load the EBR-Module's configurations to Switch Load

Auto load system configurations when system boots up

| Setting | Description | Factory Default |
|---------|---|-----------------|
| Enable | Enables Auto load system configurations when system boots up | Enable |
| Disable | Disables Auto load system configurations when system boots up | |

Save the current configurations to EBR-Module (External Backup- and Restore-Module)

To export the current configuration file of the IE-SW-PL09M-GB, click on **Save** to save it to the ABC.

Load the EBR-Module's configurations to the Switch

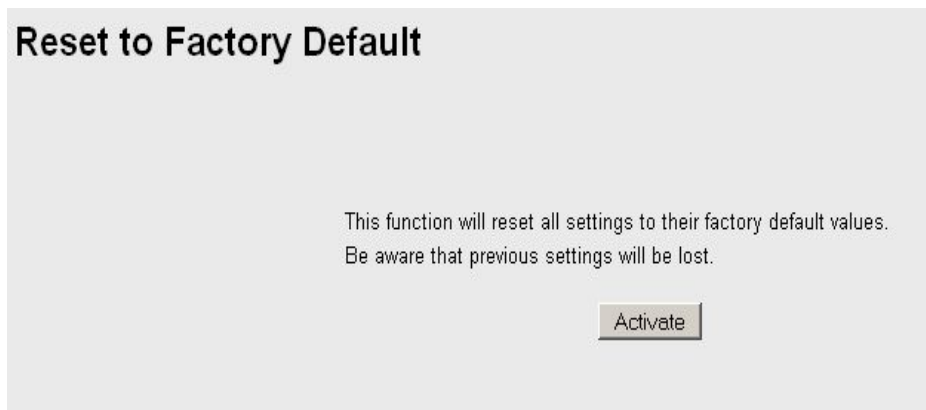
To import the configuration file of the IE-SW-PL09M-GB, click on **Load** to load it to the Switch.

Restart



This function is used to restart the Ethernet Switch.

Factory Default



The Factory Default function is included to give users a quick way of restoring IE-SW-PL09M-GB's configuration settings to their factory default values. This function is available in the Console utility (serial or Telnet), and Web Browser interface.

| | |
|-------------|---|
| NOTE | After activating the Factory Default function, you will need to use the default network settings to re-establish a web-browser or Telnet connection with your IE-SW-PL09M-GB. |
|-------------|---|

Using Port Trunking

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

The IE-SW-PL09M-GB's Port Trunking feature allows devices to communicate by aggregating up to 4 trunk groups, with a maximum of 8 ports for each group. If one of the 8 ports fails, the other seven ports will provide back up and share the traffic automatically.

Port trunking can be used to combine up to 8 ports between two IE-SW-PL09M-GB

switches. If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 8 GBps.



The Port Trunking Concept

The Weidmueller Ethernet switches are using a proprietary Port Trunking protocol that provides the following benefits:

- Gives you more flexibility in setting up your network connections, since the bandwidth of a link can be doubled, tripled, or quadrupled.
- Provides redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.
- Load sharing—MAC Client traffic may be distributed across multiple links.
- To avoid broadcast storms or loops in your network while configuring a trunk, first disable or disconnect all ports that you want to add to the trunk or remove from the trunk. After you finish configuring the trunk, enable or re-connect the ports.

If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be up to 800 Mbps on the IE-SW-PL09M-GB. This means that users can connect one SWITCH to another SWITCH by Port Trunking to double, triple, or quadruple the bandwidth of the connection.

When configuring Port Trunking, note that Each IE-SW-PL09M-GB can set a maximum of 4 Port Trunking groups (designated Trk1, Trk2, Trk3, Trk4).

When you activate Port Trunking settings, some advanced functions that you set up with the original ports will either be set to factory default values, or disabled:

- Communication Redundancy will be set to the factory default
- Traffic Prioritization will be set to the factory default
- Port-based VLAN or 802.1Q VLAN will be set to the factory default
- Multicast Filtering will be set to the factory default
- Rate Limiting will be set to the factory default
- Port Access Control will be set to the factory default
- Email and Relay Warning will be set to the factory default
- Set Device IP will be set to the factory default
- Mirror Port will be set to the factory default

You can setup these features again on your Trunking Port.

Configuring Port Trunking

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

Port Trunking Settings

Trunk Group Trk1 Trunk Type Static

Member Ports

| Port | Enable | Description | Name | Speed | FDX Flow Ctrl |
|--|--------|-------------|------|-------|---------------|
| <div style="text-align: center; margin-top: 50px;"> Up Down </div> | | | | | |

Available Ports

| Port | Enable | Description | Name | Speed | FDX Flow Ctrl |
|--------------------------|--------|-------------|-----------------|-------|---------------|
| <input type="checkbox"/> | 1 | Yes | 100TX,RJ45,POE. | | Auto Disable |
| <input type="checkbox"/> | 2 | Yes | 100TX,RJ45,POE. | | Auto Disable |
| <input type="checkbox"/> | 3 | Yes | 100TX,RJ45,POE. | | Auto Disable |
| <input type="checkbox"/> | 4 | Yes | 100TX,RJ45,POE. | | Auto Disable |

Activate

- Step 1:** Select Trk1, Trk2, Trk3, or Trk4 from the **Trunk Group** drop-down box.
- Step 2:** Select Static, or LACP from the **Trunk Type** drop-down box.
- Step 3:** Under **Member Ports** and **Available Ports**, select the specific ports.
- Step 4:** Use the **Up / Down** buttons to add/remove designated ports to/from a trunk group.

Trunk Group (Maximum of 3 trunk groups)

| Setting | Description | Factory Default |
|------------------------|--|-----------------|
| Trk1, Trk2, Trk3, Trk4 | Display or designate the Trunk Type and Member Ports for Trunk Group 1, 2, 3, 4. | Trk1 |

Trunk Type

| Setting | Description | Factory Default |
|---------|---|-----------------|
| Static | Proprietary trunking protocol | Static |
| LACP | Designated LACP (IEEE 802.3ad, Link Aggregation Control Protocol) | Static |

Available Ports/Member Port

| Setting | Description | Factory Default |
|------------------------|---|-----------------|
| Member/Available Ports | Use Up/Down buttons to add/remove specific ports from available ports to/from trunk group. | N/A |
| Check box | Check to designate which ports to add or remove. | Unchecked |
| Port | Port number | N/A |
| Port description | Displays the media type for each module's port | N/A |
| Name | Max. 63 Characters | N/A |

| | | |
|------------------|--|-----|
| Speed | Indicates the transmission speed (100M-Full, 100M-Half, 10M-Full, or 10M-Half) | N/A |
| FDX Flow Control | Indicates if the FDX flow control of this port is "Enabled" or "Disabled." | N/A |
| Up | Add designated ports into trunk group from available ports. | N/A |
| Down | Remove designated ports from trunk group to available port. | N/A |

Trunk Table

| Trunk Group | Member Port | Status |
|-------------|-------------|--------|
|-------------|-------------|--------|

Trunk Table

| Setting | Description |
|-------------|--|
| Trunk Group | Displays the Trunk Type and Trunk Group. |
| Member Port | Display which member ports belong to the trunk group. |
| Status | Success means port trunking is working properly. Fail means port trunking is not working properly. Standby means port trunking is working as a standby port. When there are more than eight ports trunked as a trunking group, the 9 th port will be the standby port. |

Configuring SNMP

The IE-SW-PL09M-GB supports SNMP V1/V2c/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 string *public/private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

SNMP security modes and security levels supported by the IE-SW-PL09M-GB 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 Type | Data Encryption | Method |
|------------------|------------------------|---------------------|-----------------|---|
| SNMP V1, V2c | V1, V2c Read Community | Community string | No | Use a community string match for authentication |

| | | | | |
|---------|------------------------------|------------------------------------|---------------------|--|
| | V1, V2c Write/Read Community | Community string | No | Use a community string match for authentication |
| SNMP V3 | No-Auth | No | No | Use 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. 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 follows.

SNMP Read/Write Settings

SNMP Versions

| Setting | Description | Factory Default |
|-------------------------------------|---|-----------------|
| V1, V2c, V3, or V1, V2c, or V3 only | Select the SNMP protocol version used to manage the switch. | V1, V2c |

V1, V2c Read Community

| Setting | Description | Factory Default |
|------------------------|--|-----------------|
| V1, V2c Read Community | Use a community string match with a maximum of 30 characters for authentication. The SNMP agent accesses all objects with read-only permissions using the community string <i>public</i> . | public |

V1, V2c Write/Read Community

| Setting | Description | Factory Default |
|------------------------------|---|-----------------|
| V1, V2c Read/Write Community | Uses a community string match with a maximum of 30 characters for authentication. The SNMP servers access all objects with read/write permissions using the community string <i>private</i> . | private |

For SNMP V3, there are two levels of privileges for different accounts to access the IE-SW-PL09M-GB. **Admin** privilege allows access, and authorization to read and write the MIB file. **User** privilege only allows reading the MIB file, but does not have authorization to write.

Admin Auth. Type (for SNMP V1, V2c, V3, and V3 only)

| Setting | Description | Factory Default |
|----------|--|-----------------|
| No-Auth | Use admin. account to access objects. No authentication | No |
| MD5-Auth | Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication. | No |
| SHA-Auth | Provide authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication. | No |

Admin Data Encryption Key (for SNMP V1, V2c, V3, and V3 only)

| Setting | Description | Factory Default |
|---------|---|-----------------|
| Enable | 8-character data encryption key is the minimum requirement for data encryption (maximum of 30 characters) | No |
| Disable | No data encryption | No |

User Auth. Type (for SNMP V1, V2c, V3 and V3 only)

| Setting | Description | Factory Default |
|----------|---|-----------------|
| No-Auth | Use admin account or user account to access objects. No authentication. | No |
| MD5-Auth | Provides authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication. | No |
| SHA-Auth | Provides authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication. | No |

User Data Encryption Key (for SNMP V1, V2c, V3 and V3 only)

| Setting | Description | Factory Default |
|---------|---|-----------------|
| Enable | 8-character data encryption key is the minimum requirement for data encryption (maximum of 30 characters) | No |
| Disable | No data encryption | No |

Trap Settings

SNMP traps allow an SNMP agent to notify the NMS of a significant event. The IE-SW-PL09M-GB supports two SNMP modes, **Trap** mode and **Inform** mode.

SNMP Trap Mode

In **Trap** mode, the SNMP agent sends an SNMPv1 trap PDU to the NMS. No acknowledgment is sent back from the NMS so the agent has no way of knowing if the trap reached the NMS.

Trap Mode

Retries (1~99)

Timeout (1~300s)

SNMP Inform Mode

SNMPv2 provides an inform mechanism. When an inform message is sent from the SNMP agent to the NMS, the receiver sends a response to the sender acknowledging receipt of the event. This behavior is similar to that of the get and set requests. If the SNMP agent doesn't receive a response from the NMS for a period of time, the agent will resend the trap to the NMS agent. The maximum timeout time is 300 secs (default is 1 sec), and the maximum number of retries is 99 times (default is 1 time). When the SNMP agent receives acknowledgement from the NMS, it will stop resending the inform messages.

Trap Mode

Retries (1~99)

Timeout (1~300s)

1st Trap Server IP/Name

| Setting | Description | Factory Default |
|------------|---|-----------------|
| IP or Name | Enter the IP address or name of the 1 st Trap Server used by your network. | None |

1st Trap Community

| Setting | Description | Factory Default |
|------------------|---|-----------------|
| Character String | Use a community string match for authentication (maximum of 30 characters). | Public |

2nd Trap Server IP/Name

| Setting | Description | Factory Default |
|------------|---|-----------------|
| IP or Name | Enter the IP address or name of the 2 nd Trap Server used by your network. | None |

2nd Trap Community

| Setting | Description | Factory Default |
|------------------|---|-----------------|
| Character String | Use a community string match for authentication (maximum of 30 characters). | Public |

Inform mode select

| Setting | Description | Factory Default |
|----------|-----------------------------|-----------------|
| Retries | Enter Inform Retry number | 1 |
| Time out | Enter Inform Timeout window | 1 |

Private MIB information

Switch Object ID

| Setting | Description | Factory Default |
|-----------|-----------------------------------|-----------------|
| 8691.7.18 | IE-SW-PL09M-GB's enterprise value | Fixed |

NOTE: The Switch Object ID cannot be changed.

Using 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.

The Communication Redundancy function allows the user 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 IE-SW-PL09M-GB is used as a key communications component of a production line, several minutes of downtime could cause a big loss in production and revenue. The Ethernet Switch has implemented the following protocols to support communication redundancy functions:

- **Rapid Spanning Tree/ Spanning Tree Protocol (IEEE 802.1W/1D)**
- **Turbo Ring / Turbo Ring V2**
- **and Turbo Chain**

When configuring a redundant ring, all switches on the same ring must be configured to use the same redundancy protocol. You cannot mix the "Turbo Ring," "Turbo Ring V2," and STP/RSTP protocols on the same ring. The following table lists the key differences between each feature. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network.

| | Turbo Ring V2 | Turbo Ring | Turbo Chain | STP | RSTP |
|---------------|---------------|------------|-------------|------------------|-----------------|
| Topology | Ring | Ring | Chain | Ring, Mesh | Ring, Mesh |
| Recovery Time | < 20 ms | < 300 ms | < 20 ms | Up to 30 seconds | Up to 5 seconds |

NOTE All of Weidmüller's managed switches support three Turbo Ring protocols:

1. "Turbo Ring" refers to the original version of redundant ring protocol, which has a recovery time of under 300 ms.
2. "Turbo Ring V2" refers to the new generation Turbo Ring, which has a recovery time of under 20 ms.
3. "Turbo Chain" is a protocol with unlimited flexibility to allow you to construct any type of redundant network topology. The recovery time is under 20 ms.

In this manual, we use the terminology "Turbo Ring" ring and "Turbo Ring V2" ring to differentiate between rings configured for one or the other of these protocols.

Gigabit Ethernet Redundant Ring Capability (< 50 ms)

Ethernet has become the default data communications medium for industrial automation applications. In fact, Ethernet is often used to integrate video, voice, and high-rate industrial application data transfers into one network. Weidmüller IE-SW-PL18M, which comes equipped with a redundant Gigabit Ethernet protocol called Gigabit Turbo Ring, gives system maintainers a convenient means of setting up a versatile yet stable Gigabit Ethernet network. With Gigabit Turbo Ring, if any segment of the network gets disconnected, your automation system will be back to normal in less than 300 ms (Turbo Ring) or 50 ms (Turbo Ring V2).

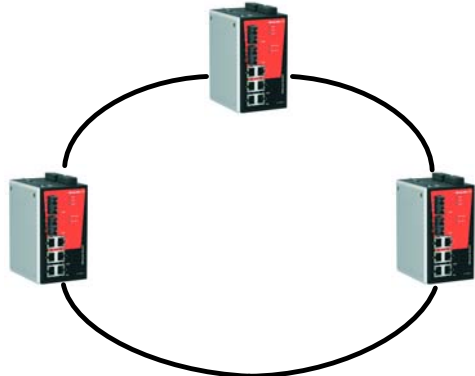


NOTE Port-trunking and Turbo Ring can be enabled simultaneously to form a backbone. Doing so will increase the bandwidth of the backbone, and also provide redundancy. For example, suppose that two physical ports, 1 and 2, are trunked to form trunk group Trk1, and then Trk1 is set as one Turbo Ring path, if port 1 gets disconnected, the remaining trunked port, port 2, will share the traffic. If port 1 and port 2 are both disconnected, Turbo Ring will create the back up path within 300 ms.

The Turbo Ring Concept

The Turbo Ring protocol was developed to optimize communication redundancy and achieve a faster recovery time on the network.

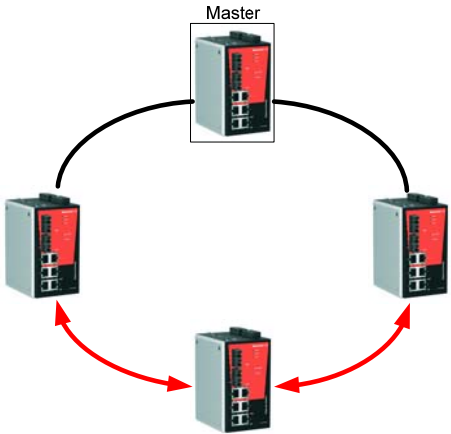
The Turbo Ring and Turbo Ring V2 protocols identify one switch as the **master** of the network, and then automatically block packets from traveling through any of the network’s redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network.

| Initial setup of a “Turbo Ring” or “Turbo Ring V2” ring | |
|--|---|
|  | <ol style="list-style-type: none"> 1. Select any two ports as redundant ports. 2. Connect the redundant ports to form the Turbo Ring. |

The user does not need to configure any of the switches as the master to use Turbo Ring or Turbo Ring V2. If none of the switches in the ring is configured as the master, then the protocol will automatically assign master status to one of the switches. In fact, the master is only used to identify which segment in the redundant ring acts as the backup path. In the following subsections, we explain how the redundant path is selected for rings configured for Turbo Ring, and Turbo Ring V2.

Determining the Redundant Path of a “Turbo Ring” Ring

In this case, the redundant segment (i.e., the segment that will be blocked during normal operation) is determined by the number of switch units that make up the ring, and where the ring master is located.

| When the number of IE-SW-PL09M-GB units in the Turbo Ring is even. | |
|---|---|
|  | <p>If there are $2N$ SWITCH units (an even number) in the “Turbo Ring” ring, then the backup segment is one of the two segments connected to the $(N+1)$st SWITCH (i.e., the SWITCH unit directly opposite the master).</p> |

When the number of IE-SW-PL09M-GB units in the Turbo Ring is odd.

If there are $2N+1$ SWITCH units (an odd number) in the “Turbo Ring” ring, with SWITCH units and segments labeled counterclockwise, then segment $N+1$ will serve as the backup path.

For the example shown here, $N=1$, so that $N+1=2$.

Determining the Redundant Path of a “Turbo Ring V2” Ring

For a “Turbo Ring V2” ring, the backup segment is the segment connected to the 2nd redundant port on the master.

See **Configuring “Turbo Ring V2”** in the **Configuring “Turbo Ring” and “Turbo Ring V2”** section below.

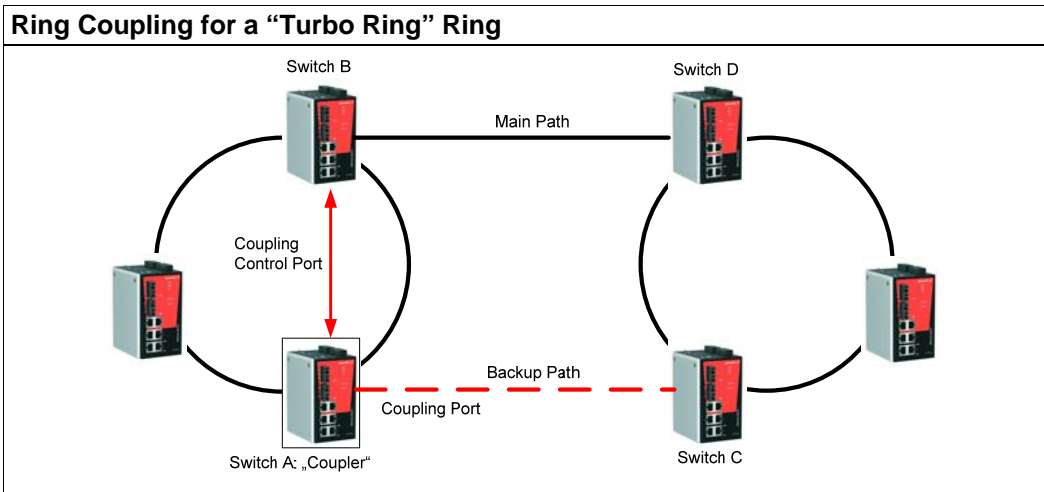
Ring Coupling Configuration

For some systems, it may not be convenient to connect all devices in the system to create one **big** redundant ring, since some devices could be located in a remote area. For these systems, “**Ring Coupling**” can be used to separate the devices into different smaller redundant rings, but in such a way that they can still communicate with each other.



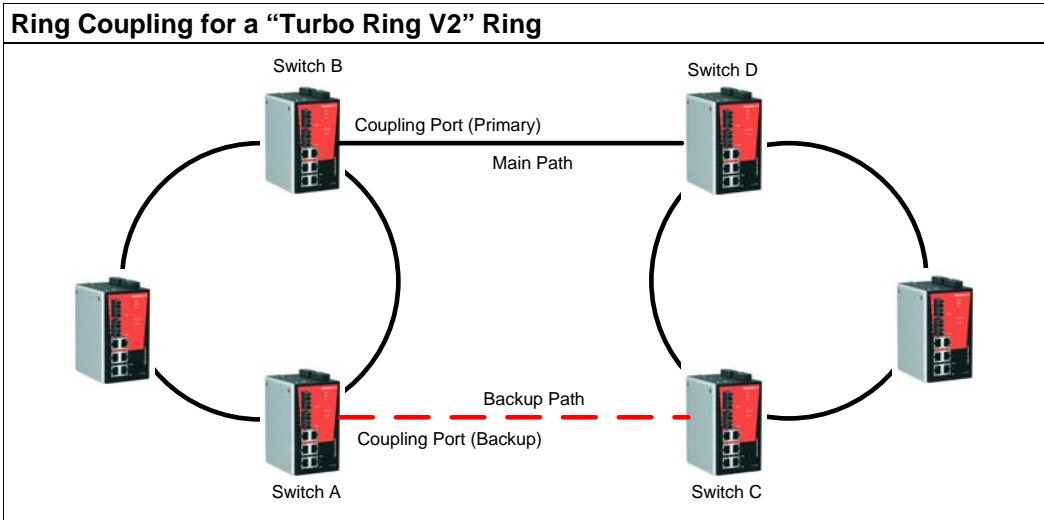
ATTENTION

In a VLAN environment, the user must set “**Redundant Port**” “**Coupling Port**” and “**Coupling Control Port**” to join all VLANs, since these ports act as the “**backbone**” to transmit all packets of different VLANs to different switch units.



To configure the Ring Coupling function for a **“Turbo Ring”** ring, select two switch units (e.g., Switch A and B in the above figure) in the ring, and another two switch units in the adjacent ring (e.g., Switch C and D). Decide which two ports in each switch are appropriate to be used as coupling ports, and then link them together. Next, assign one switch (e.g., Switch A) to be the **“coupler”** and connect the coupler’s coupling control port with Switch B (for this example).

The coupler switch (i.e., Switch A) will monitor switch B through the coupling control port to determine whether or not the coupling port’s backup path should be recovered.



Note that the ring coupling settings for a **“Turbo Ring V2”** ring are different from a **“Turbo Ring”** ring. For Turbo Ring V2, Ring Coupling is enabled by configuring the **“Coupling Port (Primary) on Switch B and the “Coupling Port (Backup) on Switch A** only. You do not need to set up a coupling control port, so that a **“Turbo Ring V2”** ring does not use a coupling control line.

The **“Coupling Port (Backup)”** on Switch A is used for the backup path, and connects directly to an extra network port on Switch C. The **“Coupling Port (Primary)”** on Switch B monitors the status of the main path, and connects directly to an extra network port on Switch D. With ring coupling established, Switch A can activate the backup path as soon as it detects a problem with the main path.



ATTENTION

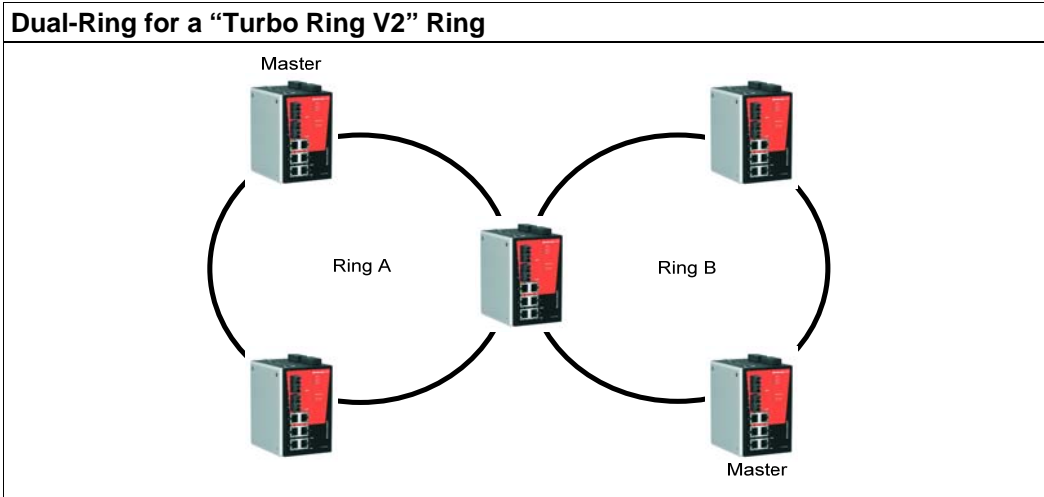
Ring Coupling only needs to be enabled on one of the switches serving as the Ring Coupler. The Coupler must designate different ports as the two Turbo Ring ports and the coupling port.

NOTE

You do not need to use the same Switch unit for both Ring Coupling and Ring Master.

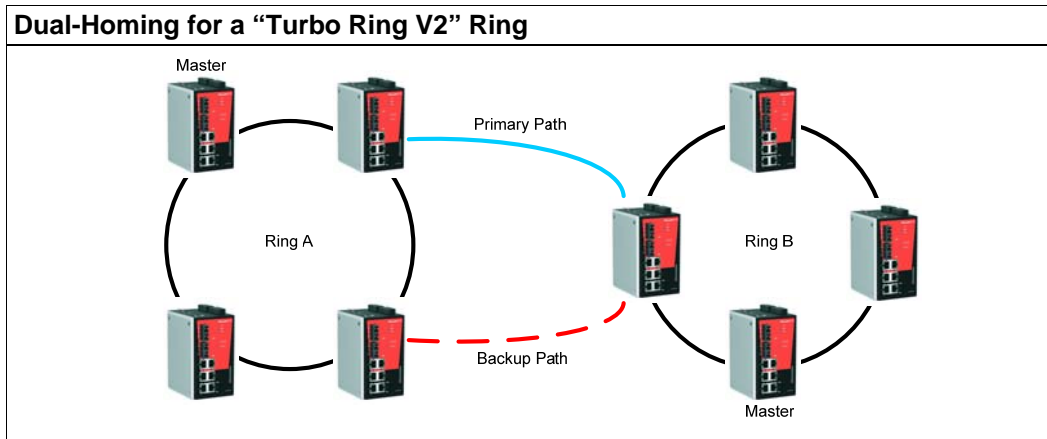
Dual-Ring Configuration (applies only to “Turbo Ring V2”)

The “**dual-ring**” option provides another ring coupling configuration, in which two adjacent rings share one switch. This type of configuration is ideal for applications that have inherent cabling difficulties.



Dual-Homing Configuration (applies only to “Turbo Ring V2”)

The “**dual-homing**” option uses a single Ethernet switch to connect two networks. The primary path is the operating connection, and the backup path is a back-up connection that is activated in the event that the primary path connection fails.



Configuring “Turbo Ring” and “Turbo Ring V2”

Use the **Communication Redundancy** page to configure select “**Turbo Ring**” or “**Turbo Ring V2**” Note that configuration pages for these two protocols are different.

Configuring “Turbo Ring”

Communication Redundancy

Current Status

| | | |
|----------------------------|-------------|-----|
| Now Active | None | |
| Master/Slave | --- | |
| Redundant Ports Status | 1st Port | --- |
| | 2nd Port | --- |
| Ring Coupling Ports Status | --- | |
| Coupling Port | --- | |
| Coupling Control Port | --- | |

Settings

| | | |
|---|----------|------------|
| Redundancy Protocol | | Turbo Ring |
| <input type="checkbox"/> Set as Master | | |
| Redundant Ports | 1st Port | G8 |
| | 2nd Port | G9 |
| <input type="checkbox"/> Enable Ring Coupling | | |
| Coupling Port | | G7 |
| Coupling Control Port | | G6 |

Explanation of “Current Status” Items

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **RSTP**, or **none**.

Master/Slave

Indicates whether or not this device is the Master of the Turbo Ring. (This field appears only when selected to operate in Turbo Ring or Turbo Ring V2 mode.)

NOTE The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the switch units in the ring. The master is only used to determine which segment serves as the backup path.

Redundant Ports Status (1st Port, 2nd Port)

Ring Coupling Ports Status (Coupling Port, Coupling Control Port)

The “Ports Status” indicators show **Forwarding** for normal transmission, **Blocking** if this port is connected to a backup path and the path is blocked, and **Link down** if there is no connection.

Explanation of “Settings” Items

Redundancy Protocol

| Setting | Description | Factory Default |
|-----------------------|---|---|
| Turbo Ring | Select this item to change to the Turbo Ring configuration page. | None RSTP (IEEE 802.1W/1D) is selected but the Ports are not RSTP-enabled |
| Turbo Ring V2 | Select this item to change to the Turbo Ring V2 configuration page. | |
| Turbo Chain | Select this item to change the Turbo Chain configuration page | |
| RSTP (IEEE 802.1W/1D) | Select this item to change to the RSTP configuration page. | |
| None | Ring redundancy is not active | |

Set as Master

| Setting | Description | Factory Default |
|----------|-------------------------------------|-----------------|
| Enabled | Select this switch as Master | Not checked |
| Disabled | Do not select this switch as Master | |

Redundant Ports

| Setting | Description | Factory Default |
|----------|---|-----------------|
| 1st Port | Select any port of the switch to be one of the redundant ports. | port G2 |
| 2nd Port | Select any port of the switch to be one of the redundant ports. | port G3 |

Enable Ring Coupling

| Setting | Description | Factory Default |
|---------|--------------------------------------|-----------------|
| Enable | Select this switch as Coupler | Not checked |
| Disable | Do not select this switch as Coupler | |

Coupling Port

| Setting | Description | Factory Default |
|---------------|---|-----------------|
| Coupling Port | Select any port of the switch to be the coupling port | port 7 |

Coupling Control Port

| Setting | Description | Factory Default |
|-----------------------|---|-----------------|
| Coupling Control Port | Select any port of the switch to be the coupling control port | port G1 |

Configuring “Turbo Ring V2”

NOTE When using the Dual-Ring architecture, users must configure settings for both Ring 1 and Ring 2. In this case, the status of both rings will appear under “Current Status.”

Explanation of “Current Status” Items

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **RSTP**, or **none**.

Ring 1/2—Status

Shows **Healthy** if the ring is operating normally, and shows **Break** if the ring's backup link is active.

Ring 1/2—Master/Slave

Indicates whether or not this SWITCH is the Master of the Turbo Ring. (This field appears only when selected to operate in Turbo Ring or Turbo Ring V2 mode.)

NOTE The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the SWITCH units in the ring. The master is only used to determine which segment serves as the backup path.

Ring 1/2—1st Ring Port Status

Ring 1/2—2nd Ring Port Status

The “Ports Status” indicators show **Forwarding** for normal transmission, **Blocking** if this port is connected to a backup path and the path is blocked, and **Link down** if there is no connection.

Coupling—Mode

Indicates either **None**, **Dual Homing**, or **Ring Coupling**.

Coupling—Coupling Port status

Indicates either **Primary**, or **Backup**.

Explanation of “Settings” Items

Redundancy Protocol

| Setting | Description | Factory Default |
|-----------------------|---|---|
| Turbo Ring | Select this item to change to the Turbo Ring configuration page. | None RSTP (IEEE 802.1W/1D) is selected but the Ports are not RSTP-enabled |
| Turbo Ring V2 | Select this item to change to the Turbo Ring V2 configuration page. | |
| Turbo Chain | Select this item to change the Turbo Chain configuration page | |
| RSTP (IEEE 802.1W/1D) | Select this item to change to the RSTP configuration page. | |
| None | Ring redundancy is not active | |

Enable Ring 1

| Setting | Description | Factory Default |
|----------|-----------------------------|-----------------|
| Enabled | Enable the Ring 1 settings | Not checked |
| Disabled | Disable the Ring 1 settings | |

Enable Ring 2*

| Setting | Description | Factory Default |
|----------|-----------------------------|-----------------|
| Enabled | Enable the Ring 2 settings | Not checked |
| Disabled | Disable the Ring 2 settings | |

*You should enable both Ring 1 and Ring 2 when using the Dual-Ring architecture.

Set as Master

| Setting | Description | Factory Default |
|----------|-------------------------------------|-----------------|
| Enabled | Select this SWITCH as Master | Not checked |
| Disabled | Do not select this SWITCH as Master | |

Redundant Ports

| Setting | Description | Factory Default |
|----------|---|-----------------|
| 1st Port | Select any port of the SWITCH to be one of the redundant ports. | port G2 |
| 2nd Port | Select any port of the SWITCH to be one of the redundant ports. | port G3 |

Enable Ring Coupling

| Setting | Description | Factory Default |
|---------|--------------------------------------|-----------------|
| Enable | Select this SWITCH as Coupler | Not checked |
| Disable | Do not select this SWITCH as Coupler | |

Coupling Mode

| Setting | Description | Factory Default |
|-------------------------|--|---|
| Dual Homing | Select this item to change to the Dual Homing configuration page | Primary Port: port G1 Backup Port: port G2 |
| Ring Coupling (backup) | Select this item to change to the Ring Coupling (backup) configuration page | port G1 |
| Ring Coupling (primary) | Select this item to change to the Ring Coupling (primary) configuration page | port G1 |

Primary/Backup Port

| Setting | Description | Factory Default |
|--------------|---|-----------------|
| Primary Port | Select any port of the SWITCH to be the primary port. | port G1 |
| Backup Port | Select any port of the SWITCH to be the backup port. | port G2 |

The Turbo Chain Concept

The Turbo Chain is an advanced software-technology that gives network administrators the flexibility of constructing any type of redundant network topology. When using the “chain” concept, you first connect the Ethernet switches in a chain and then simply link the two ends of the chain to an Ethernet network, as illustrated in the following figure.

Turbo Chain can be used on industrial networks that have a complex topology. If the

industrial network uses a multi-ring architecture, Turbo Chain can be used to create flexible and scalable topologies with a fast media-recovery time.

Setting Up Turbo Chain

1. Select the Head switch, Tail switch, and Member switches.
2. Configure one port as the Head port and one port as the Member port in the Head switch, configure one port as the Tail port and one port as the Member port in the Tail switch, and configure two ports as Member ports in each of the Member switches.
3. Connect the Head switch, Tail switch, and Member switches as shown in the diagram.

The path connecting to the Head port is the main path, and the path connecting to the Tail port is the back up path of the Turbo Chain. Under normal conditions, packets are transmitted through the Head Port to the LAN Network. If any Turbo Chain path is disconnected, the Tail Port will be activated to continue packet transmission.

Configuring “Turbo Chain”

Head Switch Configuration

Communication Redundancy

Current Status
 Now Active: **None**

Settings

Redundancy Protocol: Turbo Chain

Role: Head

| Port Role | Port Num | Port Status |
|-------------|----------|-------------|
| Head Port | G1 | --- |
| Member Port | G2 | --- |

Member Switch Configuration

Communication Redundancy

Current Status
Now Active: None

Settings

Redundancy Protocol: Turbo Chain

Role: Member

| Port Role | Port Num | Port Status |
|-----------------|----------|-------------|
| 1st Member Port | G1 | --- |
| 2nd Member Port | G2 | --- |

Tail Switch Configuration

Communication Redundancy

Current Status
Now Active: None

Settings

Redundancy Protocol: Turbo Chain

Role: Tail

| Port Role | Port Num | Port Status |
|-------------|----------|-------------|
| Tail Port | G1 | --- |
| Member Port | G2 | --- |

Explanation of “Current Status” Items

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **RSTP**, **Turbo Chain** or **None**.

The “Ports Status” indicators show **Forwarding** for normal transmission, **Blocked** if this port is connected to the Tail port as a backup path and the path is blocked, and **Link down** if there is no connection.

Explanation of “Settings” Items

Redundancy Protocol

| Setting | Description | Factory Default |
|---------------|---|-----------------|
| Turbo Ring | Select this item to change to the Turbo Ring configuration page. | None |
| Turbo Ring V2 | Select this item to change to the Turbo Ring V2 configuration page. | |

| | | |
|-----------------------|--|--|
| Turbo Chain | Select this item to change to the Turbo Chain configuration page | |
| RSTP (IEEE 802.1W/1D) | Select this item to change to the RSTP configuration page. | |
| None | Ring redundancy is not active | |

Role

| Setting | Description | Factory Default |
|---------|-------------------------------------|-----------------|
| Head | Select this SWITCH as Head Switch | Member |
| Member | Select this SWITCH as Member Switch | |
| Tail | Select this SWITCH as Tail Switch | |

Head Role

| Setting | Description | Factory Default |
|-------------|--|-----------------|
| Head Port | Select any port of the SWITCH to be the head port. | port G2 |
| Member Port | Select any port of the SWITCH to be the member port. | port G3 |

Member Role

| Setting | Description | Factory Default |
|-----------------------------|---|-----------------|
| 1 st Member port | Select any port of the SWITCH to be the 1 st member port | port G2 |
| 2 nd Member port | Select any port of the SWITCH to be the 2 nd member port | port G3 |

Tail Role

| Setting | Description | Factory Default |
|-------------|--|-----------------|
| Tail Port | Select any port of the SWITCH to be the tail port. | port G2 |
| Member Port | Select any port of the SWITCH to be the member port. | port G3 |

The STP/RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures in a network, and provide protection from loops. Networks that have a complicated architecture are prone to broadcast storms caused by unintended loops in the network. Weidmueller IE-SW-PL09M-GB's STP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every IE-SW-PL09M-GB connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and

Protocol defined by IEEE Std 802.1w-2001. 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 IE-SW-PL09M-GB. This feature is particularly helpful when IE-SW-PL09M-GB 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 the *Differences between RSTP and STP* section in this chapter.

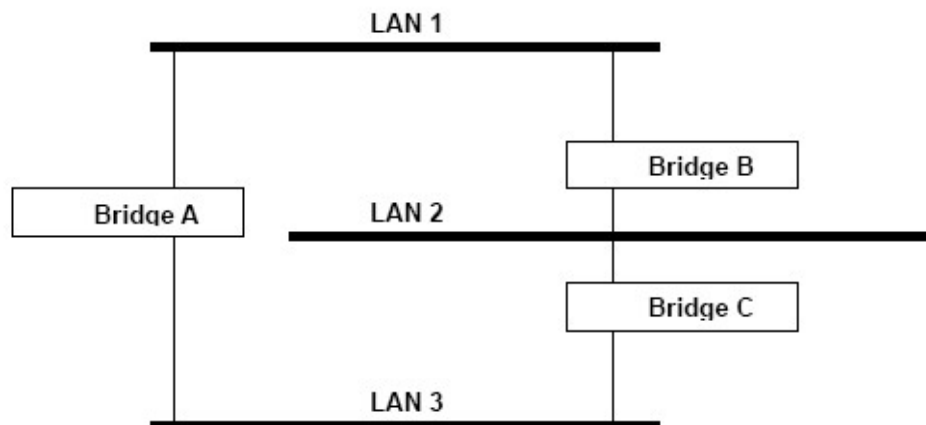
NOTE The STP protocol is part of the IEEE Std 802.1D, 1998 Edition bridge specification. The following explanation uses bridge instead of switch.

What is STP?

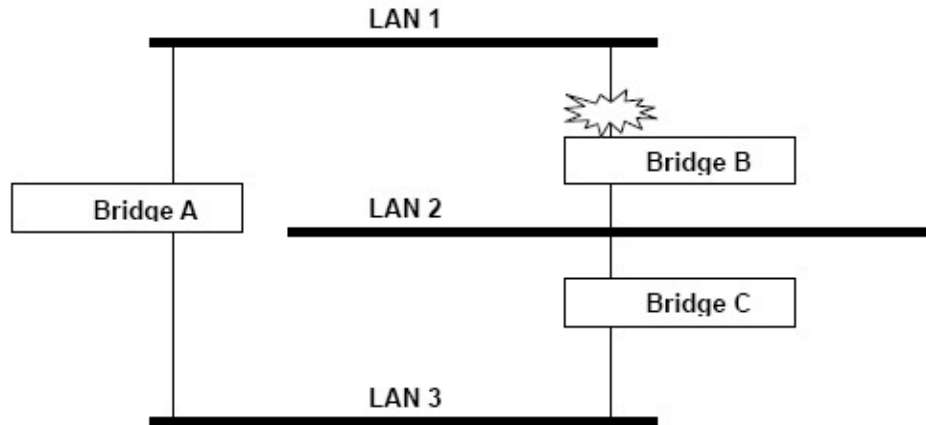
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

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

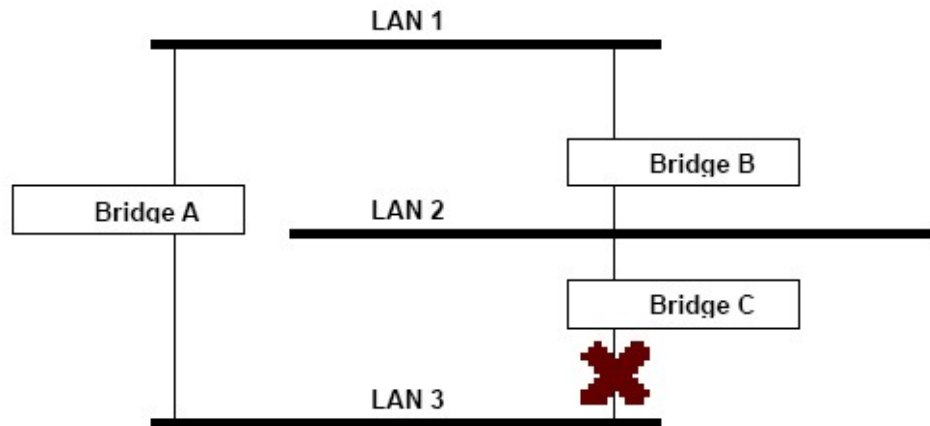
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



If STP is enabled, it will detect duplicate paths and prevent, or *block*, one of them 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. Because 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 assigns 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.

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:

- Communication between all the bridges. This 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. The default priority of IE-SW-PL09M-GB 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 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 BPDUs 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 gone down. This will trigger the

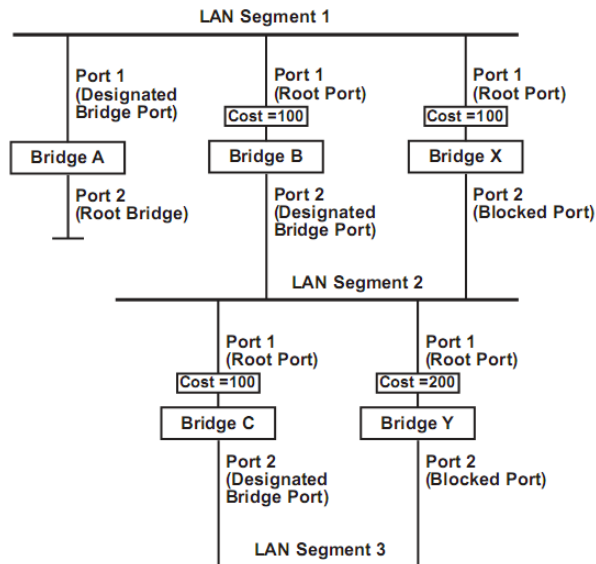
bridge to reconfigure the network to account for the change. If you have configured an SNMP trap destination, when the topology of your network changes, the first bridge to detect the change sends out an SNMP trap.

Differences between RSTP and STP

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.



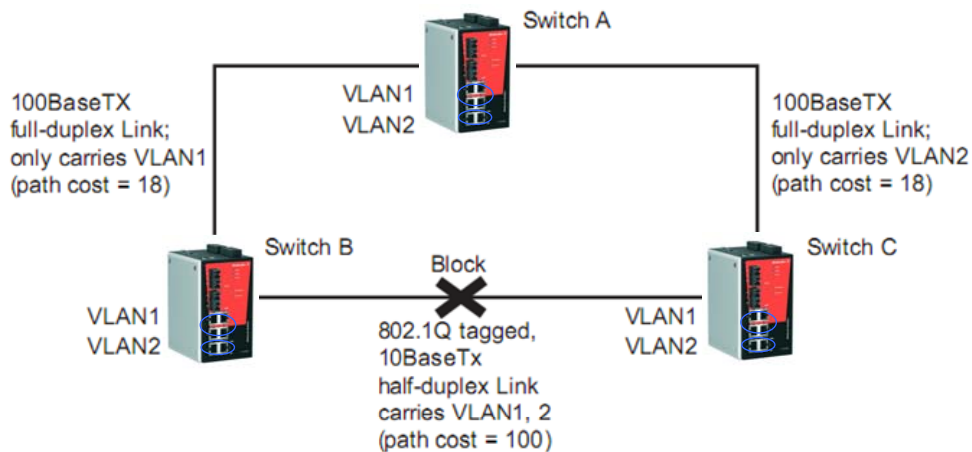
- Bridge A has been selected as the Root Bridge, since it was determined to have the lowest Bridge Identifier on the network.
- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.
- Ports 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.

Using STP on a Network with Multiple VLANs

IEEE Std 802.1D, 1998 Edition, does not take into account VLANs when calculating STP information—the calculations only depend on the physical connections. Consequently, some network configurations will result in VLANs being subdivided into a number of isolated sections by the STP system. You must ensure that every VLAN configuration on your network takes into account the expected STP topology and alternative topologies that may result from link failures.

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

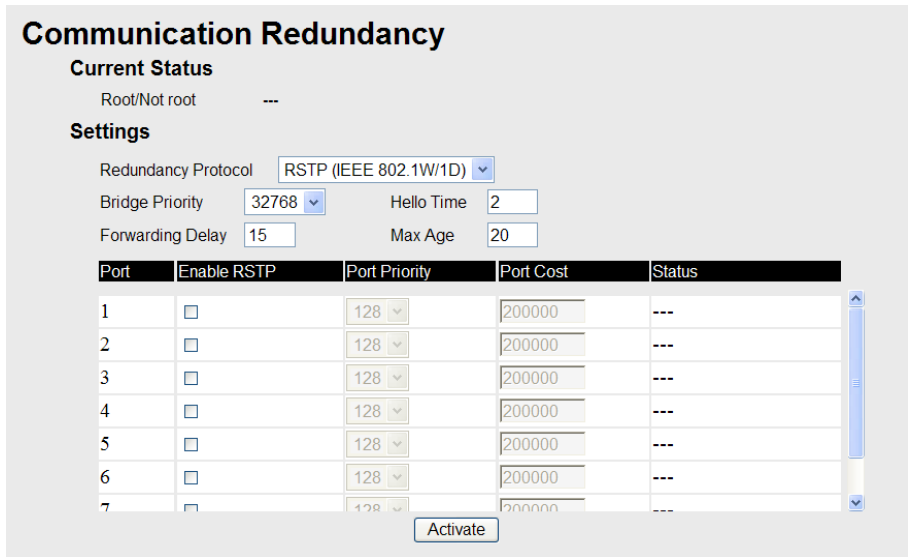


To avoid subdividing VLANs, all inter-switch connections should be made members of all available 802.1Q VLANs. This will ensure connectivity at all times. For example, the connections between Switches A and B, and between Switches A and C should be 802.1Q tagged and carrying VLANs 1 and 2 to ensure connectivity.

See the “**Configuring Virtual LANs**” section for more information about VLAN Tagging.

Configuring STP/RSTP

The following figures indicate which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter follows.



At the top of this page, the user can check the “**Current Status**” of this function. For RSTP, you will see:

Now Active:

This will show which communication protocol is being used—Turbo Ring, RSTP, or neither.

Root/Not Root

This field will appear only when selected to operate in RSTP mode. It indicates whether or not this IE-SW-PL09M-GB is the Root of the Spanning Tree (the root is determined automatically).

At the bottom of this page, the user can configure the “**Settings**” of this function. For RSTP, you can configure:

Protocol of Redundancy

| Setting | Description | Factory Default |
|-----------------------|---|-----------------|
| Turbo Ring | Select this item to change to the Turbo Ring configuration page. | None |
| Turbo Ring V2 | Select this item to change to the Turbo Ring V2 configuration page. | |
| Turbo Chain | Select this item to change to the Turbo Chain configuration page | |
| RSTP (IEEE 802.1W/1D) | Select this item to change to the RSTP configuration page. | |
| None | Ring redundancy is not active | |

Bridge 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 |

Forwarding Delay

| 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 (sec.) |

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 |

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 |

Enable STP 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.

Port 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 |

Port 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. | 200000 |

Port Status

The Port Status indicates the current Spanning Tree status of this port. “Forwarding” for normal transmission, or “Blocking” to block transmission.

Configuration Limits of RSTP/STP

The Spanning Tree Algorithm places limits on three of the configuration items described previously:

[Eq. 1]: 1 sec Hello Time 10 sec

[Eq. 2]: 6 sec Max. Age 40 sec

[Eq. 3]: 4 sec Forwarding Delay 30 sec

These three variables are further restricted by the following two inequalities:

[Eq. 4]: $2 * (\text{Hello Time} + 1 \text{ sec}) \leq \text{Max. Age} \leq 2 * (\text{Forwarding Delay} - 1 \text{ sec})$

The switch’s firmware will alert you immediately if any of these restrictions are violated. For example, setting

Hello Time = 5 sec, Max. Age = 20 sec, and Forwarding Delay = 4 sec does not violate Eqs. 1 through 3, but does violate Eq. 4, since in this case,

$2 * (\text{Hello Time} + 1 \text{ sec}) = 12 \text{ sec}$, and $2 * (\text{Forwarding Delay} - 1 \text{ sec}) = 6 \text{ sec}$.

You can remedy the situation in many ways. One solution is simply to increase the Forwarding Delay value to at least 11 sec.

HINT: Perform the following steps to avoid guessing:

Step 1: Assign a value to “**Hello Time**” and then calculate the left most part of Eq. 4 to get the lower limit of “Max. Age.”

Step 2: Assign a value to “**Forwarding Delay**” and then calculate the right most part of Eq. 4 to get the upper limit for “Max. Age.”

Step 3: Assign a value to “**Forwarding Delay**” that satisfies the conditions in Eq. 3 and Eq. 4.

Using Traffic Prioritization

IE-SW-PL09M-GB’s traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The IE-SW-PL09M-GB can inspect both IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information to provide consistent classification of the entire network. IE-SW-PL09M-GB’s QoS capability improves the performance and determinism of industrial networks for mission critical applications.

The Traffic Prioritization Concept**What is Traffic Prioritization?**

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

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

How Traffic Prioritization Works

Traffic prioritization uses the four traffic queues that are present in your IE-SW-PL09M-GB to ensure that high priority traffic is forwarded on a different queue from lower priority traffic. This is what provides Quality of Service (QoS) to your network.

IE-SW-PL09M-GB traffic prioritization depends on two industry-standard methods:

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

IEEE 802.1D Traffic Marking

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

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

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

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

- It requires an additional 4-byte tag in the frame, which is normally optional in Ethernet networks. Without this tag, the scheme cannot work.

- The tag is part of the IEEE 802.1Q header, so to implement QoS at layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.

It is only supported on a LAN and not routed across WAN links, since the IEEE 802.1Q tags are removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking

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

Advantages of DiffServ over IEEE 802.1D are:

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

Traffic Prioritization

IE-SW-PL09M-GB classifies traffic based on layer 2 of the OSI 7 layer model, and the switch prioritizes received traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1D frame and is assigned to the appropriate priority queue based on the IEEE 802.1p service level value defined in that packet. Service level markings (values) are defined in the IEEE 802.1Q 4-byte tag, and consequently traffic will only contain 802.1p priority markings if the network is configured with VLANs and VLAN tagging. The traffic flow through the switch is as follows:

1. A packet received by the IE-SW-PL09M-GB may or may not have an 802.1p tag associated with it. If it does not, then it is given a default 802.1p tag (which is usually 0). Alternatively, the packet may be marked with a new 802.1p value, which will result in all knowledge of the old 802.1p tag being lost.
2. As the 802.1p priority levels are fixed to the traffic queues, the packet will be placed in the appropriate priority queue, ready for transmission through the appropriate egress port. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port is tagged for that VLAN. If it is, then the new 802.1p tag is used in the extended 802.1D header.

The IE-SW-PL09M-GB will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based upon the IEEE 802.1p value (service levels) in that tag. It is this 802.1p value that determines to which traffic queue the packet is mapped.

Traffic Queues

The IE-SW-PL09M-GB hardware has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the IE-SW-PL09M-GB without being delayed by lower priority traffic. As each packet arrives in the IE-SW-PL09M-GB, it passes through any ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue.

IE-SW-PL09M-GB supports two different queuing mechanisms:

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

Configuring Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization capability to ensure that important data is delivered consistently and predictably. IE-SW-PL09M-GB Series can inspect IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information, to provide a consistent classification of the entire network. IE-SW-PL09M-GB Series' QoS capability improves your industrial network's performance and determinism for mission critical applications.

QoS Classification

QoS Classification

Queuing Mechanism: Weight Fair(8:4:2:1)

| Port | Inspect ToS | Inspect CoS | Port Priority |
|------|-------------------------------------|-------------------------------------|---------------|
| G5 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 3(Normal) ▾ |
| G6 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 3(Normal) ▾ |
| G7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 3(Normal) ▾ |
| G8 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 3(Normal) ▾ |
| G9 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 3(Normal) ▾ |
| Trk1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 3(Normal) ▾ |

Activate

Weidmueller IE-SW-PL09M-GB supports inspection of layer 3 TOS and/or layer 2 CoS tag information to determine how to classify traffic packets.

Queuing Mechanism

| Setting | Description | Factory Default |
|---------------|---|-----------------|
| Weighted Fair | IE-SW-PL09M-GB has 4 priority queues. In the weighted fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames. | Weight Fair |
| Strict | In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures all high priority frames to egress the switch as soon as possible. | |

Port Highest Priority

| Setting | Description | Factory Default |
|----------------|---|-----------------|
| Enable/Disable | Set the Port Priority of the ingress frames to “High” queues. | Disable |

Inspect TOS

| Setting | Description | Factory Default |
|----------------|---|-----------------|
| Enable/Disable | Select the option to enable IE-SW-PL09M-GB to inspect the Type of Service (TOS) bits in IPV4 frame to determine the priority of each frame. | Enable |

Inspect COS

| Setting | Description | Factory Default |
|----------------|--|-----------------|
| Enable/Disable | Select the option to enable IE-SW-PL09M-GB to inspect the 802.1p COS tag in the MAC frame to determine the priority of each frame. | Enable |

NOTE The priority of an ingress frame is determined in order by:

1. Inspect TOS
2. Inspect CoS
3. Port Highest Priority

NOTE The designer can enable these classifications individually or in combination. For instance, if a ‘hot,’ higher priority port is required for a network design, “**Inspect TOS**” and “**Inspect CoS**” can be disabled. This setting leaves only port default priority active, which results in all ingress frames being assigned the same priority on that port.

CoS Mapping

Mapping Table of CoS Value and Priority Queues

| CoS | Priority Queue |
|-----|----------------|
| 0 | Low |
| 1 | Low |
| 2 | Normal |
| 3 | Normal |
| 4 | Medium |
| 5 | Medium |
| 6 | High |
| 7 | High |

Activate

| Setting | Description | Factory |
|----------------------------|---|--|
| Low/Normal/ Medium/High | Set the mapping table of different CoS values to 4 different egress queues. | 0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High |

TOS/DiffServ Mapping

Mapping Table of ToS (DSCP) Value and Priority Queues

| ToS | Level | ToS | Level | ToS | Level | ToS | Level |
|----------|--------|----------|--------|----------|--------|----------|--------|
| 0x00(1) | Low | 0x04(2) | Low | 0x08(3) | Low | 0x0C(4) | Low |
| 0x10(5) | Low | 0x14(6) | Low | 0x18(7) | Low | 0x1C(8) | Low |
| 0x20(9) | Low | 0x24(10) | Low | 0x28(11) | Low | 0x2C(12) | Low |
| 0x30(13) | Low | 0x34(14) | Low | 0x38(15) | Low | 0x3C(16) | Low |
| 0x40(17) | Normal | 0x44(18) | Normal | 0x48(19) | Normal | 0x4C(20) | Normal |
| 0x50(21) | Normal | 0x54(22) | Normal | 0x58(23) | Normal | 0x5C(24) | Normal |
| 0x60(25) | Normal | 0x64(26) | Normal | 0x68(27) | Normal | 0x6C(28) | Normal |
| 0x70(29) | Normal | 0x74(30) | Normal | 0x78(31) | Normal | 0x7C(32) | Normal |
| 0x80(33) | Medium | 0x84(34) | Medium | 0x88(35) | Medium | 0x8C(36) | Medium |
| 0x90(37) | Medium | 0x94(38) | Medium | 0x98(39) | Medium | 0x9C(40) | Medium |
| 0xA0(41) | Medium | 0xA4(42) | Medium | 0xA8(43) | Medium | 0xAC(44) | Medium |
| 0xB0(45) | Medium | 0xB4(46) | Medium | 0xB8(47) | Medium | 0xBC(48) | Medium |

Activate

| Setting | Description | Factory Default |
|----------------------------|---|--|
| Low/Normal/ Medium/High | Set the mapping table of different TOS values to 4 different egress queues. | 1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High |

Using Virtual LAN

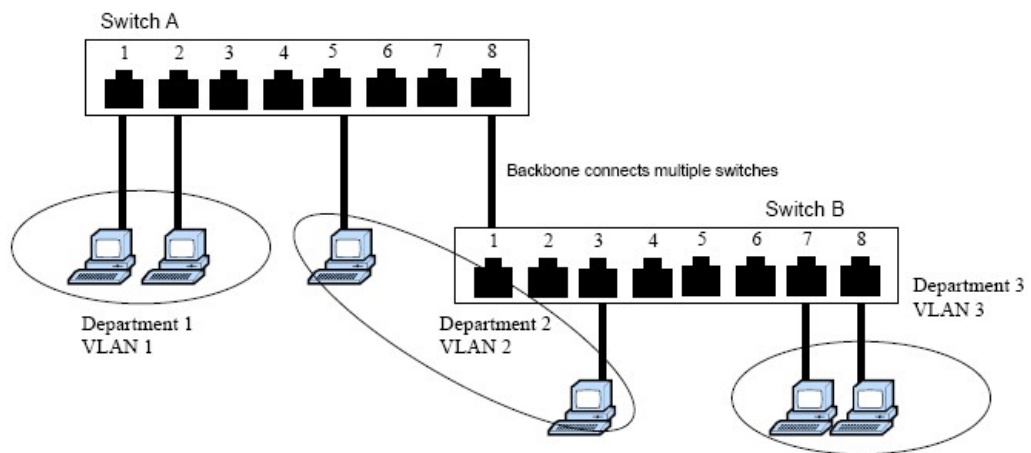
Setting up Virtual LANs (VLANs) on your IE-SW-PL09M-GB increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

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. As an example, with VLANs you can segment your network according to:

- **Departmental groups**—You could have one VLAN for the Marketing department, another for the Finance department, and another for the 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 e-mail 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 and Weidmueller Industrial Ethernet Switch

Your IE-SW-PL09M-GB provides support for VLANs using IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The

IEEE Std 802.1Q-1998 standard allows each port on your IE-SW-PL09M-GB to be placed in:

- Any one VLAN defined on the IE-SW-PL09M-GB.
- Several VLANs at the same time using 802.1Q tagging.

The standard requires that you define the *802.1Q VLAN ID* for each VLAN on your IE-SW-PL09M-GB before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized IE-SW-PL09M-GB contains a single VLAN—the Default VLAN. This VLAN has the following definition:

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

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the IE-SW-PL09M-GB over the network.

Communication Between VLANs

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

VLANs: Tagged and Untagged Membership

The IE-SW-PL09M-GB supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical (backbone, trunk) link. When setting up VLANs you need to understand when to use untagged and tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, tagged membership must be defined.

A typical host (e.g., clients) will be untagged members of one VLAN, defined as “Access Port” in the IE-SW-PL09M-GB, while inter-switch connections will be tagged members of all VLANs, defined as “Trunk Port” in the IE-SW-PL09M-GB.

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

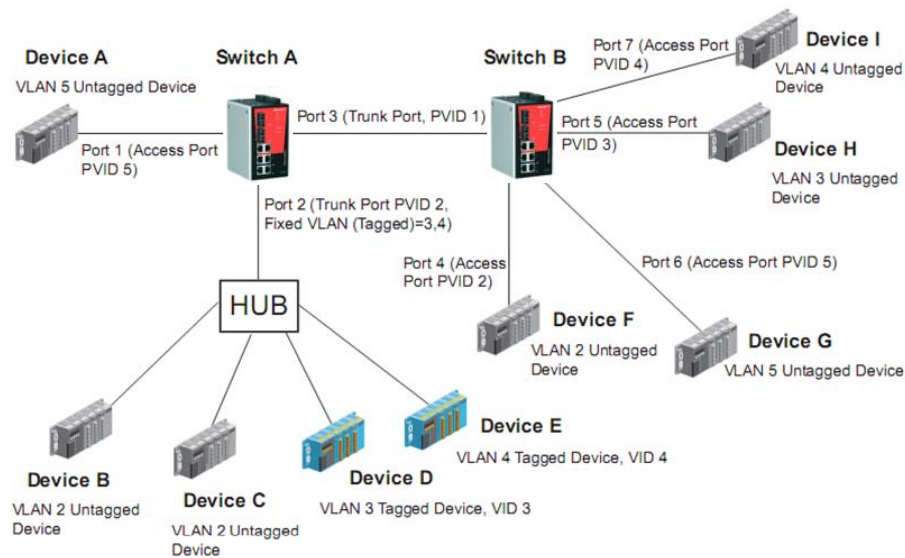
To carry multiple VLANs across a single physical (backbone, trunk) link, each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong to which VLAN. To communicate between VLANs, a router must be used.

The IE-SW-PL09M-GB supports two types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that determines to which VLAN the device belongs. Once the ingress packet of this Access Port egresses to another Trunk Port (the port reswitch all packets to carry tag information), the IE-SW-PL09M-GB will insert this PVID into this packet to help the next 802.1Q VLAN switch recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices/tagged devices and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the port default PVID as its VID.

The following section illustrates how to use these ports to set up different applications.

Sample Applications of VLANs using Weidmueller IE-SW-PL09M-GB



In this application,

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as “Access Port” with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as “Trunk Port” with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port can only belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as “Trunk Port.” GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as “Access Port” with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as “Access Port” with PVID 3.
- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as “Access Port” with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as “Access Port” with PVID 4.

After proper configuration:

- Packets from device A will travel through “Trunk Port 3” with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by device G, and vice versa.
- Packets from device B and C will travel through “Trunk Port 3” with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by device F, and vice versa.

- Packets from device D will travel through “Trunk Port 3” with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by device H. Packets from device H will travel through “Trunk Port 3” with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device D.
- Packets from device E will travel through “Trunk Port 3” with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by device I. Packets from device I will travel through “Trunk Port 3” with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device E.

Configuring Virtual LAN

VLAN Settings

To configure the IE-SW-PL09M-GB’s **802.1Q VLAN**, use the VLAN Settings page to configure the ports.

802.1Q VLAN Settings

VLAN Mode: 802.1Q VLAN

Management VLAN ID: 1

Enable GVRP:

| Port | Type | PVID | Fixed VLAN (Tagged) | Forbidden VLAN |
|------|--------|------|---------------------|----------------|
| 1 | Access | 1 | | |
| 2 | Access | 1 | | |
| 3 | Access | 1 | | |
| 4 | Access | 1 | | |
| 5 | Access | 1 | | |
| 6 | Access | 1 | | |
| 7 | Access | 1 | | |
| 8 | Access | 1 | | |

VLAN Mode

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

Management VLAN ID

| Setting | Description | Factory Default |
|-------------------------------|---|-----------------|
| VLAN ID ranges from 1 to 4094 | Set the management VLAN of this IE-SW-PL09M-GB. | 1 |

Enable GVRP

| Setting | Description | Factory Default |
|----------------|--|-----------------|
| Enable/Disable | Select the option to enable/disable the GVRP | Enable |

| | | |
|--|----------|--|
| | function | |
|--|----------|--|

Port Type

| Setting | Description | Factory Default |
|---------|--|-----------------|
| Access | This port type is used to connect single devices without tags. | Access |
| Trunk | Select "Trunk" port type to connect another 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs. | |

**ATTENTION**

For communication redundancy in the VLAN environment, set "Redundant Port," "Coupling Port," and "Coupling Control Port" as "Trunk Port," since these ports act as the "backbone" to transmit all packets of different VLANs to different IE-SW-PL09M-GB units.

Port PVID

| Setting | Description | Factory Default |
|--------------------------|---|-----------------|
| VID range from 1 to 4094 | Set the port default VLAN ID for untagged devices that connect to the port. | 1 |

Fixed VLAN List (Tagged)

| Setting | Description | Factory Default |
|--------------------------|--|-----------------|
| VID range from 1 to 4094 | This field will be active only when selecting the "Trunk" port type. Set the other VLAN ID for tagged devices that connect to the "Trunk" port. Use commas to separate different VIDs. | None |

Forbidden VLAN List

| Setting | Description | Factory Default |
|--------------------------|---|-----------------|
| VID range from 1 to 4094 | This field will be active only when selecting the "Trunk" port type. Set the VLAN IDs that will not be supported by this trunk port. Use commas to separate different VIDs. | None |

To configure the IE-SW-PL09M-GB's Port-based VLAN, use the VLAN Setting page to configure the ports.

Port-based VLAN Settings

VLAN Mode Port-based VLAN

| VLAN | Port | G5 | G6 | G7 | G8 | G9 | Trk1 |
|------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <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"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | <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"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

VLAN Mode

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

Port

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

VLAN Table

VLAN Table

VLAN Mode
VLAN Mode 802.1Q VLAN

Management VLAN
Management VLAN 1

Current 802.1Q VLAN List

| Index | VID | Joined Access Port | Joined Trunk Port |
|-------|-----|---------------------------|-------------------|
| 1 | 1 | G5, G6, G7, G8, G9, Trk1, | |

In 802.1Q VLAN table, you can review the VLAN groups that were created, Joined Access Ports, and Trunk Ports, and in Port-based VLAN table, you can review the VLAN group and Joined port.

NOTE The physical network can have a maximum of 64 VLAN settings.

Using Multicast Filtering

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

implemented on your IE-SW-PL09M-GB.

The Concept of Multicast Filtering

What is an IP Multicast?

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

Benefits of Multicast

The benefits of using IP multicast are that it:

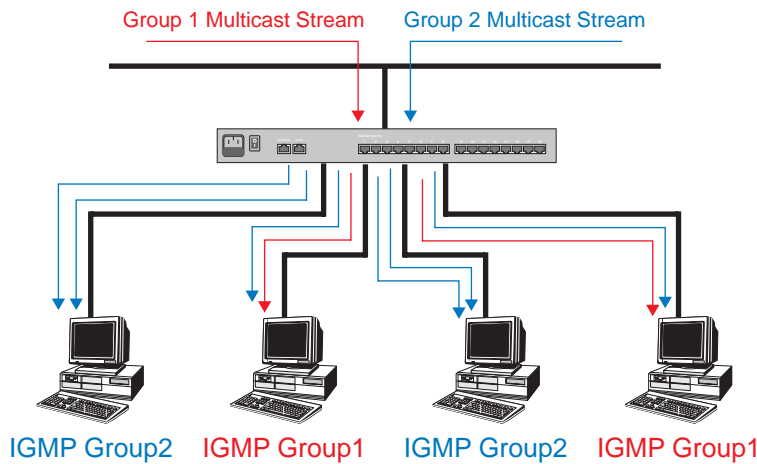
- Uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- Reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- Makes efficient use of network bandwidth and scales well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

Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all end-stations would cause a substantial reduction in network performance. Furthermore, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use multicast. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

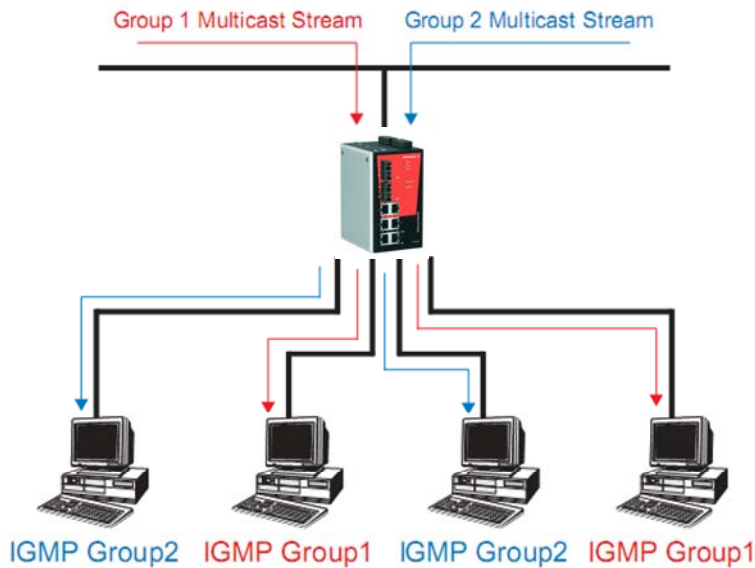
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves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

Network without multicast filtering



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

Network with multicast filtering



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

Multicast Filtering and Weidmueller Ethernet Switches

The IE-SW-PL09M-GB has three ways to achieve multicast filtering: IGMP (Internet Group Management Protocol) Snooping, GMRP (GARP Multicast Registration Protocol), and adding a static multicast MAC manually to filter multicast traffic automatically.

IGMP (Internet Group Management Protocol)

Snooping Mode

Snooping Mode allows your switch to forward multicast packets only to the appropriate

ports. The switch “snoops” on exchanges between hosts and an IGMP device, such as a router, to find those ports that want to join a multicast group, and then configures its filters accordingly.

Query Mode

Query mode allows the IE-SW-PL09M-GB to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs. IGMP querying is enabled by default on the IE-SW-PL09M-GB to help prevent interoperability issues with some multicast routers that may not follow the lowest IP address election method. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers).

| | |
|------|--|
| NOTE | The IE-SW-PL09M-GB is compatible with any device that conforms to the IGMP v2 device protocol. |
|------|--|

IGMP Multicast Filtering

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

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

GMRP (GARP Multicast Registration Protocol)

The IE-SW-PL09M-GB supports IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol), which differs from IGMP (Internet Group Management Protocol). GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or de-register Group membership information dynamically. GMRP functions similarly to GVRP, except that GMRP registers multicast addresses on ports. When a port receives a **GMRP-join** message, it will register the multicast address to its database if the multicast address is not registered, and all the multicast packets with that multicast address are able to be forwarded from this port. When a port receives a **GMRP-leave** message, it will de-register the multicast address from its database, and all the multicast packets with this multicast address are not able to be forwarded from this port.

Static Multicast MAC

Some devices may only support multicast packets, but not support either IGMP Snooping or GMRP. The IE-SW-PL09M-GB supports adding multicast groups manually to enable multicast filtering.

Enabling Multicast Filtering

Use the serial console or Web interface to enable or disable IGMP Snooping and IGMP querying. If IGMP Snooping is not enabled, then IP multicast traffic is always forwarded, flooding the network.

Configuring IGMP Snooping

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

IGMP Snooping Settings

IGMP Snooping Setting

Current VLAN List

IGMP Snooping Enable Query Interval (s)

IGMP Snooping Enhanced Mode

| Index | VID | IGMP Snooping | Querier | Static Multicast Querier Port | | | | | | | |
|-------|-----|--|--|-------------------------------|----------------------------|----------------------------|----------------------------|----------------------------|----------------------------|----------------------------|----------------------------|
| 1 | 1 | <input checked="" type="checkbox"/> Enable | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> 1 | <input type="checkbox"/> 2 | <input type="checkbox"/> 3 | <input type="checkbox"/> 4 | <input type="checkbox"/> 5 | <input type="checkbox"/> 6 | <input type="checkbox"/> 7 | <input type="checkbox"/> 8 |

IGMP Snooping Enable

| Setting | Description | Factory Default |
|----------------|--|-----------------|
| Enable/Disable | Select the option to enable the IGMP Snooping function globally . | Disabled |

IGMP Snooping Enhanced Mode

| Setting | Description | Factory Default |
|---------|---|-----------------|
| Enable | IGMP Multicast packets will forward to : <ul style="list-style-type: none"> Learned Multicast Querier Ports Member Ports | Enable |
| Disable | IGMP Multicast packets will forward to : <ul style="list-style-type: none"> Learned multicast Querier Ports Static Multicast Querier Ports Querier Connected Ports Member Ports | |

Query Interval

| Setting | Description | Factory Default |
|-------------------------------|---|-----------------|
| Numerical value input by user | Set the query interval of the Querier function globally. Valid settings are from 20 to 600 seconds. | 125 seconds |

IGMP Snooping

| Setting | Description | Factory Default |
|----------------|--|---|
| Enable/Disable | Select the option to enable the IGMP Snooping function per VLAN . | Enabled if IGMP Snooping Enabled Globally |

NOTE **We suggest the following IGMP Snooping configurations-**

- **When the network is mixed with third party switches, such as Cisco:**
 - IGMP Snooping Enable:
 - IGMP Snooping Enhanced Mode:
- **When the network consists entirely of Weidmueller switches:**
 - IGMP Snooping Enable:
 - IGMP Snooping Enhanced Mode:

Querier

| Setting | Description | Factory Default |
|----------------|--|--|
| Enable/Disable | Select the option to enable the IE-SW-PL09M-GB's querier function. | Enabled if IGMP Snooping is Enabled Globally |

Static Multicast Router Port

| Setting | Description | Factory Default |
|-----------------|--|-----------------|
| Select/Deselect | Select the option to select which ports will connect to the multicast routers. It's active only when IGMP Snooping is enabled. | Disabled |

NOTE At least one switch must be designated the Querier or enable IGMP snooping and GMRP when enabling Turbo Ring and IGMP snooping simultaneously.

IGMP Table

The IE-SW-PL09M-GB displays the current active IGMP groups that were detected.

| Current Active IGMP Groups | | | | | | | |
|----------------------------|-------------------------------------|-------------------------------|------------------------|----------------|--------------------|-----|--------------|
| VID | Auto Learned Multicast Querier Port | Static Multicast Querier Port | Querier Connected Port | Act as Querier | Active IGMP Groups | | |
| | | | | | IP | MAC | Members Port |
| | | | | | | | |

The information includes **VID**, **Auto-learned Multicast Router Port**, **Static Multicast Router Port**, **Querier Connected Port**, and the **IP** and **MAC** addresses of active IGMP groups.

Add Static Multicast MAC

If required, the IE-SW-PL09M-GB also supports adding multicast groups manually.

Static Multicast MAC Address
 Current Static Multicast MAC Address List

| All | Index | MAC Address | Join Port |
|---------------|-------|-------------|-----------|
| Remove Select | | | |

Add New Static Multicast MAC Address to the List

MAC Address - - - - -

Join Port 1 2 3 4 5 6 7 8

Activate

Add New Static Multicast Address to the List

| Setting | Description | Factory Default |
|-------------|---|-----------------|
| MAC Address | Input the multicast MAC address of this host. | None |

MAC Address

| Setting | Description | Factory Default |
|---------|---|-----------------|
| integer | Input the number of the VLAN to which the host with this MAC Address belongs. | None |

Join Port

| Setting | Description | Factory Default |
|-----------------|---|-----------------|
| Select/Deselect | Select the appropriate options to select the join ports for this multicast group. | None |

Configuring GMRP

GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or un-register Group membership information dynamically.

GMRP Settings

| Port | GMRP |
|------|---------------------------------|
| 1 | <input type="checkbox"/> Enable |
| 2 | <input type="checkbox"/> Enable |
| 3 | <input type="checkbox"/> Enable |
| 4 | <input type="checkbox"/> Enable |
| 5 | <input type="checkbox"/> Enable |
| 6 | <input type="checkbox"/> Enable |
| 7 | <input type="checkbox"/> Enable |
| 8 | <input type="checkbox"/> Enable |

Activate

GMRP enable

| Setting | Description | Factory Default |
|----------------|--|-----------------|
| Enable/Disable | Select the option to enable the GMRP function for the port listed in the Port column | Disable |

GMRP Table

The IE-SW-PL09M-GB displays the current active GMRP groups that were detected.

GMRP Status

| Multicast Address | Fixed Ports | Learned Ports |
|-------------------|-------------|---------------|
| | | |

| Setting | Description |
|---------------|--|
| Fixed Ports | This multicast address is defined by static multicast. |
| Learned Ports | This multicast address is learned by GMRP. |

Using Bandwidth Management

In general, one host should not be allowed to occupy unlimited bandwidth, particularly when the device malfunctions. For example, so-called “**broadcast storms**” could be caused by an incorrectly configured topology, or a malfunctioning device. The IE-SW-PL09M-GB series not only prevents broadcast storms, but can also be configured to a different ingress rate for all packets, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

Traffic Rate Limiting Settings

Traffic Rate Limiting Settings

Ingress

| Port | Policy | Priority Queue Rate | | | |
|------|-----------------|---------------------|--------|--------|------|
| | | Low | Normal | Medium | High |
| 1 | Limit Broadcast | 8M | 8M | 8M | 8M |
| 2 | Limit Broadcast | 8M | 8M | 8M | 8M |
| 3 | Limit Broadcast | 8M | 8M | 8M | 8M |
| 4 | Limit Broadcast | 8M | 8M | 8M | 8M |
| 5 | Limit Broadcast | 8M | 8M | 8M | 8M |
| 6 | Limit Broadcast | 8M | 8M | 8M | 8M |

Activate

Ingress

| Setting | Description | Factory Default |
|--------------|---|-----------------|
| Ingress rate | Select the ingress rate for all packets from the following options: Not Limited, 128K, 256K, 512K, 1M, 2M, 4M, 8M | N/A |

Using Port Access Control

The IE-SW-PL09M-GB provides two kinds of Port-Based Access Controls. One is Static Port Lock and the other is IEEE 802.1X.

Static Port Lock

The IE-SW-PL09M-GB can also be configured to protect static MAC addresses for a specific port. With the Port Lock function, these locked ports will not learn any additional addresses, but only allow traffic from preset static MAC addresses, helping to block crackers and careless usage.

IEEE 802.1X

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

The IEEE 802.1X Concept

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

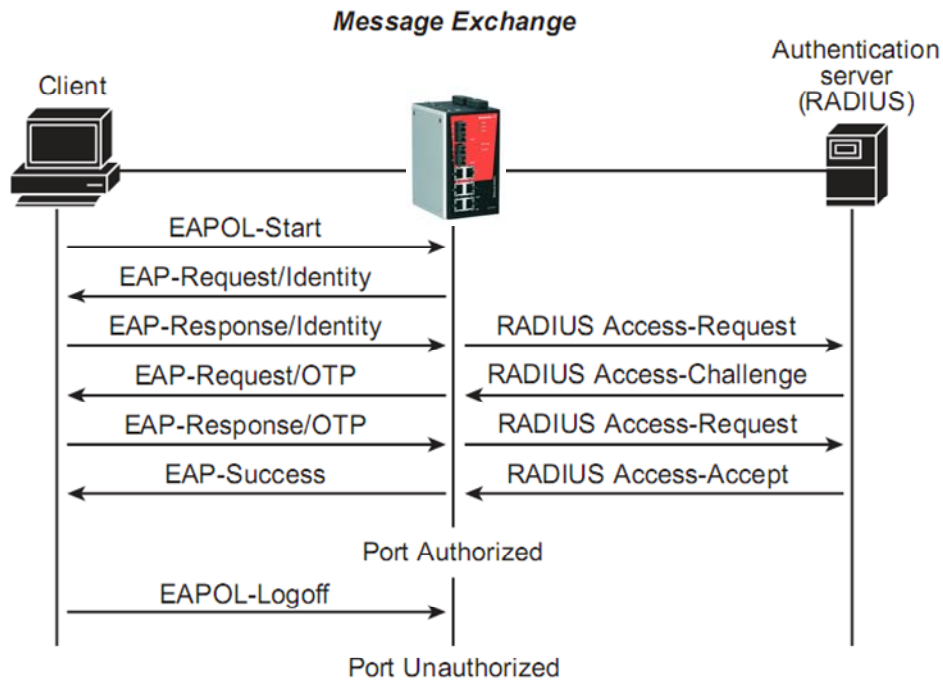
Supplicant: The end station that requests access to the LAN and switch services and responds to the requests from the switch.

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

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

The IE-SW-PL09M-GB acts as an authenticator in the 802.1X environment. A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server, or implement the authentication server in the IE-SW-PL09M-GB by using a Local User Database as the authentication look-up table. When we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames between each other.

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



1. When the supplicant receives an “EAP Request/Identity” frame, it sends an “EAP Response/Identity” frame with its username back to the authenticator.
2. If the RADIUS server is used as the authentication server, the authenticator relays the “EAP Response/Identity” frame from the supplicant by encapsulating it into a “RADIUS Access-Request” frame and sends to the RADIUS server. When the authentication server receives the frame, it looks up its database to check if the username exists. If the username is not present, the authentication server replies with a “RADIUS Access-Reject” frame to the authenticator if the server is a RADIUS server or just indicates failure to the authenticator if the Local User Database is used. The authenticator sends an “EAP-Failure” frame to the supplicant.
3. The RADIUS server sends a “RADIUS Access-Challenge,” which contains an “EAP Request” with an authentication type to the authenticator to ask for the password from the client. RFC 2284 defines several EAP authentication types, such as “MD5-Challenge,” “One-Time Password,” and “Generic Token Card.” Currently, only “MD5-Challenge” is supported. If the Local User Database is used, this step is skipped.
4. The authenticator sends an “EAP Request/MD5-Challenge” frame to the supplicant. If the RADIUS server is used, the “EAP Request/MD5-Challenge” frame is retrieved directly from the “RADIUS Access-Challenge” frame.
5. The supplicant responds to the “EAP Request/MD5-Challenge” by sending an “EAP Response/MD5-Challenge” frame that encapsulates the user’s password using the MD5 hash algorithm.
6. If the RADIUS server is used as the authentication server, the authenticator relays the “EAP Response/MD5-Challenge” frame from the supplicant by encapsulating it into a “RADIUS Access-Request” frame along with a “Shared Secret,” which must be the same within the authenticator and the RADIUS server, and sends the frame to the RADIUS server. The RADIUS server checks against the password with its database,

and replies with “RADIUS Access-Accept” or “RADIUS Access-Reject” to the authenticator. If the Local User Database is used, the password is checked against its database and indicates success or failure to the authenticator.

- The authenticator sends “EAP Success” or “EAP Failure” based on the reply from the authentication server.

Configuring Static Port Lock

The IE-SW-PL09M-GB supports adding unicast groups manually if required.

Static Port Lock

Add Static Unicast MAC Address

MAC Address - - - - -

Port

| Setting | Description | Factory Default |
|-------------|--|-----------------|
| MAC Address | Add the static unicast MAC address into the address table. | None |
| Port | Fix the static address with a dedicated port. | 1 |

Configuring IEEE 802.1X

802.1X Settings

Database Option Re-Auth

Radius Server Re-Auth Period

Server Port

Shared Key

| Port | 802.1X |
|------|---------------------------------|
| 1 | <input type="checkbox"/> Enable |
| 2 | <input type="checkbox"/> Enable |
| 3 | <input type="checkbox"/> Enable |
| 4 | <input type="checkbox"/> Enable |
| 5 | <input type="checkbox"/> Enable |
| 6 | <input type="checkbox"/> Enable |
| 7 | <input type="checkbox"/> Enable |
| 8 | <input type="checkbox"/> Enable |

Database Option

| Setting | Description | Factory Default |
|-----------------------|--|-----------------|
| Local (Max. 32 users) | Select this option when setting the Local User Database as the authentication database. | Local |
| Radius | Select this option to set an external RADIUS server as the authentication database. The authentication | Local |

| | | |
|---------------|--|-------|
| | mechanism is "EAP-MD5." | |
| Radius, Local | Select this option to make an external RADIUS server as the authentication database with first priority. The authentication mechanism is "EAP-MD5." The first priority is to set the Local User Database as the authentication database. | Local |

Radius Server

| Setting | Description | Factory Default |
|---------------------------|--|-----------------|
| IP address or domain name | The IP address or domain name of the RADIUS server | localhost |

Server Port

| Setting | Description | Factory Default |
|-----------|-----------------------------------|-----------------|
| Numerical | The UDP port of the RADIUS Server | 1812 |

Shared Key

| Setting | Description | Factory Default |
|-----------------------------------|---|-----------------|
| alphanumeric (Max. 40 characters) | A key to be shared between the external RADIUS server and the IE-SW-PL09M-GB. Both ends must be configured to use the same key. | None |

Re-Auth

| Setting | Description | Factory Default |
|----------------|--|-----------------|
| Enable/Disable | Select to require re-authentication of the client after a preset time period of no activity has elapsed. | Disable |

Re-Auth Period

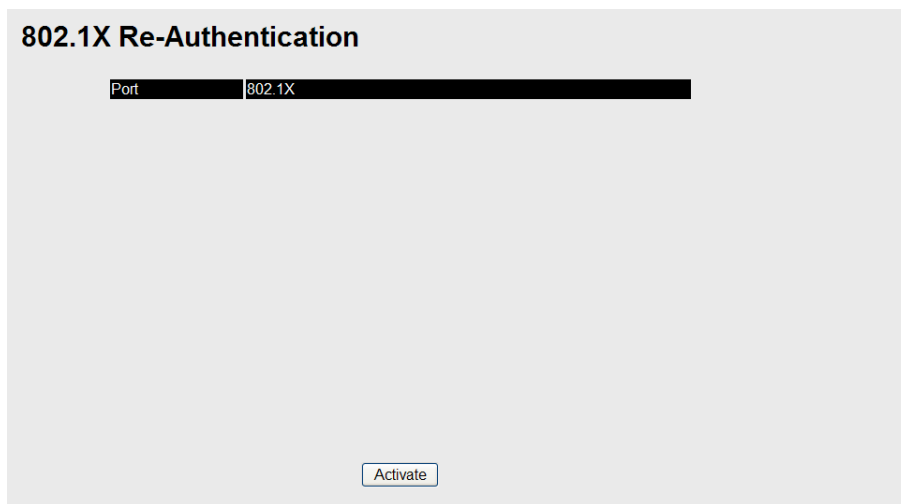
| Setting | Description | Factory Default |
|---------------------------|---|-----------------|
| Numerical (60-65535 sec.) | Specify how frequently the end stations need to reenter usernames and passwords in order to stay connected. | 3600 |

802.1X

| Setting | Description | Factory Default |
|----------------|---|-----------------|
| Enable/Disable | Select the option under the 802.1X column to enable IEEE 802.1X for one or more ports. All end stations must enter usernames and passwords before access to these ports is allowed. | Disable |

802.1X Re-Authentication

The IE-SW-PL09M-GB can force connected devices to be re-authorized manually.

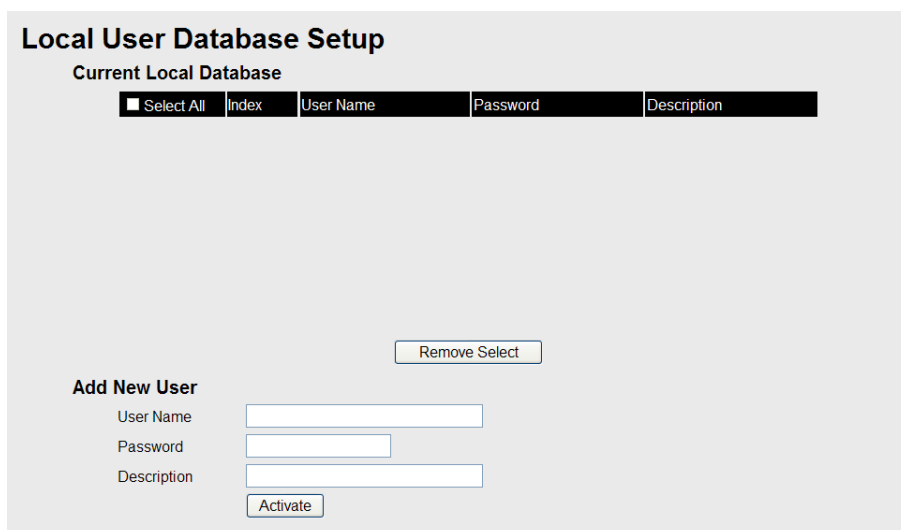


802.1X Re-Authentication

| Setting | Description | Factory Default |
|----------------|--|-----------------|
| Enable/Disable | Select the option to enable 802.1X Re-Authentication | Disable |

Local User Database Setup

When setting the Local User Database as the authentication database, set the database first.



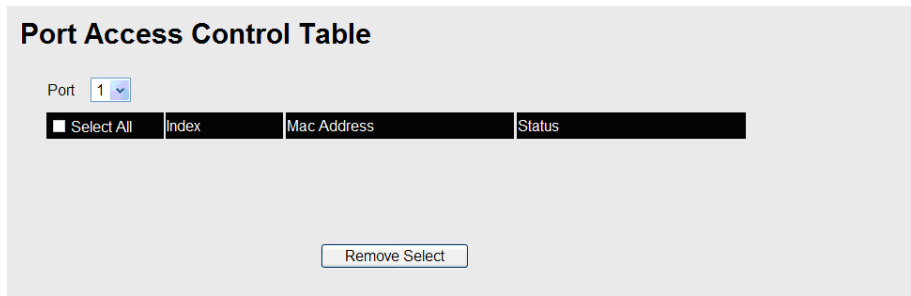
Local User Database Setup

| Setting | Description | Factory Default |
|-----------|-----------------------------------|-----------------|
| User Name | User Name for Local User Database | None |

| | | |
|-------------------------------------|-------------------------------------|------|
| (Max. 30 characters) | | |
| Password (Max. 16 characters) | Password for Local User Database | None |
| Description (Max. 30 characters) | Description for Local User Database | None |

NOTE The user name for the Local User Database is case-insensitive.

Port Access Control Table



The port status will indicate whether the access is authorized or unauthorized.

Using Auto Warning

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 IE-SW-PL09M-GB supports different approaches to warn engineers automatically, such as by using email and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms using email and relay output.

Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place.

Three basic steps are required to set up the Auto Warning function:

1. **Configuring Email Event Types**
 Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Email Alarm Events setting* subsection).
2. **Configuring Email Settings**
 To configure the IE-SW-PL09M-GB's email setup from the Console interface or browser interface, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address to which warning messages will be sent.

- 3. Activate your settings and if necessary, test the email**
 After configuring and activating your IE-SW-PL09M-GB's Event Types and Email Setup, you can use the **Test Email** function to see if your e-mail addresses and mail server address have been properly configured.

Event Type

Email Warning Events Settings

System Events

Switch Cold Start
 Switch Warm Start
 Power Transition(On->Off)
 Power Transition(Off->On)
 DI 1(Off)
 DI 1(On)
 DI 2(Off)
 DI 2(On)
 Config. Change
 Auth. Failure
 Comm. Redundancy Topology Changed

Port Events

| Port | Link-ON | Link-OFF | Traffic-Overload | Rx-Threshold(%) | Traffic-Duration(s) |
|------|--------------------------|--------------------------|--------------------------|--------------------------------|--------------------------------|
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> | <input type="text" value="1"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> | <input type="text" value="1"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> | <input type="text" value="1"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> | <input type="text" value="1"/> |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> | <input type="text" value="1"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> | <input type="text" value="1"/> |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> | <input type="text" value="1"/> |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> | <input type="text" value="1"/> |

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.

| System Events | Warning e-mail is sent when... |
|-----------------------------------|---|
| Switch Cold Start | Power is cut off and then reconnected. |
| Switch Warm Start | The IE-SW-PL09M-GB is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.). |
| Power Transition (On→Off) | The device is powered down. |
| Power Transition (Off→On) | The device is powered up. |
| DI1 (On→Off) | Digital Input 1 is triggered by on to off transition |
| DI1 (Off→On) | Digital Input 1 is triggered by off to on transition |
| DI2 (On→Off) | Digital Input 2 is triggered by on to off transition |
| DI2 (Off→On) | Digital Input 2 is triggered by off to on transition |
| Configuration Change Activated | A configuration item has been changed. |
| Authentication Failure | An incorrect password is entered. |
| Comm. Redundancy Topology Changed | Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). The Master of the Turbo Ring has changed or the backup path is activated. |

| Port Events | Warning e-mail is sent when... |
|-------------------------|---|
| Link-ON | The port is connected to another device. |
| Link-OFF | The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down). |
| Traffic-Overload | The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled). |
| Traffic-Threshold (%) | Enter a non-zero number if the port's Traffic-Overload item is Enabled. |
| Traffic-Duration (sec.) | A Traffic-Overload warning is sent every <i>Traffic-Duration</i> seconds if the average Traffic-Threshold is surpassed during that time period. |

NOTE The **Traffic-Overload**, **Traffic-Threshold (%)**, and **Traffic-Duration (sec.)** Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a non-zero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

NOTE Warning e-mail messages will have the **sender** field formatted in the form:
Managed_Switch_0001@Switch_Location
 where **Managed_Switch** is the default Switch Name, **0001** is the IE-SW-PL09M-GB's serial number, and **Switch_Location** is the default Server Location.
 Refer to the Basic **Settings** section to see how to modify Switch Name and Switch Location.

Email Setup

Email Warning Events Settings

Mail Server IP/Name:

SMTP Port:

Account Name :

Account Password :

Change Account Password

Old Password :

New Password :

Retype Password :

1st email address :

2nd email address :

3rd email address :

4th email address :

Mail Server IP/Name

| Setting | Description | Factory Default |
|------------|--------------------------------------|-----------------|
| IP address | The IP Address of your email server. | None |

Account Name

| Setting | Description | Factory Default |
|--------------------|--|-----------------|
| Max. 45 Characters | Your email account name (typically your user name) | None |

Password Setting

| Setting | Description | Factory Default |
|-----------------------------------|--|-----------------|
| Disable/Enable to change Password | To reset the Password from the Web Browser interface, click the Change password check-box, type the Old Password, type the New Password, retype the New password, and then click Activate; Max. 45 Characters. | Disable |
| Old Password | Type the current password when changing the password | None |
| New Password | Type new password when enabled to change password; Max. 45 Characters. | None |
| Retype Password | If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password. | None |

Email Address

| Setting | Description | Factory Default |
|--------------------|--|-----------------|
| Max. 30 characters | You can set up to 4 email addresses to receive alarm emails from the IE-SW-PL09M-GB. | None |

Send Test Email

After configuring the email settings, you should first click **Activate** to activate those settings, and then click **Send Test Email** to verify that the settings are correct.

NOTE Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PLAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism.

We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.

Configuring Relay Warning

The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

1. **Configuring Relay Event Types**
Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Relay Alarm Events setting*)

subsection).

2. **Activate your settings**

After completing the configuration procedure, you will need to activate your IE-SW-PL09M-GB's Relay Event Types.

Event Setup

Relay Warning Events Settings

System Events

Override Relay 1 Warning Settings Override Relay 2 Warning Settings

Power Input 1 failure(On->Off) Power Input 2 failure(On->Off)

DI 1 (Off) DI 2 (Off)

DI 1 (On) DI 2 (On)

Turbo Ring Break

Port Events

| Port | Link | Traffic-Overload | Rx-Threshold(%) | Traffic-Duration(s) |
|------|---------------------------------------|--|--------------------------------|--------------------------------|
| 1 | <input type="button" value="Ignore"/> | <input type="button" value="Disable"/> | <input type="text" value="1"/> | <input type="text" value="1"/> |
| 2 | <input type="button" value="Ignore"/> | <input type="button" value="Disable"/> | <input type="text" value="1"/> | <input type="text" value="1"/> |
| 3 | <input type="button" value="Ignore"/> | <input type="button" value="Disable"/> | <input type="text" value="1"/> | <input type="text" value="1"/> |
| 4 | <input type="button" value="Ignore"/> | <input type="button" value="Disable"/> | <input type="text" value="1"/> | <input type="text" value="1"/> |
| 5 | <input type="button" value="Ignore"/> | <input type="button" value="Disable"/> | <input type="text" value="1"/> | <input type="text" value="1"/> |
| 6 | <input type="button" value="Ignore"/> | <input type="button" value="Disable"/> | <input type="text" value="1"/> | <input type="text" value="1"/> |
| 7 | <input type="button" value="Ignore"/> | <input type="button" value="Disable"/> | <input type="text" value="1"/> | <input type="text" value="1"/> |
| 8 | <input type="button" value="Ignore"/> | <input type="button" value="Disable"/> | <input type="text" value="1"/> | <input type="text" value="1"/> |

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. The IE-SW-PL09M-GB supports two relay outputs. You can configure which relay output is related to which events. This helps administrators identify the importance of the different events.

| System Events | Warning Relay output is triggered when... |
|-------------------------------------|---|
| Power Transition (On→Off) | The device is powered on. |
| Power Transition (Off→On) | The device is powered down. |
| DI1 (On→Off) | Digital Input 1 is triggered by on to off transition |
| DI1 (Off→On) | Digital Input 1 is triggered by off to on transition |
| DI2 (On→Off) | Digital Input 2 is triggered by on to off transition |
| DI2 (Off→On) | Digital Input 2 is triggered by off to on transition |
| Turbo Ring Break (Ring Master Only) | When the IE-SW-PL09M-GB is the Master of this Turbo Ring, and the Turbo Ring is disconnected. |

| Port Events | Warning e-mail is sent when... |
|-----------------------|---|
| Link-ON | The port is connected to another device. |
| Link-OFF | The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down). |
| Traffic-Overload | The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled). |
| Traffic-Threshold (%) | Enter a non-zero number if the port's Traffic-Overload item is Enabled. |

| | |
|-------------------------|---|
| Traffic-Duration (sec.) | A Traffic-Overload warning is sent every <i>Traffic-Duration</i> seconds if the average Traffic-Threshold is surpassed during that time period. |
|-------------------------|---|

NOTE The **Traffic-Overload**, **Traffic-Threshold (%)**, and **Traffic-Duration (sec)** Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a non-zero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

Override relay alarm settings

Select this option to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition.

Warning List

Use this table to see if any relay alarms have been issued.

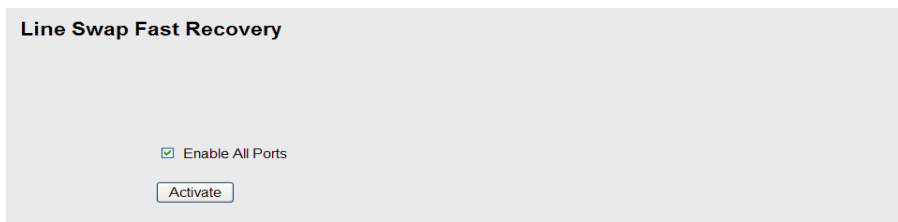
Current Warning List

| Index | Event | Relay |
|-------|-------|-------|
| | | |

Using Line-Swap-Fast-Recovery

The Line-Swap Fast Recovery function, which is enabled by default, allows the IE-SW-PL09M-GB to return to normal operation extremely quickly after devices are unplugged and then re-plugged into different ports. The recovery time is on the order of a few milliseconds (compare this with standard commercial switches for which the recovery time could be on the order of several minutes). To disable the Line-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access either the Console utility's **Line-Swap recovery** page, or the Web Browser interface's **Line-Swap fast recovery** page, as the following figure shows:

Configuring Line-Swap Fast Recovery



Enable Line-Swap-Fast-Recovery

| Setting | Description | Factory Default |
|----------------|---|-----------------|
| Enable/Disable | Select this option to enable the Line-Swap-Fast-Recovery function | Enable |

Using Set Device IP

To reduce the effort required to set up IP addresses, the IE-SW-PL09M-GB series comes equipped with DHCP/BOOTP server and RARP protocol to set up IP addresses of Ethernet-enabled devices automatically.

When enabled, the **Set device IP** function allows the IE-SW-PL09M-GB to assign specific IP addresses automatically to connected devices that are equipped with *DHCP Client* or *RARP* protocol. In effect, the IE-SW-PL09M-GB 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 IE-SW-PL09M-GB sends the device the desired IP address.

Perform the following steps to use the **Set device IP** function:

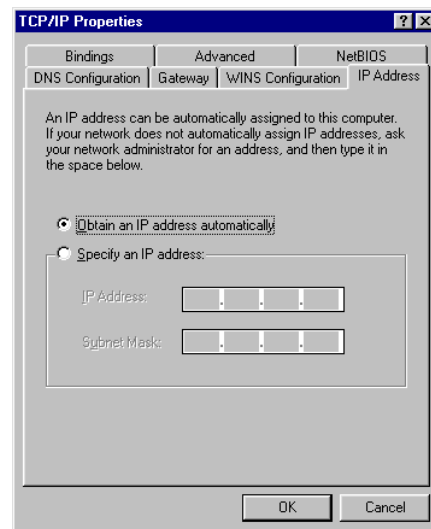
STEP 1—set up the connected devices

Set up those Ethernet-enabled devices connected to the IE-SW-PL09M-GB for which you would like IP addresses to be assigned automatically. The devices must be configured to *obtain* their IP address automatically.

The devices' configuration utility should include a setup page that allows you to choose an option similar to **Obtain an IP address automatically**.

For example, Windows' **TCP/IP Properties** window is shown at the right. Although your device's configuration utility may look quite a bit different, this figure should give you some idea of what to look for.

You also need to decide to which of the IE-SW-PL09M-GB's ports your Ethernet-enabled devices will be connected. You will need to set up each of these ports separately, as described in the following step.



STEP 2

Configure the IE-SW-PL09M-GB's **Set device IP** function, either from the Console utility or from the Web Browser interface. In either case, you simply need to enter the **Desired IP** for each port that neswitch to be configured.

STEP 3

Be sure to activate your settings before exiting.

- When using the Web Browser interface, activate by clicking **Activate**.
- When using the Console utility, activate by first highlighting the **Activate** menu option, and then press **Enter**. You should receive the **Set device IP settings are now active! (Press any key to continue)** message.

Configuring Set Device IP

Automatic Set Device IP by DHCP/BootP/RARP

| Port | Device's current IP | Active function | Desired IP address |
|------|---------------------|-----------------|----------------------|
| G1 | NA | -- | <input type="text"/> |
| G2 | NA | -- | <input type="text"/> |
| G3 | NA | -- | <input type="text"/> |
| G4 | NA | -- | <input type="text"/> |
| G5 | NA | -- | <input type="text"/> |
| G6 | NA | -- | <input type="text"/> |
| G7 | NA | -- | <input type="text"/> |
| G8 | NA | -- | <input type="text"/> |
| G9 | NA | -- | <input type="text"/> |

Desired IP Address

| Setting | Description | Factory Default |
|------------|--|-----------------|
| IP Address | Set the desired IP of connected devices. | None |

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.

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—a combination of physical port number and VLAN ID. The format of the "Circuit ID" is as described below:

FF-VV-VV-PP

Where the first byte "FF" is fixed to "01", the second and the third byte "VV-VV" is formed by the port VLAN ID in hex, and the last byte "PP" is formed by the port number in hex. For example,

01-00-0F-03 is the "Circuit ID" of port number 3 with port VLAN ID 15.

The "Remote ID" is to identify the relay agent itself and it can be one of the following:

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

DHCP Relay Agent

Server IP Address

1st Server

2nd Server

3rd Server

4th Server

DHCP Option 82

Enable Option 82

Type

Value

Display

DHCP Function Table

| Port | Circuit-ID | Option 82 |
|------|------------|---------------------------------|
| 1 | 01000101 | <input type="checkbox"/> Enable |
| 2 | 01000102 | <input type="checkbox"/> Enable |
| 3 | 01000103 | <input type="checkbox"/> Enable |
| 4 | 01000104 | <input type="checkbox"/> Enable |
| 5 | 01000105 | <input type="checkbox"/> Enable |
| 6 | 01000106 | <input type="checkbox"/> Enable |
| 7 | 01000107 | <input type="checkbox"/> Enable |

Server IP Address

1st Server

| Setting | Description | Factory Default |
|------------------------------------|---|-----------------|
| IP address for the 1st DHCP server | This assigns the IP address of the 1st DHCP server that the switch tries to access. | None |

2nd Server

| Setting | Description | Factory Default |
|------------------------------------|---|-----------------|
| IP address for the 2nd DHCP server | This assigns the IP address of the 2nd DHCP server that the switch tries to access. | None |

3rd Server

| Setting | Description | Factory Default |
|------------------------------------|---|-----------------|
| IP address for the 3rd DHCP server | This assigns the IP address of the 3rd DHCP server that the switch tries to access. | None |

4th Server

| Setting | Description | Factory Default |
|------------------------------------|---|-----------------|
| IP address for the 4th DHCP server | This assigns the IP address of the 4th DHCP server that the switch tries to access. | None |

DHCP Option 82

Enable Option82

| Setting | Description | Factory Default |
|-------------------|--|-----------------|
| Enable or Disable | Enable or disable DHCP Option 82 function. | Disable |

Type

| Setting | Description | Factory Default |
|-----------|---|-----------------|
| IP | Use switch IP address as the remote ID sub-option. | IP |
| MAC | Use switch MAC address as the remote ID sub-option. | IP |
| Client-ID | Use the combination of switch MAC address and IP address as the remote ID sub-option. | IP |
| Other | Use the user-defined value as the remote ID sub-option. | IP |

Value

| Setting | Description | Factory Default |
|--------------------|---|-------------------|
| | Displays the value which you've set. | |
| Max. 12 characters | If you set the type as Other, you will have to fill it. | switch IP address |

Display

| Setting | Description | Factory Default |
|---------|---|-----------------|
| | The actual hexadecimal value set at the DHCP server for the Remote-ID. This value is automatically generated according to the Value field. Users can not modify it. | COA87FFD |

DHCP Function Table

Enable

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

Using Diagnosis

The IE-SW-PL09M-GB provides two important tools for administrators to diagnose network systems.

Mirror Port

The screenshot shows a configuration window titled "Mirror Port Settings". It contains three labels on the left: "Monitored port", "Watch direction", and "Mirror port". Each label is followed by a dropdown menu. The "Watch direction" dropdown is currently set to "Bi-directional". Below these dropdowns is a button labeled "Activate".

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

Perform the following steps to set up the **Mirror Port** function:

STEP 1

Configure the IE-SW-PL09M-GB's **Mirror Port** function from either the Console utility or Web Browser interface. You will need to configure three settings:

Monitored Port Select the port number of the port whose network activity will be monitored.

Mirror Port Select the port number of the port that will be used to monitor the activity of the monitored port.

Watch Direction Select one of the following three watch direction options:

- **Input data stream**
Select this option to monitor only those data packets coming *in through* the IE-SW-PL09M-GB's port.
- **Output data stream**
Select this option to monitor only those data packets being sent *out through* the IE-SW-PL09M-GB's port.
- **Bi-directional**
Select this option to monitor data packets both coming *into*, and being sent *out through*, the IE-SW-PL09M-GB's port.

STEP 2

Be sure to activate your settings before exiting.

- When using the Web Browser interface, activate by clicking **Activate**.
- When using the Console utility, activate by first highlighting the Activate menu option, and then press **Enter**. You should receive the **Mirror port settings are now active! (Press any key to continue)** message.

Ping

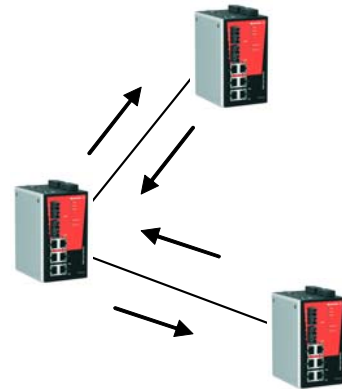


The **Ping** function uses the *ping* command to give users a simple but powerful tool for troubleshooting network problems. The function’s most unique feature is that even though the ping command is entered from the user’s PC keyboard, the actual ping command originates from the IE-SW-PL09M-GB itself. In this way, the user can essentially control the IE-SW-PL09M-GB and send ping commands out through its ports.

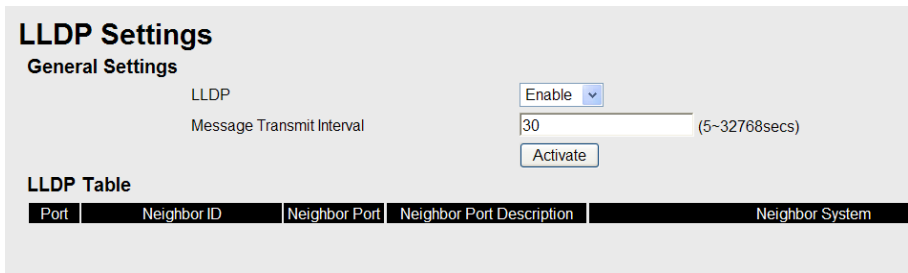
To use the Ping function, type in the desired IP address, and then press **Enter** from the Console utility, or click **Ping** when using the Web Browser interface.

LLDP Function 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.



LLDP Web Interface



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 Weidmueller’s MXview to automatically display the network’s topology as well as system setup details such as VLAN, and Trunking for the entire network.

LLDP Settings

Enable LLDP

| Setting | Description | Factory Default |
|-------------------|----------------------------------|-----------------|
| Enable or Disable | Enable or disable LLDP function. | Enable |

Value

| Setting | Description | Factory Default |
|---------------------------|--|-----------------|
| Numbers from 5~32768 secs | To set the transmit interval of LLDP messages. Unit is in seconds. | 30 (seconds) |

LLDT Table

| Port | Neighbor ID | Neighbor Port | Neighbor Port Description | Neighbor System |
|------|-------------|---------------|---------------------------|-----------------|
| | | | | |

Port: The port number that connects to the neighbor device.

Neighbor ID: A unique entity which identifies a neighbor device; this is typically the MAC address.

Neighbor Port: The port number of the neighbor device.

Neighbor Port Description: A textual description of the neighbor device's interface.

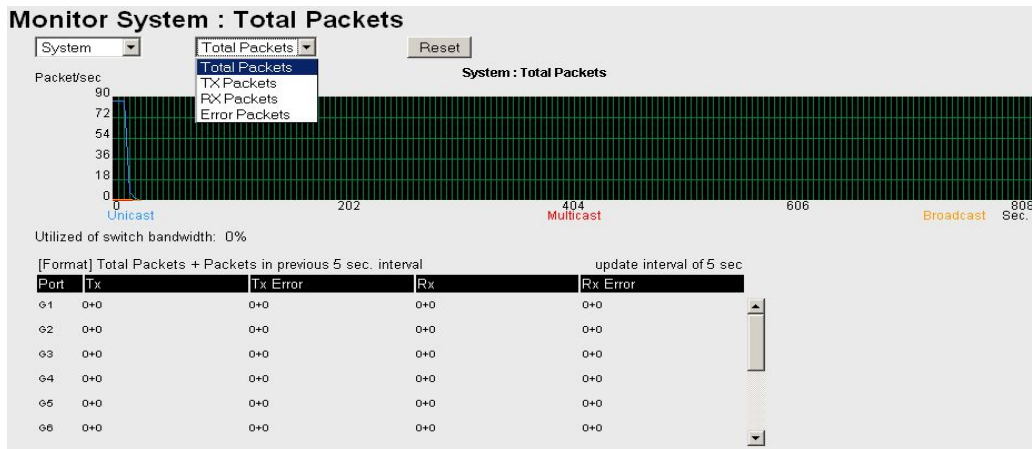
Neighbor System: Hostname of the neighbor device.

Using Monitor

You can monitor statistics in real time from the IE-SW-PL09M-GB's web console and serial console.

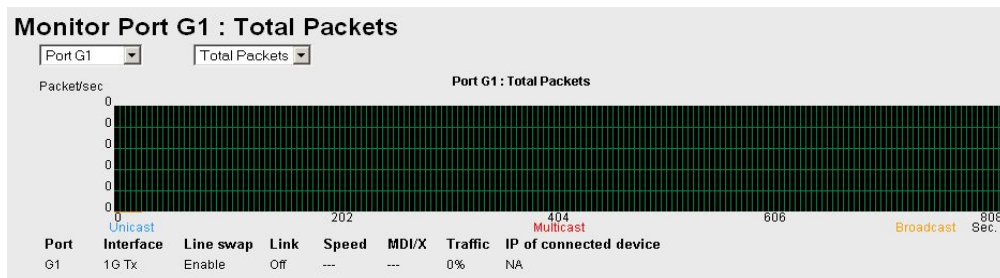
Monitor by Switch

Access the Monitor by selecting "System" from the left selection bar. Monitor by System allows the user to view a graph that shows the combined data transmission activity of all the IE-SW-PL09M-GB's 18 ports. Click one of the four options—**Total Packets**, **TX Packets**, **RX Packets**, or **Error Packets**—to view transmission activity of specific types of packets. Recall that TX Packets are packets sent out from the IE-SW-PL09M-GB, RX Packets are packets received from connected devices, and Error Packets are packets that did not pass TCP/IP's error checking algorithm. The Total Packets option displays a graph that combines TX, RX, and TX Error, RX Error Packets activity. The graph displays data transmission activity by showing **Packets/s** (i.e., packets per second, or pps) versus **sec.** (seconds). In fact, three curves are displayed on the same graph: **Unicast** packets (in red color), **Multicast** packets (in green color), and **Broadcast** packets (in blue color). The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



Monitor by Port

Access the Monitor by Port function by selecting **ALL 10/100M or 1G Ports** or **Port *i***, in which ***i* = 1, 2, ..., G2**, from the left pull-down list. The **Port *i*** options are identical to the Monitor by System function discussed above, in that users can view graphs that show All Packets, TX Packets, RX Packets, or Error Packets activity, but in this case, only for an individual port. The **All Ports** option is essentially a graphical display of the individual port activity that can be viewed with the Console Monitor function discussed above. The All Ports option shows three vertical bars for each port. The height of the bar represents **Packets/s** for the type of packet, at the instant the bar is being viewed. That is, as time progresses, the height of the bar moves up or down so that the user can view the change in the rate of packet transmission. The blue colored bar shows **Unicast** packets, the red colored bar shows **Multicast** packets, and the orange colored bar shows **Broadcast** packets. The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



Using the MAC Address Table

This section explains the information provided by the IE-SW-PL09M-GB's MAC address table.

All MAC Address List

All Page 1/1

| Index | MAC | Type | Port |
|-------|-------------------|----------|------|
| 1 | 00-21-27-d8-da-d0 | ucast(l) | G9 |

The MAC Address table can be configured to display the following IE-SW-PL09M-GB MAC address groups.

| | |
|----------------------|--|
| ALL | Select this item to show all IE-SW-PL09M-GB MAC addresses |
| ALL Learned | Select this item to show all IE-SW-PL09M-GB Learned MAC addresses |
| ALL Static Lock | Select this item to show all IE-SW-PL09M-GB Static Lock MAC addresses |
| ALL Static | Select this item to show all IE-SW-PL09M-GB Static/Static Lock /Static Multicast MAC addresses |
| ALL Static Multicast | Select this item to show all IE-SW-PL09M-GB Static Multicast MAC addresses |
| Port x | Select this item to show all MAC addresses of dedicated ports |

The table will display the following information:

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

Using Event Log

Event Log Table

Page 15/16

| Index | Bootup | Date | Time | System Startup Time | Event |
|-------|--------|------------|----------|---------------------|--------------------------------|
| 211 | 46 | -- | -- | 0d0h0m0s | Cold start |
| 212 | 46 | -- | -- | 0d0h0m41s | Port G9 link on |
| 213 | 46 | -- | -- | 0d0h1m31s | 192.168.1.254 admin Auth. ok |
| 214 | 46 | -- | -- | 0d0h12m11s | Port G9 link off |
| 215 | 46 | -- | -- | 3d19h41m40s | Port G9 link on |
| 216 | 46 | -- | -- | 3d19h45m23s | 192.168.1.254 admin Auth. ok |
| 217 | 46 | -- | -- | 3d22h36m1s | 192.168.1.254 admin Auth. ok |
| 218 | 46 | -- | -- | 4d1h38m47s | Port G9 link off |
| 219 | 46 | -- | -- | 4d22h49m20s | Port G9 link on |
| 220 | 46 | -- | -- | 4d22h50m29s | 192.168.1.254 admin Auth. ok |
| 221 | 46 | 2011/02/08 | 14:51:46 | 4d23h6m14s | Configuration change activated |
| 222 | 46 | 2011/02/08 | 15:14:08 | 4d23h28m36s | Configuration change activated |
| 223 | 46 | 2011/02/08 | 16:55:44 | 5d1h10m12s | 192.168.1.254 admin Auth. ok |
| 224 | 46 | 2011/02/08 | 17:50:40 | 5d2h5m8s | Port G9 link off |
| 225 | 46 | 2011/02/09 | 11:10:55 | 5d19h25m23s | Port G9 link on |

Clear

| | |
|--------|--|
| Bootup | This field shows how many times the IE-SW-PL09M-GB has been rebooted |
|--------|--|

| | |
|---------------------|---|
| | or cold started. |
| Date | The date is updated based on how the current date is set in the “Basic Setting” page. |
| Time | The time is updated based on how the current time is set in the “Basic Setting” page. |
| System Startup Time | The system startup time related to this event. |
| Events | Events that have occurred. |

NOTE The following events will be recorded into the IE-SW-PL09M-GB's Event Log table:

1. Cold start
2. Warm start
3. Configuration change activated
4. Power 1/2 transition (Off → On), Power 1/2 transition (On → Off)
5. Authentication fail
6. Topology changed
7. Master setting is mismatched
8. DI 1/2 transition (Off → On), DI 1/2 transition (On → Off)
9. Port traffic overload
10. dot1x Auth Fail
11. Port link off / on

Using Syslog

This function provides the event logs for the syslog server. The function supports 3 configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a syslog UDP packet to the specified syslog servers.

Syslog Settings

Syslog Server 1

Port Destination (1~65535)

Syslog Server 2

Port Destination (1~65535)

Syslog Server 3

Port Destination (1~65535)

Syslog Server 1

| Setting | Description | Factory Default |
|-------------------------------|---|-----------------|
| IP Address | Enter the IP address of 1st Syslog Server used by your network. | None |
| Port Destination (1 to 65535) | Enter the UDP port of 1st Syslog Server. | 514 |

Syslog Server 2

| Setting | Description | Factory Default |
|-------------------------------|---|-----------------|
| IP Address | Enter the IP address of 2nd Syslog Server used by your network. | None |
| Port Destination (1 to 65535) | Enter the UDP port of 2nd Syslog Server. | 514 |

Syslog Server 3

| Setting | Description | Factory Default |
|-------------------------------|---|-----------------|
| IP Address | Enter the IP address of 3rd Syslog Server used by your network. | None |
| Port Destination (1 to 65535) | Enter the UDP port of 3rd Syslog Server. | 514 |

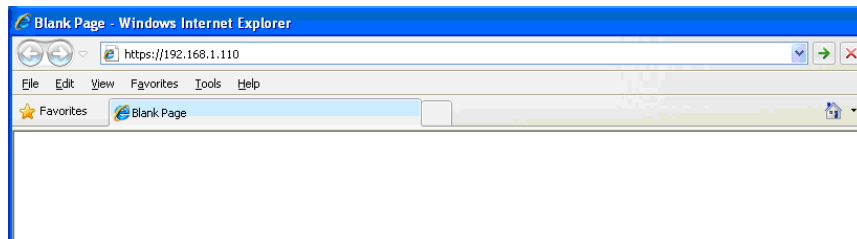
NOTE The following events will be recorded into the IE-SW-PL09M-GB's Event Log table, and will then be sent to the specified Syslog Server:

1. Cold start
2. Warm start
3. Configuration change activated
4. Power 1/2 transition (Off → On), Power 1/2 transition (On → Off)
5. Authentication fail
6. Topology changed
7. Master setting is mismatched
8. DI 1/2 transition (Off → On), DI 1/2 transition (On → Off)
9. Port traffic overload
10. dot1x Auth Fail
11. Port link off / on

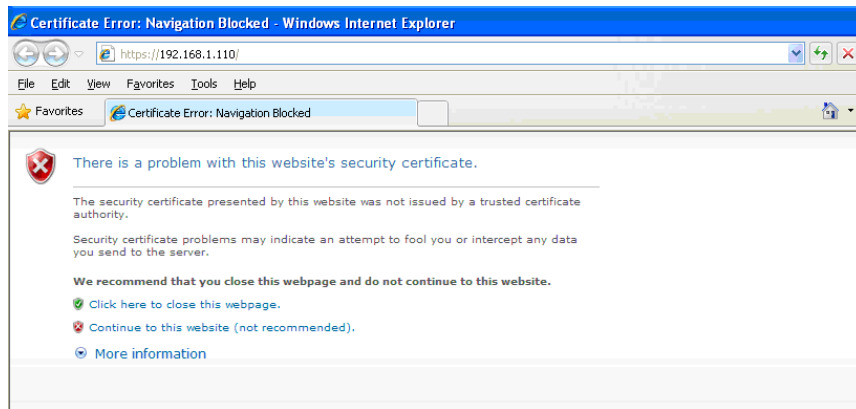
Using HTTPS/SSL

To secure your HTTP access, the IE-SW-PL09M-GB supports HTTPS/SSL to encrypt all HTTP traffic. Perform the following steps to access the web browser interface via HTTPS/SSL.

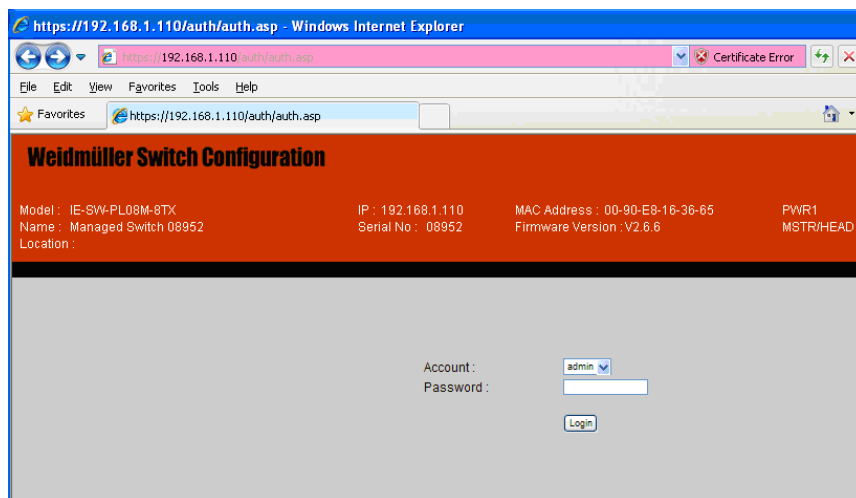
1. Open Internet Explorer and type **https://<IE-SW-PL09M-GB's IP address>** in the address field. Press Enter to establish the connection.



- 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 **Yes** to enter the IE-SW-PL09M-GB's web browser interface and access the web browser interface secured via HTTPS/SSL.



4

Weidmüller Switch Configuration Utility

The Weidmüller Switch configuration utility (WM_Switch_Utility.exe) is a comprehensive Windows-based GUI that can be used to configure and maintain multiple Weidmüller managed switches.

A suite of useful functions is available to help you

- to locate Ethernet Switches which are attached to the same LAN as the PC host (regardless of whether or not you know the IP addresses of the switches),
- to connect to an Ethernet Switch whose IP address is known,
- to modify the network configurations of one or multiple Ethernet Switches
- and to update the firmware of one or more Ethernet Switches.

The Weidmüller Switch Configuration Utility is designed to provide you with instantaneous control of your Ethernet Switches regardless of location. You may download the Weidmüller Switch Configuration Utility software from Weidmüller's website free of charge.

The following topics are covered in this chapter:

- Starting**
- Broadcast Search**
- Search by IP address**
- Upgrade Firmware**
- Modify IP Address**
- Export Configuration**
- Import Configuration**
- Unlock the Ethernet Switch**

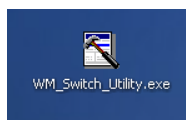
Starting Weidmüller SWITCH Configuration Utility

To start the Weidmüller Switch Configuration Utility, locate and then run the executable file **WM_Switch_UTILITY.exe**.

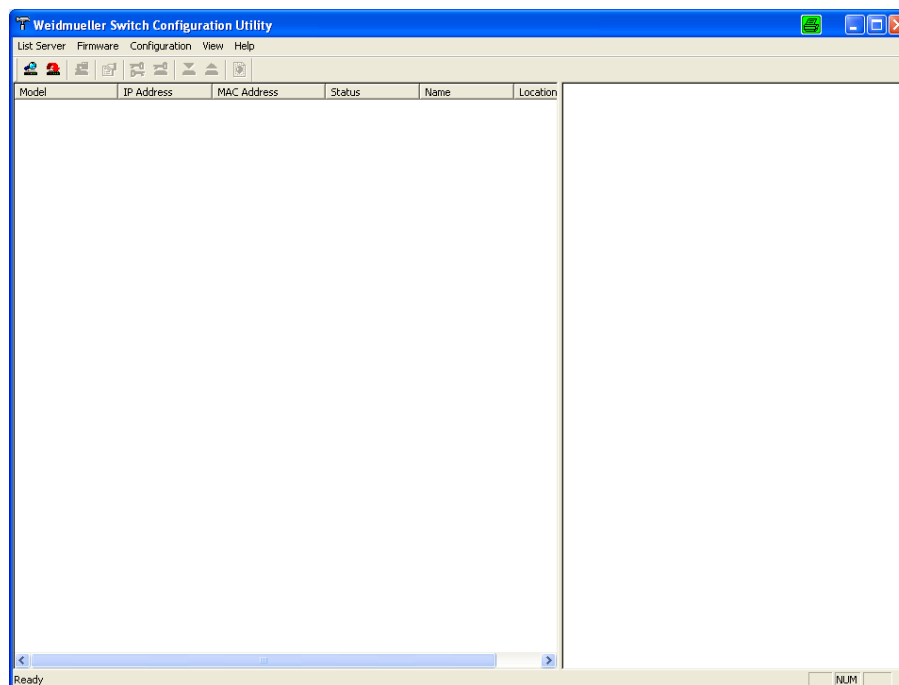
NOTE You may download the Weidmüller Switch Configuration Utility from the Weidmüller website using the following path:

1. Open www.Weidmueller.com/Downloads
 2. Select page "Software"
 3. Select page "Industrial Ethernet"
 4. Select category "Value and Premium Line managed Switches – Software Tools"
- Download "Weidmueller Switch Configuration Utility"

For example, if the file was placed on the Windows desktop, it should appear as follows. Simply double click on the icon to run the program.




The Weidmüller Switch Configuration Utility window will open, as shown below.

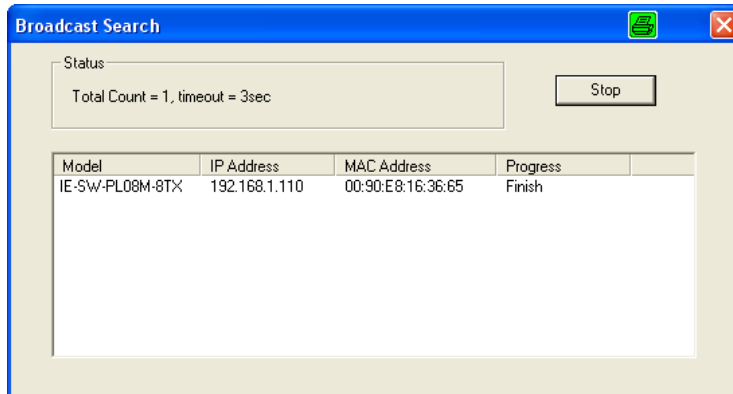


Broadcast Search

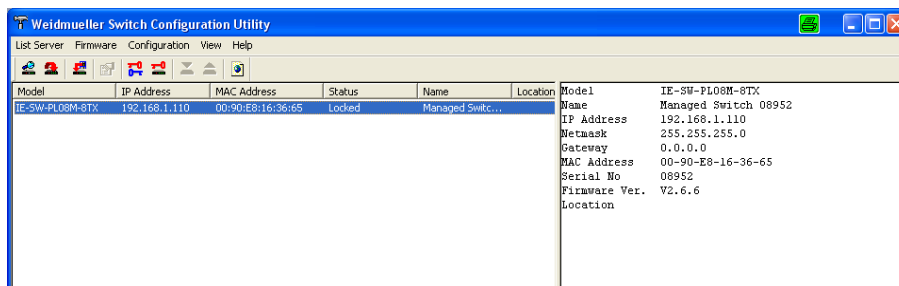
Use the Broadcast Search utility to search the LAN for all IE-SW-PL09M-GB switches

that are connected to the LAN. Note that since the search is done by MAC address, Broadcast Search will not be able to locate Weidmueller Ethernet Switches connected outside the PC host's LAN. Start by clicking the Broadcast Search icon , or by selecting **Broadcast Search** under the **List Server** menu.

The Broadcast Search window will open, displaying a list of all switches located on the network, as well as the progress of the search.




Once the search is complete, the Configurator window will display a list of all switches that were located.

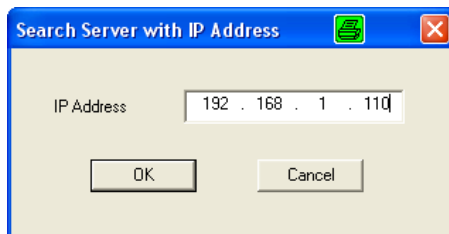


Search by IP address

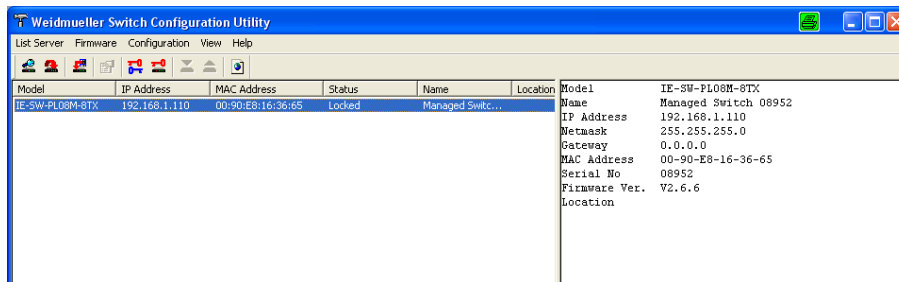
This utility is used to search for IE-SW-PL09M-GB switches one at a time. Note that the search is conducted by IP address, so you should be able to locate any IE-SW-PL09M-GB that is properly connected to your LAN, WAN, or even the Internet.

Start by clicking the Specify by IP address icon , or by selecting **Specify IP address** under the **List Server** menu.

The **Search Server with IP Address** window will open. Enter the IP address of the switch you wish to search for, and then click **OK**.



Once the search is complete, the Configurator window will add the switch to the list of switches.



Upgrade Firmware

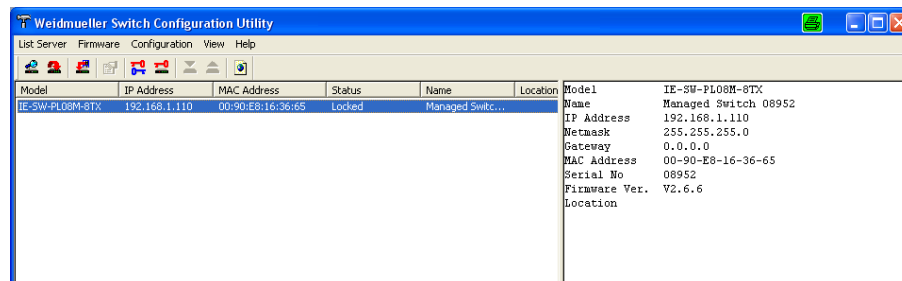
NOTE You may download the latest Firmware from the Weidmüller website using the following path:


1. Open www.Weidmueller.com/Downloads
2. Select page "Software"
3. Select page "Industrial Ethernet"
4. Select category "Value and Premium Line managed Switches – Firmware Updates"
5. Select the entry "IE-SW-PL09M-5GC-4GT" for Firmware download

Note: The unzipped Firmware file has the extension *.rom

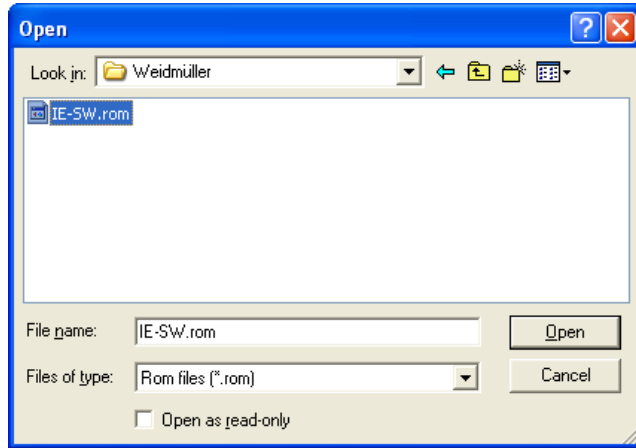
Keep your IE-SW-PL09M-GB up to date with the latest firmware from Weidmüller. Perform the following steps to upgrade the firmware:

1. Download the updated firmware (*.rom) file from the Weidmüller website (www.Weidmueller.com).
2. Click the switch (from the **Configurator** window) whose firmware you wish to upgrade to highlight it.




3. Click the **Upgrade Firmware** toolbar icon , or select **Upgrade** under the **Firmware** menu. If the switch is Locked, you will be prompted to input the switch's User Name and Password.

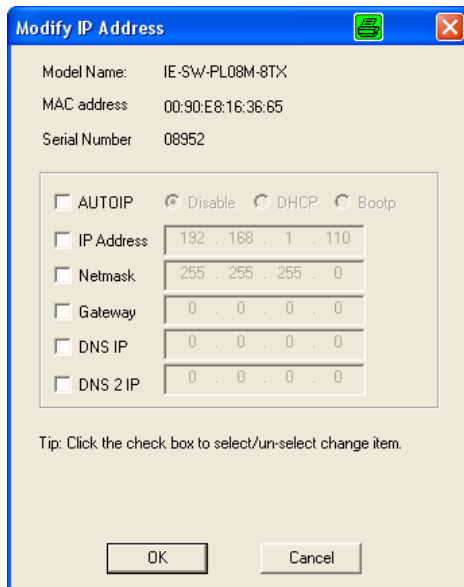
4. Use the **Open** window to navigate to the folder that contains the firmware upgrade file, and then click the correct “*.rom” file (**switch.rom** in the example shown below) to select the file. Click **Open** to activate the upgrade process.



Modify IP Address

You may use the Modify IP Address function to reconfigure IE-SW-PL09M-GB’s network settings. Start by clicking the Modify IP address icon , or by selecting **Modify IP address** under the **Configuration** menu.


The **Setup Configuration** window will open. Checkmark the box to the left of those items that you wish to modify, and then Disable or Enable DHCP, and enter IP Address, Subnet mask, Gateway, and DNS IP. Click **OK** to accept the changes to the configuration.

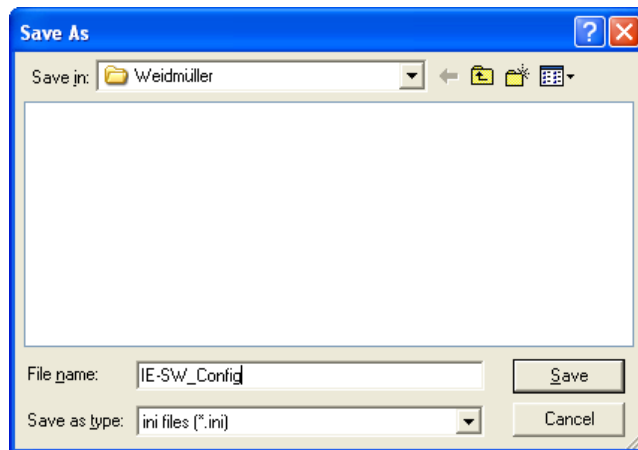


Export Configuration

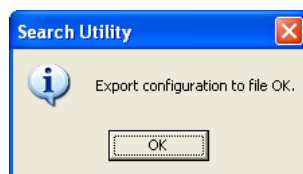
The **Export Configuration** utility is used to save the entire configuration of a particular IE-SW-PL09M-GB to a text file. Take the following steps to export a configuration:

1. Highlight the switch (from the Server list in the Configurator window’s left pane), and

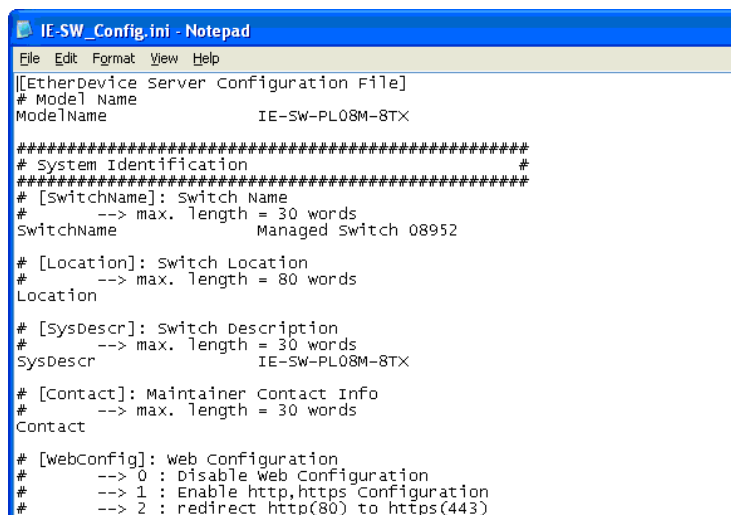
then click the **Export** toolbar icon  or select **Export Configuration** from the **Configuration** menu. Use the **Open** window to navigate to the folder in which you want to store the configuration, and then type the name of the file in the File name input box. Click **Open**.



2. Click **OK** when the **Export configuration to file OK** message appears.



3. You may use a standard text editor, such as Notepad under Windows, to view and modify the newly created configuration file.



```

IE-SW_Config.ini - Notepad
File Edit Format View Help
[[EtherDevice Server Configuration File]
# Model Name
ModelName                IE-SW-PL08M-8TX
#####
# System Identification
#####
# [SwitchName]: Switch Name
# --> max. length = 30 words
SwitchName                Managed Switch 08952

# [Location]: Switch Location
# --> max. length = 80 words
Location

# [SysDescr]: Switch Description
# --> max. length = 30 words
SysDescr                  IE-SW-PL08M-8TX

# [Contact]: Maintainer Contact Info
# --> max. length = 30 words
Contact


# [webConfig]: web configuration
# --> 0 : Disable web configuration
# --> 1 : Enable http,https configuration
# . --> 2 : redirect_http(80) to https(443)

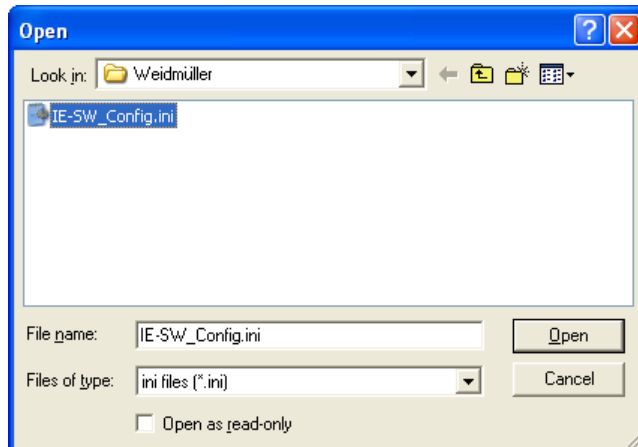
```

Import Configuration

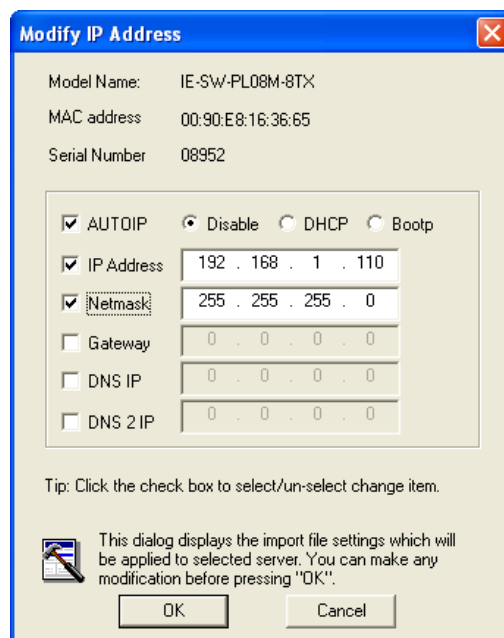
The **Import Configuration** function is used to import an entire configuration from a text

file to the IE-SW-PL09M-GB. This utility can be used to transfer the configuration from one IE-SW-PL09M-GB to another, by first using the Export Configuration function (described in the previous section) to save a switch configuration to a file, and then using the Import Configuration function. Perform the following steps to import a configuration:

1. Highlight the Switch in the Configurator window's left pane and then click the **Import** toolbar icon , or select **Import Configuration** from the **Configuration** menu.
2. Use the **Open** window to navigate to the text file that contains the desired configuration. Once the file is selected, click **Open** to initiate the import procedure.



3. The **Setup Configuration** window will be displayed, with a special note attached at the bottom. Parameters that have been changed will be activated with a checkmark. You may make more changes if necessary, and then click **OK** to accept the changes.




4. Click **Yes** in response to the following warning message to accept the new settings.



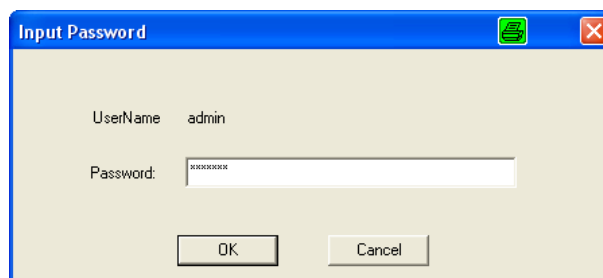
Unlock the Ethernet Switch

The Unlock function is used to open a password protected switch so that the user can modify its configuration, import/export a configuration, etc. There are six possible responses under the **Status** column. The **Status** of an IE-SW-PL09M-GB indicates how the switch was located (by Switch Configuration Utility), and what type of password protection it has.

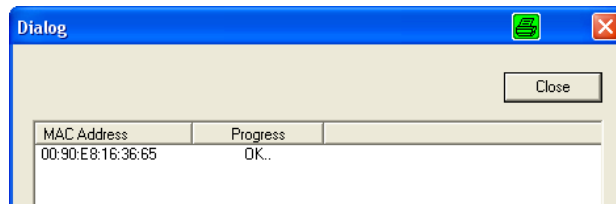
- **Locked**
The switch is password protected, “Broadcast Search” was used to locate it, and the password has not yet been entered from within the current Configurator session.
- **Unlocked**
The switch is password protected, “Broadcast Search” was used to locate it, and the password has been entered from within the current Configurator session. Henceforth during this Configurator session, activating various utilities for this switch will not require re-entering the server password.
- **Blank**
The IE-SW-PL09M-GB is not password protected, and “Broadcast Search” was used to locate it.

Follow the steps given below to unlock a locked IE-SW-PL09M-GB (i.e., an IE-SW-PL09M-GB with Status “Locked” or “Locked Fixed”). Highlight the server in the Configurator window’s left pane, and then click the **Unlock** toolbar icon , or select **Unlock** from the **Configuration** menu.

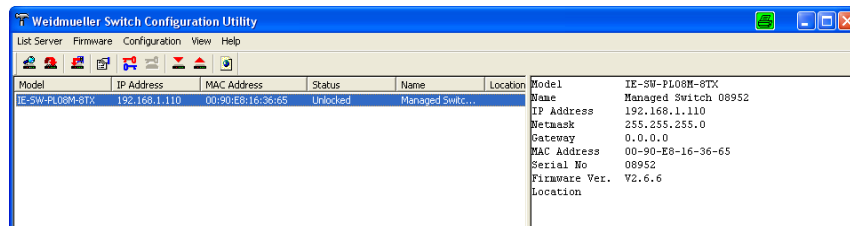
1. Enter the switch’s **User Name** and **Password** when prompted, and then click **OK**.



- When the **Unlock status** window reports Progress as **OK**, click the **Close** button in the upper right corner of the window.



- The status of the switch will now read **Unlocked**.



The IE-SW-PL09M-GB comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold/warm start trap, line up/down trap, and RFC 1213 MIB-II.

The standard MIB groups that the IE-SW-PL09M-GB series support are:

MIB II.1 – System Group

sysORTable

MIB II.2 – Interfaces Group

ifTable

MIB II.4 – IP Group

ipAddrTable

ipNetToMediaTable

IpGroup

IpBasicStatsGroup

IpStatsGroup

MIB II.5 – ICMP Group

IcmpGroup

IcmpInputStatus

IcmpOutputStats

MIB II.6 – TCP Group

tcpConnTable

TcpGroup

TcpStats

MIB II.7 – UDP Group

udpTable

UdpStats

MIB II.10 – Transmission Group

dot3

dot3StatsTable

MIB II.11 – SNMP Group

SnmpBasicGroup

SnmpInputStats

SnmpOutputStats

MIB II.17 – dot1dBridge Group

dot1dBase

dot1dBasePortTable

dot1dStp

dot1dStpPortTable

dot1dTp

dot1dTpFdbTable

dot1dTpPortTable

dot1dTpHCPortTable

dot1dTpPortOverflowTable

pBridgeMIB

dot1dExtBase

dot1dPriority

dot1dGarp

qBridgeMIB

dot1qBase

dot1qTp

dot1qFdbTable

dot1qTpPortTable

dot1qTpGroupTable

dot1qForwardUnregisteredTable

dot1qStatic

dot1qStaticUnicastTable

dot1qStaticMulticastTable

dot1qVlan

dot1qVlanCurrentTable

dot1qVlanStaticTable

dot1qPortVlanTable

The IE-SW-PL09M-GB also provides a private MIB file, located in the file "Weidmueller-PL09M-5GC-4GT.mib" on the IE-SW-PL09M-GB Series utility CD-ROM or downloadable from the Weidmueller website

Public Traps:

1. Cold Start
2. Link Up
3. Link Down
4. Authentication Failure
5. dot1dBridge New Root
6. dot1dBridge Topology Changed

Private Traps:

1. Configuration Changed
2. Power On
3. Power Off
4. Traffic Overloaded
5. Turbo Ring Topology Changed
6. Turbo Ring Coupling Port Changed
7. Turbo Ring Master Mismatch

Modbus information v1.0

Read Only Registers (Support Function Code 4) 1 Word = 2Bytes

| Address | Data Type | Description |
|---------------------------|-----------|---|
| System Information | | |
| 0x0000 | 1 word | Vendor ID = 0xFFFF |
| 0x0001 | 1 word | Unit ID (Ethernet = 1) |
| 0x0002 | 1 word | Product Code = 0x0006 |
| 0x0010 | 20 word | Vendor Name = "Weidmueller" Word 0 Hi byte = 'W' Word 0 Lo byte = 'e' Word 1 Hi byte = 'i' Word 1 Lo byte = 'd' Word 2 Hi byte = 'm' Word 2 Lo byte = 'u' Word 3 Hi byte = 'e' Word 3 Lo byte = 'l' Word 4 Hi byte = 'l' Word 4 Lo byte = 'e' Word 5 Hi byte = 'r' Word 5 Lo byte = '' Word 6 Hi byte = '\0' Word 6 Lo byte = '\0' |
| 0x0030 | 20 word | Product Name = "IE-SW-PL09M-GB" Word 0 Hi byte = 'I' Word 0 Lo byte = 'E' Word 1 Hi byte = '-' Word 1 Lo byte = 'S' Word 2 Hi byte = 'W' Word 2 Lo byte = '-' Word 3 Hi byte = 'P' Word 3 Lo byte = 'L' Word 4 Hi byte = '0' Word 4 Lo byte = '9' Word 5 Hi byte = 'M' Word 5 Lo byte = '-' Word 6 Hi byte = '\G' Word 6 Lo byte = '\B' |
| 0x0050 | 1 word | Product Serial Number |

| | | |
|-------------------------|--------|---|
| 0x0051 | 2 word | Firmware Version Word 0 Hi byte = major (A) Word 0 Lo byte = minor (B) Word 1 Hi byte = release (C) Word 1 Lo byte = build (D) |
| 0x0053 | 2 word | Firmware Release Date Firmware was released on 2007-05-06 at 09 o'clock Word 0 = 0x0609 Word 1 = 0x0705 |
| 0x0055 | 3 word | Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0x00 Word 0 Lo byte = 0x01 Word 1 Hi byte = 0x02 Word 1 Lo byte = 0x03 Word 2 Hi byte = 0x04 Word 2 Lo byte = 0x05 |
| 0x0058 | 1 word | Power 1 0x0000:Off 0x0001:On |
| 0x0059 | 1 word | Power 2 0x0000:Off 0x0001:On |
| 0x005A | 1 word | Fault LED Status 0x0000:No 0x0001:Yes |
| 0x0080 | 1 word | DI1 0x0000:Off 0x0001:On |
| 0x0081 | 1 word | DI2 0x0000:Off 0x0001:On |
| 0x0082 | 1 word | DO1 0x0000:Off 0x0001:On |
| 0x0083 | 1 word | DO2 0x0000:Off 0x0001:On |
| Port Information | | |
| 0x1000~0x1011 | 1 word | Port 1~10 Status 0x0000:Link down 0x0001:Link up 0x0002:Disable 0xFFFF:No port |
| 0x1100~0x1111 | 1 word | Port 1~10 Speed 0x0000:10M-Half 0x0001:10M-Full 0x0002:100M-Half 0x0003:100M-Full 0x0004:1G-Half 0x0005:1G- Full 0xFFFF:No port |

| | | |
|--|---------|---|
| 0x1200~0x1211 | 1 word | Port 1~10 Flow Ctrl 0x0000:Off 0x0001:On 0xFFFF:No port |
| 0x1300~0x1311 | 1 word | Port 1~10 MDI/MDIX 0x0000:MDI 0x0001:MDIX 0xFFFF:No port |
| 0x1400~0x1413(Port 1) 0x1414~0x1427(Port 2) | 20 word | Port 1~10 Description Port Description = "100TX,RJ45." Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '0' Word 1 Lo byte = 'T' ... Word 4 Hi byte = '4' Word 4 Lo byte = '5' Word 5 Hi byte = '.' Word 5 Lo byte = '\0' |
| Packet Information | | |
| 0x2000~0x2023 | 2 word | Port 1~10 Tx Packets Ex: port 1 Tx Packets = 0x44332211 Word 0 = 4433 Word 1 = 2211 |
| 0x2100~0x2123 | 2 word | Port 1~10 Rx Packets Ex: port 1 Rx Packets = 0x44332211 Word 0 = 4433 Word 1 = 2211 |
| 0x2200~0x2223 | 2 word | port 1~10 Tx Error Packets Ex: port 1 Tx Error Packets = 0x44332211 Word 0 = 4433 Word 1 = 2211 |
| 0x2300~0x2323 | 2 word | port 1~10 Rx Error Packets Ex: port 1 Rx Error Packets = 0x44332211 Word 0 = 4433 Word 1 = 2211 |
| Redundancy Information | | |
| 0x3000 | 1 word | Redundancy Protocol 0x0000:None 0x0001:RSTP 0x0002:Turbo Ring 0x0003:Turbo Ring V2 0x0004:Turbo Chain |
| 0x3100 | 1 word | RSTP Root 0x0000:Not Root 0x0001:Root 0xFFFF:RSTP Not Enable |

| | | |
|---------------|--------|--|
| 0x3200~0x3211 | 1 word | RSTP Port 1~10 Status 0x0000:Port Disabled 0x0001:Not RSTP Port 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:RSTP Not Enable |
| 0x3300 | 1 word | TR Master/Slave 0x0000:Slave 0x0001:Master 0xFFFF:Turbo Ring Not Enable |
| 0x3301 | 1 word | TR 1st Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding |
| 0x3302 | 1 word | TR 2nd Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding |
| 0x3303 | 1 word | TR Coupling 0x0000:Off 0x0001:On 0xFFFF:Turbo Ring Not Enable |
| 0x3304 | 1 word | TR Coupling Port status 0x0000:Port Disabled 0x0001:Not Coupling Port 0x0002:Link Down 0x0003:Blocked 0x0005:Forwarding 0xFFFF:Turbo Ring Not Enable |
| 0x3305 | 1 word | TR Coupling Control Port status 0x0000:Port Disabled 0x0001:Not Coupling Port 0x0002:Link Down 0x0003:Blocked 0x0005:Forwarding 0x0006:Inactive 0x0007:Active 0xFFFF:Turbo Ring Not Enable |
| 0x3500 | 1 word | TR2 Coupling Mode 0x0000:None 0x0001:Dual Homing 0x0002:Coupling Backup 0x0003:Coupling Primary 0xFFFF:Turbo Ring V2 Not Enable |

| | | |
|--------|--------|--|
| 0x3501 | 1 word | TR2 Coupling Port Primary status (Using in Dual Homing, Coupling Backup, Coupling Primary) 0x0000:Port Disabled 0x0001:Not Coupling Port 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Not Enable |
| 0x3502 | 1 word | TR2 Coupling Port Backup status (Only using in Dual Homing) 0x0000:Port Disabled 0x0001:Not Coupling Port 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Not Enable |
| 0x3600 | 1 word | TR2 Ring 1 status 0x0000:Healthy 0x0001:Break 0xFFFF:Turbo Ring V2 Not Enable |
| 0x3601 | 1 word | TR2 Ring 1 Master/Slave 0x0000:Slave 0x0001:Master 0xFFFF:Turbo Ring V2 Ring 1 Not Enable |
| 0x3602 | 1 word | TR2 Ring 1 1st Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Ring 1 Not Enable |
| 0x3603 | 1 word | TR2 Ring 1 2nd Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Ring 1 Not Enable |
| 0x3680 | 1 word | TR2 Ring 2 status 0x0000:Healthy 0x0001:Break 0xFFFF:Turbo Ring V2 Ring 2 Not Enable |
| 0x3681 | 1 word | TR2 Ring 2 Master/Slave 0x0000:Slave 0x0001:Master 0xFFFF:Turbo Ring V2 Ring 2 Not Enable |

| | | |
|--------|--------|--|
| 0x3682 | 1 word | TR2 Ring 2 1st Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Ring 2 Not Enable |
| | | |
| 0x3700 | 1 word | Turbo Chain Switch Role 0x0000:Head 0x0001:Member 0x0002:Tail 0xFFFF: Turbo Chain Not Enable |
| 0x3701 | 1 word | Turbo Chain 1st Port status 0x0000: Link Down 0x0001: Blocking 0x0002: Blocked 0x0003: Forwarding 0xFFFF:Turbo Ring V2 Ring 2 Not Enable |
| 0x3702 | 1 word | Turbo Chain 2nd Port status 0x0000: Link Down 0x0001: Blocking 0x0002: Blocked 0x0003: Forwarding 0xFFFF:Turbo Ring V2 Ring 2 Not Enable |

