TECHDOCS

Manual

WAGO ETHERNET Accessories 852

852-0603

Industrial Managed Switch

8 Ports 100BASE-TX, 2 x 1000BASE-SX/LX, PROFINET; EXT

1.0.0

WAGO Kontakttechnik GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69

E-Mail: info@wago.com

Web: www.wago.com

Technical Support

Phone: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

E-Mail: support@wago.com

Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail: documentation@wago.com

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Notes about this Documentation

Note

Always retain this documentation!
This documentation is part of the product. Therefore, retain the documentation during the entire service life of the product. Pass on the documentation to any subsequent user. In addition, ensure that any supplement to this documentation is included, if necessary.

1.1 Validity of this Documentation

This documentation is only applicable to WAGO ETHERNET accessory products “Industrial Managed Switch” (852-0603).

1.2 Copyright

1.3 Symbols

⚠ DANGER

Personal Injury!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.

⚠ DANGER

Personal Injury Caused by Electric Current!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.

⚠ WARNING

Personal Injury!
Indicates a moderate-risk, potentially hazardous situation which, if not avoided, could result in death or serious injury.

⚠ CAUTION

Personal Injury!
Indicates a low-risk, potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

NOTICE

Damage to Property!
Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

NOTICE

Damage to Property Caused by Electrostatic Discharge (ESD)!
Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

Note

Important Note!
Indicates a potential malfunction which, if not avoided, however, will not result in damage to property.

Information

Additional Information:
Refers to additional information which is not an integral part of this documentation (e.g., the Internet).

1.4 Number Notation

Table 1: Number Notation

Number Code	Example	Note
Decimal	100	Normal notation
Hexadecimal	0x64	C notation
Binary	'100' '0110.0100'	In quotation marks, nibble separated with dots (.)

1.5 Font Conventions

Table 2: Font Conventions

Font Type	Indicates
italic	Names of paths and data files are marked in italic-type. e.g.: *C:\Program Files\WAGO Software*
Menu	Menu items are marked in bold letters. e.g.: **Save**
>	A greater-than sign between two names means the selection of a menu item from a menu. e.g.: **File** > **New**
Input	Designation of input or optional fields are marked in bold letters, e.g.: **Start of measurement range**
“Value”	Input or selective values are marked in inverted commas. e.g.: Enter the value “4 mA” under **Start of measurement range**.
[Button]	Pushbuttons in dialog boxes are marked with bold letters in square brackets. e.g.: **[Input]**
[Key]	Keys are marked with bold letters in square brackets. e.g.: **[F5]**

2 Important Notes

This section includes an overall summary of the most important safety requirements and notes that are mentioned in each individual section. To protect your health and prevent damage to devices as well, it is imperative to read and carefully follow the safety guidelines.

2.1 Legal Bases

2.1.1 Subject to Changes

WAGO Kontakttechnik GmbH & Co. KG reserves the right to provide for any alterations or modifications. WAGO Kontakttechnik GmbH & Co. KG owns all rights arising from the granting of patents or from the legal protection of utility patents. Third-party products are always mentioned without any reference to patent rights. Thus, the existence of such rights cannot be excluded.

2.1.2 Personnel Qualification

All sequences implemented on Series 852 devices may only be carried out by electrical specialists with sufficient knowledge in automation. The specialists must be familiar with the current norms and guidelines for the devices and automated environments.

All changes to the controller should always be carried out by qualified personnel with sufficient sufficient skills in PLC programming.

2.1.3 Proper Use of the Industrial Switches

The device is designed for the IP30 protection class. It is protected against the insertion of solid items and solid impurities up to 2.5 mm in diameter, but not against water penetration. Unless otherwise specified, the device must not be operated in wet and dusty environments.

2.1.4 Technical Condition of Specified Devices

The devices to be supplied ex works are equipped with hardware and software configurations, which meet the individual application requirements. These modules contain no parts that can be serviced or repaired by the user. The following actions will result in the exclusion of liability on the part of WAGO Kontakttechnik GmbH & Co. KG:

- Repairs,
- Changes to the hardware or software that are not described in the operating instructions,
- Improper use of the components.

Further details are given in the contractual agreements. Please send your request for modified and new hardware or software configurations directly to WAGO Kontakttechnik GmbH & Co. KG.

2.1.5 Standards and Regulations for Operating the Industrial Switches

Please observe the standards and regulations that are relevant to installation:

- The data and power lines must be connected and installed in compliance with the standards to avoid failures on your installation and eliminate any danger to personnel.
- For installation, startup, maintenance and repair, please observe the accident prevention regulations of your machine (e.g., DGUV Regulation “Electrical Installations and Equipment”).
- Emergency stop functions and equipment must not be deactivated or otherwise made ineffective. See relevant standards (e.g., EN 418).
- Your installation must be equipped in accordance to the EMC guidelines so electromagnetic interferences can be eliminated.
- Please observe the safety measures against electrostatic discharge according to EN 61340-5-1/-3. When handling the modules, ensure that environmental factors (persons, workplace and packing) are well grounded.
- The relevant valid and applicable standards and guidelines regarding the installation of switch cabinets must be observed.

2.2 Safety Advice (Precautions)

For installing and operating purposes of the relevant device to your system the following safety precautions shall be observed:

DANGER

Do not work on devices while energized!
All power sources to the device shall be switched off prior to performing any installation, repair or maintenance work.

DANGER

Only install in appropriate housings, cabinets or electrical operation rooms!
WAGO's 852 Series ETHERNET Switches are considered exposed operating components. Therefore, only install these switches in lockable housings, cabinets or electrical operation rooms. Access must be limited to authorized, qualified staff having the appropriate key or tool.

DANGER

Ensure a standard connection!
To minimize any hazardous situations resulting in personal injury or to avoid failures in your system, the data and power supply lines shall be installed according to standards, with careful attention given to ensuring the correct terminal assignment. Always adhere to the EMC directives applicable to your application.

NOTICE

Do not use in telecommunication circuits!
Only use devices equipped with ETHERNET or RJ-45 connectors in LANs. Never connect these devices with telecommunication networks.

NOTICE

Replace defective or damaged devices!
Replace defective or damaged device/module (e.g., in the event of deformed contacts).

NOTICE

Protect the components against materials having seeping and insulating properties!

The components are not resistant to materials having seeping and insulating properties such as: aerosols, silicones and triglycerides (found in some hand creams). If you cannot exclude that such materials will appear in the component environment, then install the components in an enclosure being resistant to the above-mentioned materials. Clean tools and materials are imperative for handling devices/modules.

NOTICE

Clean only with permitted materials!

Clean housing and soiled contacts with propanol.

NOTICE

Do not use any contact spray!

Do not use any contact spray. The spray may impair contact area functionality in connection with contamination.

NOTICE

Do not reverse the polarity of connection lines!

Avoid reverse polarity of data and power supply lines, as this may damage the devices involved.

NOTICE

Avoid electrostatic discharge!

The devices are equipped with electronic components that may be destroyed by electrostatic discharge when touched. Please observe the safety precautions against electrostatic discharge per DIN EN 61340-5-1/-3. When handling the devices, please ensure that environmental factors (personnel, work space and packaging) are properly grounded.

⚠ CAUTION

Laser radiation warning!

Do not stare into openings of the connections when no cable is connected, so as not to expose the radiation.
It can emit invisible radiation.
It concerns here a laser class 1 according EN 60825-1.

Note

Radio interference in residential areas

This is a Class A device. This device can cause radio interference in residential areas; in this case, the operator can be required to take appropriate measures to prevent such interference.

2.3 Special Use Conditions for ETHERNET Devices

If not otherwise specified, ETHERNET devices are intended for use on local networks. Please note the following when using ETHERNET devices in your system:

- Do not connect control components and control networks directly to an open network such as the Internet or an office network. WAGO recommends putting control components and control networks behind a firewall.
- In the control components (e.g., for WAGO I/-CHECK and CODESYS) close all ports and services not required by your application to minimize the risk of cyber attacks and to enhance cyber security.
  Only open ports and services during commissioning and/or configuration.
- Limit physical and electronic access to all automation components to authorized personnel only.
- Change the default passwords before first use! This will reduce the risk of unauthorized access to your system.
- Regularly change the passwords used! This will reduce the risk of unauthorized access to your system.
- If remote access to control components and control networks is required, use a Virtual Private Network (VPN).
- Regularly perform threat analyses. You can check whether the measures taken meet your security requirements.
- Use “defense-in-depth” mechanisms in your system's security configuration to restrict the access to and control of individual products and networks.

3 General

3.1 Scope of Supply

- 1 Industrial managed switch with multipoint connector
- Protective covers for unused ports
- Data cable RS-232 for CLI

3.2 Industrial ETHERNET Technology

WAGO's rugged switches are designed for industrial use in compliance with the following standards:

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3z
- IEEE 802.3x
- IEEE 802.1d
- IEEE 802.1w
- IEEE 802.1s
- IEEE 802.1Q
- IEEE 802.1p
- IEEE 802.1ab
- PROFINET

The switches have a power supply with a supply voltage range of 12 … 60 V.

Features such as auto-negotiation and auto-MDI/MDIX (crossover) are realized in all 10/100-TX ports.

3.3 PROFINET

The PROFINET real-time communication system is one of the most flexible and widespread fieldbus systems in automation technology. Thanks to its global market presence, PROFINET is recognized and accepted in many industries. PROFIBUS & PROFINET International (PI) is the global association of manufacturers and users.

PROFINET is considered the successor to the conventional PROFIBUS fieldbus and thus is frequently selected as soon as communication is converted from conventional fieldbuses to an ETHERNET-based fieldbus system. From a technical point of view, PROFINET offers an array of advantages, which, depending on the requirements of the environment of use, may tip the scales in favor of this fieldbus system. These advantages also allow PROFINET to be used in a great variety of industries.

PROFINET permits a combination of standard ETHERNET subscribers with real-time subscribers in the same network. PROFINET ensures that fieldbus communication is not interrupted by standard communication based on TCP/IP. This flexibility offers a great advantage over other ETHERNET real-time systems in which standard IT devices cannot be integrated into the network at all, can only be integrated at designated locations or can only be integrated into communication with continuous control. The figure “Parallel Use of Standard ETHERNET and PROFINET” schematically illustrates this parallel use via the same physical connection.

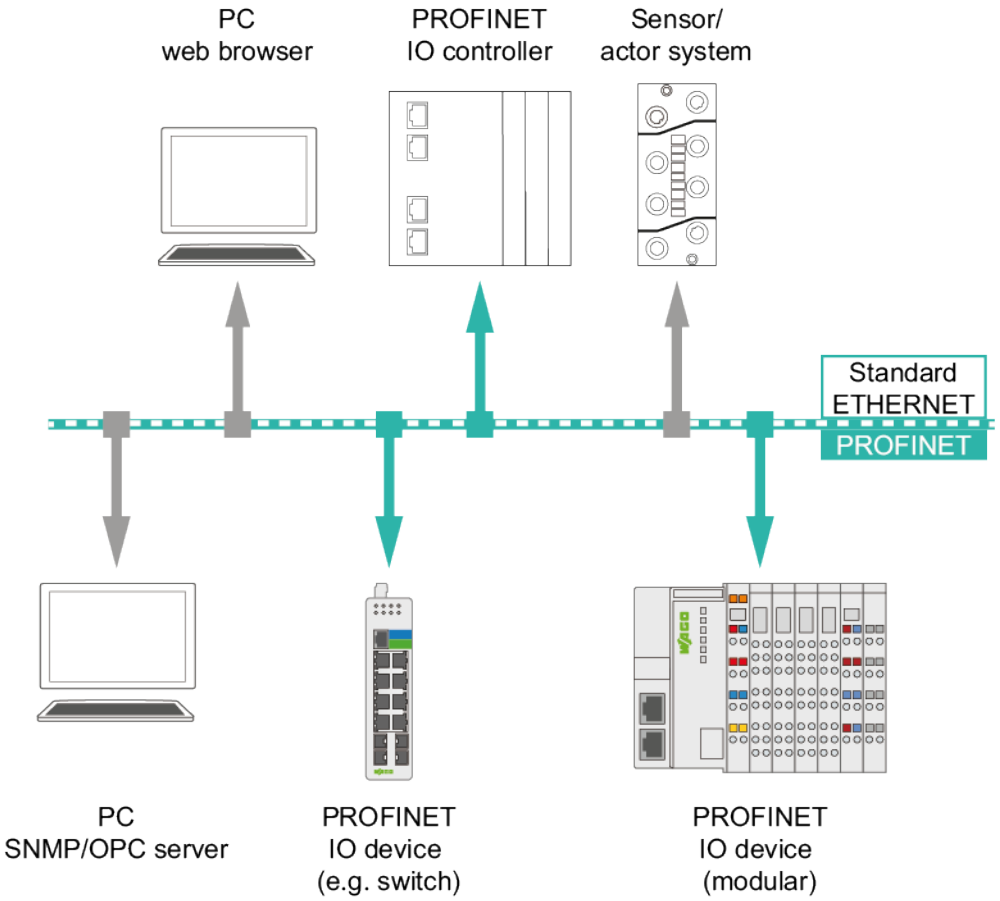


Figure 1: Parallel Use of Standard ETHERNET and PROFINET

PROFINET separates real-time-capable and non-real-time-capable devices. They are separated in different ways depending on the real-time class (RT_Class):

- For RT_Class_1, the separation is achieved by prioritizing the real-time telegrams via VLAN.
- For RT_Class_3, the separation is achieved via special PROFINET switches which reserve bandwidth for the real-time telegrams.

This separation of real-time-capable and non-real-time-capable devices ensures that any standard IT device can be operated at any point in a PROFINET network without the need to take special precautions concerning the physical connection.

Any ETHERNET-capable device can be connected to any interface in the automation network. For RT_Class_1, it is necessary to take the permissible network load of standard data traffic into account.

Diagnostics can be performed from any interface in the automation network with a PC – the operating state of the automation system is irrelevant. This function permits optimal physical adaptation of the network structure to the existing circumstances and allows operation without any limitation on the physical topology:

- Ring topology (only when using a protocol for media redundancy, e.g., MRP)
- Line topology
- Star topology
- Meshed network

In many cases, this also makes it possible to combine previously separate networks, taking the permissible network load into account.

3.4 Switching Technology

Industrial ETHERNET primarily uses switching technology. This technology allows any network subscriber to send at any time because the subscriber always has an open peer-to-peer connection to the next switch. The connection is bidirectional, i.e., the subscriber can send and receive at the same time (full duplex).
The targeted use of switching technology can increase real-time capability because the peer-to-peer connection prevents collisions in network communication.

3.5 Autonegotiation

Autonegotiation allows the switch to detect the transmission rate and operating mode for each port and the connected subscriber or subscribers, and to set them automatically. The highest possible mode (transmission speed and operating mode) is set.
Autonegotiation is available to ETHERNET subscribers connected to the switch via copper cable.
This make the switch a plug-and-play device.

3.6 Autocrossing

Autocrossing (MDI/MDI-X, “Medium Dependent Interface”) automatically reconfigures the receive and transmit signals for twisted-pair interfaces as needed. This allow users to use wired and crossover cables in the same manner 1:1.

3.7 Store-and-forward switching mode

In “Store and Forward” mode, the ETHERNET switch caches the entire data telegram, checks it for errors (CRC checksum) and if there are no errors, puts it in a queue. Subsequently, the data telegram (MAC table) is selectively forwarded to the port that has access to the addressed node.

The time delay required by the data telegram to pass the store-and-forward switch depends on the telegram length.

Advantage of “Store and Forward”:
The data telegrams are checked for correctness and validity. This prevents faulty or damaged data telegrams from being distributed via the network.

3.8 Transmission Methods

2 modes are available for data transmission in ETHERNET networks:

- Half duplex
  - An ETHERNET device can only send or receive data at one time.
  - Collision detection (CSMA/CD) is enabled.
  - The length of the network is limited by the propagation delays of the devices and transmission media.

- Full duplex
  - An ETHERNET device can send and receive data at the same time.
  - Collision detection (CSMA/CD) is disabled.
  - The length of the network only depends on the performance limits of the send and receive components used.

4 Device Description

The 852-603 Industrial Managed Switch is a configurable ETHERNET switch equipped with eight 10/100BASE-TX copper ports and two SFP-slots.
SFP modules with 100 MBit/s (100BASE-FX) or with 1 GBit/s (1000BASE-SX/LX) can be connected to these SFP ports.
Corresponding SFP modules are available as an option.

The properties of the switch include the following:

- A robust housing
- A redundant power supply
- Function monitoring with relays

The PROFINET device description (GSD – **G**eneral **S**tation **D**escription) file enables simple integration into an automation system.

4.1 View

4.1.1 Front View

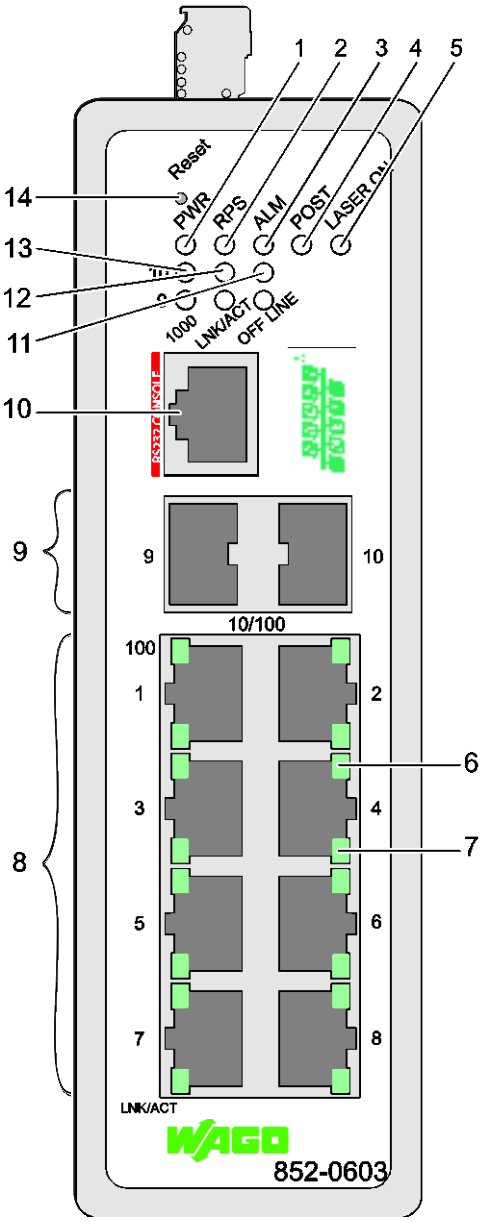


Figure 2: Front View of the Industrial Managed Switch

Table 3: Legend for Figure „Front View of the Industrial Managed Switch“

No.	Descrip-tion	Meaning	Details see Section
1	PWR	Status LED Power Supply	“Device Description” > “Display Elements”
2	RPS	Status LED, redundant, supply voltage	“Device Description” > “Display Elements”
3	ALM	Status LED, alarm	“Device Description” > “Display Elements”
4	POST	Status LED, POST	“Device Description” > “Display Elements”

Table 3: Legend for Figure „Front View of the Industrial Managed Switch“

No.	Descrip-tion	Meaning	Details see Section
5	LASER ON	Status LED LASER ON	“Device Description” > “Display Elements”
6	-	Status LED TX port 100-Mbit/s (1 LED for each port)	“Device Description” > “Display Elements”
7	-	Status LED TX Port LNK/ACT (1 LED for each port)	“Device Description” > “Display Elements”
8	-	Port 8 x RJ-45 (10/100BASE-TX)	“Device Description” > “Connections”
9	-	Port 2 x SFP (1000BASE-SX/-LX, fiber optic)	“Device Description” > “Connections”
10	-	Port 1 x RJ-45 (RS-232)	“Device Description” > “Connections”
11	OFFLINE	Status LED 1000 Mbit/s for fiber optic Port Offline (2)	“Device Description” > “Display Elements”
12	LNK/ACT	Status LED LNK/ACT for fiber optic (2)	“Device Description” > “Display Elements”
13	1000	Status LED 1000 for fiber optic (2)	“Device Description” > “Display Elements”
14	Reset	Reset button	“Device Description” > “Operating Elements”

4.1.2 Top View

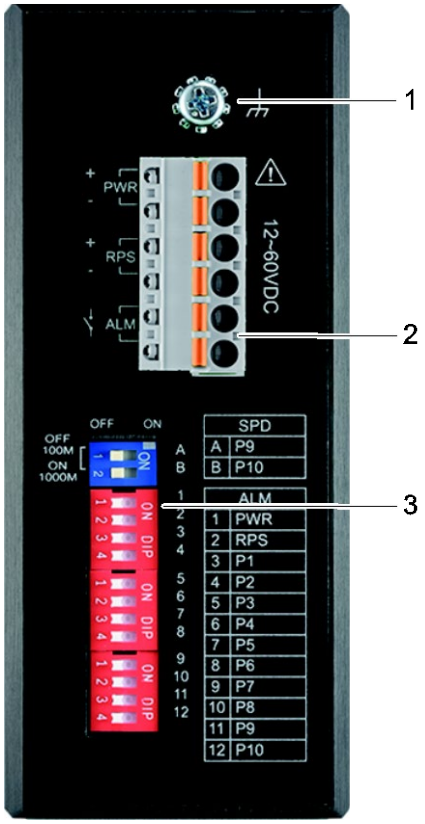


Figure 3: Top View of the Industrial Managed Switch

Table 4: Legend for the Figure “Top View of the Industrial Managed Switch”

No.	Descrip-tion	Meaning	Details see Section
1	-	Grounding screw	-
2	-	Connector (male) for power consumption (PWR/RPS/ALM) and potential-free alarm contact	"Device Description" > "Connections"
3	-	DIP Switches	"Device Description" > "Operating Elements"

4.2 Connectors

4.2.1 Power Supply (PWR/RPS)

The female connector (item no. 2231-106/026-000) can easily be connected to the 6-pole male header located on the top of the switch.

The male connector has the following pin assignment:

Figure 4: Power Supply Connection (PWR/RPS)

Table 5: Legend for Figure “Power Supply Connection (PWR/RPS)”

Connection	Name	Description
+	PWR	Primary DC input
-	PWR	Primary DC input
+	RPS	Secondary DC input
-	RPS	Secondary DC input
	HW ALM	Contact for external alarm
	HW ALM	Contact for external alarm

NOTICE

Warning against damage to property caused by electrostatic discharge!
DC powered switch: Power is supplied through an external DC power source. Since the switch does not include a power switch, plugging its power adapter into a power outlet will immediately power it on.

4.2.2 Network Connection

The Industrial managed switch uses ports with fiber optic or copper connectors that ca be used with ETHERNET, Fast ETHERNET and Gigabit Ethernet protocols.

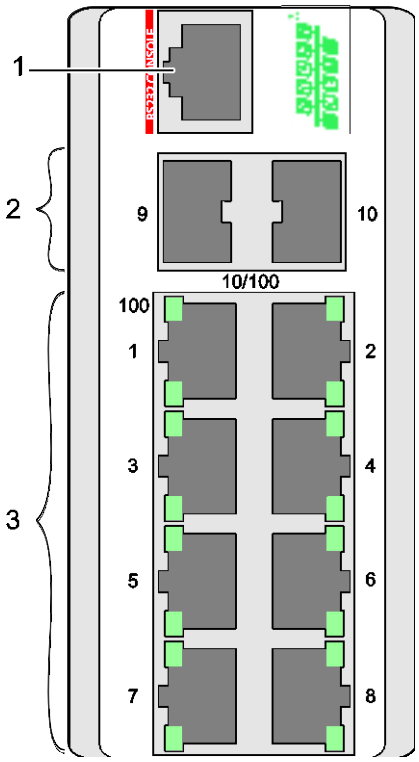


Figure 5: Network Connections

Table 6: Legend for Figure “Network Connections“

No.	Descrip-tion	Meaning	Details see Section
1	-	1 x RJ-45 connection (RS-232 port)	“Device Description” > … > “RJ-45 connection”
2	-	2 x SFP connection (SFP 100BASE-FX and/or SFP-1000BASE-SX/-LX, fiber optic)	“Device Description” > … “SFP 1000BASE-FX and/or SFP 1000BASE-SX/LX Connections”
3	-	8 x RJ-45 connection (10/100BASE-TX)	“Device Description” > … “10/100BASE-TX connection”

4.2.2.1 RJ-45 Connection

The connection to ETHERNET-based fieldbuses is made via the RJ-45 connector.

The pin assignment for ETHERNET RJ-45 plugs is specified in the EIA/TIA 568 standard.

The conductor colors also correspond to this standard. The pin assignment and conductor color differ depending on the number of assigned conductors (4- or 8-core).

4.2.2.2 SFP 100BASE-FX or SFP 1000BASE-SX/LX Ports

The 1000BASE-SX/-LX ports are designed to connect the gigabit SFP modules, which support transmission speeds of 1000 Mbit/s.
Additionally the connection of 100BASE-FX with a network speed of 100 Mbit/s is possible.

4.2.2.3 10/100BASE-TX Ports

The 10/100BASE-TX ports support network speeds of either 10 Mbit/s or 100 Mbit/s, and can operate in half- and full-duplex transfer modes. The ports also offer automatic MDI/MDI-X crossover detection that gives true “plug and play” capability – just plug the network cables into the ports and the ports will adjust according to the end-node devices. The following are the recommended cables for the RJ-45 connectors:

- Cat. 5e or better with a max. cable length 100 m

4.3 Display Elements

The industrial managed switch is equipped with device LEDs and port LEDs.

4.3.1 Device LEDs

The device LEDs allow you to identify the switch status quickly.

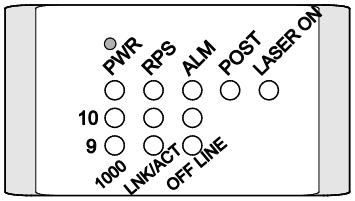


Figure 6: Device LEDs

Table 7: Legend for Figure „Device LEDs“

LED	Name	Status	Description
PWR	Primary power LED	Green	The industrial managed switch uses the primary power supply.
		Off	The primary power supply has been switched off, or a fault has occurred.
RPS	Redundant power system LED	Green	The industrial managed switch uses the redundant power supply.
		Off	The redundant power supply has been switched off, or a fault has occurred.
ALM [1)]	Alarm LED	Red	Failure of a port connection; miscellaneous alarm; the alarm contact is activated.
		Off	No alarm to report.
ALM [2)]	Alarm LED	Red	PROFINET error
		Flashing	No application relation
		Off	No alarm to report.
POST	Power-on self test LED	Green	Switch is ready or running.
		Off	Switch is not ready.
LASER ON	LASER ON LED	Yellow	Lights, when the fiber optic port SFP 1000BASE-SX/LX or SFP 100BASE-FX is used.
		Off	No fiber optic port SFP 1000BASE-SX/LX or SFP 100BASE-FX is used.

Table 7: Legend for Figure „Device LEDs“

LED		Name	Status	Description
9/ 10	1000	1000 Mbit/s LED	Green	Port running at 1000 Mbit/s.
			Off	No proper link established at the port.
	LNK/ ACT	LNK/ACT LED	Green	Lights up when port is linked.
			Flashing	Data traffic being routed via the port.
			Off	No proper link established at the port.
	OFF- LINE	OFFLINE LED	Red	Lights up when no SFP device is present.
			Off	Both SFP devices are properly connected.
[1] PROFINET mode inactive [2] PROFINET mode active; alarm contact is not controlled via the PROFINET diagnostics.				

4.3.2 Port LEDs

The port LEDs provide information about connection actions.

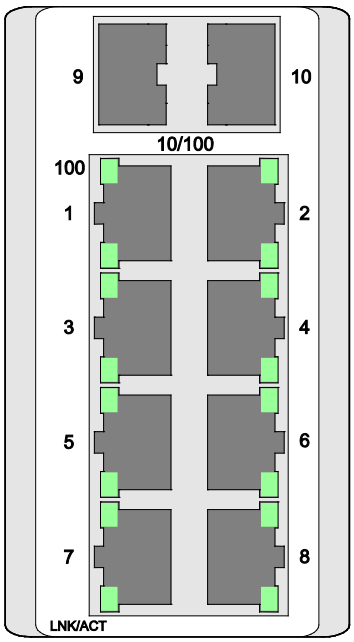


Figure 7: LEDs for RJ-45 Ports

Table 8: Legend for Figure „ LEDs for RJ-45 Ports “

LED	Name	Status	Description
100	10/100BASE TX port LED (1 LED for each port)	Green	Port running at 100 Mbit/s.
		Off	Port operates at less than 100 Mbit/s.
LNK/ ACT	LNK/ACT LED (1 LED for each port)	Green	Lights up when the port is connected.
		Flashing	Data traffic is being routed via the port.
		Off	No proper link established at the port.

4.4 Control Elements

4.4.1 DIP Switches

DIP switches for alarm configuration are located on the top of the industrial managed switch. When the alarm reporting function is active, the alarm contact is switched when an alarm event occurs.

If PROFINET mode is inactive, activation of the alarm reporting function is also indicated via the “ALM” device LED (see section “Display Elements”).

The meanings of the DIP switch settings are described below:

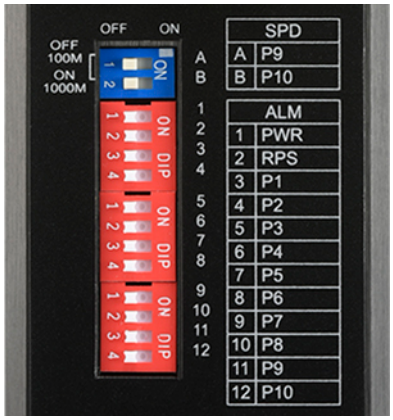


Figure 8: DIP Switches

Table 9: Legend for the Figure “DIP Switches”

No.	Name	Status	Description
A	P9	ON	Port 9 (SFP) is activated for the transmission speed of 1000 Mbit/s.
		OFF	Port 9 (SFP) is activated for the transmission speed of 100 Mbit/s.
B	P10	ON	Port 10 (SFP) is activated for the transmission speed of 1000 Mbit/s.
		OFF	Port 10 (SFP) is activated for the transmission speed of 100 Mbit/s.
1	PWR	ON	The alarm reporting function for the primary power supply is enabled.
		OFF	The alarm reporting function for the primary power supply is disabled.
2	RPS	ON	The alarm reporting function for the secondary power supply is enabled.
		OFF	The alarm reporting function for the secondary power supply is disabled.
3 … 12	P1 … P10	ON	The alarm reporting function for connection errors is enabled for port x.
		OFF	The alarm reporting function for connection errors is disabled for port x.

The user can manually switch the alarm function on and off with the DIP switches, both for each port and for the primary or redundant power supply.

Enabling the corresponding alarm function requires the DIP switch to be set to “ON.” The default setting is “OFF.”

The following is the recommended procedure for configuring and setting DIP switches during initial installation:

1. Set the DIP switches to “OFF.”
2. Install the industrial managed switch in your network.
3. Select the port to be monitored or the alarm to be activated. Multiple selections are possible.
4. Set the DIP switch of the corresponding port to “ON.”
5. Turn the industrial managed switch on.

4.4.2 Reset Button

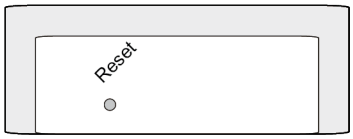


Figure 9: Reset Button

Table 10: Legend for the Figure “Reset Button”

Name	Status	Description
Reset	Press the Reset button for two seconds and release.	The system restarts.

Note

Important Note!
Use a suitable object (e.g., ballpoint pen or straightened paper clip) to press the Reset button.

4.5 Label

There is a label with the “MAC Address” and “Serial NO” on the back of the industrial managed switch.

Figure 10: Label (Example)

Table 11: Legend for Figure „Label (Example)“

No.	“Serial NO” Description
01	Firmware version (left number sequence)
01	Hardware version (right number sequence)

4.6 Technical Data

4.6.1 Device Data

Table 12: Technical Data – Device Data

Width	50 mm
Height	162 mm (from the top edge of the carrier rail)
Depth	120 mm
Weight	885 g
Degree of protection	IP30

4.6.2 System Data

Table 13: Technical Data – System Data

MAC table	Up to 16000 addresses
VLAN	Port-based und Tag-based (4094 VIDs)
Jumbo Frame Size	10240 Byte
Wavelength optical fibers	Depends on SFP module
Maximum lengths	10/100BASE-TX: 100 m; Fiber optic: 2 … 80 km RS-232: 15 m

4.6.3 Power Supply

Table 14: Technical Data – Power Supply

Supply voltage	DC 12 … 60 V
Power consumption, max.	12 W

4.6.4 Communication

Table 15: Technical Data – Communication

Configuration and Update	1 x USB-Host 2.0
Ports (copper; RJ-45)	8 x 10/100BASE-TX 1 x RS-232
Ports (LWL)	2 x 1000BASE-SX/-LX and/or 100BASE-FX
Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/-FX IEEE 802.3z 1000BASE-SX/LX IEEE 802.3x Flow Control IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1Q VLAN Tagging IEEE 802.1p Class of Service IEEE 802.1ab Link Layer Discovery Protocol (LLDP) PROFINET CC-B

Network management	• CLI via console port, Telnet and SSH
	• RJ45 port for local management
	• Web-Based Management
	• Status indicator and event report via Web-Based Management
	• Port management
	  • Autonegotiation
	  • Duplex mode
	  • 802.3x flow control
	  • Jumbo frame support
	• SNMP v1 and v2c management
	• SNMP trap
	  • Link UP/Down
	  • Change of configuration
	  • Cold start
	  • Warm start
	  • Trap transmission: 5 lines
	• Providing fault, power, configuration and security management
	• RMON: 4 RMON groups 1, 2, 3 and 9 (statistics, history, alarms and events) for better traffic management, monitoring and analysis

Network security	• ACL
	  • Port-based authentication of network access
	  • MAC-based authentication of network access
	• SNMP v3 security
	• SSH
	• Web authentication

4.6.5 Environmental Conditions

Table 16: Technical Data – Environmental Conditions

Surrounding air temperature (operation)	-40 … +70 °C
Surrounding air temperature (storage)	-40 …+80 °C
Relative humidity (without condensation)	10 … 95 %
Vibration resistance	EN 60068-2-6
Shock resistance	EN 60068-2-27
EMC-1 immunity to interference	EN 55024 EN 61000-6-2 EN 61000-4-2 EN 61000-4-3 EN 61000-4-4 EN 61000-4-5 EN 61000-4-6 EN 61000-4-8
EMC-1 Emission of interference	FCC Part 15 EN 55022: class A EN 55011: class A EN 61000-6-4

4.7 Approvals

The following approvals have been granted for the WAGO ETHERNET accessory product “Industrial Managed Switch” (852-0603):

CE	Conformity Marking	
cULus	Ordinary Locations	UL61010-2-201 (E175199)

5 PROFINET

5.1 System Overview

5.1.1 Structure

5.1.1.1 Device Classes

With PROFINET IO, process data is exchanged on the basis of the provider/consumer model:

- “Providers” generate data and send it via data telegrams without a specific request.
- “Consumers” receive data and process it.

Table 17: Examples of Providers and Consumers

Data	Provider	Consumer
Process data (inputs)	IO devices	IO controllers
Process data (outputs)	IO controllers	IO devices
Parameter data	IO controllers	IO devices

PROFINET IO defines the following device classes (also see the figure “PROFINET IO Device Classes”):

- **IO controller**:
  An IO controller is typically a component of a higher-level PLC (“**P**rogrammable **L**ogic **C**ontroller”) on which the automation program runs and the incoming process and diagnostic data is processed. The IO controller is the provider of the output and parameter data and consumer of the input data of the IO devices.

- **IO device:**
  An IO device is a remote field device coupled via PROFINET IO to one or more IO controllers. An IO device is the provider of the input data and consumer of the output and parameter data.
  WAGO’s PROFINET switches are IO devices.

  - **I-device:**
    An I-device is an intelligent IO device with an integrated control unit (e.g., an integrated PLC) that can handle pre-processing functions (e.g., I/O systems). An I-device is the provider of the input data and consumer of the output and parameter data.

- **IO supervisor:**
  The IO supervisor (e.g., an engineering station) is typically a PD (“**P**rogramming **D**evice”), PC or HMI (“**H**uman **M**achine **I**nterface”) device for commissioning or diagnostics. Use of the IO supervisor is often only needed temporarily for planning the network and configuring the IO controller.

In a PROFINET IO system, there is always at least one IO controller and one or more IO devices. The IO supervisor is usually only connected temporarily during commissioning and troubleshooting.

5.1.1.2 Device Model of an IO Device

PROFINET supports the following IO device configurations:

- Compact field devices:
  The scope is already determined upon delivery and cannot be modified by the user.

- Modular field devices:
  The scope can be customized to the individual application during the planning of the system.

The device model serves to describe the technical and functional capabilities of the IO device. This device model is specified in the GSDML file by the DAP ("**D**evice **A**ccess **P**oint") for a specific family of devices. A DAP is the access point for the field device's communication with the ETHERNET port and the automation program.

The following structures have been standardized for the device model of an IO device:

- The **DAP** identifies the IO device as a unit.

- The **slot** identifies the physical slot of an I/O module in a modular IO device. The slots are used to address the configured modules. These modules in turn contain one or more subslots for data exchange.

- The **subslots** within a slot form the actual interface to the inputs and outputs, and thus to the process. The granularity of a subslot, and thus the division of the I/O data, is manufacturer-specific. A subslot's data content is always accompanied by status information that determines the validity of the data.
  Each slot must contain at least one subslot.

- The **index** only applies to acyclic data exchange. The index specifies the data that can be read or written within a slot/subslot. Certain indices are specified in standards. Other indices can be defined on a manufacturer-specific basis.

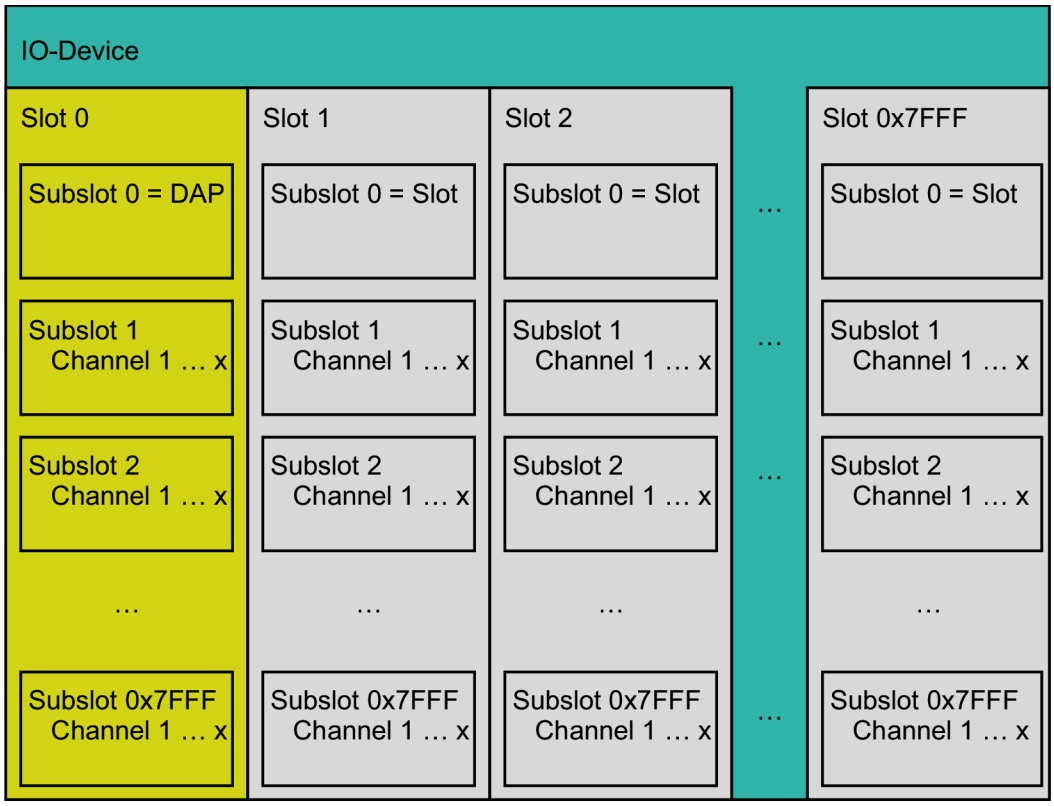


Figure 11: Addressing the Data of an IO Device via Slots/Subslots

The data addressing depends on the transmission mode:

Table 18: Data Addressing as a Function of Transmission Mode

Transmission Mode	**Addressing through Combination of**		
	Slot	**Subslot**	**Index**
Cyclic	X	X	–
Acyclic	X	X	X

The slot–subslot combination information can be defined on a manufacturer-specific basis.

WAGO's PROFINET managed switch only includes slot 0. The following figure illustrates the subslot assignment. Each switch port corresponds to one subslot.

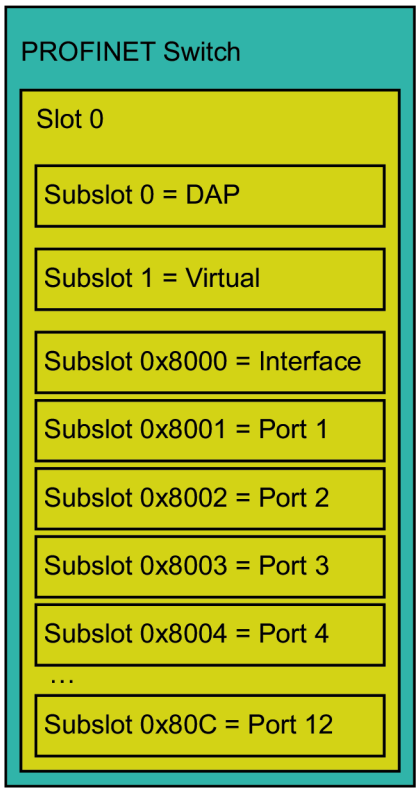


Figure 12: Assignment of Subslots in WAGO's PROFINET Managed Switch

5.2 Communication

In PROFINET networks, communication occurs via industrial ETHERNET.

To establish a communication link between the IO controller and an IO device (e.g., the WAGO PROFINET managed switch), the communication paths must be established. These communication paths are set up during system startup by the IO controller on the basis of the project planning data. Thus the communication relation for the data exchange is uniquely specified.

Each data exchange is embedded in an AR (“**A**pplication **R**elation”). General communication parameters and manufacturer-specific parameters are loaded through the AR.

The following ARs are defined for PROFINET:

- Implicit AR
  This AR defines an application reference between the IO controller/IO supervisor and the IO device for reading data from the IO device acyclically. Write access is not allowed with an implicit AR.
  This AR does not need to be established specifically; the IO devices always have access to it.

- IOCAR (“**IO C**ontroller **A**pplication **R**elation”)
  This AR is for exchanging cyclic input and output data, acyclic data and bidirectional alarms.

- IOSAR (“**IO S**upervisor **A**pplication **R**elation”)
  This AR is for data exchange between an IO supervisor and the IO device, as well as for taking over one or more submodules of an IO device that are assigned to corresponding IO controllers. The data exchange can correspond to that of an IOCAR.

Within the AR, so-called CRs (“**C**ommunication **R**elations”) uniquely specify the data:

- Record Data CR (R-CR):
  Communication channel for acyclic data exchange
- IO Data CR (IO-CR):
  Communication channels for cyclic data exchange (input and output data)

- Alarm CR (A-CR):
  Communication channel for the alarms

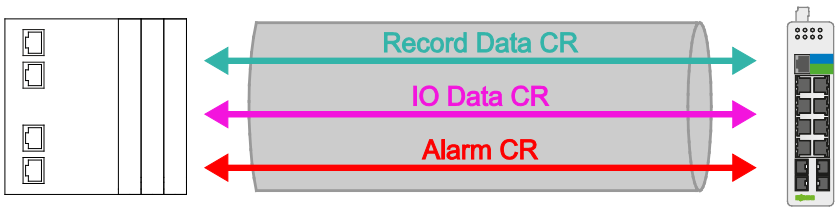


Figure 13: Communication Relations for PROFINET

Multiple IO controllers can be used in a PROFINET system with WAGO's PROFINET managed switches. One IO controller can establish one AR with each of multiple IO devices.

5.3 Data Transfer

As a general rule, process data in PROFINET networks is transferred in real time (RT). Furthermore, data telegrams can also be transferred in NRT ("**N**on-**R**eal **T**ime") via standard ETHERNET. PROFINET uses the following options:

- NRT communication within and between networks:
  This communication corresponds to "normal" communication in ETHERNET networks. Real-time conditions are not met. This communication can be established with HMI devices, for example.

- RT communication within a network:
  This communication aims at a high degree of determinism. Therefore, it uses the RT channel. UDP/IP is not used in this configuration.

- RT communication between networks:
  This communication involves additional logging. Therefore, it uses the RT channel. UDP/IP is also used.

5.3.1 Real-Time Communication

Data telegrams in PROFINET format are prioritized over standard data telegrams in accordance with IEEE 802.1Q. This ensures the necessary determinism in the automation technology. In this method, the data is transferred via prioritized ETHERNET data telegrams.

5.3.2 Transfer Methods

Data in PROFINET networks is transferred in full duplex mode:

- A PROFINET device can send and receive data at the same time.
- Collision detection (CSMA/CD) is disabled.
- The length of the network only depends on the performance limits of the send and receive components used.

5.3.3 Transfer Types

PROFINET supports the following transfer types:

Acyclic Transfer

Data for the following is transferred acyclically:

- Establishing the real-time connection
- Parameterizing the PROFINET managed switch and its submodules
- Reading diagnostic information
- Reading identification, maintenance and service information
- Reading I/O data
- Reading alarm information
- Etc.

Cyclic Transfer

Process data and other user data is transferred cyclically.

The cyclic I/O data is transferred as real-time data without acknowledgment. The cycle time can be customized.

The data connection is monitored on the basis of time monitoring, which is derived from a multiple of the parameterized transfer cycle time.

For transfer in the real-time telegram, a subslot's data is supplemented with accompanying use data (the provider status). This status information is evaluated by the corresponding consumer of the I/O data. Therefore, this consumer can only assess the validity of the data from the cyclic data exchange. For this purpose, the consumer's status information is transferred to the provider in the opposite direction.
Depending on the I/O type of a submodule, it may be possible for provider and consumer statuses to be transferred in both directions too.

Following the data, the data telegrams contain further status information (the APDU status). The corresponding consumer of the communication relation checks whether the data fails to appear. If the data is not received within the monitoring time according to the configuration, the corresponding consumer terminates the connection.

5.3.4 Telegram Structure

In PROFINET, a data telegram has the following structure:

Dest. addr.	Source addr.	VLAN tag	Ether type	FrameID	Application data	Cycle counter	Data status	Transfer status	FCS

Table 19: Sections of the PROFINET Telegram

Section	Size	Description
Dest. addr.	6 bytes	Destination address (MAC address)
Source addr.	6 bytes	Source address (MAC address)
VLAN tag	4 bytes	For transferring the priority
Ether type	2 bytes	0x8892 → Telegram type PROFINET RT
FrameID	2 bytes	Contains the exchanged FrameID (also see the table "'FrameID' Examples").
Application data	0 bytes … 1440 bytes	User data
Cycle counter	2 bytes	Contains the cycle number in multiples of 31.25 µs. Example: Cycle time = 4 ms: Cycle counter = 128 (128 × 31.25 µs = 4 ms)
Data status	1 byte	Contains information on the data status (see table "'Data Status' Example").
Transfer status	1 byte	RT_Class_1: 0 RT_Class_3: 0/1 (1 = replacement frame)
FCS	4 bytes	Checksum for detecting transfer errors

5.4 Addressing

A device's address in a PROFINET network consists of multiple parts:

- The device name
- The MAC address
- The IP addressing (IP address, subnet mask and gateway address)

By default, the PROFINET managed switch has the following IP address: **0.0.0.0**

An IP address is assigned to the PROFINET switch via the DCP protocol. It can be assigned by the IO controller, for example.

5.4.1 Device Name

Before the IO controller can address an IO device, both devices must be given device names. This method was selected for PROFINET because names are easier to handle than IP addresses.

Note

There are restrictions on character use!
PROFINET only supports selected characters for name assignment. These characters include 0 … 9, the lower case letters a … z, the hyphen "-" and the period "."
The device name can contain at most 127 characters; up to 63 letters or digits can be used between hyphens and periods.
Spaces are not allowed!

The PROFINET managed switch does not yet have a device name when delivered. However, the PROFINET managed switch cannot be identified by an IO supervisor (PG or PC) for an IO controller in the network until a device name has been assigned. After the IP settings are then assigned, the connection can be established on the basis of the project planning data.

5.5 Conformance Classes

The requirements on an application with PROFINET IO can be divided into to three CCs (“**C**onformance **C**lasses”), which build on each other. The IEC 61784-2 standard defines the three conformance classes for PROFINET: **CC-A**, **CC-B** and **CC-C**.

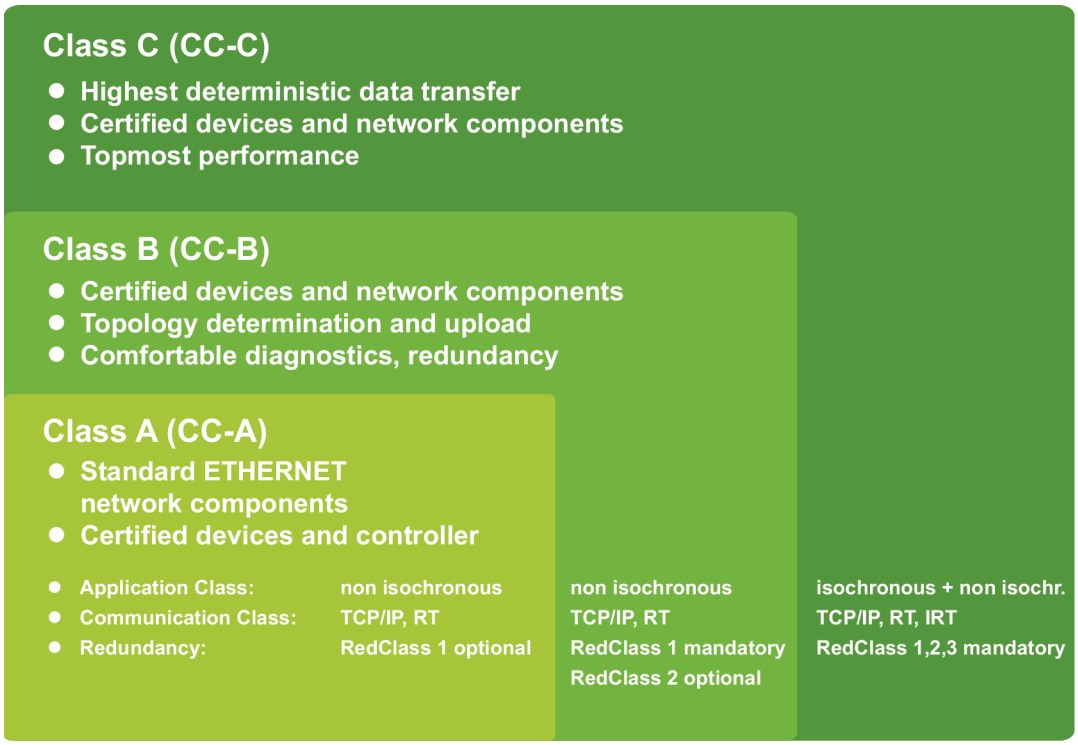


Figure 14: Overview of Conformance Classes A through C

These three conformance classes can be assigned to specific applications:

CC-A: Plant Control

- Meets the requirements on simple equipment automation.
- The PROFINET devices used are certified.
- Offers basic functions for PROFINET IO with RT communication.
- All IT services can be used without restriction.
- For cycle times up to 100 ms (e.g., in plant automation)
- Use of existing building cabling is possible.
- Definition of integration of wireless systems like *Bluetooth*® or WLAN.
- Definition of integration of existing fieldbuses like PROFIBUS, INTERBUS or DeviceNet (manufacturer)
- Security concepts for access from the Internet for remote diagnostics without the possibly of unauthorized intrusion.

CC-B: Machine Control

- Meets the requirements on machine automation.
- The devices and network infrastructure must be certified.
- Expands the concept with network diagnostics via IT mechanisms and topology information.
- The “system redundancy” function (e.g., for process automation) is contained in an extension of CC-B to CC-B(PA).
- For data transfer cycle times up to 10 ms (e.g., a PLC as a typical controller for a machine)
- The infrastructure must follow clearly defined guidelines.
- Only PROFINET components are allowed. The switches and cables must also meet the minimum PROFINET requirements.
- Cables must have continuous shielding in order to guarantee EMC.

CC-C: Motion Control

- Meets the requirements on motion automation.
- The devices and network infrastructure must be certified.
- Describes the basic functions for devices with hardware-supported bandwidth reservation and synchronization (IRT communication).
- Forms the basis for synchronous applications.
- For cycle times under 1 ms (e.g., for control of movements).
- All components must be class C devices and can be synchronized.
- Isochronous communication is the precondition for achieving the required cycle times. The subscribers are isochronous if they all have the same time (“clock synchronization”).

The individual conformance classes can be combined with each other. A system with PROFINET IO can contain different conformance classes. Multiple zones of the same conformance class are also possible without difficulty.

For this division to be implemented, the devices of a conformance class must meet certain minimum requirements on the implemented functions and protocols.

Table 20: Comparison of Conformance Classes

Requirement	Class A (CC-A)	Class B (CC-B)	Class C (CC-C)
Basic functions	• RT communication • Cyclic I/O • Parameters • Alarms	• RT communication • Cyclic I/O • Parameters • Alarms • Network diagnostics • Topology information • System redundancy	• RT communication • Cyclic I/O • Parameters • Alarms • Network diagnostics • Topology information • Reserved bandwidth (IRT) • Synchronization
Wiring	Per IEC 61784-5-3 and IEC 24702 • Copper • Fiber optic • Wireless	Per IEC 61784-5-3 • Copper • Fiber optic	Per IEC 61784-5-3 • Copper • Fiber optic
Typical use	• Infrastructure • Building automation	• Manufacturing automation • Process automation	• Motion control

In practice, devices that correspond to conformance class CC-A can certainly include individual functionalities of CC-B, or even CC-C.

5.6 Media Redundancy

PROFINET implements media redundancy with the help of the MRP protocol. The PROFINET devices are arranged in a ring topology.

In the ring topology, one device plays the role of the redundancy manager. All other devices in the ring are redundancy clients.

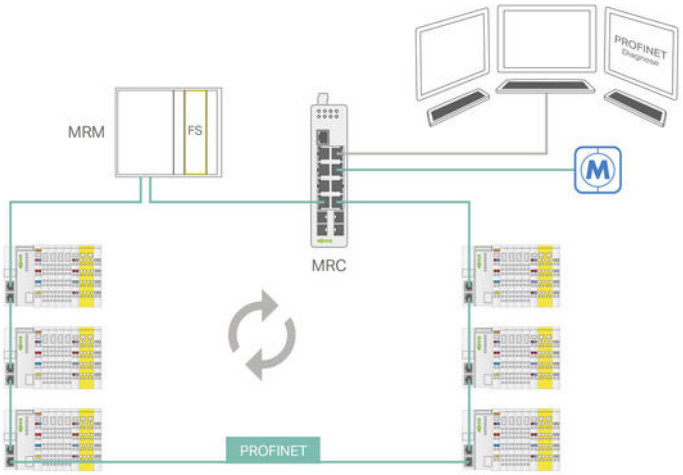


Figure 15: Media Redundancy in PROFINET (Ring Topology)

Figure 21: Legend for Figure “Media Redundancy in PROFINET (Ring Topology)”

Abbreviation	Explanation
MRM	Redundancy manager
MRC	Redundancy client

The ring port is selected and determined during project planning. Each port on the product can function as a redundancy manager or redundancy client.

Media Redundancy Function

During trouble-free communication, one of the two ring ports is blocked in the redundancy manager. This ensures that no data telegram circulate. From the point of view of data communicate, the ring becomes a line topology.

The redundancy manager monitors the ring topology for disruptions by sending test telegrams from both ring ports. The test telegrams go through the ring topology in both directions until they arrive at the other ring port of the redundancy manager. If receipt of a telegram is not confirmed, there is a disruption in the communication. There are two possible causes for this disruption:

- Failure of the connection between two devices
- Malfunction of a device in the ring topology

If there is a disruption, the redundancy manager interconnects its two ring ports. This alternative path establishes a functioning connection between all remaining devices in the form of a line topology.

The time between the ring disruption and restoration of a functional line topology is called the reconfiguration time.

As soon as the disruption is corrected, the original transfer paths are reestablished, the two ring ports in the redundancy manager are disconnected from each other, and the redundancy clients are notified of the change. The redundancy clients then use the familiar paths to the other devices.

All devices (IO controllers, IO devices, switches etc.) that are connected via a ring topology must support the “media redundancy” function. These devices form a so-called redundancy domain.

For a PROFINET managed switch, the “media redundancy” function is implemented through the following procedure:

MRP (“Media Redundancy Protocol”)

This redundancy method is the standard method and based on the IEC 61158 standard, Type 10 “PROFINET.” With this method, at most 50 devices can be connected in a ring topology. The typical reconfiguration time is 200 ms.

The following requirements must be met for fault-free operation with MRP:

- All devices that are connected in the ring topology must support MRP.
- The “MRP” function must be enabled for all devices.
- All devices must be connected to each other through their ring ports.
- The ring topology must consist of at most 50 devices.
- No IRT functionality can be configured for the devices.

5.7 Protocols

This section lists PROFINET protocols that are used in the PROFINET managed switch.

DCP

The devices in an ETHERNET system can be configured via DCP (“**D**ynamic **C**onfiguration **P**rotocol”) per IEC 61158. For example, device names and IP settings can be distributed to unaddressed devices in order for these devices to be reachable in the network via the IP protocol.

DCP provides various services for querying and distributing address information:

- DCP_Identify queries
- DCP_Get services
- DCP_Set services

The first time it is commissioned, the ETHERNET device has the default settings. There is no device name (empty string, NIL), and the **Address**, **Subnet Mask** and **Standard Gateway** are each set to 0.0.0.0.

The ETHERNET device is not available via ICMP until a device name and valid IP settings are assigned to it via corresponding DCP_Set services.

LLDP

LLDP (“**L**ink **L**ayer **D**iscovery **P**rotocol”) is a protocol on layer 2 of the ISO/OSI reference model.

LLDP allows an ETHERNET device in the LAN (“**L**ocal Area **N**etwork”) to send information about itself and receive information from neighboring devices. The device stores the information received in its LLDP MIB (“**M**anagement **I**nformation **B**ase”), which can be read by a network management system via SNMP.

LLDP telegrams are sent with EtherType 0x88CC, both at periodic intervals and in the event of LLDP MIB changes, to multicast MAC address **01:80:C2:00:00:0E**. The telegrams are only received and processed by the immediate neighbors in the network.

MRP

MRP (“**M**edia **R**edundancy **P**rotocol”) is specified per IEC 62439 and, in the event of a fault, allows the communication paths for TCP/IP and RT_Class_1 traffic to be switched over within 200 ms. Use of this method requires one MRM (“**M**edia **R**edundancy **M**anager”) and one or more MRCs (“**M**edia-**R**edundancy **C**lients”) arranged in a ring topology. The installed devices must have at least two ETHERNET ports.

The MRM is usually implemented in an IO controller or a PROFINET switch. During fault-free operation, the MRM only processes the telegram traffic to the

devices located in the ring topology via one of the two ring ports. Thus it splits the ring topology up into a virtual line topology. Furthermore, the MRM checks the planned ring topology for any disruptions with cyclic test telegrams. The MRC merely passes these test telegrams on to the next subscriber. If the MRM does not receive the test telegrams that were sent to its first ring port at its second ring port, it checks which point the ring topology was interrupted at. It then switches the telegram traffic to the elements that are no longer reachable via the first ring port over to the second ring port.

RTC

RTC (“**R**eal **T**ime **C**yclic”) is a cyclic PROFINET protocol.

The real-time technology handles the TCP/IP levels in such a way that the deterministic performance of applications achieves a speed of 1 to 10 milliseconds. This makes PROFINET RT ideal for applications in which control of digital and analog I/Os is crucial for production cycles. By skipping TCP/IP and the transfer of data messages from the physical ETHERNET layer to the application layer, “PROFINET Real Time” offers high-precision determinism.

5.8 PROFINET Managed Switch

The PROFINET managed switch has the following PROFINET properties:

Cyclic functions (PROFINET RT):

- Minimum interval: 32 ms
- Extended and legacy start-up
- Support for establishing connection:
  - 1x IOC_AR, 1x DA_AR
  - 1 x input CR
  - 1 x output CR
  - 1 x alarm CR

Acyclic functions:

- Connected mode:
  - Read diagnostic information of the IO device (record).
  - Write various configuration parameters.
  - Output alarms to an IO controller
- Disconnected mode:
  - Read diagnostic information of the IO device (record).

General functions:

- MRP client/manager, single instance (freely configurable for each port)
- LLDP & LLDP MIB
- Easy replacement of devices
- Certified for Netload II

The following functions are not supported:

- DHCP
- FSU
- Shared input
- Shared device
- IOS_AR
- IOS_AR TakeOver
- IRT, RT_CLASS_3 data exchange
- PROFIenergy
- Precision Transparent Clock Protocol (PTCP)

5.9 GSDML File

5.9.1 Introduction

The technical and functional properties of all IO devices are described in a manufacturer-specific file. This GSDML (“**G**eneral **S**tation **D**escription **M**arkup **L**anguage”) file is XML-based. It contains all data required for engineering and for the IO controller’s data exchange. This includes:

- Description of the individual IO devices (input and output devices)
- Options for inserting the I/O devices into the slots
- Parameters that are necessary for correct operation of the IO device
- Diagnostics and their meanings, which are supplied by an IO device
- Description of multiple devices of a family in one file

The GSD file has a multilingual design.

The name of a GSD file corresponds to the following template:

GSDML-<version>-<manufacturer>-<devicename>-<date>.xml

Example GSD file name:

GSDML-V2.33-WAGO-852-20190213.xml

5.9.2 Structure of a GSDML File

The content of the GSDML file is structured according to ISO 15745.

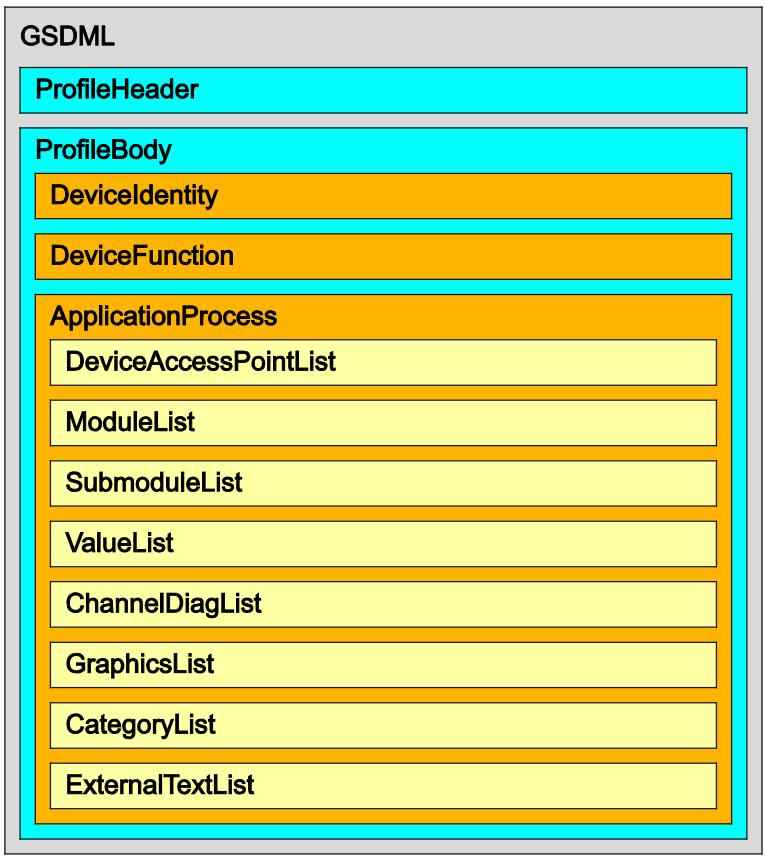


Figure 16: General Structure of a GSDML File

ProfileHeader

The structure and content are specified by the standard.
The following information is provided:

- ProfileIdentification
- ProfileRevision
- ProfileName
- ProfileSource
- ProfileClassID
- ISO15745Reference

ProfileBody

Contains all device-specific data on the IO device/device family.
The ProfileBody section is divided into:

- DeviceIdentity
- DeviceFunction
- ApplicationProcess

DeviceIdentity

- Contains information to identify the IO device.
  Consists of:
  - The Vendor_ID
    (this ID is assigned by the PNO and contains the company identifier;
    it is unique for each manufacturer),
  - The Device_ID
    (the Device_ID can be defined on a manufacturer-specific basis)
  - The InfoText (description of the device family)
  - The VendorName.

DeviceFunction

Information on the function of the device family

ApplicationProcess

Contains the actual data on the IO device
This section is divided into:
- DeviceAccessPointList
- ModuleList
- SubmoduleList
- ValueList
- ChannelDiagList
- GraphicsList
- CategoryList
- ExternalTextList

DeviceAccessPointList

Contains the description of all bus interface connections available with the device family (DAP = “**D**evice **A**ccess **P**oint”).
This includes:
- ModuleInfo (name, description, item number, version etc.)
- CertificationInfo (conformance, application and netload class)
- SubslotList
- IOConfigData (maximum length of the transferred data)
- UseableModules (only for IO devices with a modular structure)
- VirtualSubmoduleList
- SystemDefinedSubmoduleList
- Graphics (system representation of the IO device)

ModuleList

Contains the description of the individual modules of the IO device.

SubmoduleList

Contains the description of the individual submodules of an IO device.

ValueList

Contains the parameters that can be set for the IO device, as well as the association between the value and name.
The name is determined via the **TextID** in the **ExternalTextList**.

ChannelDiagList

Contains the assignment of an error to the corresponding text.
The corresponding text is determined via the ID in the **ExternalTextList**.

GraphicsList

Contains the references to the graphic symbols of all IO devices of the device family.

CategoryList

Contains the assignment of the modules to a specific category.
This assignment serves to organize the module catalog for this IO device in the corresponding engineering software.

ExternalTextList

Contains all text that can be referenced via the corresponding **TextID** in the other sections of the GSDML file.
This list can have a language-specific structure.

5.9.3 Unique Identification of IO Devices

The following identifiers uniquely identify IO devices in a GSDML file:

- Vendor_ID (manufacturer identifier; see **DeviceIdentity**)
- Device_ID (unique device identifier; see **DeviceIdentity**)
- Module ID (unique identifier for all modules that can be used within a specific IO device; see **ModuleList**)
- Submodule ID (unique identifier for all submodules that can be used within a module; see **SubmoduleList**)

5.10 Project Planning via GSDML File

This section describes the general procedure without going into detail on manufacturer-specific configuration tools. You can get descriptions of these configuration tools from the respective manufacturers.

Project planning for PROFINET managed switches basically consists of the following phases:

1 Planning (integration into the topology etc.)
2 Parameterization/configuration via engineering tool
3 Network setup
4 Testing
5 Commissioning

5.10.1 Configuring

The process of actually configuring the PROFINET managed switch with the engineering tool can begin once the following requirements are met:

- The selection phase for the devices and network topology is complete.
- All other general planning issues have also been resolved.

Note

Observe the documentation of the engineering tool!
This section contains general information on configuring the PROFINET system. For operation of the engineering tool used, please consult the corresponding manufacturer's documentation.

There are basically two different configuration methods:

- **Offline**
  Initially, no real PROFINET system is connected to the engineering tool. The project is created and configured with the devices and topology according to the plan. The real PROFINET system is then connected to the engineering tool, and the project that has been created is loaded onto the real IO controller.
- **Online**
  A real PROFINET system is connected to the engineering tool. The project is created with the real configuration and loaded onto the IO controller.

The general procedure is comparable with both methods. The offline configuration procedure is described below.

5.10.1.1 Engineering Tools (Overview)

A selection of various manufacturer-specific engineering tools exists for planning, project planning and configuration of a PROFINET system.

The following table contains a selection of PROFINET engineering tools from various manufacturers, listed alphabetically. The list does not claim to be exhaustive and does not constitute a recommendation.

Table 22: Overview of Engineering Tools

Manufacturer	Engineering Tool
3S	CODESYS
Beckhoff	TwinCAT
Hilscher	SYCON.net
Phoenix Contact	PCWorx
Siemens	STEP 7 (TIA Portal)

The general project planning procedure is largely identical for all the engineering tools.

The engineering tool used should be able to handle at least the following tasks:

- Managing PROFINET devices in the hardware catalog
- Linking devices in a (graphical) network view and/or hardware configuration view
- Assigning device names and addresses
- Monitoring and controlling variables online
- Accessing process data online
- Diagnosing the PROFINET devices
- Diagnosing the network devices (e.g., the switches)
- Representing the project in a hierarchical structure (e.g., a tree structure)
- Checking the project for consistency, errors and compliance with the quantity structure
- Supporting the user in creating system documentation

The following descriptions use the “TIA” tool from Siemens as an example.

Note

Pay attention to the application note!
You can find detailed instructions on configuring the PROFINET managed switch with the “TIA” engineering tool from Siemens in the application note “TIA Portal – WAGO PROFINET Managed Switch.” You can download this document from the Internet at www.wago.com

5.10.1.2 General Project Planning Procedure for a PROFINET System

The steps listed below may differ according to the engineering tool used. However, the procedure is basically identical to the one described.

1. If necessary, import the corresponding GSD files for the new PROFINET devices.
   With an existing project, it is usually on necessary to reimport the GSD file if an IO device is expanded with I/O module types that the corresponding IO device does not yet contain.

2. For a new PROFINET system, create a new project in the engineering tool. To expand an existing PROFINET system, open an existing project.

3. Add the new PROFINET devices to the opened project as device instances from the hardware catalog.

4. Assign the device names/IP addresses to the new PROFINET devices according to the plan (if necessary).
   For “Conformance Class” B and higher, each PROFINET network element must be given a device name and IP address.
   As far as possible, assign devices descriptive names so they can be recognized more easily (e.g., in diagnostic messages).
   Depending on the engineering tool and data structure used, it may be possible to assign the device names and/or IP addresses automatically.

5. If the PROFINET device is a modular IO device (e.g., a WAGO I/O-SYSTEM), select the modules to be used from the hardware catalog and add them to the project. Adjust the structure of the input and output data on the basis of the corresponding submodules.
   Among other things, this determines the structure of the process images for the input and output data.

Information

Pay attention to the size of the process images!
The size of the process images can be determined from the sum of the input/output data for all modules/submodules configured on the PROFINET node.
By specifically selecting suitable submodule types for the digital modules, it is possible, on a device-dependent basis, to optimize the structure of the process images for the input and output data. The content of the process images is exchanged with the IO controller during real-time data traffic.

6. Link the new PROFINET devices according to the planned topology.
   The representation of the topology depends on the engineering tool used and may differ from the real topology.

7. If necessary, adapt the cross-station settings to the corresponding submodule of the IO device.

8. For the IO devices, adapt the parameterizations for the planned modules/submodules if necessary.

9. Select the communication class (NRT or RT) on the corresponding submodule of the IO device.

10. Check the update time/transmission cycle and the connection monitoring of the connection to the IO controller and adjust these settings if necessary.

11. If you want to use the station in a network with media redundancy (a ring topology), assign the IO device the role of the MRP client and adjust the name of the MRP domain if necessary.

12. Check the connection settings on the submodules of the IO device port and adjust them if necessary.

13. Check the planned PROFINET system and then save it.
    The engineering tool checks the logical correctness of the planned system and compliance with the required quantity structure, for example.

14. Document the planned PROFINET system.
    Depending on the engineering tool used, this documentation step may be performed automatically.

15. If necessary, create/adapt the corresponding user programs and test the changes.
    The extent of this step mostly depends on whether a completely new PROFINET system is being created or an existing one extended.

16. If necessary, adjust the user management:
    - Creating new user roles
    - Creating users
    - Assigning the corresponding rights

Note

Disable unused ports!
According to the PNO “PROFINET Security” guidelines, unused ports must be disabled.

This concludes the offline configuration.

5.10.1.3 Loading the Project onto the IO Controller

In order to be able to load the project onto the IO controller, you must implement your planned PROFINET system configuration and set up the topology.

You can then conclude the project planning phase as follows:

1. If necessary, create the target configuration of the PROFINET network with the standard tools of the PROFINET network.
   The target configuration is essential for integrating the IO device into an IRT domain.
   Declaring the target configuration is also a precondition, if you want to swap out devices without a subsequent tool-based station “christening” step.
   If the target and actual configurations match, you can forego a tool-based station “christening” during the initial commissioning if necessary.

2. Then switch on the power supply for the fieldbus coupler.

3. As an alternative to the topology-based station “christening,” you can assign the device name via a DCP tool.
   You also have the option of specifying the device name via DIP switches if present.

4. Load the system data onto the IO controller.

Once the system data has been successfully loaded, data can be exchanged between the IO controller and IO device.

5.10.2 Parameters

The PROFINET managed switch parameters can be set via the engineering tool used.

Following the figures, the individual parameters are explained, and their relationships to the GSDML file are illustrated.

The following descriptions use the “TIA” tool from Siemens as an example.

Note

Pay attention to the application note!
You can find detailed instructions on configuring the PROFINET managed switch with the “TIA” engineering tool from Siemens in the application note “TIA Portal – WAGO PROFINET Managed Switch.” You can download this document from the Internet at www.wago.com.

5.10.2.1 “General” Section

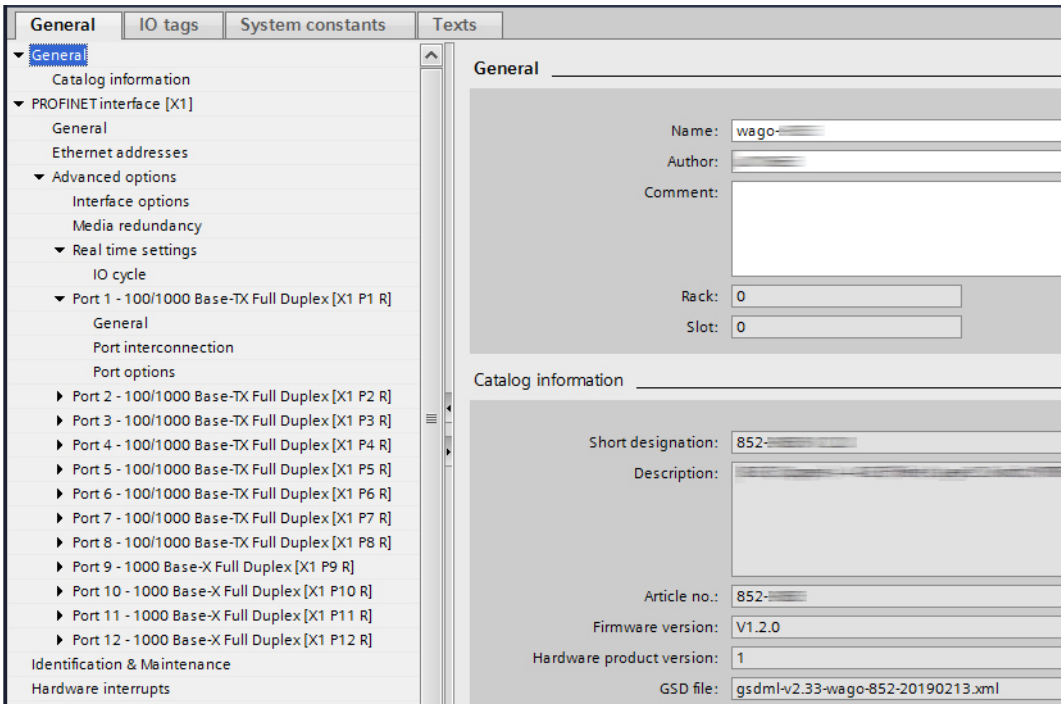


Figure 17: PROFINET Parameters – “General” Section

Table 23: PROFINET Parameters for “General” Section

Parameter	Description	Tag in the GSDML
Name	DAP name	DeviceAccessPointItem [DNS_CompatibleName]
Author	Person who processed the device in the engineering tool	–
Comment	Comment field	–
Rack	Precise description of the installation location	–
Slot	Precise description of the installation location	–
Short designation	Module name	Module info/name
Description	Description of the module	ModuleInfo/InfoText
Article no.	Module item number	ModuleInfo/OrderNumber
Firmware version	Firmware version	ModuleInfo/SoftwareRelease
Hardware product version	Hardware version	ModuleInfo/HardwareRelease
GSD File	GSDML filename	–

5.10.2.2 “PROFINET Interface [X1]” Section

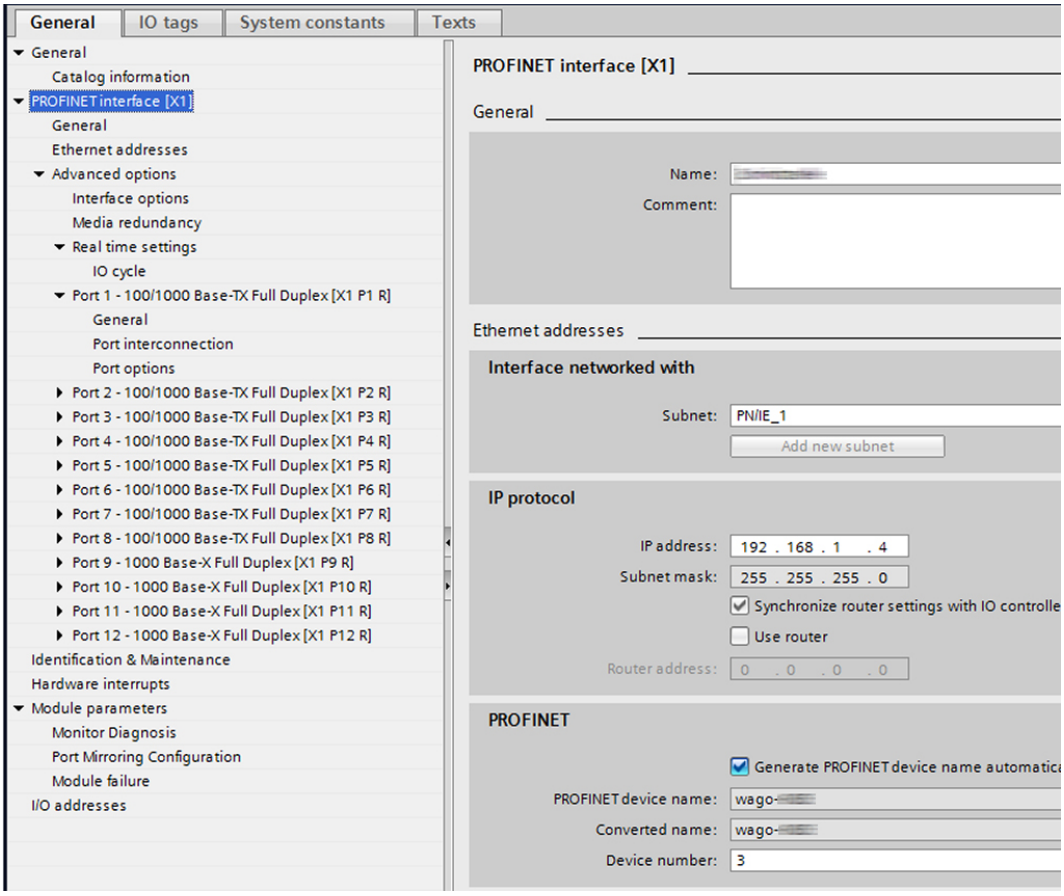


Figure 18: PROFINET Parameters – “PROFINET Interface [X1]” Section

Table 24: PROFINET Parameters for “PROFINET Interface [X1]” Section

Parameter	Description	Tag in the GSDML
Name	Interface name	SystemDefinedSubmoduleList/ InterfaceSubmoduleItem
Comment	Comment field	–
Subnet	Subnet name	–
IP address	IP address (default: 0.0.0.0)	–
Subnet mask	Subnet mask	–
PROFINET device name	Device name; can be loaded automatically from the GSDML file.	DeviceAccessPointItem [DNS_CompatibleName]
Converted name	Device name; is loaded automatically from the GSDML file.	DeviceAccessPointItem [DNS_CompatibleName]
Device number	Device number in the network	–

5.10.2.3 “Advanced Options” Section

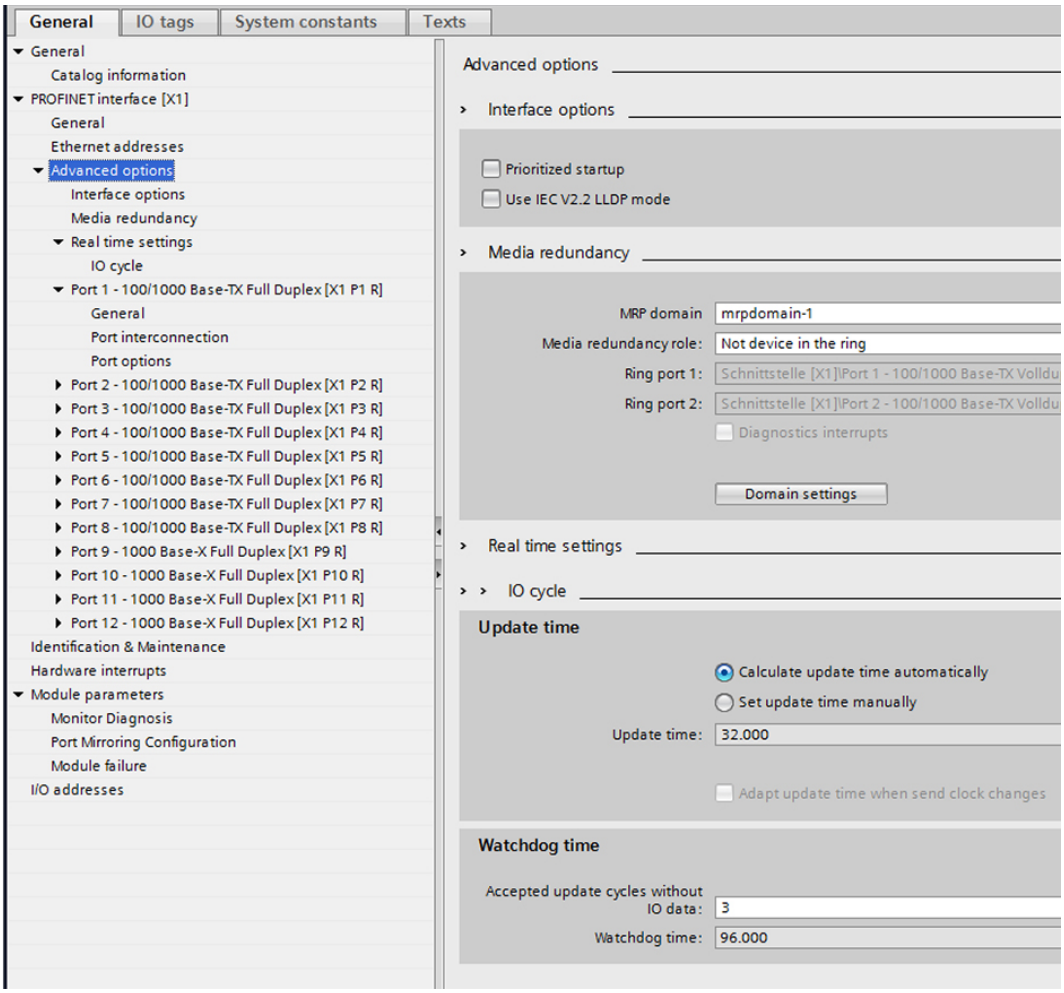


Figure 19: PROFINET Parameters – “Advanced Options” Section

Table 25: PROFINET Parameters for “Advanced Options” Section

Parameter	Description	Tag in the GSDML
MRP domain	Name of the MRP	–
Media redundancy role	Client (MRC) or Manager (MRM) in the ring	SystemDefinedSubmoduleList/ InterfaceSubmoduleItem/ MediaRedundancy
Ring port 1	The 1st port assigned to the MRP ring	–
Ring port 2	The 2nd port assigned to the MRP ring	–
Update time	Cycle time for I/O data	SystemDefinedSubmoduleList/ InterfaceSubmoduleItem/ ApplicationRelations
Accepted update cycles without IO data	Factor of the update time after which an error is generated.	–
Watchdog time	Product of update time and factor	–

5.10.2.4 “Port 1” Section

The following descriptions use port 1 as an example. They also apply to ports 2 to 12 accordingly.

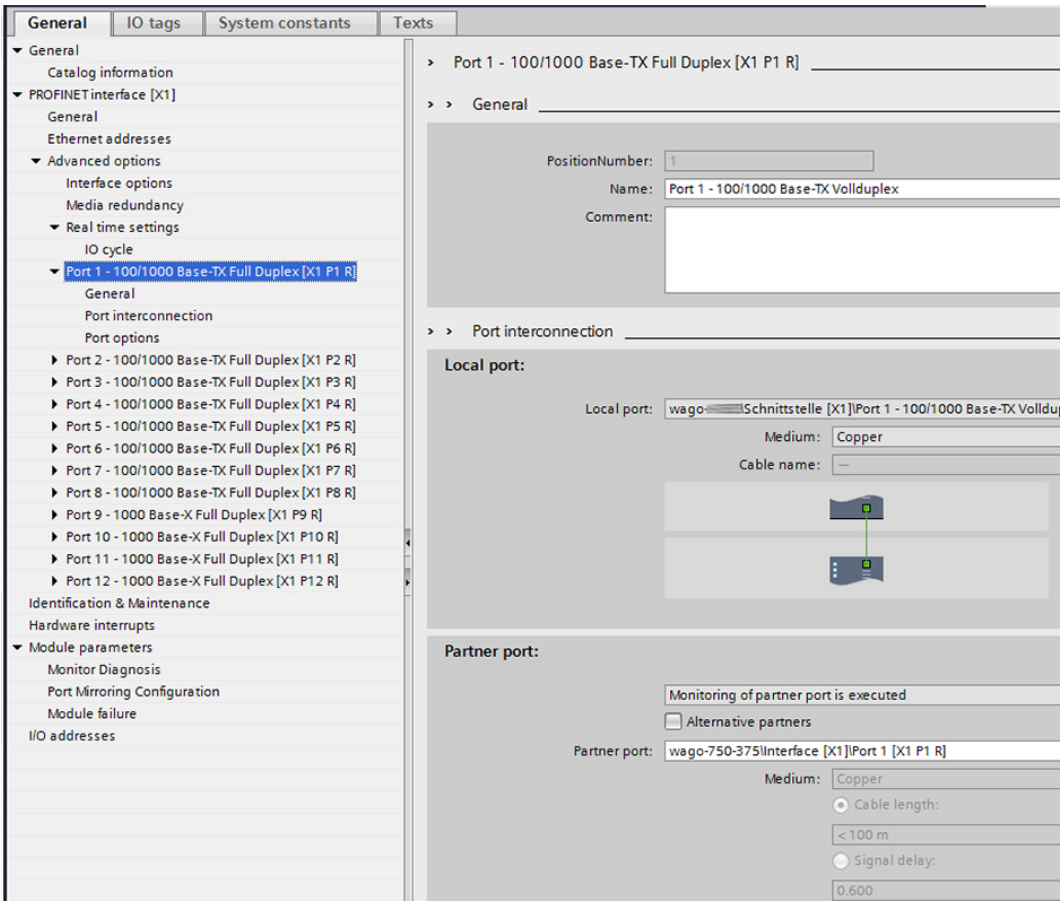


Figure 20: PROFINET Parameters – “Port 1” Section

Table 26: PROFINET Parameters for “Port 1” Section

Parameter	Description	Tag in the GSDML
Name	Port name	SystemDefinedSubmoduleList/ PortSubmoduleItem
Comment	Comment field	–
Local port	Local port location information	–
Medium	Transmission medium	–
Partner Port	Connected port	–

5.10.2.5 “Port Options” Section

The following descriptions use port 1 as an example. They also apply to ports 2 to 12 accordingly.

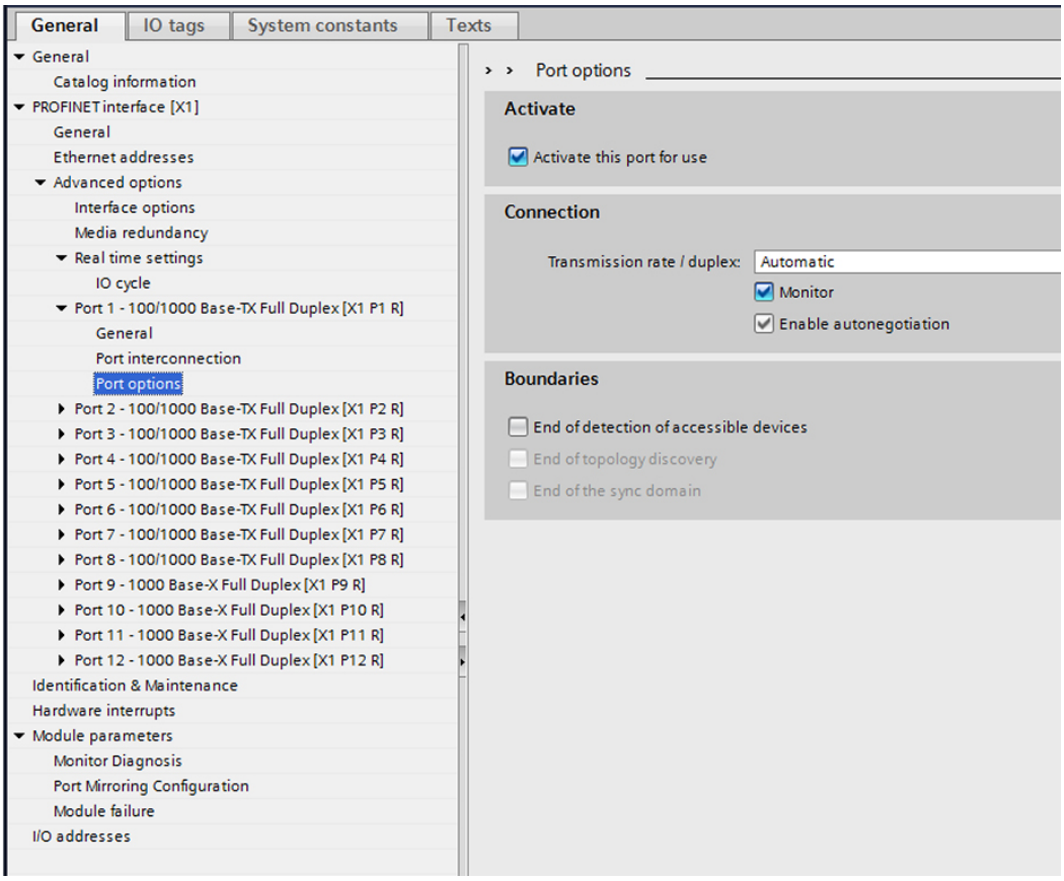


Figure 21: PROFINET Parameters – “General” Section

Table 27: PROFINET Parameters for “Advanced Options” Section

Parameter	Description	Tag in the GSDML
Activate	Enable/disable port.	–
Transmission rate/duplex	Transmission rate and duplex mode setting	ValueList/ ValueItem[ID=“ID_RV_PORT_RATE”]
Monitor	Enable/disable monitoring.	–
Enable autonegotiation	Enable/disable autonegotiation.	–

5.10.2.6 “Identification & Maintenance” Section

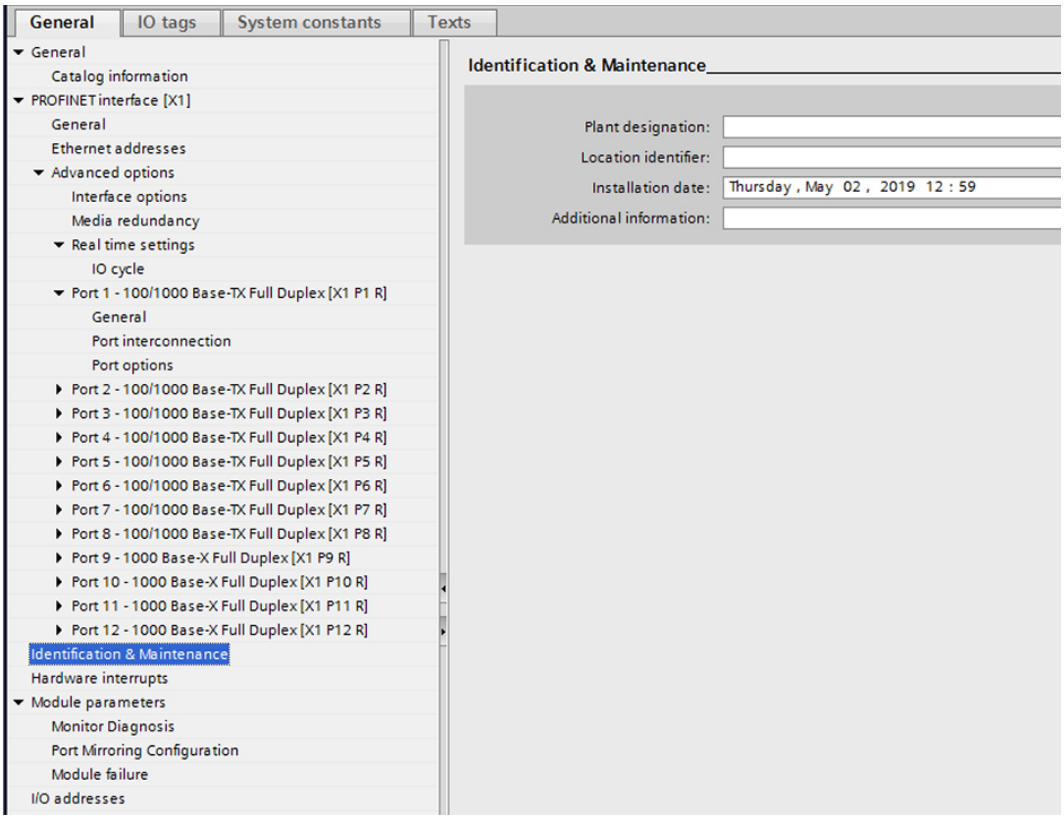


Figure 22: PROFINET Parameters – “Identification & Maintenance” Section

Table 28: PROFINET Parameters for “Identification & Maintenance” Section

Parameter	Description	Tag in the GSDML
Plant designation	Identifier for the system	–
Location Identifier	Identifier for the installation location	–
Installation date	Date for installation	–
Additional information	Comment field	–

5.10.2.7 “Process Alarms” Section

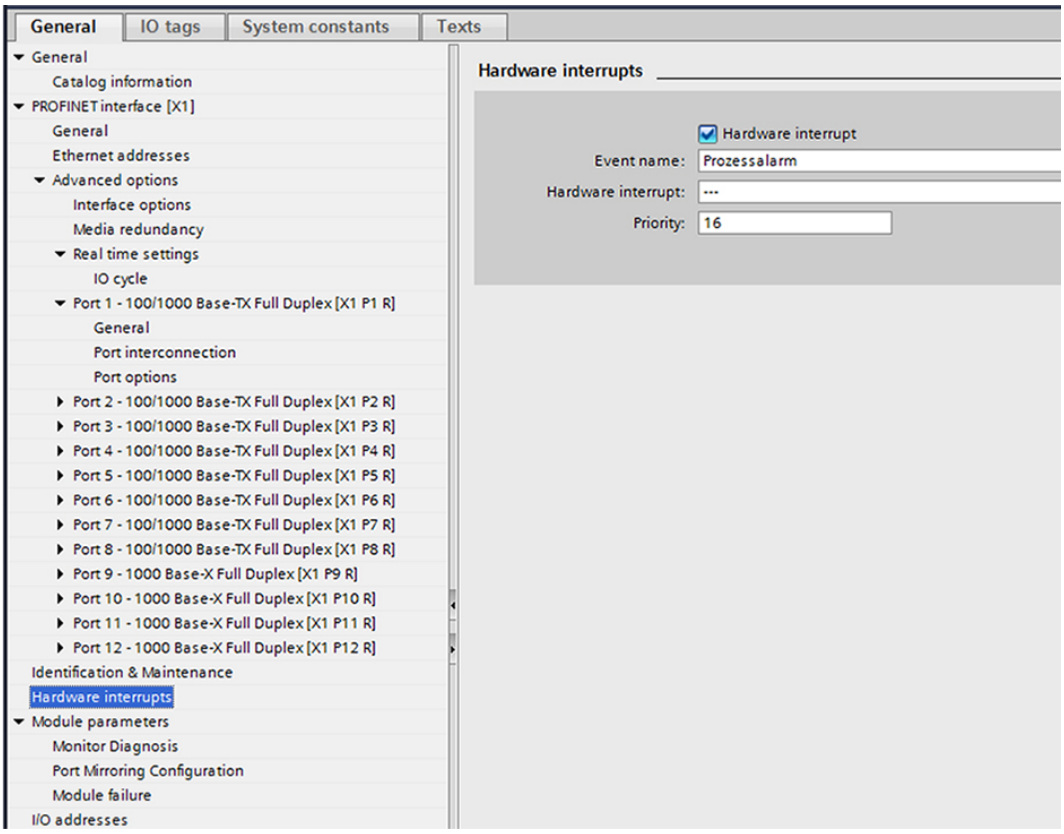


Figure 23: PROFINET Parameters – “Process Alarms” Section

Table 29: PROFINET Parameters for “Process Alarms” Section

Parameter	Description	Tag in the GSDML
Event Name	Alarm name	–
Hardware interrupt	Enable/disable process alarm monitoring.	DeviceAccessPointItem/ VirtualSubmoduleList/ VirtualSubmoduleItem
Priority	Priority for the data transfer	–

5.10.2.8 “Assembly Parameters” Section

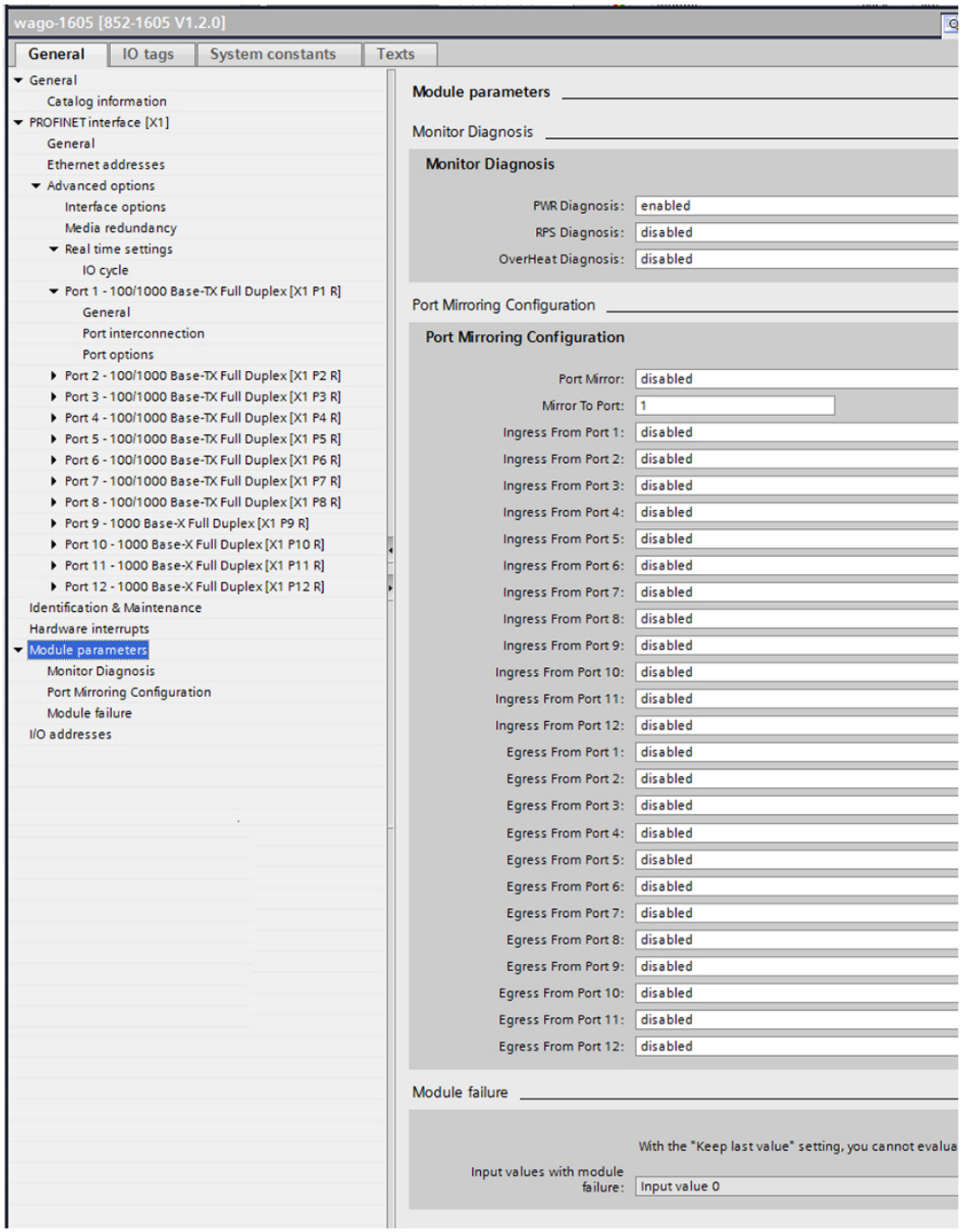


Figure 24: PROFINET Parameters – “Assembly Parameters” Section

Table 30: PROFINET Parameters for “Assembly Parameters” Section

Parameter	Description	Tag in the GSDML
PWR Diagnostics	“Primary power supply” diagnostics	ChannelDiagList/ SystemDefinedChannelDiagItem [ErrorType = “2”]
RPS Diagnostics	“Secondary power supply" diagnostics	ChannelDiagList/ SystemDefinedChannelDiagItem [ErrorType = “3”]
Overheating Diagnostics	“Overheating” diagnostics	ChannelDiagList/ SystemDefinedChannelDiagItem [ErrorType = “5”]
Port Mirror	Port mirroring enabled/disabled	DeviceAccessPointItem/ VirtualSubmoduleList/ VirtualSubmoduleItem/RecordDataList/ ParameterRecordDataItem
Mirror to Port	The port that should be mirrored	DeviceAccessPointItem/ VirtualSubmoduleList/ VirtualSubmoduleItem/RecordDataList/ ParameterRecordDataItem
Ingress From Port (x)	“Input” port mirroring for port (x) enabled/disabled	DeviceAccessPointList/ SystemDefinedSubmoduleList/ PortSubmoduleItem
Egress From Port (x)	“Output” port mirroring for port (x) enabled/disabled	DeviceAccessPointList/ SystemDefinedSubmoduleList/ PortSubmoduleItem
Input values with module failure	The value is used in the event of assembly failure	–

5.10.2.9 “I/O Addresses” Section

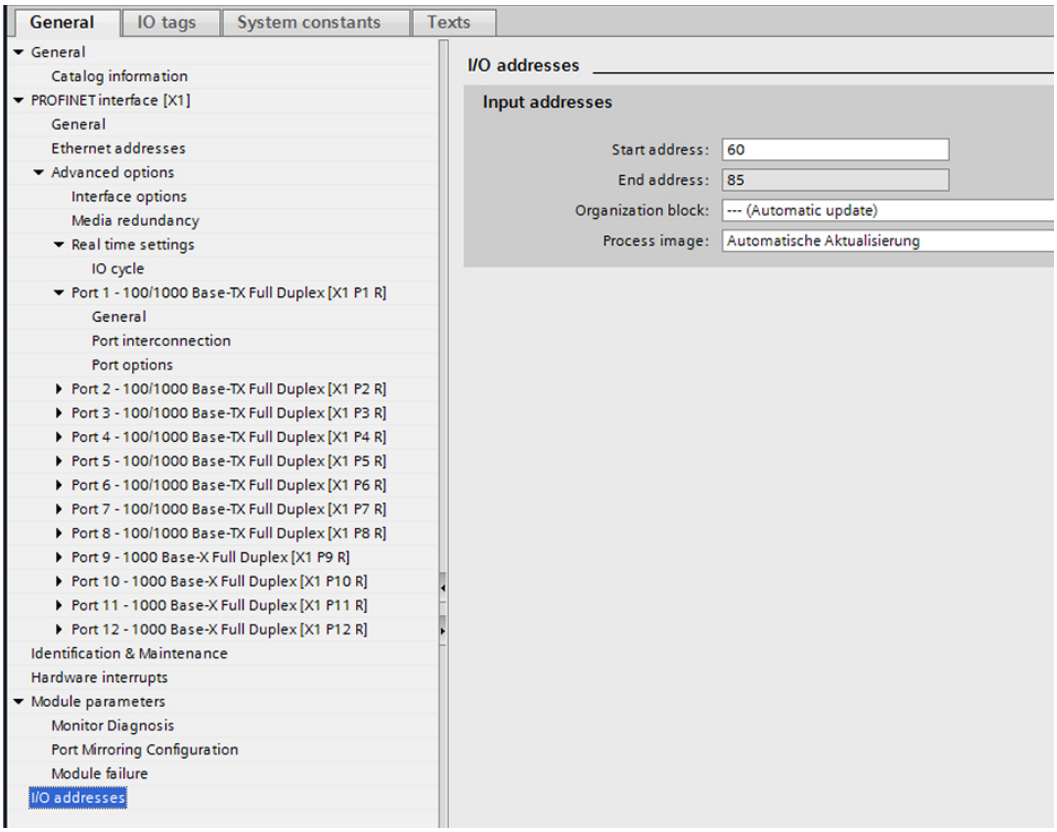


Figure 25: PROFINET Parameters – “I/O Addresses” Section

Table 31: PROFINET Parameters for “I/O Addresses” Section

Parameter	Description	Tag in the GSDML
Start address	Start address of the cyclic address image	–
End address	Is generated automatically	–
Organization block	Update of organization block	–
Process image	Update of the I/O data process image	–

5.11 Cyclic I/O Data

Cyclic I/O data is always sent between PLCs and switches for a specified period. This data is transferred almost in real time. For example, status information on the switches and variables that need to be written to the switch is typically part of the cyclic data.

Cyclic I/O data is linked to the submodules.

Subslot 0 is not standardly used for I/O submodules.

PROFINET distinguishes three types of submodules:

- Virtual submodules
- Interface submodules
- Port submodules

All these submodules can be linked with I/O data.

Subslot 1 always contains the virtual submodule.

The PROFINET managed switch defines all cyclic I/O data only in the virtual submodule. This virtual submodule is assigned to slot 0/subslot 1.

The cyclic I/O data comprises 26 bytes. The first two data bytes provide diagnostic information on the device. The following 24 bytes represent the port status information (two bytes of data per port).

The cyclic I/O data is only generated if it has been configured correspondingly with the respective engineering tool.

The following overview illustrates the cyclic I/O data format.

Table 32: Format for Cyclic I/O Data – PROFINET

Byte Offset	Size	Description
0	16 bits	Diagnostic status of the PROFINET managed switch
2	16 bits	PORT 1 status
4	16 bits	PORT 2 status
6	16 bits	PORT 3 status
8	16 bits	PORT 4 status
10	16 bits	PORT 5 status
12	16 bits	PORT 6 status
14	16 bits	PORT 7 status
16	16 bits	PORT 8 status
18	16 bits	PORT 9 status
20	16 bits	PORT 10 status
22	16 bits	PORT 11 status
24	16 bits	PORT 12 status

5.11.1 Example of Cyclic I/O Data

The following example is based on the “TIA” engineering tool from Siemens.

When cyclic IO data that is addressed with slot 0/subslot 1 is dragged and dropped from the hardware catalog into the network view, the TIA portal automatically generates a mapping address for it.

The user can then use the mapping address to access each data bit via the PLC tags.

The data is represented as a WORD (16 bits).

The following overview shows the detailed structure of the data:

Table 33: Cyclic Input for Device Diagnostics

TAG	Bit	Description	Value	Comment
DIAG.%X0	0	pn_diagcode_board_temp	0 = NO 1 = YES	Mainboard overheating
DIAG.%X1	1	pn_diagcode_cpu_temp	0 = NO 1 = YES	CPU overheating
DIAG.%X2	2	pn_diagcode_phy_temp	0 = NO 1 = YES	PHY overheating
DIAG.%X3	3	pn_diagcode_pwr_ovolt	0 = NO 1 = YES	Primary power supply overvoltage
DIAG.%X4	4	pn_diagcode_rps_ovolt	0 = NO 1 = YES	Secondary power supply overvoltage
DIAG.%X5	5	pn_diagcode_pwr_uvolt	0 = NO 1 = YES	Primary power supply undervoltage
DIAG.%X6	6	pn_diagcode_rps_uvolt	0 = NO 1 = YES	Secondary power supply undervoltage
DIAG.%X7	7	pn_diagcode_pwr_nopwr	0 = NO 1 = YES	Primary power supply not present.
DIAG.%X8	8	pn_diagcode_rps_nopwr	0 = NO 1 = YES	Secondary power supply not present.
DIAG.%X9	9	MRP ring state	0 = inactive 1 = active	
DIAG.%X10	10	MRP ring running status	0 = closed 1 = open	Note: Only makes sense if DIAG.%X9 = 1
DIAG.%X11 … DIAG.%X14	11 … 14	Reserved		
DIAG.%X15	15	Device status	0 = OK 1 = error	PROFINET stack does not generate alarm if DIAG.%X15 = 0.

Table 34: Cyclic Input for Status of Port Pn (n = 1 … 12)

TAG	Bit	Description	Value	Comment
Pn.%X0	0	Port power status	0 = Off 1 = on	
Pn.%X1	1	Port duplex mode	0 = full duplex 1 = half duplex	
Pn.%X2	2	Port link status	0 = link off 1 = link on	
Pn.%X3	3	Port speed	0b000 = 10 M 0b001 = 100 M 0b010 = 1000 M 0b111 = auto	This bit is combined with Pn.%X4 and Pn.%X5.
Pn.%X4	4			
Pn.%X5	5			
Pn.%X6	6	Port current link activity	1 = disable 2 = block 3 = listen 4 = learn 5 = forward	This bit is combined with Pn.%X7 and Pn.%X8.
Pn.%X7	7			
Pn.%X8	8			
Pn.%X9	9	Port LLDP admin status	0 = disabled 1 = Txonly 2 = Rxonly 3 = TxRx	This bit is combined with Pn.%X10.
Pn.%X10	10			
Pn.%X11 … Pn.%X15	11 … 15	Reserved		

5.12 DAP Parameters

DAP parameters are used for configuring the IO device.

After the IO device starts up, these parameters are transferred:

- The IO controller reads these parameters from the IO device to get the functions of the IO device.
- The IO controller writes these parameters to the IO device to configure the functions of the IO device.

The following DAP parameters are provided for the PROFINET managed switch:

Table 35: DAP Parameters for WAGO PROFINET Switch

Index	Subslot	Access	Length	Description
1	0x1	R/W	3	Enable/disable diagnostic messages.
2	0x8001 … 0x800C	R	6	Reading the port status (for each port)
3	0x1	R	12	Reading the device diagnostics
4	0x1	R/W	10	Configuring the port mirroring function

Below you can find the detailed data structure of the individual parameter indices.

INDEX=1

Table 36:Enable/Disable Diagnostic Messages

Offset	Value	Description	Default Value
0	0	Enable “PWR Diagnostics” alarm.	0
	1	Disable “PWR Diagnostics” alarm.	
1	0	Enable “RPS Diagnostics” alarm.	0
	1	Disable “RPS Diagnostics” alarm.	
2	0	Enable temperature diagnostics.	0
	1	Disable temperature diagnostics.	

INDEX=2

Table 37: Reading the Port Status (for Each Port)

Offset	Value	Description	Default Value
0	0	Port switched off	0
	1	Port switched on	
1	0	Port: modus – full duplex	0
	1	Port: mode – half duplex	
2	0	Port: link – off	0
	1	Port: link – on	
3	0	Port: transmission speed – 10 Mbit/s	0
	1	Port: transmission speed – 100 Mbit/s	
	2	Port: transmission speed – 1 Gbit/s	
	7	Port: transmission speed – automatic	
4	1	Port: link activity – disabled	5
	2	Port: link activity – blocked	
	3	Port: link activity – listen	
	4	Port: link activity – learn	
	5	Port: link activity – forward	
5	0	Port: LLDP admin status – disabled	0
	1	Port: LLDP admin status – Tx only	
	2	Port: LLDP admin status – Rx only	
	3	Port: LLDP admin status – Tx/Rx	

INDEX=3

Table 38: Reading the Device Diagnostics

Offset	Value	Description	Default Value
0	0	Mainboard – no overheating	0
	1	Mainboard – overheating	
1	0	CPU – no overheating	0
	1	CPU – overheating	
2	0	ETHERNET PHY – no overheating	0
	1	ETHERNET PHY – overheating	
3	0	PWR – no overvoltage	0
	1	PWR – overvoltage	
4	0	RPS – no overvoltage	0
	1	RPS – overvoltage	
5	0	PWR – no undervoltage	0
	1	PWR – undervoltage	
6	0	RPS – no undervoltage	0
	1	RPS – undervoltage	
7	0	PWR has voltage.	0
	1	PWR has no voltage.	
8	0	RPS has voltage.	0
	1	RPS has no voltage.	
9	0	MRP ring disabled.	0
	1	MRP ring enabled.	
10	0	MRP ring opened (makes sense if byte 9 = 1)	0
	1	MRP ring closed (makes sense if byte 9 = 1)	
11	0	Device has errors (alarm).	0
	1	Device is functioning normally; no alarm set.	

INDEX=4, Configure Port Mirror

Table 39: Configuring the Port Mirroring Function

Byte Offset	Bit Offset	Value	Description	Default Value
0	–	0	Disable port mirroring.	0
		1	Enable port mirroring.	
1	–	0 … 255	Destination port for mirroring	0
2	0	0	Disable mirroring for port 1 input.	0
		1	Enable mirroring for port 1 input.	
	1	0	Disable mirroring for port 2 input.	0
		1	Enable mirroring for port 2 input.	
…				
3	3	0	Disable mirroring for port 12 input.	0
		1	Enable mirroring for port 12 input.	
…				
6	0	0	Disable mirroring for port 1 output.	0
		1	Enable mirroring for port 1 output.	
…				
9	7	0	Disable mirroring for port 12 output.	0
		1	Enable mirroring for port 12 output.	

Unlike the cyclic I/O data, the DAP parameters are accessed via RDREC/WRREC function blocks (e.g., in TIA; also see the application note on the WAGO PROFINET managed switch).

5.13 Access via Console Port (CLI)

5.13.1 Assigning the IP Addresses with the Console Port

The PROFINET managed switch is provided with the following IPv4 settings:

- IP address 0.0.0.0
- Subnet mask 0.0.0.0
- Default gateway 0.0.0.0

In PROFINET mode, the network parameters can only be assigned by the engineering tool or the PROFINET controller.

Below we described how the IP address of the PROFINET managed switch can be configured with the help of the console port.

1. Connect the computer to the console port on the switch using the appropriate cable.

2. Use the following settings for the console port:

Table 40: Default Settings for the Console Port

Setting	Default Value
Baud rate	38400
Parity	None
Number of data bits	8
Number of stop bits	1
Flow control	None

3. Press **[ENTER]** to open the login screen.

```
L2SWITCH login:
```

4. Enter **[admin]** to go to CLI mode.

```
PN-SWITCH login: admin
PN-SWITCH>
```

5. Enter **[enable]** to switch to privileged mode. Use the following default values for the username and password.

```
PN-SWITCH>enable
user:admin
password: wago
```

6. Enter **[show running config]** to see the current device configuration.

```
PN-SWITCH#show running-config
Current configuration:
vlan 1
name VLAN1
fixed 1-12
!
interface gigabitethernet1/0/1
!
interface gigabitethernet1/0/2
!
interface gigabitethernet1/0/3
!
interface gigabitethernet1/0/4
!
interface gigabitethernet1/0/5
!
interface gigabitethernet1/0/6
!
interface gigabitethernet1/0/7
!
interface gigabitethernet1/0/8
!
interface gigabitethernet1/0/9
!
interface gigabitethernet1/0/10
!
interface gigabitethernet1/0/11
!
interface gigabitethernet1/0/12
!
interface eth0
ip address 0.0.0.0/0
ip address default-gateway 0.0.0.0
!
profinet enable
lldp enable

mrp ring-id 1
no ring enable
ring uuid ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
ring port-1 1
ring port-2 2
ring vlan 1
!
model-name 852-0603
```

7. Enter **[configure terminal]** to configure the device.

```
PN-SWITCH#configure terminal
PN-SWITCH(config)#
```

8. Enter **[profinet disable]** to disable PROFINET on the device.

```
PN-SWITCH(config)#profinet disable
Success!
```

9. Enter **[interface eth0]** to configure the network parameters of the switch.

```
PN-SWITCH(config)#interface eth0
PN-SWITCH(config-if)#
```

10. Enter **[ip address 192.168.1.254/24]** to configure a new IP address (e.g., 192.168.1.254) or subnet mask (e.g., 255.255.255.0).

```
PN-SWITCH(config-if)#ip 192.168.1.254/24
Warning: Default gateway works in different subnet from
IP.
```

11. Enter **[exit]** to exit the network parameter configuration menu.

```
PN-SWITCH(config-if)#exit
PN-SWITCH(config)#
```

12. Enter **[exit]** to exit the device configuration menu.

```
PN-SWITCH(config)#exit
PN-SWITCH#
```

13. Enter **[show running config]** to see the current device configuration.

```
PN-SWITCH#show running-config
Current configuration:
vlan 1
name VLAN1
fixed 1-12
!
interface gigabitethernet1/0/1
!
interface gigabitethernet1/0/2
!
interface gigabitethernet1/0/3
!
interface gigabitethernet1/0/4
!
interface gigabitethernet1/0/5
!
interface gigabitethernet1/0/6
!
interface gigabitethernet1/0/7
!
interface gigabitethernet1/0/8
!
interface gigabitethernet1/0/9
!
interface gigabitethernet1/0/10
!
```

```
interface gigabitethernet1/0/11
!
interface gigabitethernet1/0/12
!
interface eth0
ip address 192.168.1.254/24
ip address default-gateway 0.0.0.0
!
lldp enable

mrp ring-id 1
no ring enable
ring uuid ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
ring port-1 1
ring port-2 2
ring vlan 1
!
model-name 852-0603
```

You can now reach the PROFINET managed switch with your Web browser at the IP address 192.168.1.254.

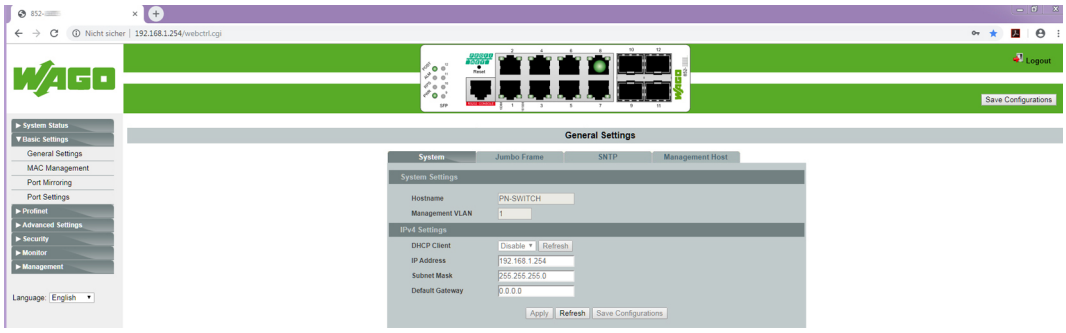


Abbildung 26: Aufrufen des PROFINET-Managed-Switches über das WBM

5.14 Parameterization via WBM in PROFINET Mode

An internal file system and integrated Webserver can be used for configuration and administration of the PROFINET managed switch. Together, they are referred to as WBM (“**W**eb-**B**ased **M**anagement system”).

The PROFINET managed switch is supplied with PROFINET mode enabled. The following settings apply upon delivery:

- IP address: 0.0.0.0
- Subnet mask: 0.0.0.0

In order to be able to use WBM, you must first assign an IP address. Various options exist:

- Use a corresponding engineering tool (see section “Project Planning”)
- Use the console port (also see section “Access via Console [CLI]”)
- use DCP with an external tool (e.g., PRONETA from Siemens or PROFINET Commander)

Only limited WBM functionality is available in PROFINET mode.

Note

More information on WBM
This section describes the functionalities that can be implemented via WBM with PROFINET mode enabled.
You can find comprehensive information on WBM in the section “Configuring in the Web-Based Management System (WBM).”

If PROFINET mode is enabled, a large number of parameters are configured by the IO controller. If configuration in WBM is not possible, this is indicated in WBM by the sentence “**Configuration in PROFINET mode is performed by the PNIO controller**.”

WBM can be reached at the IP address according to the configuration.

The HTML pages stored internally provide you with information about the configuration and status of the fieldbus node. In addition, you can also change the configuration of the device here.
You can also save HTML pages you created yourself via the implemented file system.

Note

Always restart after making changes to the configuration!
The system must always be restarted for the changed configuration settings to take effect.

1. Open a Web browser in order to open WBM. For using WBM, we recommend using an up-to-date version of Google Chrome or Firefox.

2. Enter the IP address of the PROFINET managed switch in the address bar.

3. Click **[Enter]** to confirm.

4. Enter your username and password in the login window:

   Default user = “admin”
   Default password = “wago”

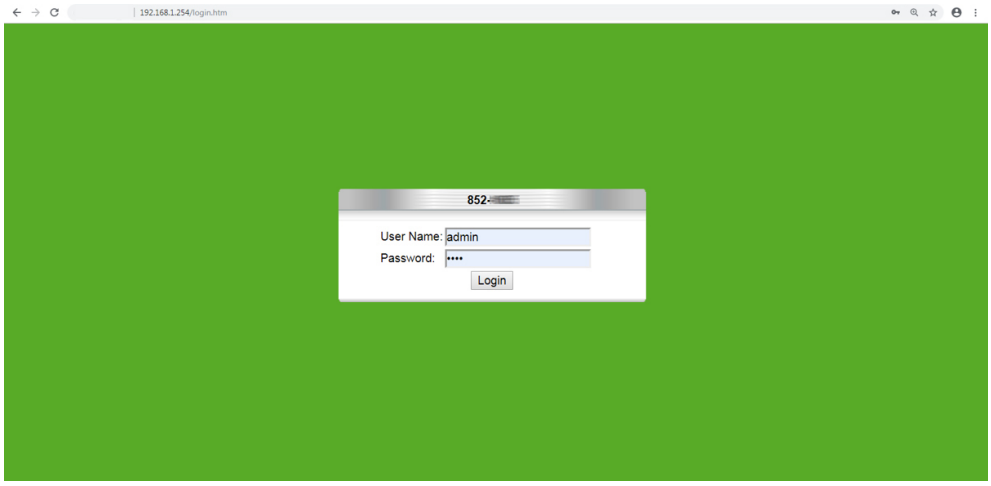


Figure 27: Login Window for WBM

   WAGO recommends changing the username and password after the initial login. You can find these settings in the **Management** > **SNMP** > **User Account** menu.

5. The WBM start page loads.

6. Make the desired settings.

7. Click **[Apply]** or **[Update]** to confirm your changes, or click **[Delete]** or **[Discard]** to discard your changes.

8. To apply the settings, confirm your changes with the **[Save Configuration]** button.

You can access the corresponding WBM pages via the links in the navigation bar:

Table 41: Overview – Navigation Links and WBM Pages

Navigation Links and WBM Pages
▶ **[System Status]**
• System Information
▶ **[Basic Settings]**
• General Settings • Port Mirroring • Port Settings
▶ **[PROFINET]**
• Configuration • Information • Diagnostics
▶ **[Advanced Settings]**
• MRP
▶ [Security]
▶ [Monitor]
▶ **[Management]**
[SNMP] • Upload File • User Account

The settings/configuration of the PROFINET managed switch can be made on these WBM pages.

There are tab pages on some WBM pages for the settings/configurations.

The default values are shown in **bold**.

5.14.1 System Status

5.14.1.1 System Information

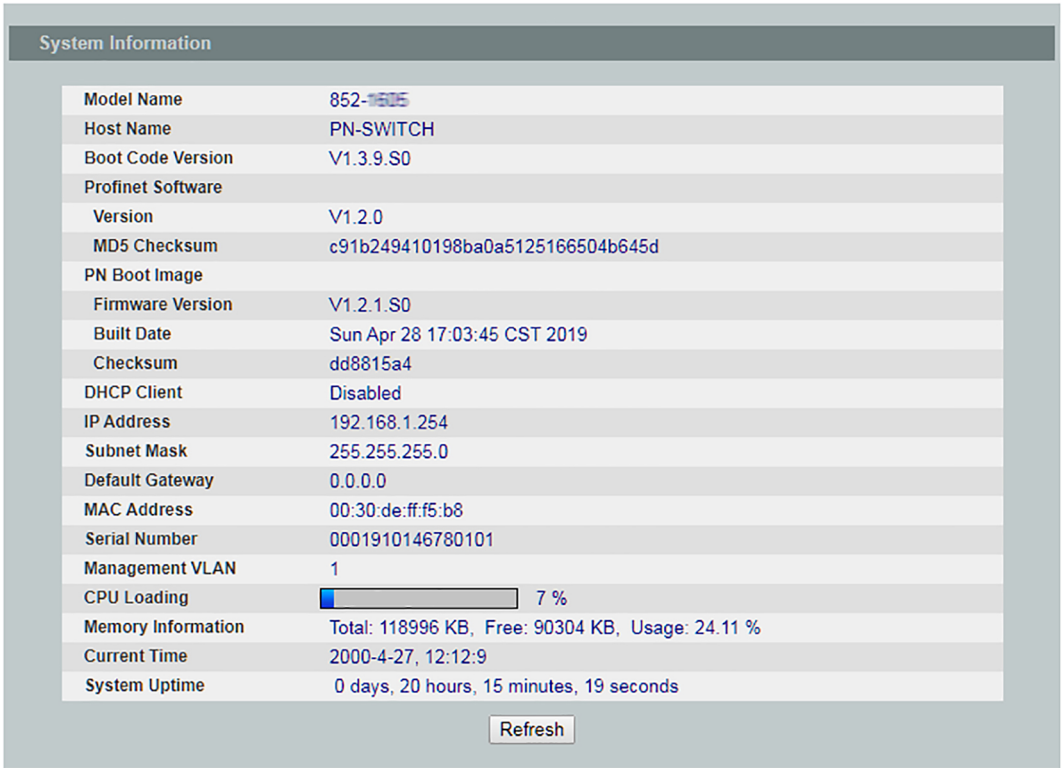


Figure 28: WBM Page “System Information”

Table 42: WBM Page “System Information”

Parameter	Description
Model Name	This field shows the model name of the switch.
Host Name	This field shows the host name of the switch.
Boot Code Version	This field shows the boot code version.
Profinet Software Version	ID number of the PROFINET software version
Profinet Software MD5 Checksum	Checksum of the PROFINET software version
PN Boot Image Firmware Version	This field shows the PROFINET boot image version.
PN Boot Image Build Date	This field shows the firmware build date.
PN Boot Image Checksum	This field shows the PROFINET boot image checksum.
DHCP Client	This field indicates whether the DHCP client function is enabled.
IP Address	This field shows the IP address of the switch.
Subnet Mask	This field shows the subnet mask of switch.
Default Gateway	This field shows the default gateway of the switch.
MAC Address	This field shows the MAC (Media Access Control) address of the switch.
Serial Number	This field shows the serial number.
Management VLAN	This field shows the VLAN ID required for the switch management process.
CPU Loading	This field shows the system load of the switch as a percentage.
Memory Information	This field shows the total memory (“Total”), memory available at the moment (“Free”) and memory used (“Usage”) of the switch.
Current Time	This field shows the current date (yyyy-mm-dd) and current time (hh:mm:ss).
System Uptime	This field shows how long the switch has been in operation since being switched on, in days, hours, minutes and seconds.

5.14.2 Basic Settings

5.14.2.1 General Settings

5.14.2.1.1 System

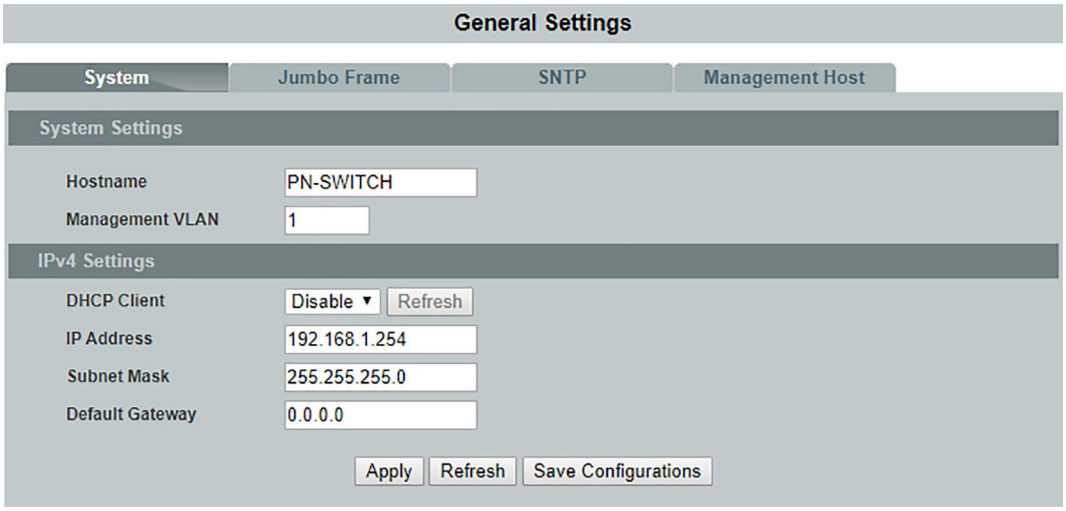


Figure 29: WBM Page “General Settings” – “System” Tab

Table 43: WBM Page “General Settings” – “System” Tab

System Settings		
Parameter	**Default**	**Description**
Hostname	**L2SWITCH**	Enter up to 64 alphanumeric characters for the name of your switch in the input field. The hostname should be a combination of numbers, letters, hyphens (-) and underscores (_).
Management VLAN	**1**	In the input field, enter a VLAN group that should be given access the switch. Valid VLAN range: 1 … 4094.
		Note  **Configuring a management VLAN** Before configuring a management VLAN, you must first create a management VLAN and assign it at least one subscriber port.
IPv4 settings		
Parameter	**Default**	**Description**
DHCP Client	**Disable**	Select “Disable” from the drop-down list if you want to manually configure the IP address of the switch.
	Enable	Select “Enable” from the drop-down list to allow the switch to get its IP address from a DHCP server automatically. Click **[Update]** to allow the switch to get an IP address from the DHCP server.
IP Address	**0.0.0.0**	Enter the IP address of the switch in decimal-point notation in the input field.
Subnet Mask	**0.0.0.0**	Enter the IP subnet mask of the switch in the input field in decimal-point notation.
Default Gateway	0.0.0.0	Enter the IP address of the default outgoing gateway in decimal-point notation in the input field.

5.14.2.2 Port Mirroring

NOTICE

Incorrect mirroring can interfere with application!

Incorrect port mirroring can interfere with the application or make it unstable. In this case, the switch in PROFINET mode can be simply restarted. The IO controller then overwrites the incorrect settings with the current configuration.

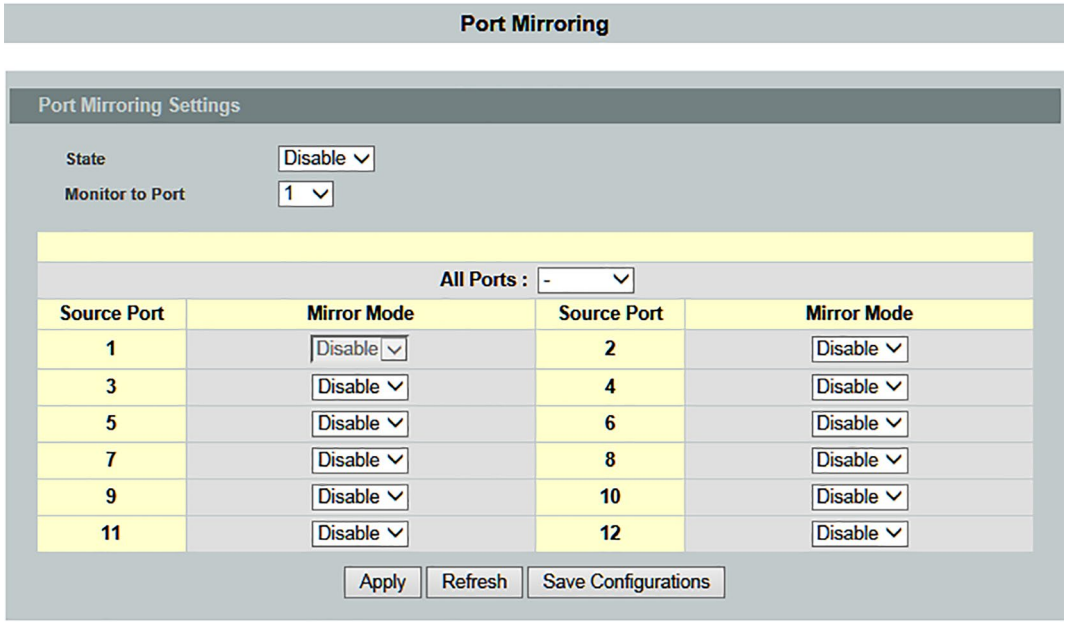


Figure 30: WBM Page “Port Mirroring Settings”

Table 44: WBM Page “Port Mirroring Settings”

Parameter	Default	Description
State	**Disable**	Select “Disable” to disable the “Port Mirroring”.
	Enable	Select “Enable” to enable the “Port Mirroring”.
Monitor to Port	**1** … 10 (12)	Select a port to be connected to a “Network Traffic Analyzer”.
All Ports:	**–**	Settings in this select box apply to all ports. Make settings here to be applied to all ports. Start here with general settings and then change the settings for individual ports.
	Disable	
	Ingress	
	Egress	
	Both	
Source Port	**1** … 10 (12)	This column displays the number of individual source ports.
Mirror Mode	**Disable**	Select “Disable” to prevent traffic being copied from the specified source port to the monitor port.
	Ingress	Select “Ingress” to only copy the input data (incoming) from the specified source ports to the monitor port.
	Egress	Select “Egress” to only copy the output data (outgoing) from the specified source ports to the monitor port.
	Both	Select “Both” to copy both incoming and outgoing data from the specified source ports to the monitor port.
	Unset	This column displays the number of individual source ports.

The PROFINET managed switch permits multi-port mirroring, i.e. multiple ports can be mirrored on one destination port.

These settings can be reset via a switch reset/reboot.

5.14.2.3 Port Settings

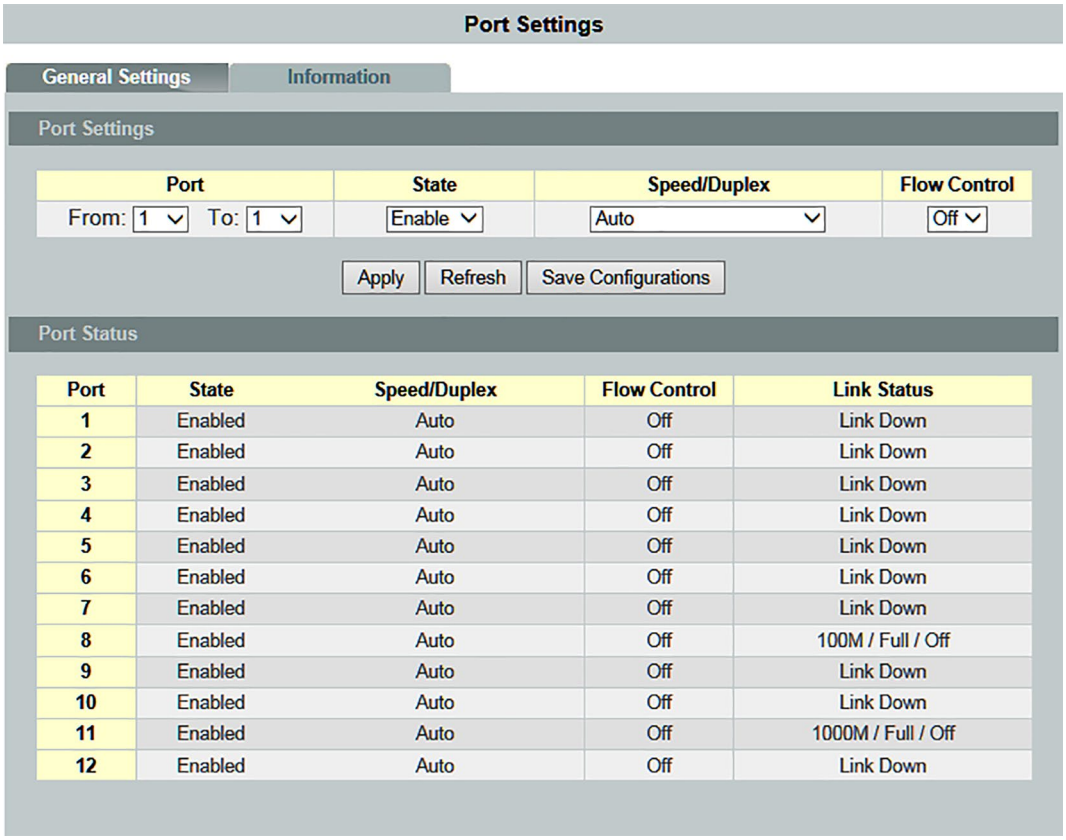


Figure 31: WBM Page “Port Settings” – “General Settings” Tab

In PROFINET mode, this page is only for information. Changing settings is not possible.

5.14.3 PROFINET

5.14.3.1 PROFINET Setting

Figure 32: WBM Page “PROFINET Setting”

PROFINET mode is activated by default upon delivery.

NOTICE

WBM settings in PROFINET mode can lead to malfunctions!
If the PROFINET managed switch is in PROFINET mode, it is configured by the IO controller. Changes to the settings in WBM can lead to a switch malfunction in the PROFINET network.
When the switch is reset, the IO controller reloads the configuration onto the device. This overwrites incorrect configurations.

Table 45: WBM Page “PROFINET Setting”

Parameter	Default	Description
State	**Enable**	Select “Enable” from the drop-down list if you want to activate “PROFINET Setting”.
	Disable	Select “Disable” from the drop-down list if you want to deactivate “PROFINET Setting”

5.14.3.2 Information

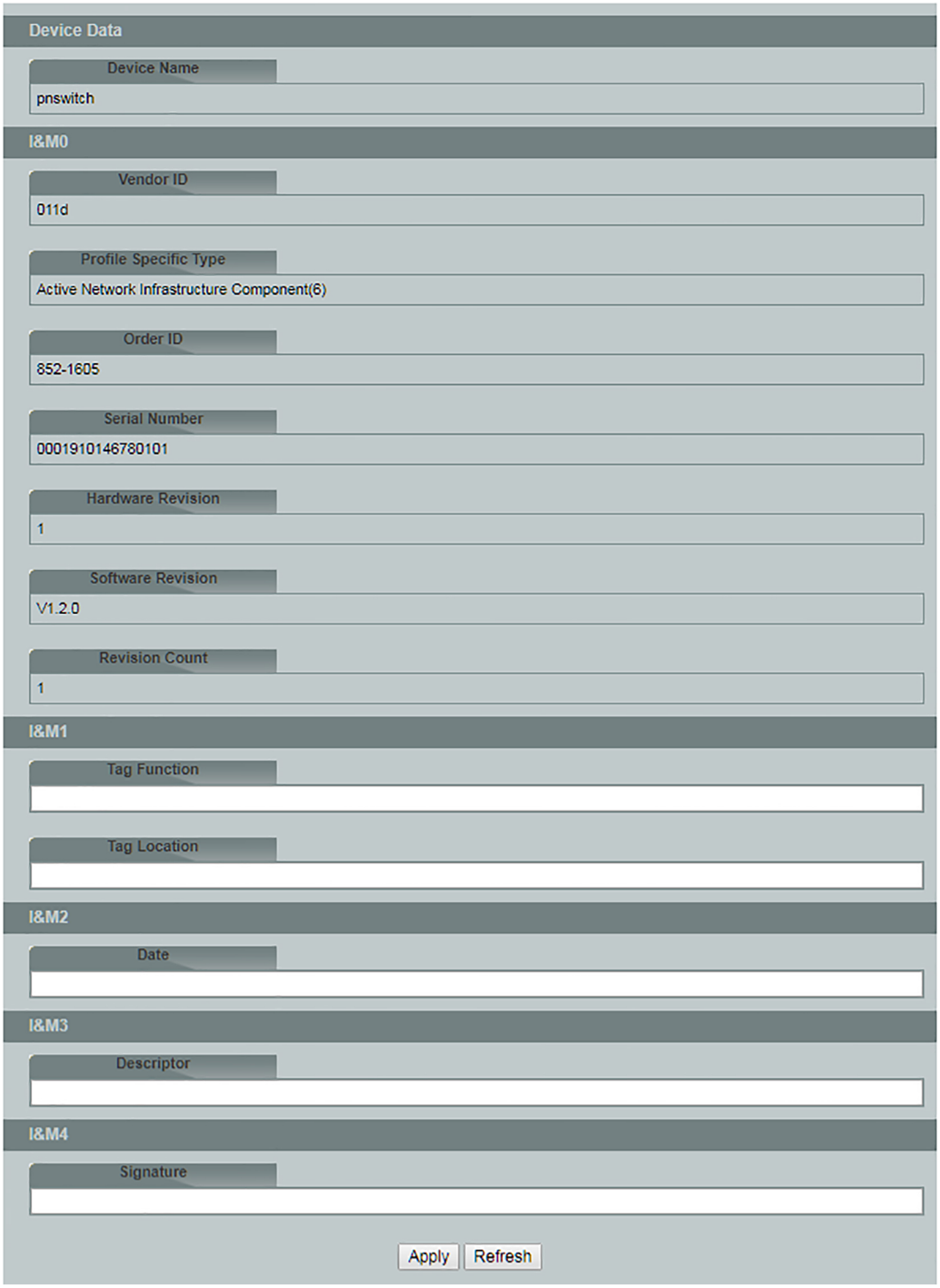


Figure 33: WBM Page “Information”

5.14.3.3 Diagnostics List

Figure 34: WBM Page “Diagnostics List”

This page displays the available diagnostics.

5.14.4 Advanced Settings

5.14.4.1 MRP

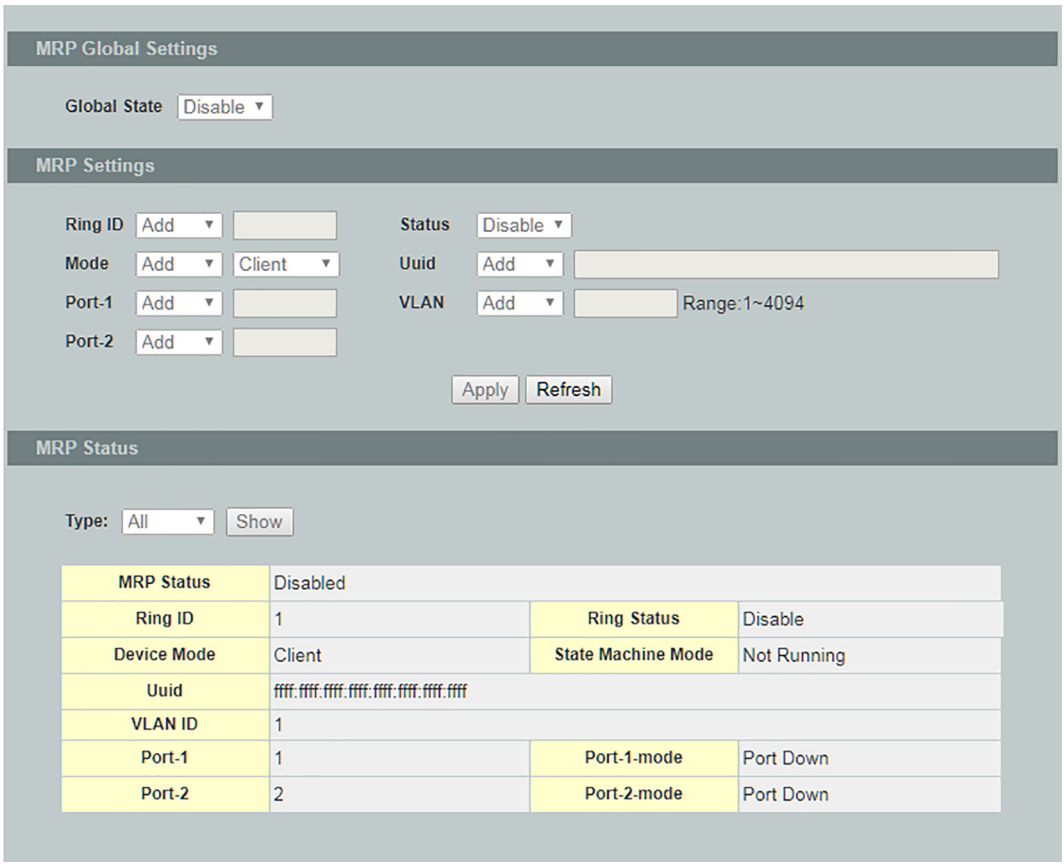


Figure 35: WBM Page “MRP”

Table 46: WBM Page “MRP”

MRP Global Settings		
Parameter	**Default**	**Description**
Global State	**Disable**	Select “Disable” in the selection box to disable the ring function of the global MRP.
	Enable	Select “Enable” in the selection box to enable the ring function of the global MRP.
MRP Settings		
Parameter	**Default**	**Description**
Ring ID	**Add**	Select “Add” in the selection box to add a (new) Ring ID.
	Remove	Select “Delete” in the selection box to delete a Ring ID.
Mode	**Add**	Select “Add” in the selection box to configure the switch either as a Client (MRC) or Manager (MRM).
	Remove	Select “Delete” in the selection box to delete the configure the switch either as a Client (MRC) or Manager (MRM).
Port-1	**Add**	Select “Add” in the selection box to add the primary port for the MRP ring.
	Remove	Select “Delete” in the selection box to delete the primary port for the MRP ring.
Port-2	**Add**	Select “Add” in the selection box to add the secondary port for the MRP ring.
	Remove	Select “Delete” in the selection box to delete the secondary port for the MRP ring.
Status	**Disable**	Select “Disable” in the selection box to switch on the respective ring.
	Enable	Select “Enable” in the selection box to switch off the respective ring.
UUID	**Add**	Configures the “Universal Unique Identifier” (UUID) for the MRP ring. This is a string of characters in hexadecimal format representing the ring to which this switch belongs. **Example:** 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
	Remove	
VLAN	**Add**	Select “Add” in the selection box and enter the VLANs which this ring should be enabled. Valid range of VLAN IDs: 1 … 4094. Use a comma (,) or hyphen (-) to specify individual VLANs or VLAN ranges.
	Remove	Select “Delete” in the selection box and enter the VLANs on which the switch should not enabled.

Table 46: WBM Page “MRP”

MRP Status		
Parameter	**Default**	**Description**
Type	**All**	Select “All” in the selection box if you want display all ring statuses.
	Ring_1 … Ring_4	Select the Ring-ID in the selection box for whose MRP status of the selected ring ID to display.
MRP Status	–	This field displays the current state of the respective MRP ring.
Ring ID	–	This field displays the ID number of the MRP ring.
Device Mode	–	This field displays the switch mode: Client (CRM)/Manager (MRM)
Uuid	–	This field displays the assigned UUID.
Vlan ID	–	This field displays the VLAN to which this ring belongs.
Port-1	–	This field displays the assigned port of the switch.
Port-2	–	This field displays the assigned port of the switch.
Ring Status	–	This field displays the current status of the MRP ring: (switched on/switched off).
State Machine Mode	–	This field displays, whether or not the MRP state machine is running.
Port-1-mode	–	This field displays the port status: (port down/port up).
Port-2-mode	–	This field displays the port status: (port down/port up).

5.14.5 Management

5.14.5.1 Upload File

The GSDML file and MIB file are embedded in the PROFINET managed switch.

You can load these files into WBM via the browser.

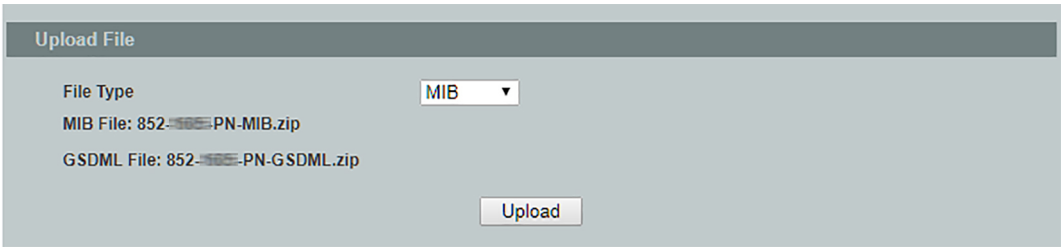


Figure 36: WBM Page “Upload File”

Table 47: WBM Page “Upload File”

Parameter	Default	Description
File Type	**MIB**	Specifies whether the MIB or GSDML file should be loaded into WBM

5.14.5.1.1 User Account

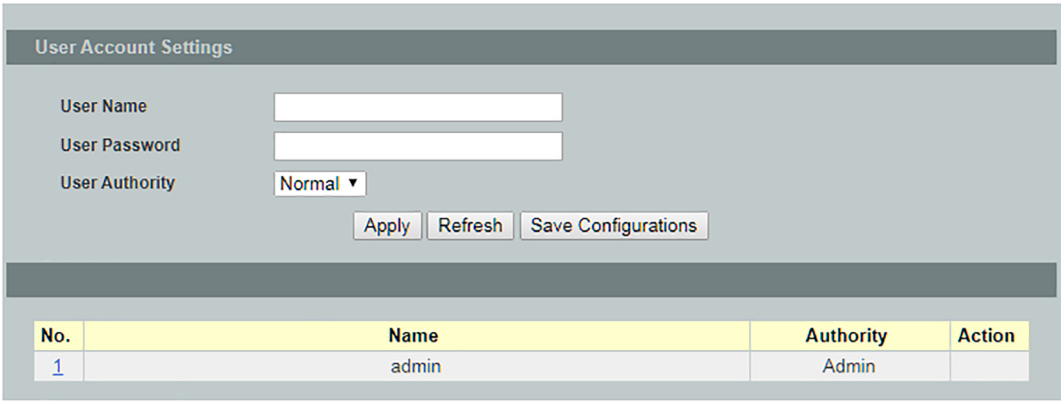


Figure 37: WBM Page “User Account”

Table 48: WBM Page “User Account”

Parameter	Default	Description
User Name	**admin**	User name
User Password	**wago**	Password
User Authority	**Admin**	Current user’s authorization group

6 Mounting

6.1 Installation Site

The location selected to install the industrial managed switch may greatly affect its performance. When selecting a site, we recommend considering the following rules:

- Install the industrial managed switch at an appropriate place. See section “Device Description” > … > “Technical Data“ for the acceptable temperature and humidity operating ranges.

Make sure that the heat output from the industrial managed switch and ventilation around it is adequate. Do not place any heavy objects on the industrial managed switch.

6.2 Installation on a Carrier Rail

The carrier rail must optimally support the EMC measures integrated into the system and the shielding of the internal data bus connections.

Place the industrial managed switch onto the DIN rail from the top and snap it into position.

6.3 Removal from Carrier ail

To remove the industrial managed switch from the carrier rail, insert a suitable tool into the metal tab under the switch and deflect the metal tab downward.

You can then release the switch down from the carrier rail and remove it upwards.

7 Connect Devices

7.1 Power Supply

The industrial managed switch uses direct current power supply for 12 … 60 V.

The primary and secondary network link is established via a 6-pin plug-in connection located on the top of the industrial managed switch.

The female connector (Item No. 2231-106/026-000) is composed of 6 connecting terminals and can be inserted and removed easily by hand to connect to the 6-pin plug connector located on the top of the switch.

The power supply for the industrial managed switch automatically adjusts to the local power source and can also be switched On if no or not all patch cables are connected.

1. Connect a suitable grounding conductor to the grounding lug on the top of the switch.

Note

Ground for the switch

The ground for the switch prevents electromagnetic interference from electromagnetic radiation.
Observe the corresponding standards for EMC-compatible installations as well.

2. Plug the female connector into the male connector of the switch if it has not already been plugged in. Check the tight fit of the multipoint connector by gently shaking it.

3. PWR +/-:
   To connect or disconnect the conductors, actuate the spring directly in the female connector using a screwdriver or an operating tool and insert or remove the conductor.

4. Check whether the power LED “PWR” on the top of the device lights up when power is supplied to the device. If not, check to ensure that the power cable is plugged in correctly and fits securely.

5. RPS +/-:
   To connect or disconnect the conductors, actuate the spring in the female connector directly using a screwdriver or an operating tool and insert or remove the conductor.

6. Check whether the power LED “RPS” on the top of the device lights up when power is supplied to the device. If not, check to ensure that the power cable is plugged in correctly and fits securely.

7.2 External Alarm Contact Port

The industrial managed switch has an alarm contact connection point on the top panel. For detailed instructions on how to connect the alarm contact power wires to the two ALM contacts of the 6-pin female connector, please refer to section “Power Supply (PWR/RPS)” (the procedure is the same).

You can connect the potential-free alarm contact to a diagnostic system that is already installed in the user’s control room or factory hall. When a fault occurs, the industrial switch sends a signal via the alarm contact to activate the external alarm. The alarm contact has two ports that form a fault circuit for connecting to alarm systems.

An alarm is signaled in the following cases:

1 Connection failure (e.g., cable disconnected, device breakdown etc.)

2 PWR/RPS:
- a Power failure (power cord is disconnected, power supply malfunction etc.)
- b Input power falls outside specification (12 … 60 V)

7.3 Console Port Cable Connection

The console port (RJ-45) provides the local management facility.

1. Insert the RJ-45 side of the (8 pin RJ-45 to DB9) cable into the RJ-45 console port on the Industrial Managed Switch and the other end into the COM port of the computer.

2. Configure the Hyper Terminal settings as mentioned in chapter “Configuration“ > … > “Console Port”.

For console port (8 pin RJ-45) pin assignment, please see in the chapter “Appendix“ > …> “Console Port (RJ-45 to DB9)”.

7.4 1000Base-SX/LX Portand 100BASE-FX, Fiber Optic

When connecting a fiber optic cable on the industrial managed switch, make sure to use the right connector type (LC) and SFP module.
There are various types of multi-mode, single mode or WDM SFP modules.
Follow the steps below to connect the fiber optic cable properly:

Note

Rubber covers
Remove and safely store the rubber covers of the fiber optic port (LC).
If no fiber optic cable is connected, the rubber cover should be installed to protect the fiber optics.

1 Insert the respective SFP modules.

2 Ensure that the fiber optic ports are clean. You can clean the cable connectors by wiping them with a clean cloth or a cotton ball soaked with a little ethanol. Dirty fiber optic cables affect the quality of the light transmitted via the cable and leads to reduced performance at the port.

3 Connect one end of the fiber optic cable to the LC port of the industrial managed switch and the other end to the fiber optic port of the other device.

Note

Proper connection of the fiber optic cable to the SFP module
For a proper connection, snap the connector of the fiber optic cable into the SFP module audibly.

4 Check the respective port LED on the industrial managed switch that the connection is established (see section “Device Description” > … > “Display Elements”).

7.5 10/100BASE-TX Ports

The 10/100BASE-TX ports (RJ-45 ETHERNET ports) of the industrial managed switch support both autosensing and autonegotiation.

1 Connect one end of the twisted pair cable of the type Category 3/4/5/5e to an available RJ-45 port on the industrial managed switch and the other end to the port of the selected network node.

2 Check the respective port LED on the industrial managed switch that the connection is established.
(see section “Display Elements” > … > “Port LEDs”).

8 Function Description

8.1 Basic Settings

8.1.1 Jumbo Frame

“Jumbo frames” are ETHERNET frames with a size greater than 1518 bytes. Jumbo frames can increase data transmission efficiency in a network. The bigger the jumbo frame is, the better the network performance is.

Note

Jumbo frame settings
The size setting for the jumbo frames applies to each port of the switch.

All connected network subscribers must support the same jumbo frame size. Data packets that are larger than the jumbo frame setting are rejected by the corresponding network subscribers.

8.1.2 SNTP

SNTP (“**S**imple **N**etwork **T**ime **P**rotocol”) is a protocol for synchronizing clocks in computer systems. It is a less complex implementation of an NTP (“**N**etwork **T**ime **P**rotocol”).
SNTP uses UTC – “**C**oordinated **U**niversal **T**ime” (French: “**T**emps **U**niversel **C**oordonné”). No information on time zones or daylight savings time is transmitted. This information falls outside the protocol range and must be obtained separately.

The SNTP port is 123.

Note

Note

1. The SNTP server always replies with the current global UTC time.
2. If the switch receives the SNTP reply time, it compares this time to the time zone configuration and configures the time for the switch accordingly.
3. If the time server’s IP address is not configured, the switch does not send an SNTP request packet.
4. If the switch does not receive an SNTP reply packet, it repeats the request indefinitely every ten seconds.
5. If the switch receives an SNTP reply, it repeats the time request from the NTP server every hour.
6. If the time zone and NTP server change, the switch repeats the request process.
7. No default SNTP server.

8.1.3 Management Host

The management host limits the number of hosts that the switch can manage. There is no management host in the default settings. Any host can manage the switch via Telnet or Web browser. If a user has configured one or more hosts, only those hosts can manage the switch. The function allows users to configure up to three entries for the management IPs.

8.1.4 MAC Management

The MAC address (“**M**edia **A**ccess **C**ontrol **address**” – hardware address for access control) is the unique hardware number of a device in a network.

Dynamic Address

When receiving frames, the switch receives the source MAC address, which it stores in the address table together with the receiving port, the VLAN and an “Age Time” (lifespan). When the “Age Time” expires, the address entry is deleted from the address table.

Static Address

A static address set by the user does not include the “Age Time” and thus is not deleted by the switch. The static address can only be deleted by a user. The switch supports an address table of size up to 16 K.

Static and dynamic addresses share the same address table.

MAC Table

The “MAC Table” (MAC address table – also known as a filter database) shows which frames are forwarded to the switch’s ports or filtered out.
If a device that belongs to a VLAN group sends a data packet that is forwarded to a port on the switch, the MAC address of the device is read from the switch’s MAC address table.
It also shows whether the MAC address is dynamic (assigned by the switch) or static (set manually).

MAC Address Table

The switch uses the MAC address table to determine how to forward frames (see figure below).

1. The switch checks a received frame and detects the port from which the source MAC address originates.

2. The switch checks whether the frame’s destination MAC address matches a source MAC address already detected in the MAC address table.

   - If the switch already knows the port for this MAC address, it forwards the frame to that port.

- If the switch does not already know the port for this MAC address, it forwards the frame to all ports. “Port flooding” (excessive forward to all ports) leads to network congestion.

- If the switch already knows the port for this MAC address, and the destination port is the same as the input port, the frame is filtered.

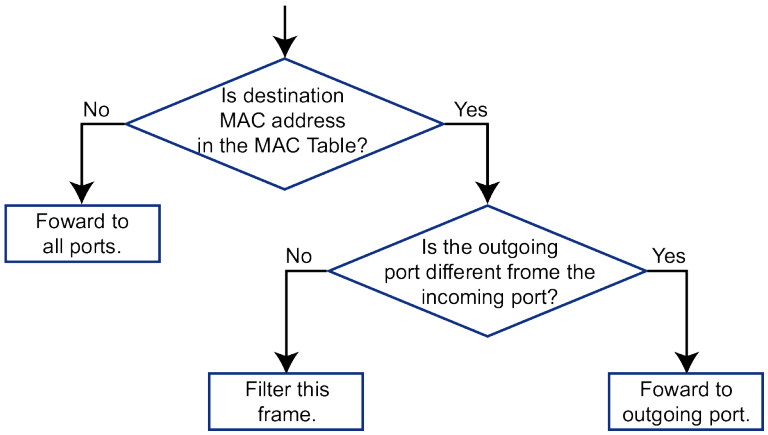


Figure 38: MAC Address Table Flowchart

8.1.4.1 Static MAC

Static MAC Addresses

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses have no “Age Time.” When you set up rules for static MAC addresses, you set static MAC addresses for a port. This may reduce data transmission needs.

8.1.5 Port Mirroring

Port mirroring is used on switches to copy sent/received network packets from one or more areas to network monitoring or another switch port (monitor port). Port mirroring is used in network systems that require monitoring of network traffic, such as an IDS (“**I**ntrusion **D**etection **S**ystem”).

Port mirroring together with an NTA (“**N**etwork **T**raffic **A**nalyzer”) can help to monitor network traffic. Users can monitor incoming and/or outgoing data packets on selected ports (“source ports”).

Source Mode

- “Ingress”: The incoming data packets are copied and forwarded to the monitor port.
- “Egress”: The outgoing data packets are copied and forwarded to the monitor port.
- Both: Both incoming and outgoing data packets are copied and forwarded to the monitor port.

Note

Note

1. The monitor port cannot be a member of a “truck port” group.
2. The monitor port cannot be an ingress or egress port.
3. If a port has been configured as a source port, and a user then configures it as a destination port, the port is automatically deleted from the source ports.

8.1.6 Port Settings

Duplex Mode

A duplex communication system is a system composed of two connected devices that can communicate with each other in both directions.

Half Duplex

A half-duplex system provides for communication in both directions, but only one direction at a time (not simultaneously).
One device receives a signal and must wait for the other device to stop transmitting before it can reply.

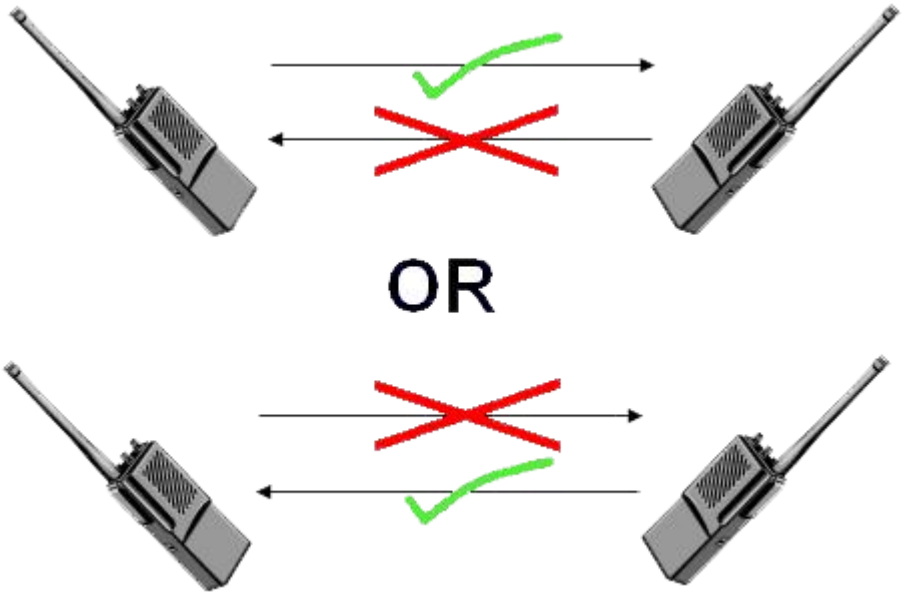


Figure 39: Half-Duplex Mode

Full Duplex

A full-duplex system (also known as a double-duplex system) can communicate simultaneously in both directions.
Fixed-line telephone networks, for example, are full-duplex, since both callers can talk and listen at the same time.

Figure 40: Full-Duplex Mode

Auto MDI/MDIX

MDI (“**M**edium-**D**ependent **I**nterface”) in information technology is part of the transmitter/receiver unit (transceiver) of a network device.

Auto MDI-X (“**Aut**omatic **M**edium-**D**ependent **I**nterface **C**rossover”) is a network technology integrated in the port that automatically detects the required network cable type (“straight-through” or “crossover” cable) and configures the connection accordingly.
Crossover cables are then unnecessary for connecting devices.
The interface corrects incorrect cabling automatically.
For auto MDI-X to work properly, the speed must be set to “auto” for the interface and in the duplex settings.

Autonegotiation

Autonegotiation is a method in which two interconnected ETHERNET network ports (e.g., the network port of a PC and a port of a router, hub or switch that is connected to it) independently negotiate and configure the maximum transmission speed and the duplex process.
Autonegotiation only applies to twisted-pair cables – not to WLAN, fiber optic or coaxial cable connections.

If the port does not support autonegotiation, or if this feature is turned off, the switch determines the connection speed by detecting the signal on the cable and using half-duplex mode.
If autonegotiation is disabled on the switch, a port uses its pre-configured settings for speed and duplex mode when establishing the connection.
This is meant to ensure that the same settings have been made on the port, allowing the connection to be established.

Flow Control

“Flow control” regulates the transmission of signals by adapting them to the bandwidth on the input port.
Higher data traffic on the port decreases the bandwidth and can cause the buffer memory to overflow, which can lead to packet and frame loss.

In accordance with IEEE 802.3x, the switch uses flow control in full-duplex mode and “backpressure flow control” in half-duplex mode.

For flow control, the switch sends a pause signal in full-duplex mode to the sending port, causing it to temporarily stop sending signals when the buffer memory of the receiving port is full.
For backpressure flow control, the switch sends a collision signal to the sending port in half-duplex mode (mimicking a state of packet collision, so to speak), causing the sending port to temporarily stop sending signals and to resend the signals later.

Note

Support for “Force Mode”
1000 BASE-T does not support force mode.

8.2 Advanced Settings

8.2.1 Bandwidth Control

8.2.1.1 QoS

Each egress port supports up to eight “transmit queues”. Each transmit queue contains a list specifying the packet transmission order. Each incoming frame is forwarded to one of the eight “transmit queues” of the assigned egress port based on its priority. The egress port transmits packets from each of the eight transmit queues according to a configurable sequence algorithm, which can be a combination of SP (“**S**trict **P**riority”) and WRR (“**W**eighted **R**ound **R**obin”).

Normally, networks operate on a best-effort delivery basis, i.e., all data traffic has equal priority and an equal chance of being transmitted in a timely manner.
If congestion occurs, all data traffic has an equal chance of being dropped.

When configuring the QoS (“**Q**uality of **S**ervice”) function, you can select specific data traffic, prioritize it according to its relative importance and use congestion management and congestion avoidance techniques to give preferential treatment to this data traffic.
Implementing QoS in a network improves network predictability and increases bandwidth utilization.

The industrial managed switch supports “802.1p Priority Queuing.”
The switch has eight priority queues. These priority queues are numbered, where class 7 has the highest priority and class 0 the lowest. The eight priority classes specified in IEEE 802.1p (p0 to p7) are mapped to the switch’s priority queues as follows:

Priority	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

Priority scheduling is implemented by the above-named priority queues. The switch operates the four hardware priority queues sequentially, starting with the highest priority queue (3) and ending with the lowest (0). Each hardware queue transmits all the packets in the switch’s buffer before the next lower priority queue is allowed to transmit its packets. If the lowest hardware priority queue has transmitted all its packets, the highest starts to transmit the packets that it received in the meantime again.

QoS Enhancement

You can configure the switch to prioritize data traffic even if the incoming packets are not marked with “IEEE 802.1p Priority Tags” or change the existing priority tags based on criteria you select. The switch allows you to choose one of the following methods for assigning priorities to incoming packets:

- 802.1p Tag Priority
  - Assign priority to packets based on the packet’s “802.1p Tag Priority.”
- Port-based QoS
  - Assign priority to packets based on the incoming port on the switch.
- DSCP-based QoS
  - Assign priority to packets based on their DSCP (“**D**ifferentiated **S**ervices **C**ode **P**oints”).

Note

Advanced QoS methods
Advanced QoS methods only affect the internal priority queue mapping for the switch. The switch does not modify the IEEE 802.1p value for the egress frames.

You can choose one of these options above to alter the way incoming packets are prioritized, or you can choose not to use any QoS extension setting on the switch.

802.1p Priority

When the 802.1p priority mechanism is used, the packet is examined for the presence of a valid 802.1p priority tag. If it has a tag, the packet is assigned to a configurable egress queue based on its priority value. The tag priority can be assigned to any of the available queues.

ETHERNET Packet

6	6	2	42-1496	4
DA	SA	Type/length	Data	FCS

6	6	4	2	42-1496	4
DA	SA	802.1Q Tag	Type/length	Data	FCS

802.1Q Tag

2 bytes	2 bytes		
Tag Protocol Identifier (TPID)	Tag Control Information (TCI)		
16 bits	3 bits	1 bits	12 bits
TPID (0x8100)	Priority	CFI	VID

- TPID (“**T**ag **P**rotocol **Id**entifier”)
  A 16-bit field is set to the value of 0x8100 to identify the frame as an “IEEE 802.1Q Tag Frame.”

- TCI (“**T**ag **C**ontrol **I**nformation”)
  - PCP (“**P**riority **C**ode **P**oint”)
    This is a three-bit field that refers to the IEEE 802.1p priority. This indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data etc.).

  - CFI (“**C**anonical **F**ormat **I**ndicator”)
    This is a single-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format. It is always set to 0 for ETHERNET switches. CFI is used for compatibility between ETHERNET and “token ring” networks. If a frame received at an ETHERNET port has a CFI of 1, the frame should not be output to an untagged port.

  - VID (“**V**LAN **Id**entifier”)
    This is a 12-bit field specifying the VLAN to which the frame belongs. A value of 0 means that the frame does not belong to any VLAN; in this case, the “802.1Q Tag” specifies only a priority and serves as a priority tag. The hexadecimal value 0xFFF is reserved for implementation purposes. All other values may be used as VLAN identifiers, allowing support for up to 4094 VLANs. On bridges, VLAN 1 is often reserved for management.

Priority Levels

PCP (“**P**riority **C**ode **P**oint”):

Table 49: Priority Levels

PCP	Network Priority	Traffic Characteristics
1	0 (lowest)	Background
0	1	Best effort
2	2	Excellent effort
3	3	Critical applications
4	4	Video, < 100 ms latency
5	5	Video, < 10 ms latency
6	6	Internetwork control
7	7 (highest)	Network control

DiffServ (DSCP)

DiffServ (“**Diff**erentiated **Serv**ices”) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for managing network traffic and providing QoS (“**Q**uality **o**f **S**ervice”) guarantees in modern IP networks. DiffServ can, for example, be used to provide low-latency GS (“**G**uaranteed **S**ervice”) to critical network traffic such as voice or video data while providing simple best effort traffic guarantees to non-critical services such as Web traffic or file transfers.

DSCP (“**D**ifferentiated **S**ervices **C**ode **P**oint”) is a six-bit field in the header of IP packets for packet classification purposes. DSCP replaces the outdated IP precedence, a three-bit field in the “Type of Service” byte of the IP header originally used to classify and prioritize types of traffic.

When the DiffServ priority mechanism is used, a packet is classified based on the DSCP field in the IP header. If the tag is present, the packet is assigned to a programmable egress queue based on its “Tagged Priority” value. The tagged priority can be assigned to any available queue.

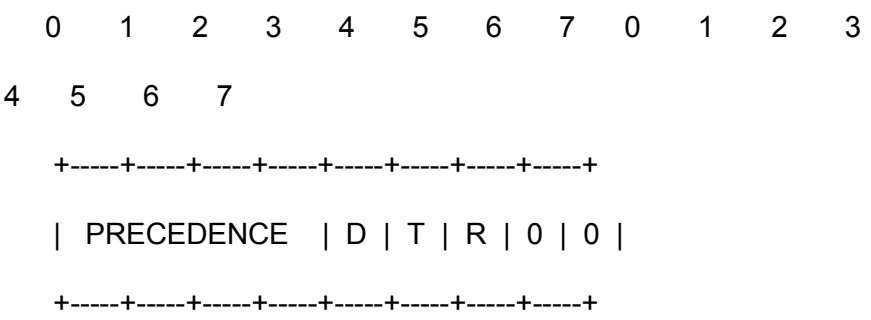
Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment offset
Time to live		Protocol	Header checksum	
Source address				
Destination address				
Options				Padding

Example Internet Data Packet Header

“Type of Service” in the IP header: 8-bit

The “Type of Service” field provides an indication of the abstract parameters of the quality of service desired. These parameters are used to guide the manual selection of the actual service parameters when a data packet is to be transmitted through a particular network. Several networks offer service precedence, which treats high precedence traffic as more important than other traffic (generally by accepting only traffic above certain precedence level at high load times). The most favorable choice is a compromise between low delay, high reliability and high throughput.

Bits 0 … 2	Precedence	
Bit 3	0 = normal delay	1 = low delay
Bit 4	0 = normal throughput	1 = high throughput
Bit 5	0 = normal reliability	1 = high reliability
Bits 6 … 7	Reserved for future use.	



Precedence

111 – Network Control
110 – Internetwork Control
101 – CRITIC/ECP
100 – Flash Override
011 – Flash
010 – Immediate
001 – Priority
000 – Routine

Specifying the Delay, Throughput and Reliability parameters can increase the service cost. In many networks, giving preference to one parameter entails a disadvantage for another. Except in very unusual cases, at most two of these three parameters should be specified.

“Type of Service” information is used to specify the type of processing of the data packet while it is transmitted through a network. Example mappings of the “Internet Type of Service” to the actual service provided in networks, such as

AUTODIN II, ARPANET, SATNET and PRNET, are specified in “Service Mappings.”

The Network Control precedence designation should only be used within a network. The actual use and control of that designation depends on the respective network. The Internetwork Control designation should only be changed by the initiators of the gateway control.

If these precedence designations apply to a specific network, it is the responsibility of that network to control the access to and use of those designations.

DSCP	Priority	DSCP	Priority	DSCP	Priority
0	0	1	0	2	0
…					
60	0	61	0	62	0
62	0				

Example:

IP Header

DSCP=50 -> 45 C8 …

Queuing Algorithms

Queuing algorithms can be used to maintain separate queues for packets, which can originate from any single source or any data flow, thus preventing one source from monopolizing the bandwidth.

SPQ

With SPQ ("**S**trict **P**riority **Q**ueuing"), the four hardware priority queues are processed sequentially – the highest priority (3) first and the lowest (0) last. Each hardware queue transmits all the packets in its buffer before the next lower priority queue is allowed to transmit its packets. If the lowest hardware priority queue has transmitted all its packets, the highest starts to transmit the packets that it received in the meantime again.

WRR

RR ("**R**ound **R**obin") is a scheduling service that queues packets on a rotating basis and is only activated when a port has more traffic than it can handle. A limited amount of bandwidth is provided to a queue, irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth and then moves to the end of the list, and so on until all queues have been processed. The entire process works in a looping fashion until a queue is empty.

WRR ("**W**eighted **R**ound **R**obin") scheduling uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you enter in the "Weight Value" field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Processing queues with higher weights takes precedence over processing lower weight ones. This queuing mechanism is highly efficient in that it divides the entire available bandwidth among the various traffic queues and allocates it to the ones that have not yet been emptied.

Note

DiffServ Function
DiffServ is disabled on the industrial managed switch.
If DiffServ is disabled, "802.1p Tag Priority" is used.

8.2.1.2 Rate Limitation

8.2.1.2.1 Storm Control

A broadcast storm occurs when the network is overwhelmed with constant broadcast or multicast traffic. Broadcast storms can eventually lead to a complete loss of network connectivity as the packets proliferate.

“Storm control” protects the switch bandwidth from packet flooding, including broadcast packets, multicast packets and DLF (“**D**estination **L**ookup **F**ailure”). The rate is a threshold that limits the total number of specific packet types. For example, if the broadcast and multicast options are selected, the total number of packets transmitted per second for these two types is not exceeded.

“Broadcast storm control” limits the number of broadcast, multicast and unknown unicast (also referred to as “Destination Lookup Failure” or DLF) packets the switch receives per second on the ports. If the maximum number of packets per second is reached, all subsequent packets are discarded. Enable this function to reduce the number of these packets in the network.

The storm control unit is 625 pps (packets per second).

8.2.1.2.2 Bandwidth Limitation (Rate Limitation)

Rate limitation is used to control the rate of traffic sent or received on a network interface.

8.2.2 IGMP Snooping

IGMP snooping (“**I**nternet **G**roup **M**anagement **P**rotocol **Snooping**”) is used for multicast data traffic. The switch can passively “snoop” on IGMP packets transmitted between IP multicast routers/switches and IP multicast hosts to discover their IP multicast group membership. IGMP snooping allows a switch to detect multicast groups without a user having to manually configure them.

It checks IGMP packets passing through it, reads the group registration information and configures multicasting accordingly.

The switch forwards multicast traffic to its multicast destination groups (which it has detected through IGMP snooping, or which you have manually configured) to ports that are members of those groups. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through the switch.

The switch can perform IGMP snooping on up to 4094 VLANs. You can configure the switch to automatically detect multicast group membership in all VLANs. The switch then performs IGMP snooping on the first VLANs that send IGMP packets.

This is referred to as “auto mode.” Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as “fixed mode.” In fixed mode, the switch does not detect multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

Immediate Leave

If you enable the “IGMP Immediate Leave” function, the switch immediately deletes a port when it receives a “leave message” with IGMP version 2 on that port. You should use the “Immediate Leave” function only when there is a single receiver present on every port in the VLAN (“Immediate Leave” is only supported on IGMP version 2 hosts).

The switch uses the “Immediate Leave” function with IGMP snooping to remove from the forwarding table an interface that sends a leave message, without the switch having to send group-specific queries to the interface. The VLAN interface is deleted from the multicast tree for the multicast group specified in the original leave message. “Immediate Leave” ensures optimal bandwidth management for all hosts in a switched network, even when multiple multicast groups are simultaneously in use.

Fast Leave

The switch allows you to configure a delay time. When the delay time has expired, the switch deletes the interface from the multicast group.

Last Member Query Interval

The “last member query interval” is the maximum response time in group-specific queries sent in response to “leave group” messages, and also indicates the time between group-specific query messages.

If the switch receives an IGMP leave message from a subscriber on a receiver port without the “Immediate Leave” function being enabled, the switch sends an IGMP-specific query on this port and waits for IGMP group membership reports. If the switch receives no messages within a specified time period, the receiver port is removed from the multicast group.

IGMP Querier

There is normally only one querier per physical network. All multicast routers start up as a querier on each connected network. If a multicast router receives a query message from a router with a lower IP address, it MUST become a non-querier in that network. If a router does not receive any query messages from another router for a certain period of time (“Other Querier Present Interval”), it assumes the role of querier. Routers periodically (“Query Interval”) send a “general query” in all attached networks for which the router is the querier in order to solicit membership information. At startup, a router SHOULD send general queries (“Startup Query Count”) spaced closely together (“Startup Query Interval”) to quickly and reliably determine membership information. A general query is addressed to an all-systems multicast group (224.0.0.1), has a group address field value of 0 and has a maximum response time of “Query Response Interval”.

Port IGMP Querier Mode

- Auto
  - The switch uses the port as an IGMP query port if the port receives IGMP query packets.

- Fixed
  - The switch always uses the port(s) as IGMP query port(s). This mode is used when connecting an IGMP multicast server to the port(s).
  - The switch always forwards the client's "report/leave" packets to the port. Normally, the port is connected to an IGMP server.
- Edge
  - The switch does not use the port as an IGMP query port.
  - The IGMP query packets received on this port are dropped. Normally, the port is connected to an IGMP client.

Note

Forwarding "IGMP Join/Leave" Packets
The industrial managed switch will forward the "IGMP join/leave" packets to the query port.

IGMP Proxy Snooping

IGMP proxy snooping can reduce the number of reports and leaves sent through an IGMP router.

Configurations

Users can enable/disable IGMP snooping on the switch. This also applies to specific VLANs. If IGMP snooping is disabled on the switch, it is disabled on all VLANs, even when enabled on some VLANs.

Note

VLAN States
There are a global state and individual VLAN states.
If the global state is disabled, IGMP snooping on the switch is disabled even if individual VLAN states have been enabled.
If the global state is enabled for IGMP snooping, the function must be individually enabled by the user for specific VLANs.

8.2.2.1 Multicast Address

A multicast address is associated with a group of interested receivers. According to RFC 3171, addresses 224.0.0.0 to 239.255.255.255 (formerly Class D addresses) are reserved as multicast addresses in IPv4.

The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped to the 23 bits of the available ETHERNET address space. This means that there is an ambiguity in delivering packets. If two hosts on the same subnet each subscribe to different multicast groups whose addresses differ only in the first five bits, ETHERNET packets for both multicast groups are sent to both hosts. The network software must discard the unnecessary packets into the host.

Table 50: Multicast Classes and Address Ranges

Class	Address Range	Support
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of two million networks
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use or research and development purposes.

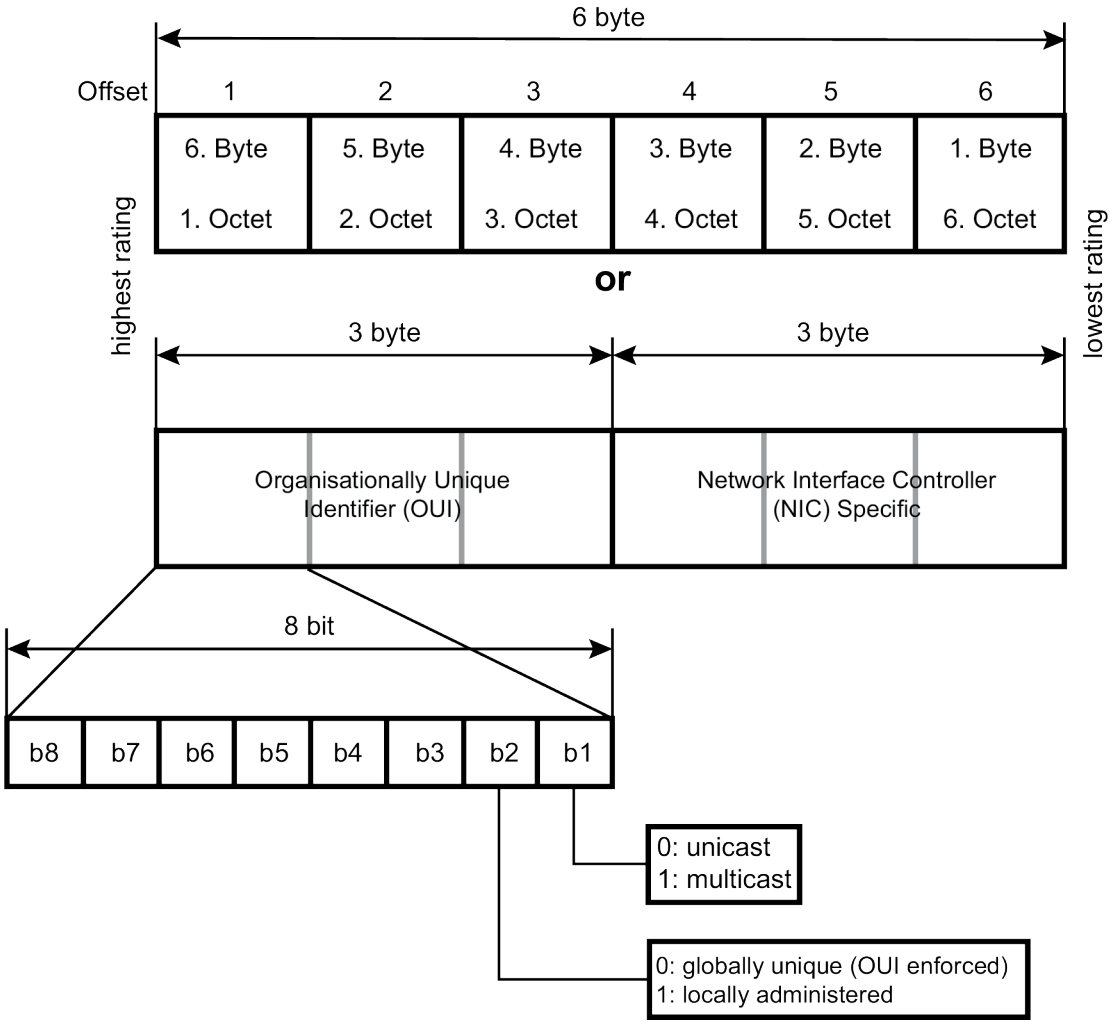


Figure 41: Multicast Address

Table 51: IP Multicast Addresses

IP Multicast Address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	The All Hosts multicast group that contains all systems on the same network segment
224.0.0.2	The All Routers multicast group that contains all routers on the same network segment
224.0.0.5	“Open Shortest Path First” (OSPF protocol), “AllSPFRouters” address. This address is used to send “Hello Packets” to all OSPF routers on a network segment.
224.0.0.6	“OSPF AllDRouters” Address This address is used to send OSPF routing information to “OSPF Designated Routers” on a network segment.
224.0.0.9	RIP (“Routing Information Protocol”) Version 2 of the group address This protocol is used to send routing information using the RIP protocol to all RIP v2-aware routers on a network segment

Table 51: IP Multicast Addresses

IP Multicast Address	Description
224.0.0.10	EIGRP group address This address is used to send EIGRP routing information to all EIGRP routers on a network segment.
224.0.0.13	PIM Version 2 (“Protocol Independent Multicast”)
224.0.0.18	Virtual Router Redundancy Protocol
224.0.0.19 - 21	IS-IS over IP
224.0.0.22	IGMP Version 3 (“Internet Group Management Protocol”)
224.0.0.102	Hot Standby Router Protocol Version 2
224.0.0.251	Multicast DNS address
224.0.0.252	“Link-local Multicast Name Resolution” address
224.0.1.1	“Network Time Protocol” address
224.0.1.39	“Cisco Auto-RP-Announce” address
224.0.1.40	“Cisco Auto-RP-Discovery” address
224.0.1.41	“H.323 Gatekeeper Discovery” address

8.2.3 VLAN

A VLAN (“**V**irtual **LAN**”) is a group of hosts with a common set of requirements that communicate as if they were attached to a broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows end stations to be grouped together even if they are not located on the same network switch. Networks can be reconfigured through software instead of spatially separated devices.

VID (“**V**LAN-**ID**”) is the identifier of a VLAN that is generally used by the IEEE 802.1Q standard. It has 12 bits and allows the identification of 4096 (2^{12}) VLANs. Of the 4096 possible VIDs, VID 0 is used to identify priority frames, and value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4094.

A “tagged VLAN” uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges – they are not confined to the switch on which they were created. VLANs can be created statically (manually by users) or dynamically via GVRP (“GARP VLAN Registration Protocol”). The VLAN ID associates a frame with a specific VLAN and provides the information that switches need in order to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (“Tag Protocol Identifier,” residing within the type/length field of the ETHERNET frame) and two bytes of TCI (“Tag Control Information,” which starts after the source address field of the ETHERNET frame).

The CFI (“Canonical Format Indicator”) is a single-bit flag, always set to zero for ETHERNET switches. If a frame received at an ETHERNET port has a CFI of 1, the frame should not be transferred to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that the user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant, and the default VID of the ingress port is used as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames, and value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4094.

TPID	User Priority	CFI	VLAN ID
2 bytes	3 bits	1 bits	12 bits

- **Forwarded Tagged and Untagged Frames**

Each port on the switch is capable of forwarding tagged and untagged frames. When a frame is forwarded from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is "VLAN 1" for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are subscribers of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

- **Port-Based 802.1Q VLAN**

As a subscriber of a port-based VLAN, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be subscribers of the same VLAN. The network administrator typically performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

As with other VLAN approaches, the packets forwarded using this method are not transmitted to other VLAN domains or networks. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN without the intervention of a Layer 3 device.

The device that is attached to the port likely has no understanding that a VLAN exists. The device simply knows that it is part of a subnet and should be able to talk to all other network subscribers by simply sending information via the cable connection. The switch is responsible for identifying information that came from a specific VLAN and for ensuring that the information gets to all other subscribers of the VLAN. The switch is also responsible for ensuring that ports in a different VLAN do not receive the information.

This approach is quite simple, fast and easy to manage, because there are no complex lookup tables required for VLAN segmentation. Designing the "Port-to-VLAN" connection with an "**A**pplication-**S**pecific **I**ntegrated **C**ircuit" (ASIC) has great performance advantages. An ASIC allows "Port-to-VLAN" mapping at the hardware level.

8.2.3.1 Port Isolation

“Port isolation” is a port-based virtual LAN function. It partitions the switching ports into virtual private domains designated on a per port basis. Data switching outside of the switch’s private domain is not allowed. The VLAN tag information of the packets is ignored.

This function can be used to configure one or more egress ports that allow the data received by the specific port to forward it. If the CPU port (port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the switch.

If you want to allow communication between two subscriber ports, you must define the egress port for both ports. CPU refers to the switch’s management port. By default, it forms a VLAN with all ETHERNET ports. If it does not form a VLAN with a specific port, then the switch cannot be managed from that port.

8.2.4 LLDP

The LLDP (“**L**ink **L**ayer **D**iscovery **P**rotocol”) described in this standard allows stations connected to a LAN according to IEEE 802® to send information to other stations connected to the same LAN. The information contains essential system functions, including the management address or addresses of an entity or entities that provide management of these functions, as well as identification of the station’s access point to the IEEE802 LAN required by the management entity or entities.

The information distributed via this protocol is stored by the recipients in a normal MIB (“**M**anagement **I**nformation **B**ase”). This allows an NMS (“**N**etwork **M**anagement **S**ystem”) to access the information using a management protocol such as SNTP (“**S**imple **N**etwork **M**anagement **P**rotocol”).

8.2.5 MAC based VLAN

The MAC-based VLAN allows users to assign individual data packets to a VLAN with priority on the basis of the MAC address.

8.2.6 Loop Detection

“Loop detection” handles problems with loops in the network periphery. These problems can occur if a port is connected to a switch that is in a loop state. A loop state occurs as a result of user error. It happens when two ports on a switch are connected to the same cable. When a switch in loop state sends out broadcast messages, the messages loop back to the switch and are re-broadcast again and again, causing a broadcast storm.

The “Loop Detection” function sends special multicast packets periodically to detect whether the port is connected to a network in loop state. The switch shuts down a port if the switch detects these special multicast packets looping back to the same port.

Loop Recovery

When loop detection is enabled, the switch sends a probe packet every two seconds and waits to receive the packet. If it receives the packet at the same port, the switch disables the port. After a defined time period (“Recovery Time”), the switch reenables the port and executes loop detection again.

The switch generates a syslog (system log), internal log messages and SNMP traps (SNMP monitoring files) if it disables a port after loop detection.

8.2.7 STP

The (R)STP (“[**R**apid] **S**panning **T**ree **P**rotocol”) can detect and stop network loops, as well as provide backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP-compliant switches in the network to ensure that only one path exists between any two stations on the network.

The switch supports both STP and RSTP as defined in the following standards:

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol

The switch uses IEEE 802.1w RSTP, which allows faster convergence of the spanning tree than STP (the switch is also backwards-compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, there are longer delays because the device that causes a topology change first notifies the root bridge and then the network. Both RSTP and STP remove unwanted learned addresses from the filtering database.

- STP has the port states “Blocking”, “Listening”, “Learning” and “Forwarding”.
- RSTP has the port states in RSTP “Discarding”, “Learning” and “Forwarding”.

STP Switch Port States

- **“Blocking”**
  If a port creates a “switching loop” (a looping connection between two ports), user data can no longer be sent or received. However, the port can go into the “Forwarding” state if the other active connections fail and the spanning tree algorithm determines that the port may transition to that state. BPDU data is still received and sent in the “Blocking” state.
- **“Listening”**
  The switch processes BPDUs and waits for possible new information that would cause it to return to the “Blocking” state.
- **“Learning”**
  Even if the port does not yet forward any frames (packets), it can learn source addresses from frames received and add them to the filter database (“switching database”).

- **“Forwarding”**
  The port is in normal operating mode and receives and sends data. STP still monitors incoming BPDUs that would indicate that the port should return to the “Blocking” state to prevent a loop.
- **“Disabled”**
  This is not strictly part of the STP because a network administrator can manually disable a port.

RSTP Bridge Port Roles

- **“Root”**
  The root port is a forwarding port that can best transmit data from the non-root bridge to the root bridge.
- **“Designated”**
  This is a forwarding port for every LAN segment.
- **“Alternate”**
  This port represents an alternate path to the root bridge. However, the path is different than for the root port.
- **Backup**
  This port serves as a backup/redundant path to a segment to which another bridge port is already connected.
- **“Disabled”**
  This is not actually part of STP because a network administrator can manually disable a port.

Note

STP/RSTP
In this document, “STP” refers to both STP and RSTP.

STP Terminology

Root Bridge

The root bridge is the “base” (root) of the spanning tree.

Path Cost

The path costs are the costs for transmitting a frame through the port in the LAN. This value should be adjusted to the transmission speed.
The valid range is 1 to 200000000. A path with higher costs is more likely to be blocked by STP if a network loop is detected.

- “**Path Cost Short”** is the original size with a 16-bit value.
  Only speeds up to 10 Gbit can be considered.
- “**Path Cost Long”** stands for a 32-bit value.
  Speeds up to 10 Tbit are supported.

Table 52: STP Path Costs

Transmission Speed	Recommended Value	Recommended Range	Permissible Range
4 Mbit/s	250	100 … 1000	1 … 65535
10 Mbit/s	100	50 … 600	1 … 65535
16 Mbit/s	62	40 … 400	1 … 65535
100 Mbit/s	19	10 … 60	1 … 65535
1 Gbit/s	4	3 … 10	1 … 65535
10 Gbit/s	2	1 … 5	1 … 65535

- Each bridge communicates with the root bridge via the root port. The root port is the port on the switch with the lowest path costs to the root bridge (the “root path cost). If there is no root port, then the switch becomes the root bridge for the spanning tree network.
- A designated bridge is selected for each LAN segment. This bridge has the lowest cost to the root bridge among the bridges connected to the LAN.

Forward Time (Forward Delay)

The “forward time” is the maximum time (in seconds) that the switch waits before it changes states. This delay is required because every switch must first receive information on topology changes before it forwards frames. In addition, each port needs time to receive information on conflicts that would make it return to the blocking state. Otherwise, temporary data loops might result. The valid range is 4 to 30 seconds.

Max Age

The “max age” is the maximum time (19 seconds) that the switch can wait without receiving a BPDU (“**B**ridge **P**rotocol **D**ata **U**nit”, configuration message) before attempting to reconfigure. All switch ports (except for designated ports) receive BPDUs at regular intervals. Each port that ages out STP information (from the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network.

Hello Time

This is the time interval in seconds between configuration messages (BPDU – Bridge Protocol Data Units) generated by the root switch.

STP

After a bridge determines the lowest cost spanning tree with STP, it enables the root port and designated ports for connected LANs and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange BPDUs periodically. If the topology changes in a LAN coupled via bridge, a new tree is spanned. Once a stable network topology has been established, all bridges listen for “Hello BPDUs” transmitted from the root bridge. If a bridge does not get a “Hello BPDU” after a predefined interval (“Max Age”), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

Edge Port

“Edge ports” are attached to a LAN that has no other bridges attached. These ports can transition directly to the “Forwarding” state. RSTP still continues to monitor the port for BPDUs in case a bridge is connected. RSTP can also be configured to automatically detect edge ports. As soon as the bridge detects a BPDU coming to an edge port, the port loses its status as an edge port.

Forward Delay

The “Forward Delay” is the maximum time (in seconds) that the root device waits before changing states (e.g., from “Listening” to “Learning” to “Forwarding”). The valid range is from 4 to 30 seconds.

Transmission Limit

The “Transmission Limit” is used to configure the minimum interval between the transmission of consecutive RSTP BPDUs. This function can only be enabled in RSTP mode. The valid range is from 1 to 10 seconds.

Bridge Priority

The “bridge priority” is used in selecting the root switch, root port and designated port. The switch with the highest priority becomes the STA root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.

Port Priority

The port priority is configured on the switch. A low numeric value indicates a high priority. A port with lower priority is more likely to be blocked by STP if a network loop is detected. The valid range is from 0 to 240.

BPDU Guard

This setting is configured separately for each port. If the port is enabled in “BDU Guard” and receives a BPDU, the port is switched to the “Disabled” state to prevent a faulty environment. The user must enable the port manually.

BPDU Filter

This function is used to set up a filter for sending or receiving BPDUs on a switch port. If the port receives BPDUs, the BPDUs are dropped. If both the BPDU filter and BPDU guard are enabled, the BPDU filter has the higher priority.

Note

BPDU Filter and BPDU Guard
If both the BPDU filter and BPDU guard are enabled, the BPDU filter has the higher priority.

Root Guard

The “Root Guard” function forces an interface to become a designated port to prevent neighboring switches from becoming a root switch. This function provides a way to specify the selection of a root bridge in a network. It prevents a designated port from becoming the root port. If a port with the “Root Guard” function receives a superior BPDU, the port moves to a root-inconsistent state (effectively equivalent to the “Listening” state) to maintain the status of the current root bridge. The port can be moved to the “Forwarding” state if it receives no superior BPDU for the time period of three “Hello Times.”

MSTP

The MSTP (“**M**ultiple **S**panning **T**ree **P**rotocol”) is an RSTP extension. It allows different spanning tree instances in conjunction with VLANs (“Virtual Local Area Networks”).

For a VLAN or group of VLANs, STP instances can be created independently that user their own different spanning trees within a LAN.

With the MSTP approach, a root bridge and the lowest path costs between the root bridge and the root ports offered of the individual bridges are determined.

The root bridge sends **B**ridge **P**rotocol **D**ata **U**nits (BPDU) to all bridges and determines the network configuration from the configuration data contained in the BPDU data packets.

8.3 Security

8.3.1 Access Control List (ACL)

The ACL (“**A**ccess **C**ontrol **L**ist”) is a list of permissions attached to an object. The list specifies who or what is allowed to access an object and what operations are allowed to be performed on the object.

The ACL function allows users to configure some rules to reject packets received from specific ingress ports or all ports. These rules check the source and destination MAC addresses of packets. If packets match these rules, the system executes the “deny” action, meaning it rejects these packets.

The packets can be filtered by:

- A source MAC or IP address
- A destination MAC or IP address
- A range of MAC or IP addresses
- Freely selected source or destination ports (e.g., UDP or TCP)

The “Action Resolution Engine” collects the information (action and metering results) from the hit entries: If more than one rule matches, the actions and measurements/counters are taken from the policy associated with the matched rule with highest priority.

8.4 Monitor

8.4.1 Alarm

This function alerts the network administrator to certain events and network situations.

Example

P1: ON – The connection to port 1 has failed.

PWR: ON – The primary power supply is interrupted.

RPS: ON – The secondary power supply is interrupted.

8.4.2 Monitor Information

This function displays some hardware information for purposes of monitoring the system and guaranteeing proper network operation.

8.4.3 RMON Statistics

This function is used to monitor or delete RMON statistics.

Jabber

Subscribers whose data packets are longer than the allowable MTU (“**M**aximum **T**ransmission **U**nit”) on a network (e.g., ETHERNET) are referred to as jabbers.

8.4.4 SFP

SFPs (“**S**mall **F**orm-factor **P**luggables”) are small standardized modules for network connections.
SFP refers to a modular interface to support various transmission media and is used in network technology for interface flexibility.

8.4.4.1 SFP Information

DDMI (“**D**igital **D**iagnostics **M**onitoring **I**nterface”) is technology that allows users to monitor the following real-time parameters in SFP modules:

- Voltage
- Bias current
- Input power
- Output power
- Temperature
- Fiber optic cable
- Connector
- Wavelength
- Transmission length
- DDM support
- Handler: name
- Handler: item number
- Handler: revision
- Handler: key number
- Date information (coded)

8.4.5 Traffic Monitor

The “Traffic Monitor” function can be used to enable or disable a specific port or the switch globally. This function can monitor the data rate of broadcast, multicast or broadcast and multicast packets. If the packet rate exceeds the specification for a user, the port is blocked. If the “Recovery” function is enabled, the port is re-enabled after the “Recovery Time” has expired.

8.5 Management

8.5.1 SNMP

SNMP (“**S**imple **N**etwork **M**anagement **P**rotocol”) represents a standard for ETHERNET device management within a TCP/IP network. The Simple Network Management Protocol (SNMP) is responsible for transporting the control data that allows the exchange of management information and status and statistical data between individual network components and a management system.

SNMP is a component of the “Internet Protocol Suite” defined by the IETF (“**I**nternet **E**ngineering **T**ask **F**orce”). It consists of a set of standards for network management, including an application layer protocol, a database schema and a set of data objects.

SNMP provides management data in the form of variables of the managed systems, which describe the system configuration. These variables can then be queried (and sometimes changed) by managing applications.

Support for MIBs

- RFC 1157 A Simple Network Management Protocol
- RFC 1213 MIB-II
- RFC 1493 Bridge MIB
- RFC 1643 ETHERNET Interface MIB
- RFC 1757 RMON Group 1,2,3,9

An “SNMP Community String” is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The string is included in every packet transmitted between the SNMP manager and the SNMP agent.

The “SNMP Community” acts like a password and is used to define the security parameters of SNMP clients in SNMP v1 and SNMP v2c environments. The default “SNMP Community” is “public” for both SNMPv1 and SNMPv2c as long as SNMPv3 is not enabled. Once SNMPv3 is enabled, the “communities” of SNMPv1 and v2c must be unique and cannot be shared.

Network ID of the trusted host:

The IP address is a combination of the network ID and host ID.

- Network ID = (host IP and mask).
- A user should only enter the network ID and leave the host ID as “0.” If a user enters a host ID, such as 192.168.1.102, the system resets the host ID to 192.168.1.0.

Note

Community String
It should allow users to configure the community string and rights only.

If a user configures the community string and the rights, and the network ID of the trusted host = 0.0.0.0 and the subnet mask = 0.0.0.0, this means that all hosts with this community string can access the switch.

8.5.1.1 SNMP Trap

A trap is an unsolicited message from an agent to the manager that an event has occurred. The SNMP manager that receives the trap can request more information.

9 Configuration

9.1 Overview of Configuration Options

The industrial managed switch provides two options for extended management functions:

Telnet/SSH Port
A menu-driven user interface can be opened from the WBM (“**W**eb **B**ased **M**anagement”) via the Telnet port.

Note

Additional information
Please refer to the section “Configuring in the Web-Based Management System (WBM)” for a detailed description.

Console Port
The CLI (“**C**ommand **L**ine **I**nterface”) can be opened via the console port on the front of the industrial managed switch (local) via an integrated management agent.

The management agent is based on SNMP (Simple Network Management Protocol). Using this SNMP agent, management software can be used to manage the industrial managed switch from any PC in the network.

The management agent includes an embedded HTTP Web agent. A standard Web browser can be used on any PC connected to the network to access the Web agent.

Note

Additional information
Please refer to the section “Appendix” > ... > “Configuring in the Command Line Interface (CLI)” for a detailed description.

9.1.1 Telnet Port

1. Connect the computer to one of the ETHERNET ports.

2. Open a Telnet session to the switch's IP address. If this is your first login, use the default values.

Table 53: Default Settings for the Telnet Port

Setting	Default Value
IP address	0.0.0.0
Subnet mask	0.0.0.0
Default gateway	0.0.0.0
Management VLAN	1
Default username	admin
Default password	wago

Note

Note information on assigning the IP address:
By default, the device is provided with IP address 0.0.0.0 and cannot be addressed directly via the Telnet port.
The IP address must be assigned via DCP or CLI. You can find extensive information on the procedure in the section "PROFINET."

9.2 Console Port

Before accessing the integrated management agent of the industrial managed switch via a network connection, you first have to configure it via a local connection or the BOOTP protocol with the default IP address, a subnet mask and a standard gateway.

After configuring the IP parameters of the industrial managed switch, you can access the integrated configuration utility from any point in the connected network or via the Internet. The integrated configuration utility can be opened via Telnet from any computer connected to the network. In addition, it can be managed from any computer via a Web browser.

Note

Precondition for establishing the connection:
Make sure that the terminal or PC is configured for the connection with the above settings. Otherwise, no connection can be established.

1. Connect the computer to the console port on the switch using the appropriate cable.

   Please refer to the section “Appendix” > ... > “RJ45 Cable” for details on the cable terminal assignment.

2. Use a terminal emulator (PuTTY) with the following settings:

Table 54: Default Settings for the Console Port

Setting	Default Value
Baud rate	38400
Parity	None
Number of data bits	8
Number of stop bits	1
Flow control	None

3. Press **[ENTER]** to open the login screen.

Table 55: Login Screen

Setting	Default Value
Default username	admin
Default password	wago

Hinweis

Follow the procedure:
You can find the exact procedure for establishing the connection and assigning the IP address via CLI in the section “PROFINET” > “Access via Console Port (CLI).”

10 Web Based Management System (WBM)

An internal file system and integrated Webserver can be used for configuration and administration of the system. Together, they are referred to as the Web-Based Management (WBM) system.

Note

In the delivery state, use of WBM is restricted!
Upon delivery, the switch is in PROFINET mode. In this mode, use of WBM is restricted (see section “PROFINET”).
Use of the full functional scope of WBM requires disabling PROFINET mode in the switch.

The HTML pages stored internally provide you with information about the configuration and status of the fieldbus node. In addition, you can also change the configuration of the device here.
You can also save HTML pages you created yourself via the implemented file system.

Note

Always restart after making changes to the configuration!
The system must always be restarted for the changed configuration settings to take effect.

1. To open WBM, launch a Web browser (e.g., Microsoft Internet Explorer or Mozilla Firefox).
2. Enter the IP address of the product in the address bar.
3. Click **[Enter]** to confirm.
4. Enter your username and password in the query dialog:

   User = “admin”
   Password = “wago”
5. The WBM start page loads.
6. Make the desired settings.
7. Click **[Apply]** or **[Update]** to confirm your changes, or click **[Delete]** or **[Discard]** to discard your changes.
8. To apply the settings, confirm your changes with the **[Save configuration]** button.

You can access the corresponding WBM pages via the links in the navigation bar:

Table 56: Overview – Navigation Links and WBM Pages

Navigation Links and WBM Pages
▶ **[System Status]**
• System Information
▶ **[Basic Settings]**
• General Settings • MAC Management • Port Mirroring • Port Settings
▶ **[PROFINET]**
• Configuration • Information • Diagnostics
▶ **[Advanced Settings]**
[Bandwidth Control] • QoS • Rate Limitation **[IGMP Snooping]** • IGMP Snooping • IGMP Filter • Multicast Address • Multicast IP Statistics **[VLAN]** • Port Isolation • VLAN • MAC VLAN • LLDP • Loop Detection • MRP • STP (RSTP/MSTP)
▶ **[Security]**
• Access Control List
▶ **[Monitor]**
• Alarm • System Information • Port Statistics • Port Load

- RMON Statistics
- SFP Information
- Traffic Monitor

▶ **[Management]**

[SNMP]

- SNMP
- SNMP Trap
- SNMPv3

- Maintenance
- System Log
- Upload File
- Ping
- User Account
- Open-Source License
- WAGO Licenses

The settings/configuration of the industrial managed switch can be made on these WBM pages.

There are tab pages on some WBM pages for the settings/configurations.

The default values are shown in **bold**.

10.1 System Status

10.1.1 System Information

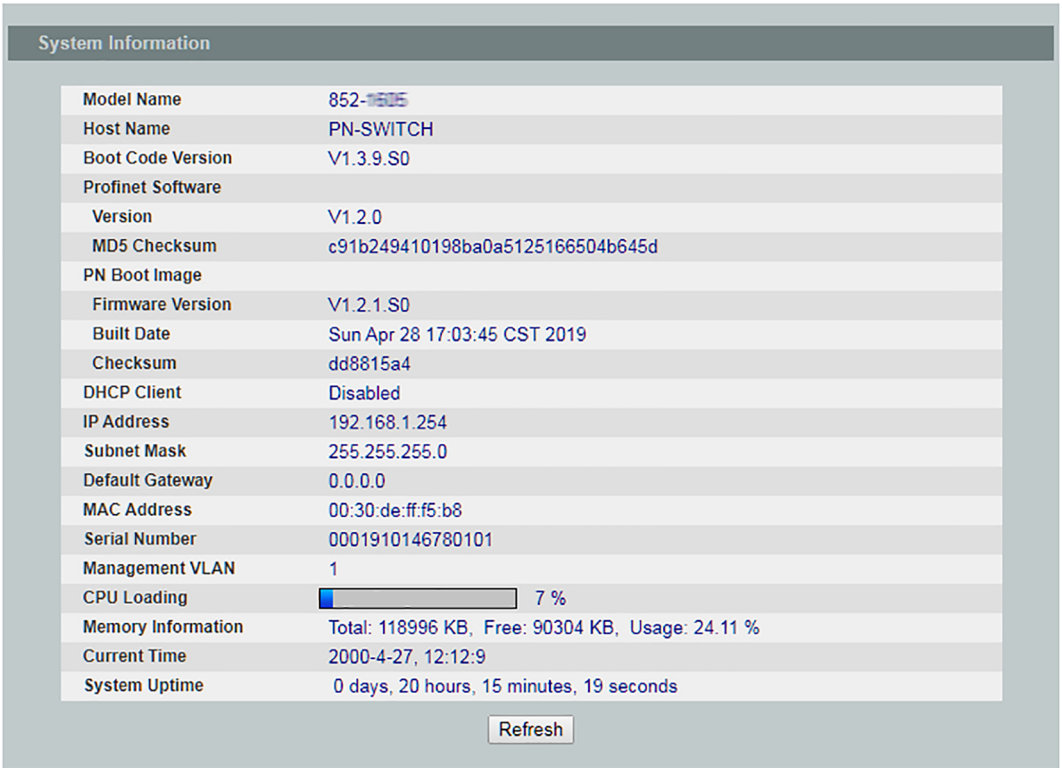


Figure 42: WBM “System Information” Page

Table 57: WBM “System Information” Page

Parameters	Description
Model Name	This field shows the model name of the switch.
Host Name	This field shows the host name of the switch.
Boot Code Version	This field shows the boot code version.
Profinet Software Version	ID number of the PROFINET software version
Profinet Software MD5 Checksum	Checksum of the PROFINET software version
PN Boot Image Firmware Version	This field shows the PROFINET boot image version.
PN Boot Image Build Date	This field shows the firmware build date.
PN Boot Image Checksum	This field shows the PROFINET boot image checksum.
DHCP Client	This field indicates whether the DHCP client function is enabled.
IP Address	This field shows the IP address of the switch.
Subnet Mask	This field shows the subnet mask of the switch.
Default Gateway	This field shows the default gateway of the switch.
MAC Address	This field shows the MAC (Media Access Control) address of the switch.
Serial Number	This field shows the serial number.
Management VLAN	This field shows the VLAN ID required for the switch management process.
CPU Loading	This field shows the system load of the switch as a percentage.
Memory Information	This field shows the total memory (“Total”), memory available at the moment (“Free”) and memory used (“Usage”) of the switch.
Current Time	This field shows the current date (yyyy-mm-dd) and current time (hh:mm:ss).
System Uptime	This field shows how long the switch remains in operation after being switched on in days, hours, minutes and seconds.

10.2 Basic Settings

10.2.1 General Settings

10.2.1.1 System

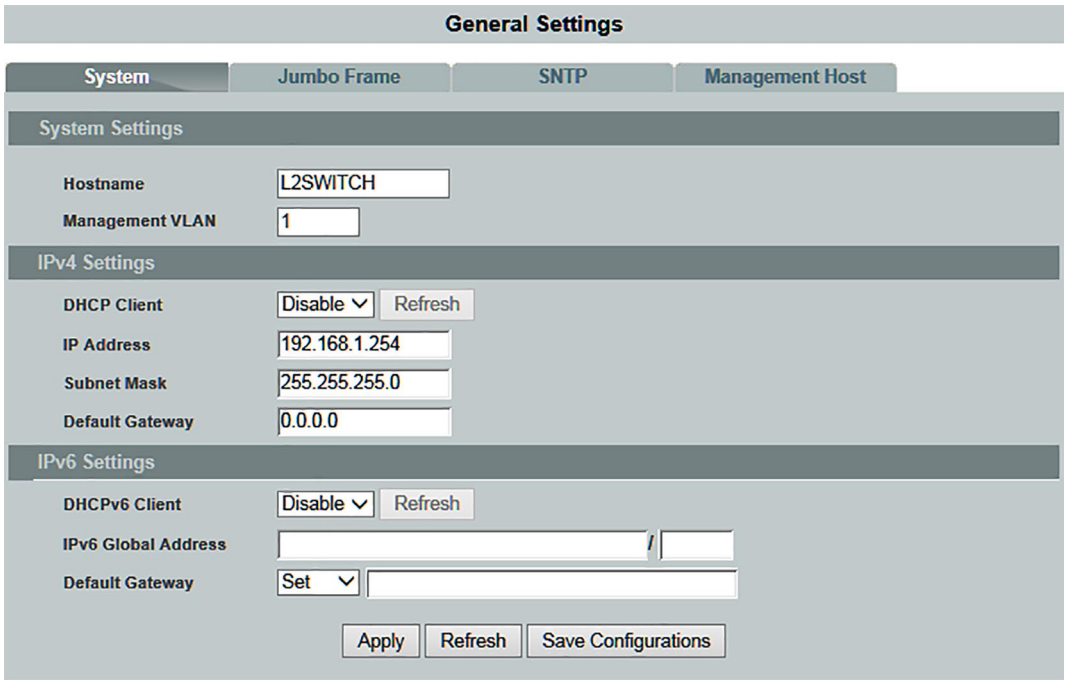


Figure 43: WBM Page, “General Settings” – “System” Tab

Table 58: WBM Page, “General Settings” – “System” Tab

System Settings		
Parameters	**Default**	**Description**
Hostname	**L2SWITCH**	Enter up to 64 alphanumeric characters for the name of your switch. The hostname should be a combination of numbers, letters, hyphens (-) or underscores (_).
Management VLAN	**1**	Specify a VLAN group to have access to the switch. Valid VLAN range: 1 … 4094. **Note** ***Note*** **Configuring a Management VLAN** Before configuring a management VLAN, you must first create a management VLAN and assign it at least one subscriber port.
IPv4 Settings		
Parameters	**Default**	**Description**
DHCP Client	**Disable**	Select “Disable” in the selection box if you want to manually configure the IP address of the switch. Click **[Renew]** to allow the switch to get an IP address from the DHCP server.
	Enable	Select “Enable” in the selection box to allow the switch to get its IP address from a DHCP server automatically. Click **[Renew]** to allow the switch to get an IP address from the DHCP server.
IP Address	**0.0.0.0**	Enter the IP address of the switch in decimal-point notation.
Subnet Mask	**0.0.0.0**	Enter the IP subnet mask of the switch in decimal-point notation.
Default Gateway	0.0.0.0	Enter the IP address of the default outgoing gateway in decimal-point notation.
IPv6 Settings		
Parameters	**Default**	**Description**
DHCPv6 Client	**Disable**	Select “Disable” in the selection box if you want to manually configure the IP address of the switch.
	Enable	Select “Enable” in the selection box to allow the switch to get its IP address by DHCP automatically. Click **[Renew]** for the switch to update the values.
Static IPv6 Address		This field displays the static IPv6 address.
Default Gateway	**Set**	Select "Set" in the selection box to enter the IP address. Enter the IP address of the default outgoing gateway in decimal-point-notation.
	Unset	Select “Unset” in the selection box if no IP address should be entered.

10.2.1.2 Jumbo Frame

Note

Additional Information

Please refer to the section “Function Description” for more information on “Jumbo Frame”.

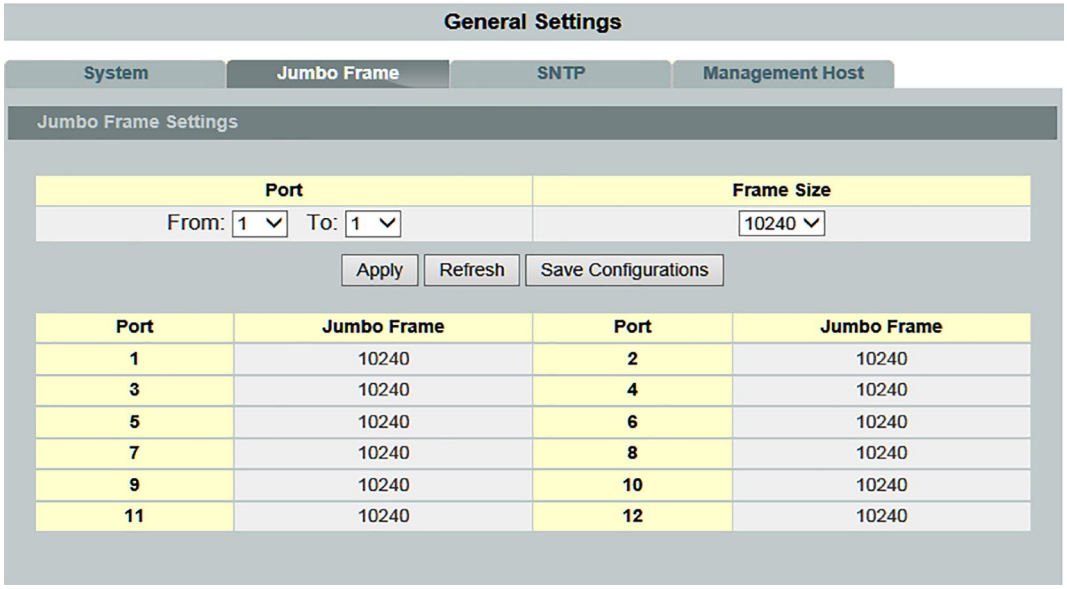


Figure 44: WBM Page, “General” – “Jumbo Frame” Tab

Table 59: WBM Page, “General” – “Jumbo Frame” Tab

Jumbo Frame Settings			
Parameters		**Default**	**Description**
Port	From:	**1**	Select a port or port range in the selection box to configure the jumbo frame.
	to:	**1**	Select a port or port range in the selection box to configure the jumbo frame.
Jumbo Frame		**10240**	Select the maximum number of bytes of a jumbo frame for all ports. The bigger the frame size, the better the network performance.
		1522	
		1536	
		1552	
		9010	
		9216	
Port		1 … 10 (12)	This column displays the port numbers.
Jumbo Frame		1522	This column displays the maximum number of bytes for a jumbo frame.
		1536	
		1552	
		9010	
		9216	
		10240	

10.2.1.3 SNTP

Note

Additional Information

Please refer to the section “Function Description” for more information on “SNTP” (**S**imple **N**etwork **T**ime **P**rotocol).

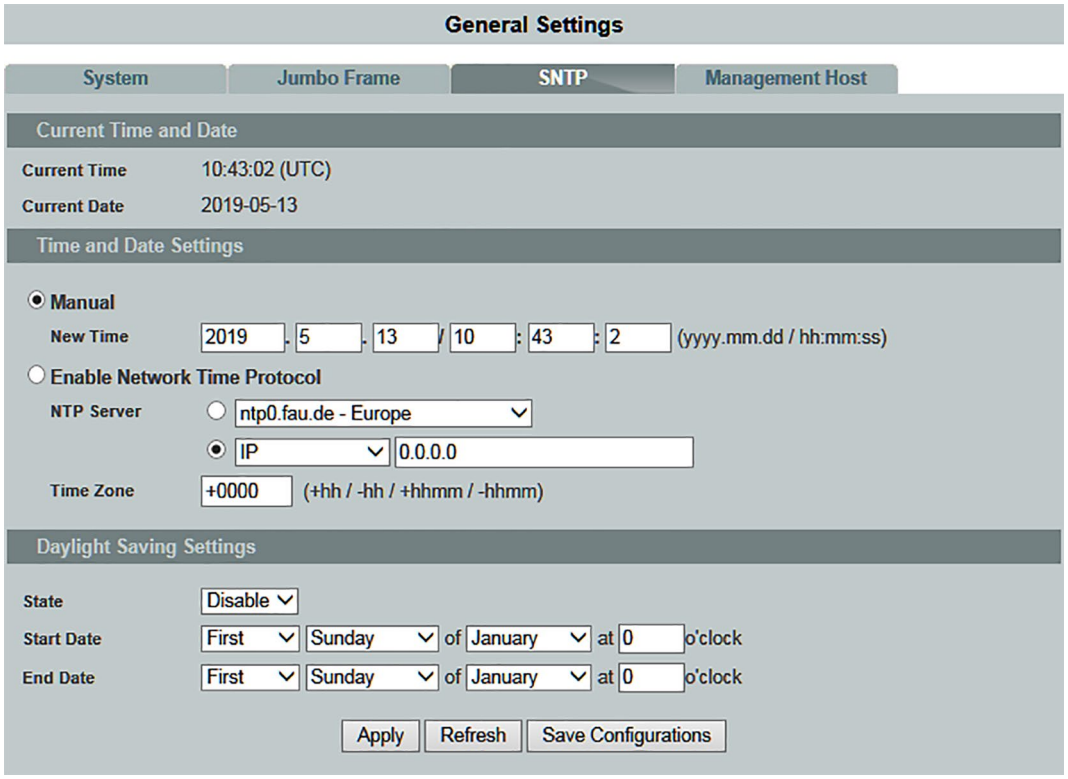


Figure 45: WBM Page, “General” – “SNTP” Tab

Table 60: WBM Page, “General” – “SNTP” Tab

Current Time and Date				
Parameters	**Default**	**Description**		
Current Time		This field displays the current time if you open or refresh the menu.		
Current Date		The field displays the current date if you open or refresh the menu.		
Time and Date Settings				
Parameters	**Default**	**Description**		
Manual	New Time ○	Select this option if you want to manually set the time and date for the system. Enter the new date in the format year/month/day format and time in the format hour/minute/second. Click **[Apply]** to display the “Current Time” and “Current Date”.		
Enable Network Time Protocol		Select this option to use NTP (“Network Time Protocol”) for the time service.		
	NTP Server ◉	◉	Select this option if you want to use a predefined time server. The switch searches for a time server for 60 seconds.	
		○	Select this option if you enter the IP address of a time server. The switch searches for a time server for 60 seconds.	
	0.0.0.0	◉	IP	Enter the IP address of the NTP server in decimal-point notation.
		○	Domain Name	Enter the domain address of the switch.
	Time Zone **+0000**	Enter the time difference between UTC (“Universal Time Coordinated”, formally GMT “Greenwich Mean Time”) and the time zone in hh.mm.		

Table 60: WBM Page, “General” – “SNTP” Tab

Daylight Saving Settings		
Parameters	**Default**	**Description**
State	**Disable**	Select “Disable” if you do not want to use daylight savings time.
	Enable	Select “Enable” if you want to use daylight savings time.
Start Date[1)]		Enter the date and time for the start of daylight savings if you have enabled this option. The time is displayed in 24-hour format.
End Date[2)]		Enter the date and time for the end of daylight savings if you have enabled this option. The time is displayed in 24-hour format.

1)	Daylight savings starts on the second Sunday of March in most places in the USA. Daylight savings starts at 2 A.M local time in each time zone in the USA. Correspondingly, you would select “Second, Sunday, March” and “2:00”. In the EU, daylight savings starts on the last Sunday in March. It starts at the same time (1:00 A.M GMT or UTC) in all EU time zones. Correspondingly, you would select “Last, Sunday, March”) and in the last field, enter the time based on your time zone. In Germany, for instance, you would select “2:00” because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
2)	In the USA, daylight savings ends on the last Sunday in October. It ends at 2:00 A.M. local time in each time zone in the USA. Correspondingly, you would select “First, Sunday, November” and “2:00”. In the EU, daylight savings ends on the last Sunday in October. Daylight savings ends at the same time (1:00 AM GMT or UTC) in all EU times zones. Correspondingly, you would select “Last, Sunday, October”) and in the last field, enter the time based on your time zone. In Germany, for instance, you would select “2:00” because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

10.2.1.4 Management Host

Note

Additional Information

Please refer to the section “Function Description” for more information on “Management Host”.

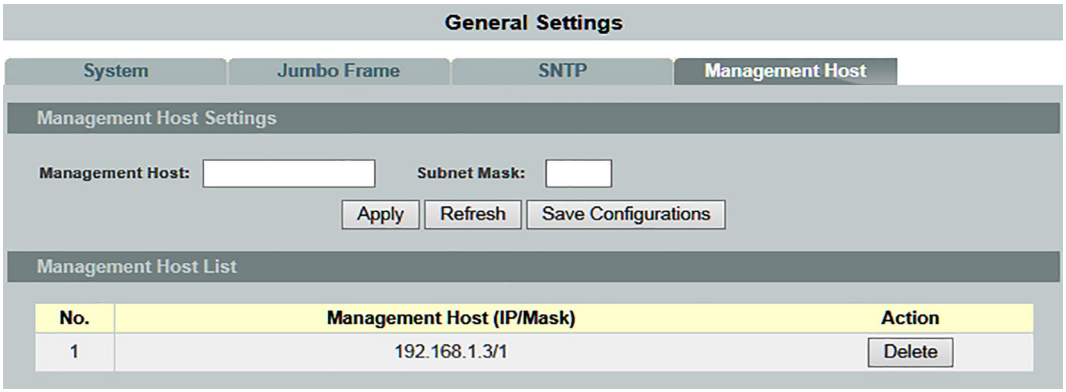


Figure 46: WBM Page, “General” – “Management Host” Tab

Table 61: WBM Page, “General” – “Management Host” Tab

Management Host Settings		
Parameters	**Default**	**Description**
Management Host		Enter the IP address of the “Management Host” in decimal-point notation.
Subnet Mask		In this input field, enter the subnet mask address number of the management host in decimal-point notation.
Management Host List		
Parameters	**Default**	**Description**
No.	1 … 3	This column displays the sequential numbers of each “Management Host”.
Management Host (IP/Mask)		This column displays the “Management Hosts”.
Action		Click **[Delete]** to delete a specific entry.

10.2.2 MAC Management

Note

Additional Information
Please refer to the section “Function Description” for more information on “MAC Management”.

10.2.2.1 Static MAC Settings

Note

Additional Information
Please refer to the section “Function Description” for more information on “Static MAC Settings” (static MAC address).

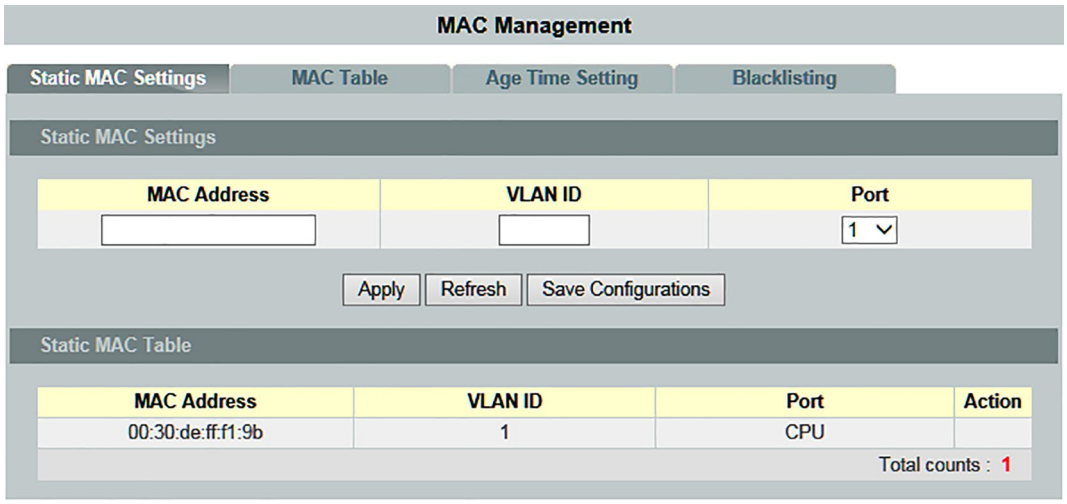


Figure 47: WBM Page, “MAC Management” – “Static MAC Settings” Tab

Table 62: WBM Page, “MAC Management” – “Static MAC Settings” Tab

Static MAC Settings		
Parameters	**Default**	**Description**
MAC Address		In this input field, enter the MAC address of a computer or device that you want to add to the MAC address table. The valid format is: hh:hh:hh:hh:hh:hh.
VLAN ID		In this input field, enter the VLAN ID to apply to the computer or device.
Port	**1** … 10	In this selection box, select the port number to which the computer or device is connected.
Static MAC Table		
Parameters	**Default**	**Description**
MAC Address		This column displays the manually entered MAC address entries.
VLAN ID		This column displays the VLAN ID of the manually entered MAC address entries.
Port	1 … 10	This column displays the port numbers of the manually entered MAC address entries. The MAC address “CPU” is the MAC address of the switch.
Action		Click **[Delete]** to delete the manually entered MAC address from the MAC address table. You cannot delete the MAC address of the switch from the static MAC address table.
Total counts		This display field displays the total number of entries in the static MAC address table.

10.2.2.2 MAC Table

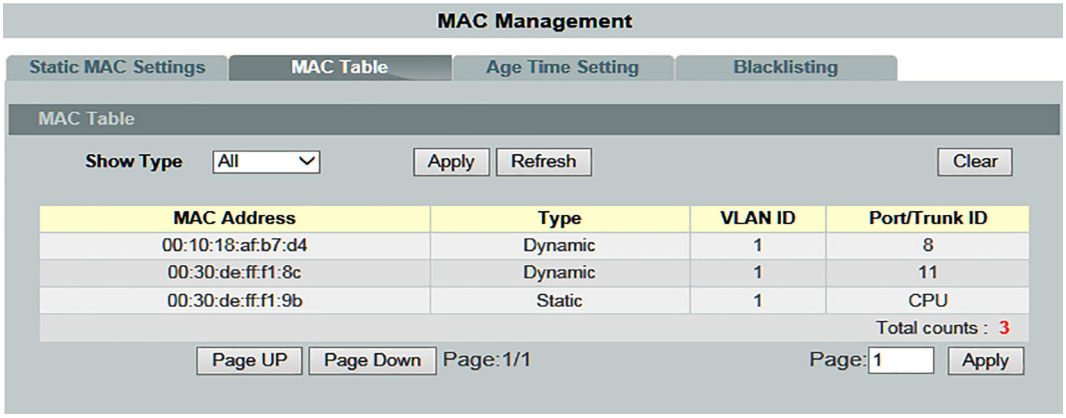


Figure 48: WBM Page, “MAC Management” – “MAC Table” Tab

Table 63: WBM Page, “MAC Management” – “MAC Table” Tab

MAC Table		
Parameters	**Default**	**Description**
Show Type	**[All]**	Select “All” to display all MAC address entries.
	Static	Select “Static” to display the static MAC address entries.
	Dynamic	Select “Dynamic” to display the dynamic MAC address entries.
	Port	Select “Port” to display the corresponding MAC address entries.
	MAC	Select “MAC” to display the corresponding MAC address entries.
MAC Address		This column displays the MAC addresses.
Type		This column displays whether the entry was entered manually (static) or pulled by the switch (dynamic).
VLAN ID		This column displays the VLAN ID of the MAC address entry.
Port/Trunk ID		This column displays the port numbers to which the MAC address entry is connected. “CPU” is the MAC address entry of the switch.
Total counts		This display field displays the total number of entries in the MAC address table.
Page UP		This button can be used to scroll up for many MAC address entries.
Page Down		This button can be used to scroll down for many MAC address entries.
Page		This display field displays the current page of the MAC address table.

10.2.2.3 Age Time Setting

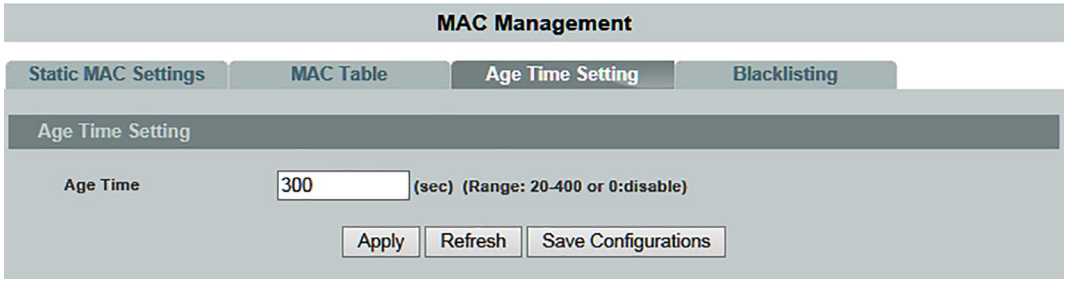


Figure 49: WBM Page, “MAC Management” – “Age Time Setting” Tab

Table 64: WBM Page, “MAC Management” – “Age Time Setting” Tab

Age Time Setting		
Parameters	**Default**	**Description**
Age Time (sec) (Range:20-400 or 0:disable)	**300**	Enter the “Age Time” in this input field. Valid range: 0 or 20 … 400 s.

10.2.2.4 Refusal MAC Settings

Note

Additional Information
Please refer to the section “Function Description” for more information on “Refusal MAC Settings”.

Note

Maximum number of MAC blacklist entries
Up to 20 entries can be configured.

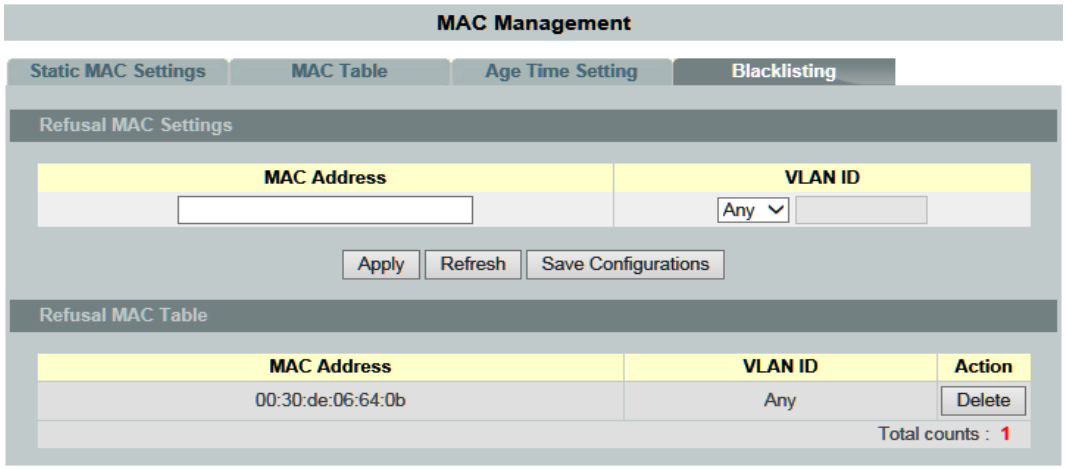


Figure 50: WBM Page, “MAC Management” – “Refusal MAC Settings” Tab

Table 65: WBM Page, “MAC Management” – “Refusal MAC Settings” Tab

Refusal MAC Settings		
Parameters	**Default**	**Description**
MAC Address		Enter the MAC address of a computer or device that you want to reject. The valid format is: hh:hh:hh:hh:hh:hh.
VLAN ID	**Any**	The switch receives any VLAN ID.
	Vlan	Enter the VLAN ID that you want to assign to the computer or device.
Refusal MAC Settings		
Parameters	**Default**	**Description**
MAC Address		This column displays the MAC addresses.
VLAN ID		This field displays the VLAN ID of the MAC address entry.
Action		Click **[Delete]**, to delete a MAC address entry manually entered from the blacklist table.
Total counts		This field displays the total number of entries in the blacklist table.

10.2.3 Port Mirroring

Note

Additional Information

Please refer to the section “Function Description” for more information on “Port Mirroring”.

Note

Monitor Port

The monitor port cannot be a member of any “Truck Port” group.
The monitor port cannot be an ingress or egress port.
If a port has been configured as a source port and a user then configures it as a destination port, the port is automatically deleted from the source ports.

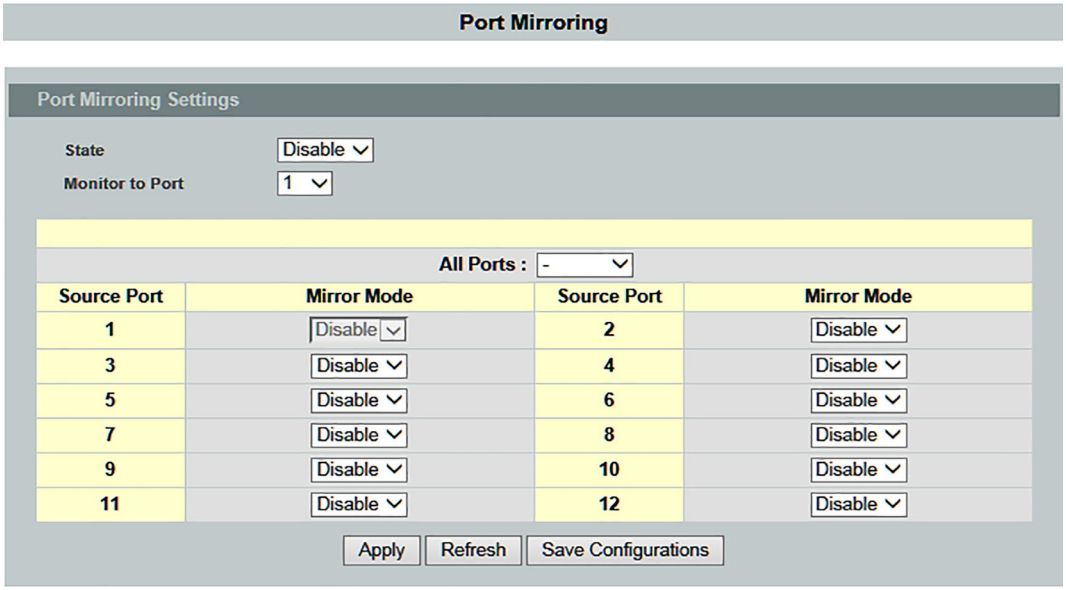


Figure 51: WBM “Port Mirroring” Page

Table 66: WBM “Port Mirroring” Page

Port Mirroring Settings		
Parameters	**Default**	**Description**
State	**Disable**	Select “Disable” to disable the “Port Mirroring”.
	Enable	Select “Enable” to enable the “Port Mirroring”.
Monitor to Port	**1** … 10 (12)	Select a port to be connected to a “Network Traffic Analyzer”.
All Ports	-	Settings in this select box apply to all ports. Make settings here to be applied to all ports. Start here with general settings and then change the settings for individual ports.
	Disable	
	Ingress	
	Egress	
	Both	
Source Port	1 … 10 (12)	This column displays the number of individual source ports.
Mirror Mode	Disable	Select “Disable” to prevent traffic being copied from the specified source port to the monitor port.
	Ingress	Select “Ingress” to only copy the input data (incoming) from the specified source ports to the monitor port.
	Egress	Select “Egress” to only copy the output data (outgoing) from the specified source ports to the monitor port.
	Both	Select “Both” to copy both incoming and outgoing data from the specified source ports to the monitor port.

10.2.4 Port Settings

10.2.4.1 General Settings

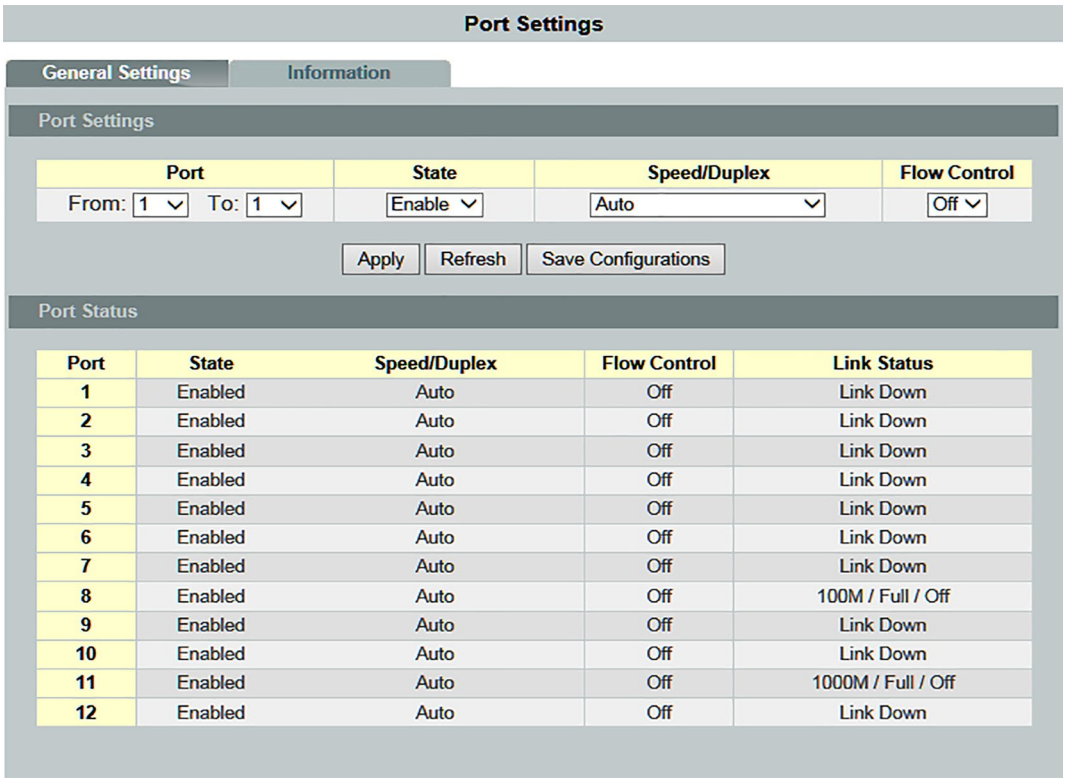


Figure 52: WBM Page, “Port Settings” – “General Settings” Tab

Table 67: WBM Page, “Port Settings” – “General Settings” Tab

Port Settings			
Parameters		**Default**	**Description**
Port	From:	**1**	Select a port or port range that you want to configure.
	to:	**1**	Select a port or port range that you want to configure.
State		**Disable**	Select “Disable” to disable the port.
		Enable	Select “Enable” to enable the port.
Speed/Duplex		**Auto**	Select the speed and duplex mode of the port.
		10 Mbit/s / Full Duplex	
		10 Mbit/s / Half Duplex	
		100 Mbit/s / Full Duplex	
		100 Mbit/s / Half Duplex	
		1000 Mbit/s / Full Duplex	
Flow Control		**Off**	Select “Off” to disable access to the port's buffer resources and to interrupt operation of the switches in the network.
		On	Select “On” to maintain access to the port's buffer resources and to ensure lossless operation of the switches in the network.
Port State			
Parameters		**Default**	**Description**
Port		1 … 10 (12)	This column displays the port numbers.
State			This column displays if the port is enabled or disabled.
Speed/Duplex			This column displays the configured speed (10 Mbit/s, 100 Mbit/s or 1000 Mbit/s) and duplex mode (full or half-duplex) for a port.
Flow Control			This column displays whether the port's “Flow Control” is set to “On” or “Off”.
Link State			This column displays the link status of a port. If the port is up, the speed, duplex mode and “Flow Control” settings are displayed. “Link Up” displays that the port is either disabled or no device is connected.

10.2.4.2 Information

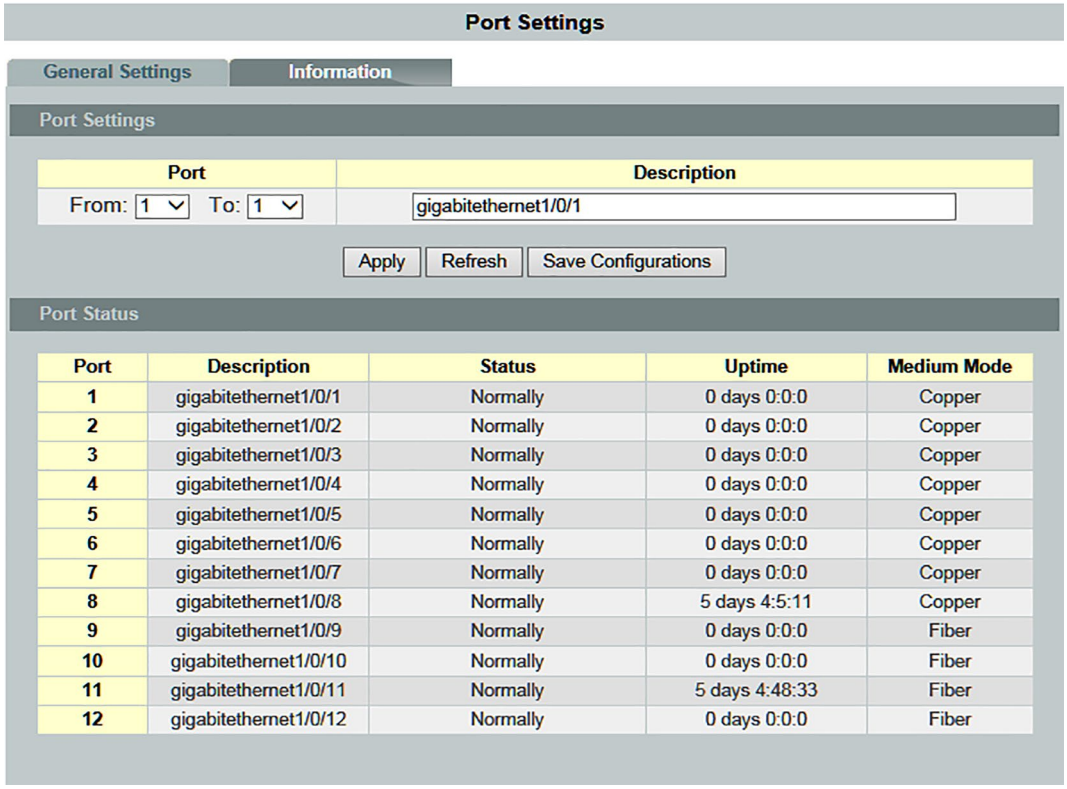


Figure 53: WBM Page, “Port Settings” – “Information” Tab

Table 68: WBM Page, “Port Settings” – “Information” Tab

Port Settings			
Parameters		**Default**	**Description**
Port	From:	**1**	Select a port or port range that you want to display.
	To:	**1**	Select a port or port range that you want to display.
Description			Enter the name for the port in the input field.
Port Status			
Parameters		**Default**	**Description**
Port		1 … 10 (12)	This column displays the port numbers.
Description			This column displays the name of the port.
Status			This column displays the status of the port.
Uptime			This column displays the operating mode of the port.
Medium Mode		Copper Fiber	This column displays the connection type. Copper wire Fiber optic cable

10.3 PROFINET

The WBM interface in the PROFINET section is described in the section “PROFINET.”

10.4 Advanced Settings

10.4.1 Bandwidth Control

10.4.1.1 QoS

Note

Additional Information
More information about “QoS” (Quality of Service) is available in the section “Function Description.”

10.4.1.1.1 Port Priority

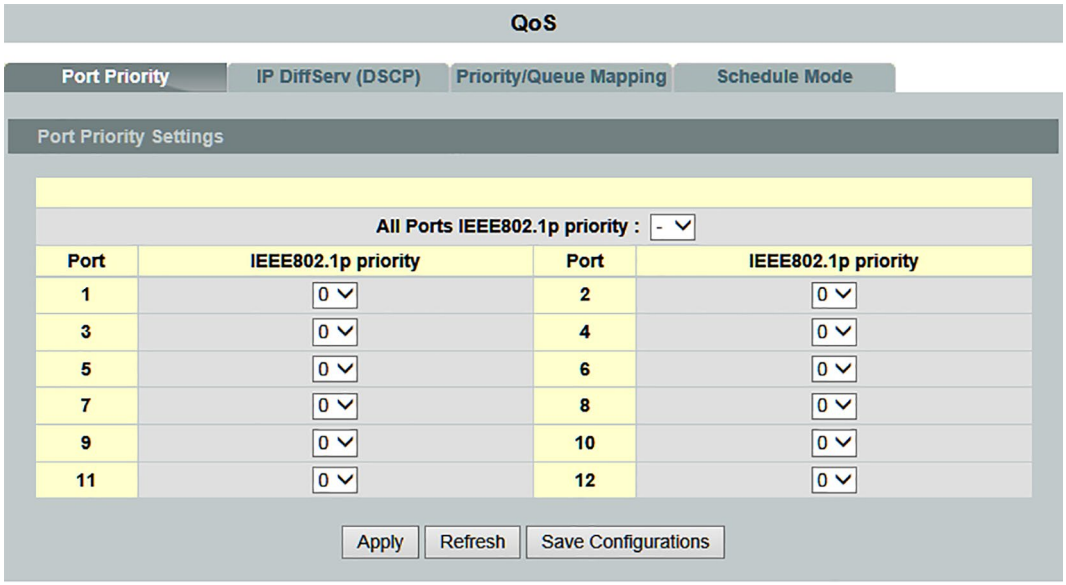


Figure 54: WBM “QoS” Page – “Port Priority” Tab

Table 69: WBM “QoS” Page – “Port Priority” Tab

Port Priority Settings		
Parameter	**Default**	**Description**
All Ports IEEE 802.1p priority.	-	In the selection box, enter the priority value for all ports. The value indicates the packet priority and is added to the “Priority Tag” field of the incoming packets.
	0 … 7	0 = Lowest priority 7 = Highest priority
Port	1 … 10 (12)	This column shows the port numbers.
IEEE 802.1p Priority	**0** … 7	In the selection box, select a priority for packets received on this port. Only packets without “IEEE 802.1p Tag Priority” are assigned the priority specified here.

10.4.1.1.2 IP-DiffServ (DSCP)

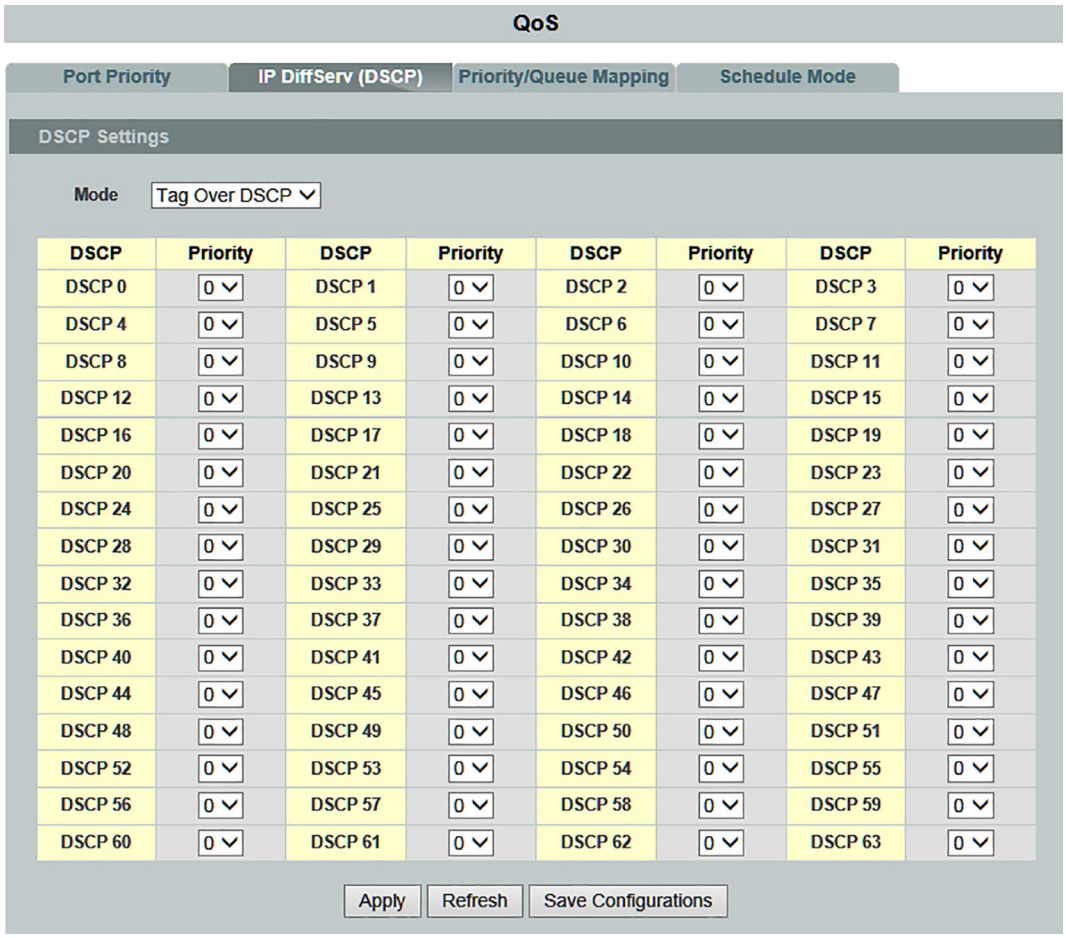


Figure 55: WBM “QoS” Page – “IP DiffServ (DSCP)” Tab

Table 70: WBM “QoS” Page – “IP DiffServ (DSCP)” Tab

DSCP Settings		
Parameter	**Default**	**Description**
Mode	**Tag over DSCP**	In the selection box, select “Tag over DSCP” if the 802.1p tag has a higher priority than DSCP.
	DSCP over Tag	In the selection box, select “DSCP over Tag” if the 802.1p tag has a lower priority than DSCP.
DSCP	DSCP 0 … DSCP 63	This column displays the DSCP fields.
Priority	**0** … 7	Select the respective priority level in the selection box. 0 = Lowest priority 7 = Highest priority

10.4.1.1.3 Priority/Queue Mapping

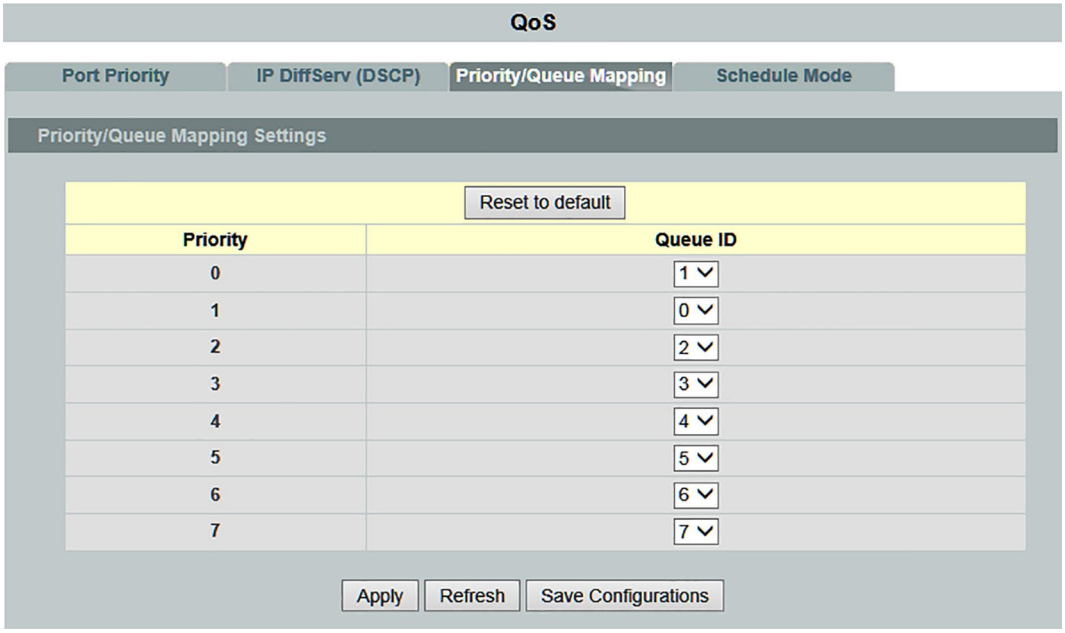


Figure 56: WBM “QoS” Page – “Priority/Queue Mapping” Tab

Table 71: WBM “QoS” Page – “Priority/Queue Mapping” Tab

Priority/Queue Mapping Settings		
Parameter	**Default**	**Description**
Reset to basic settings		Click this button to reset the priority of the queue to the default values.
Priority	0 … 7	This column displays the respective priority level. 0 = Lowest priority 7 = Highest priority
Queue ID	0 … 7	In the selection box, select the number of a queue for packets with the priority level.

Table 72: Default Settings

Priority	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

10.4.1.1.4 Schedule Mode

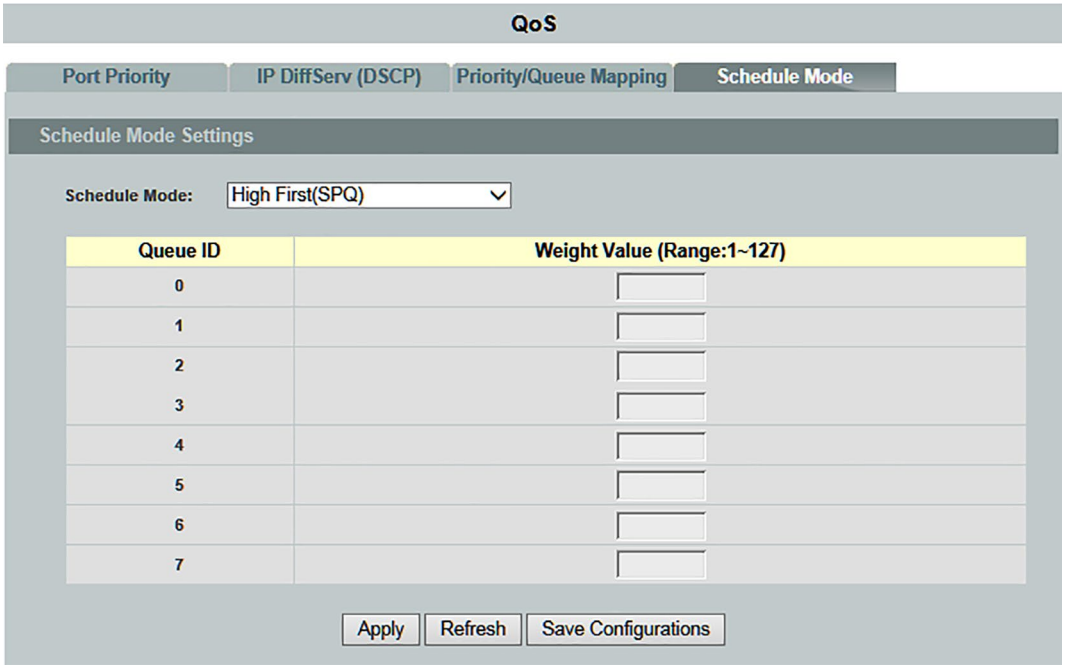


Figure 57: WBM “QoS” Page – “Schedule Mode” Tab

Table 73: WBM “QoS” Page – “Schedule Mode” Tab

Schedule Mode Settings		
Parameter	**Default**	**Description**
Schedule Mode	**Strict Priority Queuing (SPQ)**	In the selection box, select “Strict Priority Queuing (SPQ)” if you want to process the hardware priority queues sequentially.
	Weighted Round Robin (WRR)	In the selection box, select “Weighted Round Robin (WRR)” if you want to use the algorithm based on the queue weighting (the value entered in the “**Weight Value (range: 1–127)**” field). Processing queues with higher weighting is given precedence over processing those with lower weighting.
Queue ID	0 … 7	This column indicates which queue is being configured. 0 = Lowest priority 7 = Highest priority
Weight Value (range: 1~127)	**1** … 127	The “Weight Value” can only be configured if “Weighted Round Robin (WRR)” is selected. The bandwidth is divided among the different “Traffic Queues” according to their weighting. 0 = Lowest priority 127 = Highest priority
		***Note*** **Changing the “Weight Value (range: 1–127)”** If you have selected “Strict Priority Queuing (SPQ),” you cannot change the “Weight Value.” You must first select “Weighted Round Robin (WRR).” You can then change “Strict Priority Queuing (SPQ).”

10.4.1.2 Bandwidth Limitation

10.4.1.2.1 Storm Control

Note

Additional Information

Please refer to the section “Function Description” for more information on “Storm Control.”

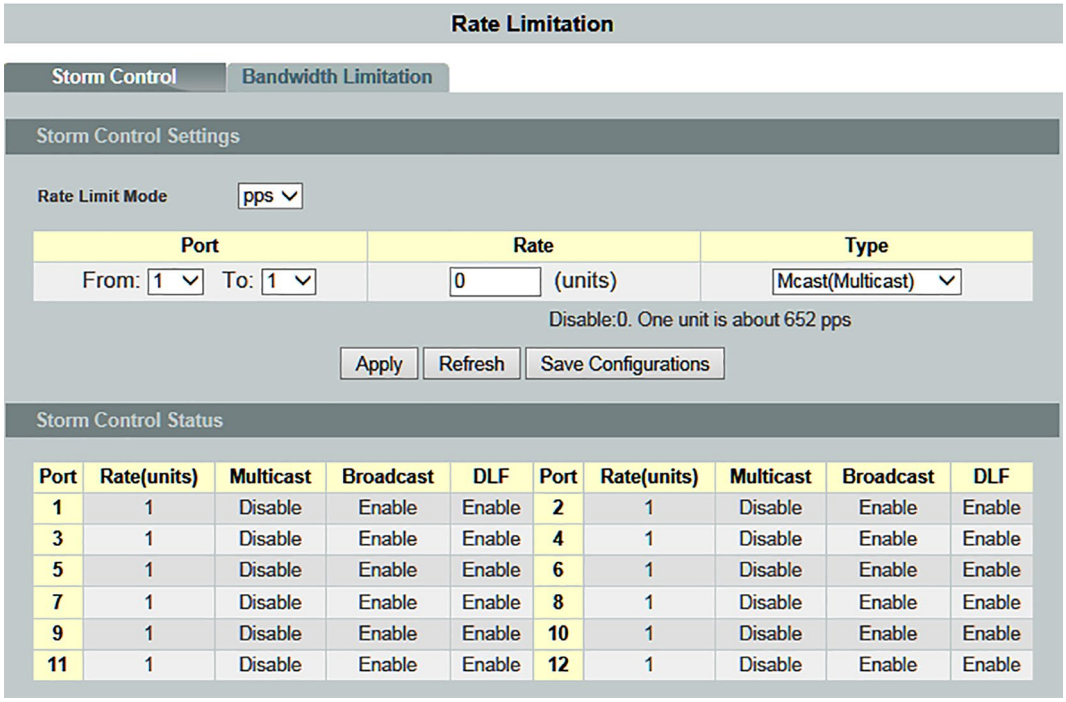


Figure 58: WBM “Rate Limitation” Page – “Storm Control” Tab

Table 74: WBM “Rate Limitation” Page – “Storm Control” Tab

Storm Control Settings			
Parameter		**Default**	**Description**
Rate Limit Mode		**pps** bps	Select the unit for band width restriction in the selection box. pps = Packets per second bps = Bits per second
Port	from:	**1**	Select a port or port range in the selection box to configure the “Storm Control Settings.”
	to:	**1**	Select a port or port range in the selection box to configure the “Storm Control Settings.”
Number (units)		**0**	In the selection box, choose the number of packets (of the type specified in the “Type” field) that the switch can receive per second.
Type		Bcast (Broadcast)	Choose “Bcast (Broadcast)” in the selection box to specify a limiting value for the number of broadcast packets received per second.
		Mcast (Multicast)	Choose “Mcast (Multicast)” in the selection box to specify a limiting value for the number of multicast packets received per second.
		DLF	Choose “DLF” in the selection box to specify a limiting value for the number of DLF packets received per second.
		Mcast+Bcast	Choose “Mcast+Bcast” in the selection box to specify a limiting value for the number of multicast and broadcast packets received per second.
		Mcast+DLF	Choose “Mcast+DLF” in the selection box to specify a limiting value for the number of multicast and DLF packets received per second.
		Bcast+DLF	Choose “Bcast+DLF” in the selection box to specify a limiting value for the number of broadcast and DLF packets received per second.
		Mcast+Bcast+ DLF	Choose “Mcast+Bcast+DLF” in the selection box to specify a limiting value for the number of multicast, broadcast and DLF packets received per second.
Storm Control Status			
Parameter		**Default**	**Description**
Port		1 … 10 (12)	This column shows the port numbers.
Rate (units)			This column displays the number of packets the switch can receive per second.
Multicast		Enable Disable	This column indicates whether the rate setting applies to multicast.
Broadcast		Enable Disable	This column indicates whether the rate setting applies to broadcast.
DLF		Enable Disable	This column indicates whether the rate setting applies to DLF.

10.4.1.2.2 Bandwidth Limitation

Note

Additional Information

Please refer to the section “Function Description” for more information on “Bandwidth Limitation.”

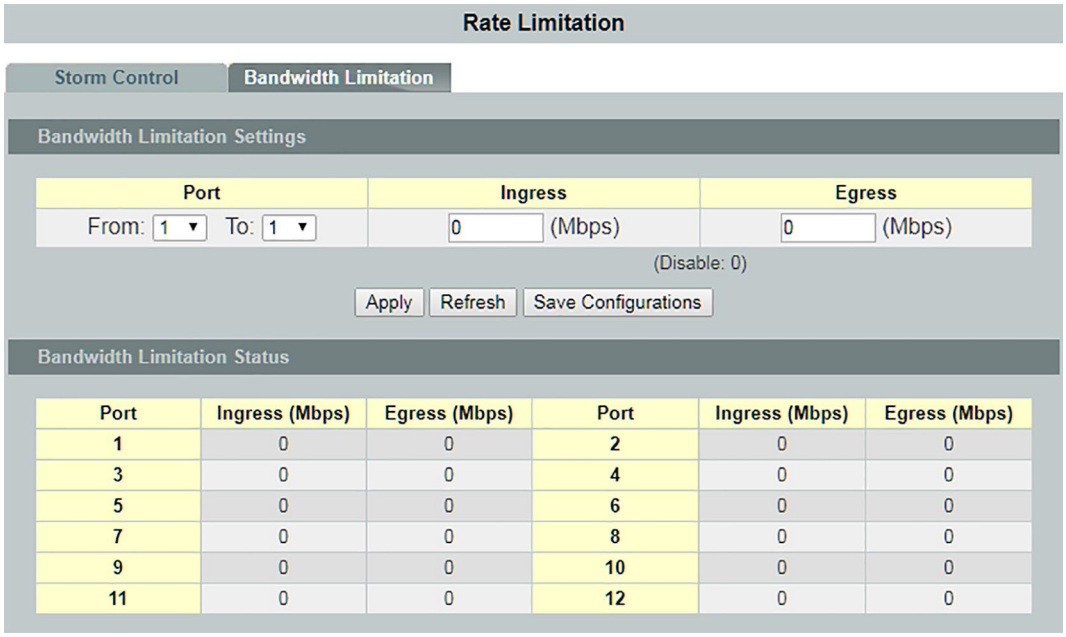


Figure 59: WBM “Rate Limitation” Page – “Bandwidth Limitation” Tab

Table 75: WBM “Rate Limitation” Page – “Rate Limitation” Tab

Bandwidth Limitation Settings			
Parameter		**Default**	**Description**
Port	from:	**1**	Select a port or port range in the selection box to configure the “Bandwidth Limitation Settings”.
	to:	**1**	Select a port or port range in the selection box to configure the “Bandwidth Limitation Settings”.
Ingress (Mbps)		**0**	Enter the “Bandwidth Limitation” for incoming packets in the input field. Port 1 … 8 0 … 100 Port 9 … 10(12) 0 … 1000
Egress (Mbps)		**0**	Enter the “Bandwidth Limitation” for outgoing packets in the input field.
Bandwidth Limitation Status			
Parameter		**Default**	**Description**
Port		1 … 10 (12)	This column shows the port numbers.
Ingress (Mbps)			This column displays the bandwidth set for ingress.
Egress (Mbps)			This column displays the bandwidth set for egress.

10.4.2 IGMP Snooping

Note

Additional Information
Please refer to the section “Function Description” for more information on “IGMP Snooping” (**I**nternet **G**roup **M**anagement **P**rotocol snooping).

10.4.2.1 IGMP Snooping

10.4.2.1.1 General Settings

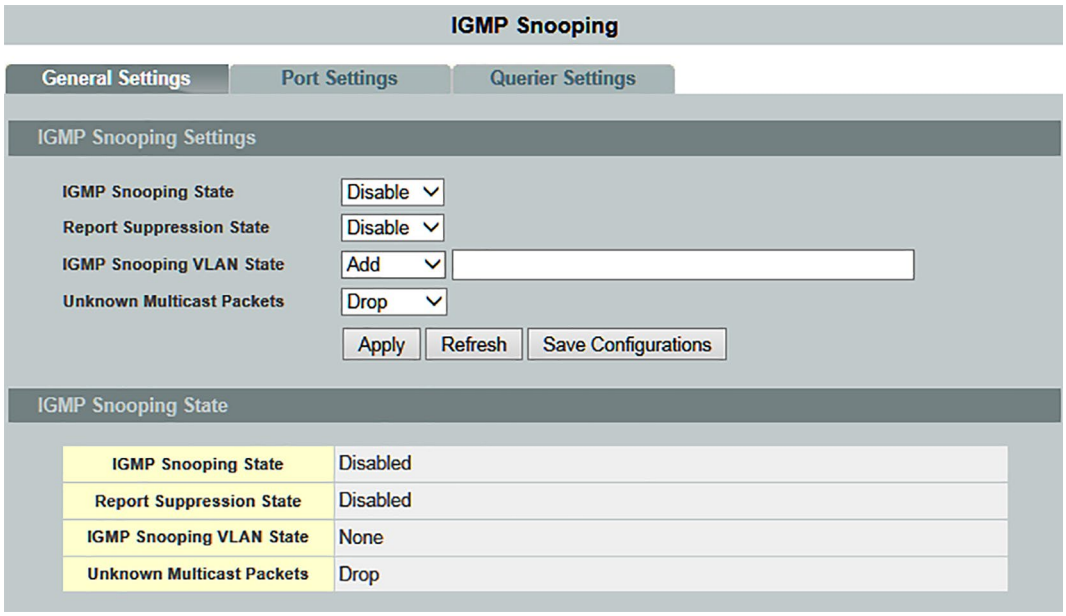


Figure 60: WBM “IGMP Snooping” Page – “General Settings” Tab

Table 76: WBM “IGMP Snooping” Page – “General Settings” Tab

IGMP Snooping Settings		
Parameter	**Default**	**Description**
IGMP Snooping State	**Disable**	Select “Disable” in the selection box to disable this function.
	Enable	Select “Enable” in the selection box to enable “IGMP Snooping” and to forward multicast group data only to ports that are members of this group.
Report Suppression State	**Disable**	Select “Disable” to disable the “Report Suppression” function for “IGMP Snooping.”
	Enable	Select “Enable” to enable the “Report Suppression” function for “IGMP Snooping.”
IGMP Snooping VLAN State	**Add**	Select “Add” in the selection box and enter the VLANs on which the switch should run “IGMP Snooping.” Valid range of VLAN IDs: 1 … 4094. Use a comma (,) or hyphen (-) to specify individual VLANs or VLAN ranges.
	Delete	Select “Delete” in the selection box and enter the VLANs on which the switch should not run “IGMP Snooping.”
Unknown Multicast Packets		In this selection box, specify the action to perform when the switch receives unknown multicast frames.
	Drop	Select “Drop” in the selection box to drop the frames.
	Flooding	Select “Flooding” in the selection box to flooding the frames to all ports.
IGMP Snooping State		
Parameter	**Default**	**Description**
IGMP Snooping State	Disable Enable	This display field indicates whether “IGMP Snooping” is enabled or disabled globally.
Report Suppression State	Disable Enable	This display field indicates whether the “Reporting Suppression Function” is enabled or disabled for “IGMP Snooping.”
IGMP Snooping VLAN Status	None 1 … 4094	This display field indicates the VLANs on which the switch runs “IGMP Snooping.” “None” is displayed if “IGMP Snooping” is not enabled for any port.
Unknown Multicast Packets	Drop Flooding	This display field indicates whether the switch drops unknown multicast packets or flooding them to all ports.

10.4.2.1.2 Port Settings

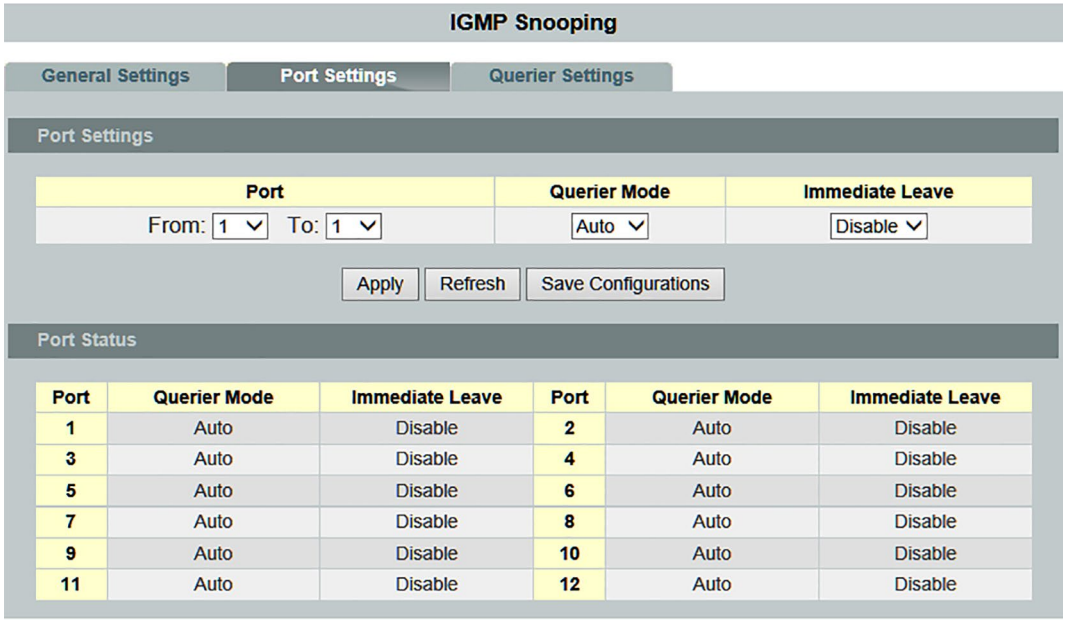


Figure 61: WBM “IGMP Snooping” Page – “Port Settings” Tab

Table 77: WBM “IGMP Snooping” Page – “Port Settings” Tab

Port Settings			
Parameter		**Default**	**Description**
Port	from:	**1**	Select a port or port range in the selection box to configure the “Port Settings”.
	to:	**1**	Select a port or port range in the selection box to configure the “Port Settings”.
Querier Mode		**Auto**	In the selection box, select the “Auto” setting if the switch should use the port as an “IGMP Query Port” if it receives “IGMP Query” packets.
		Fix	In this selection box, select the “Fix” setting if the switch should always use the port or ports as “IGMP Query Ports.” This setting is used if an IGMP multicast server is connected to the port(s).
		Edge	In this selection box, select the “Edge” setting if the switch should not use the port as an “IGMP Query Port.” In this case, the switch does not log the information that an IGMP router is connected to this port and does not forward the “IGMP Join/Leave” packets to this port.
Immediate Leave		**Disable**	In this selection box, select “Disable” to disable the “Immediate Leave” function on individual ports.
		Enable	In this selection box, select “Enable” to enable the “Immediate Leave” function on individual ports.
Port Status			
Parameter		**Default**	**Description**
Port		1 … 10 (12)	This column shows the port numbers.
Querier Mode		Auto Fix Edge	This column displays the “Querier” mode for the specific port.
Immediate Leave		Disable Enable	This column displays the “Immediate Leave” setting for the specific port.

10.4.2.1.3 Querier Settings

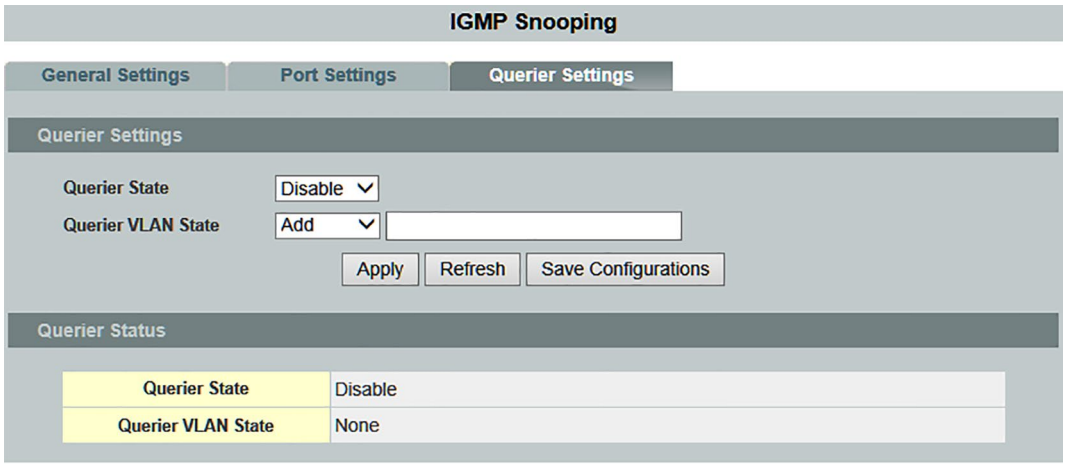


Figure 62: WBM “IGMP Snooping” Page – “Querier Settings” Tab

Table 78: WBM “IGMP Snooping” Page – “Querier Settings” Tab

Querier Settings		
Parameter	**Default**	**Description**
Querier State	**Disable**	Select “Disable” in the selection box to disable this function.
	Enable	Select “Enable” in the selection box to enable this function.
Querier VLAN State	**Add**	Select “Add” in the selection box to enter the VLAN ID.
	Delete	Select “Delete” in the selection box to delete the VLAN ID.
Querier Status		
Parameter	**Default**	**Description**
Querier State	Disable Enable	This field displays the querier status.
Querier VLAN State	None 0 … 4094	This field displays the VLAN ID.

10.4.2.2 IGMP Filtering

10.4.2.2.1 General Settings

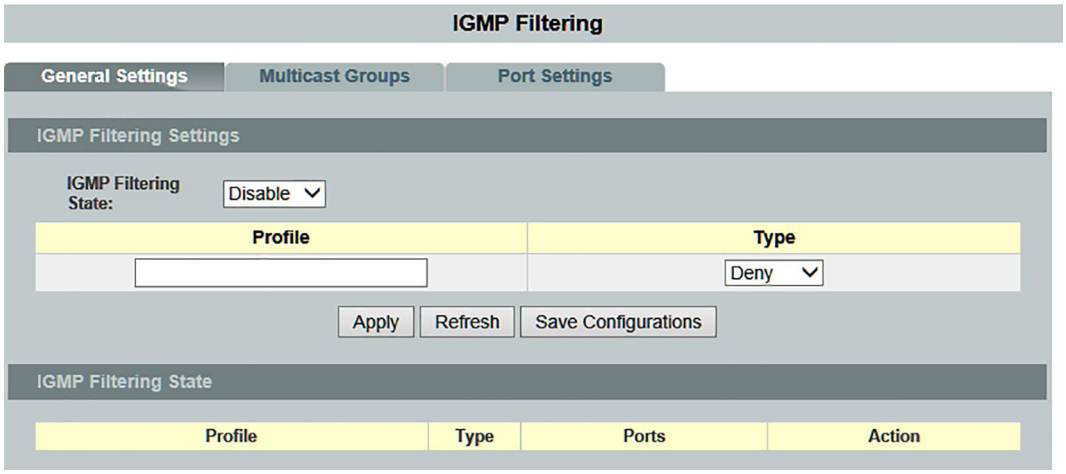


Figure 63: WBM “IGMP Filtering” Page – “General Settings” Tab

Table 79: WBM “IGMP Filtering” Page – “General Settings” Tab

IGMP Filtering Settings		
Parameter	**Default**	**Description**
IGMP Filtering Status	**Disable**	Select “Disable” in the selection box to disable this function.
	Enable	Select “Enable” in the selection box to enable this function.
Profile		Enter the name for the IGMP filter in the input field.
Type	**Deny**	In the selection box, select “Deny” to deny access to the group.
	Permit	In the selection box, select “Permit” to grant access to the group.
IGMP Filtering Status		
Parameter	**Default**	**Description**
Profile		This column displays the name of the profile. Click the name to modify the profile.
Type	Deny Permit	This column displays the type of action.
Ports	1 … 10 (12)	This column displays the ports on which the profile of the IGMP filter is enabled.
Action	Delete	Click **[Delete]** to delete the multicast addresses.

10.4.2.2.2 Multicast Groups

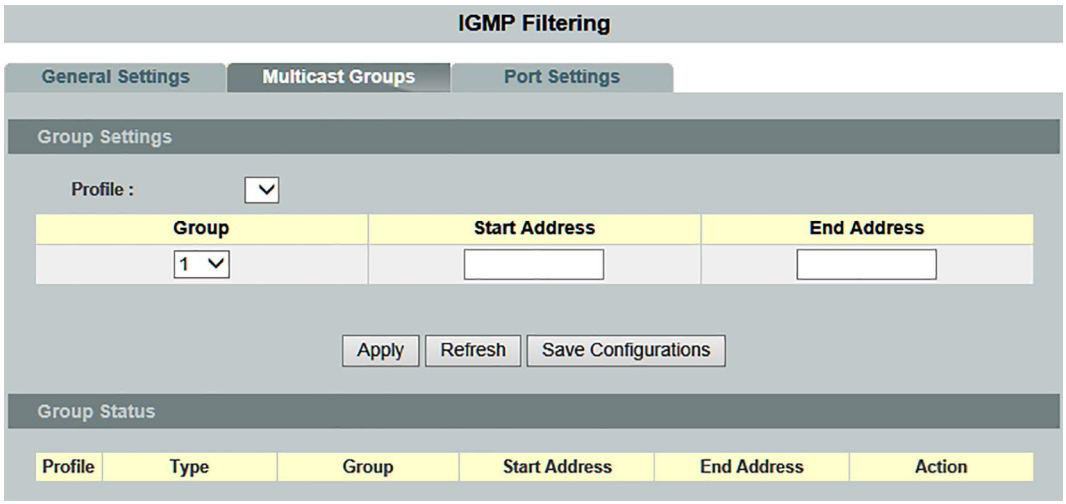


Figure 64: WBM “IGMP Filtering” Page – “Multicast Groups” Tab

Table 80: WBM “IGMP Filtering” Page – “Multicast Groups” Tab

Group Settings		
Parameter	**Default**	**Description**
Profile		Select the profile in the selection box that you want to configure for a group.
Group	**1** … 10	Select a multicast group in the selection box.
Start Address		In the input field, enter the first multicast address of the group that you want to configure.
End Address		In the input field, enter the last multicast address of the group that you want to configure.
Group Status		
Parameter	**Default**	**Description**
Profile		This column displays the name of the profile.
Type	Deny Permit	This column displays the type of action.
Group	1 … 10	This column displays the group.
Start Address		This column displays the first multicast address.
End Address		This column displays the last multicast address.
Action	Delete	Click **[Delete]** to delete the multicast addresses.

10.4.2.2.3 Port Settings

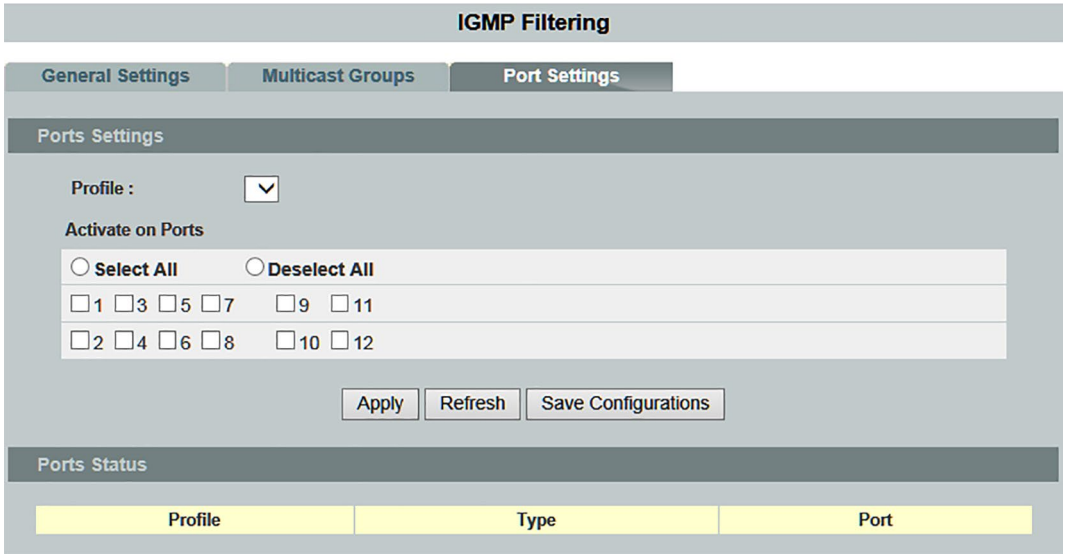


Figure 65: WBM “IGMP Filtering” Page – “Port Settings” Tab

Table 81: WBM “IGMP Filtering” Page – “Port Settings” Tab

Port Settings				
Parameter		**Default**	**Description**	
Profile			Select the profile in the selection box that you want to configure for a group.	
Port	Select All	○	○	No port is selected.
			◉	All ports are selected.
	Disable All	○	○	No port is disabled.
			◉	All ports are disabled.
	☐ 1 … ☐ 10 (12)	☐	☐	The port is not enabled.
			☑	The port is enabled.
Port Status				
Parameter		**Default**	**Description**	
Profile			This column displays the name of the profile.	
Type		Deny Permit	This column displays the type of action.	
Ports		1 … 10 (12)	This column displays the ports on which the profile of the IGMP filter is enabled.	

10.4.2.3 Static Multicast

Note

Additional Information

Please refer to the section “Function Description” for more information on “Static Multicast.”

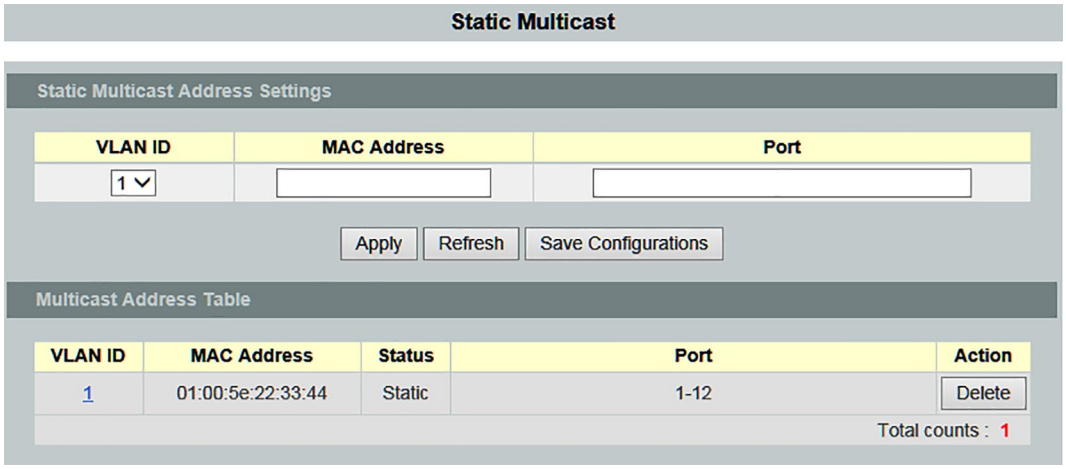


Figure 66: WBM “Static Multicast” Page

Table 82: WBM “Static Multicast” Page

Static Multicast Address Settings		
Parameter	**Default**	**Description**
VLAN ID	**1**	Select the VLAN ID in the selection box that you want to configure.
MAC Address		Enter the multicast MAC address of the respective ring in the input field. Configure a multicast MAC that should not receive an “Age Time.” The valid format is 0x:0x:0x:0x:0x:0x.
Port		Enter the subscriber port for the multicast address in the input field.
Multicast Address Table		
Parameter	**Default**	**Description**
VLAN ID	0 … 4094	This column displays the selected VLAN IDs.
MAC Address		This column displays the multicast addresses.
Status		This column displays the status of the multicast addresses.
Port	1 … 10 (12)	This column shows the port numbers.
Action		Click **[Delete]** to delete the multicast addresses.
Number of Entries		This field displays the total number of entries in the multicast address table.

10.4.2.4 Multicast Statistics

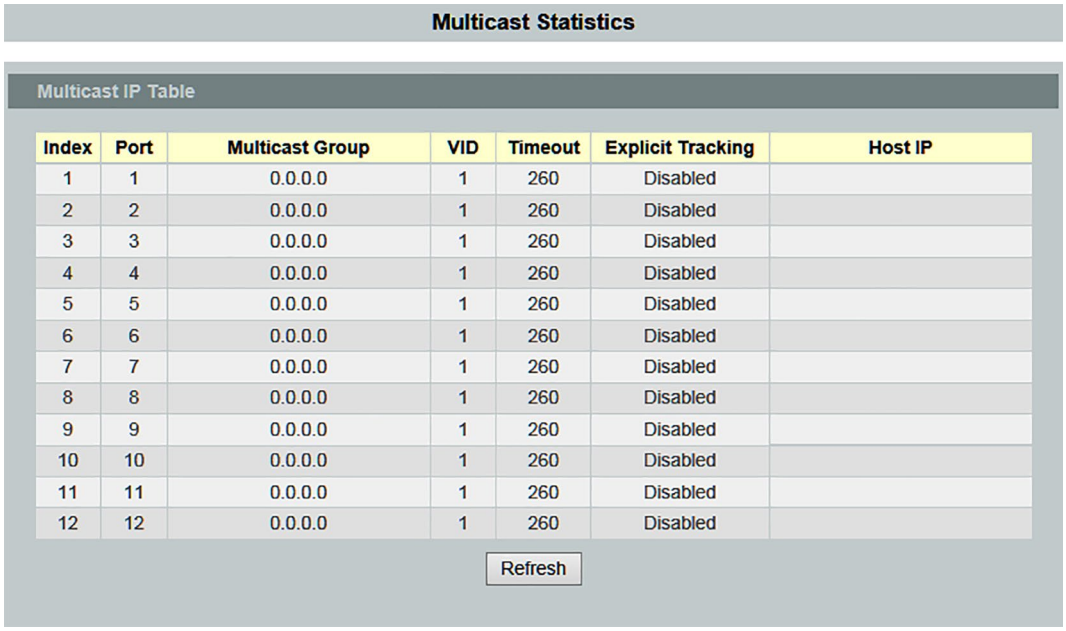


Figure 67: WBM “Multicast Statistics” Page

Table 83: WBM “Multicast Statistics” Page

Multicast IP Table		
Parameter	**Default**	**Description**
Index	1 … 10 (12)	This column displays the number of entries.
Port	1 … 10 (12)	This column displays the port number.
Multicast Group		This column displays the IP address of the multicast group.
VLAN ID		This column displays the VLAN ID.
Timeout		This column displays the timeout time.
Explicit Tracking		This column indicates whether “Explicit Tracking” is set.
Host IP		This column displays the host IP.

10.4.3 VLAN

Note

Additional Information
Please refer to the section “Function Description” for more information on “VLAN” (**V**irtual **L**ocal **A**rea **N**etwork).

10.4.3.1 Port Isolation

Note

Additional Information
Please refer to the section “Function Description” for more information on “Port Isolation.”

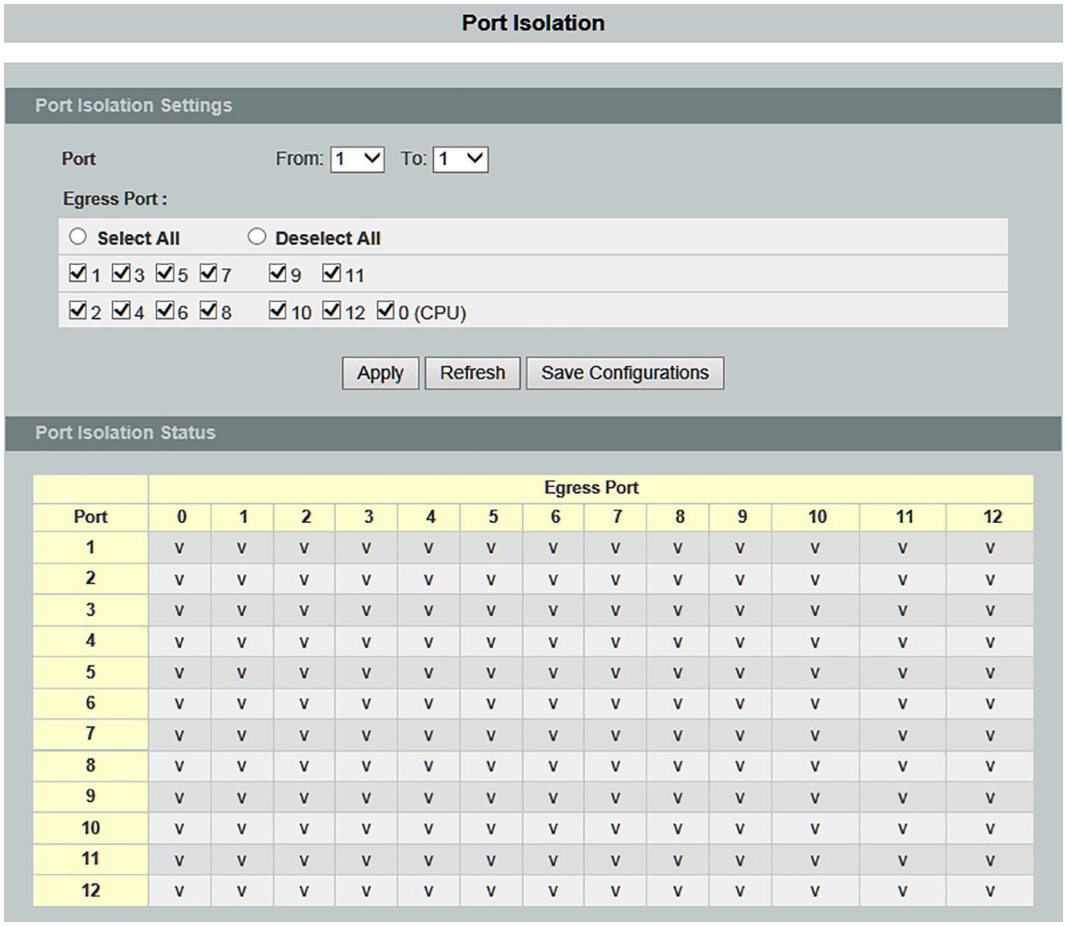


Figure 68: WBM “Port Isolation” Page

Table 84: WBM “Port Isolation” Page

Port Isolation Settings				
Parameter		**Default**	**Description**	
Port	from:	**1**	Select a port or port range in the selection box for which you want to configure the “Port Isolation” setting.	
	to:	**1**	Select a port or port range in the selection box for which you want to configure the “Port Isolation” setting.	
Egress Port			An egress port is an outgoing port through which a data packet leaves. Selecting a port as an egress port means it will communicate with the port currently being configured.	
	Select All	○	○	No egress port is selected.
			◉	All egress ports are selected.
	Disable All	○	○	No egress port is disabled.
			◉	All egress ports are disabled.
	☐ 0 (CPU) … ☐ 10 (12)	☐	☐	The egress port is not enabled.
			☑	The egress port is enabled.
Port Isolation Status				
Parameter		**Default**	**Description**	
Port		**V**	V	“V” indicates that the port’s packets can be sent to this port.
Egress Port			-	“-” indicates the port’s packets cannot be sent to this port.

10.4.3.2 VLAN

10.4.3.2.1 VLAN Settings

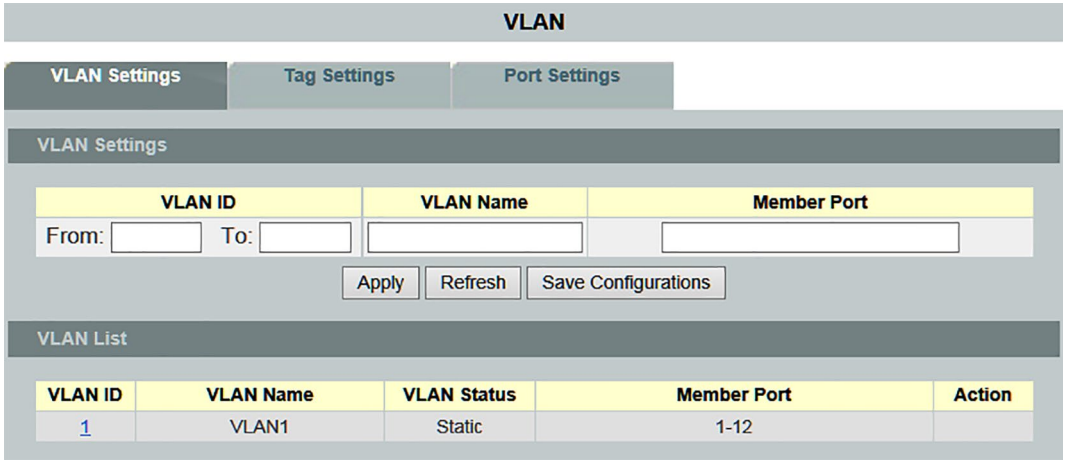


Figure 69: WBM “VLAN” Page – “VLAN Settings” Tab

Table 85: WBM “VLAN” Page – “VLAN Settings” Tab

VLAN Settings			
Parameter		**Default**	**Description**
VLAN ID	from:		Enter the VLAN ID for this entry in the input field. Valid range: 1 … 4094
	to:		Enter the VLAN ID for this entry in the input field. Valid range: 1 … 4094
VLAN Name			Enter a descriptive name for the VLAN in the input field for unique identification. The VLAN name should be a combination of numbers, letters, hyphens (-) and underscores (_).
Member Port			In the input field, enter the port numbers you want the switch to assign to the VLAN as members. You can designate multiple individual port numbers separating individual ports with a comma (,) or specifying port ranges with a hyphen (-).
VLAN List			
Parameter		**Default**	**Description**
VLAN ID		1 … 4094	This column displays the index number of the VLAN entry. Click the number to modify the VLAN entry.
VLAN Name			This column displays the name of the VLAN.
VLAN Status		Static Dynamic 802.1Q VLAN	This column displays the status of the VLAN.
Member Port		1-10 (12)	This column indicates which ports are assigned to the VLAN as subscribers.
Action			Click **[Delete]** to delete the VLAN.
			Note **Deleting VLAN1** VLAN1 cannot be deleted.

10.4.3.2.2 Tag Settings

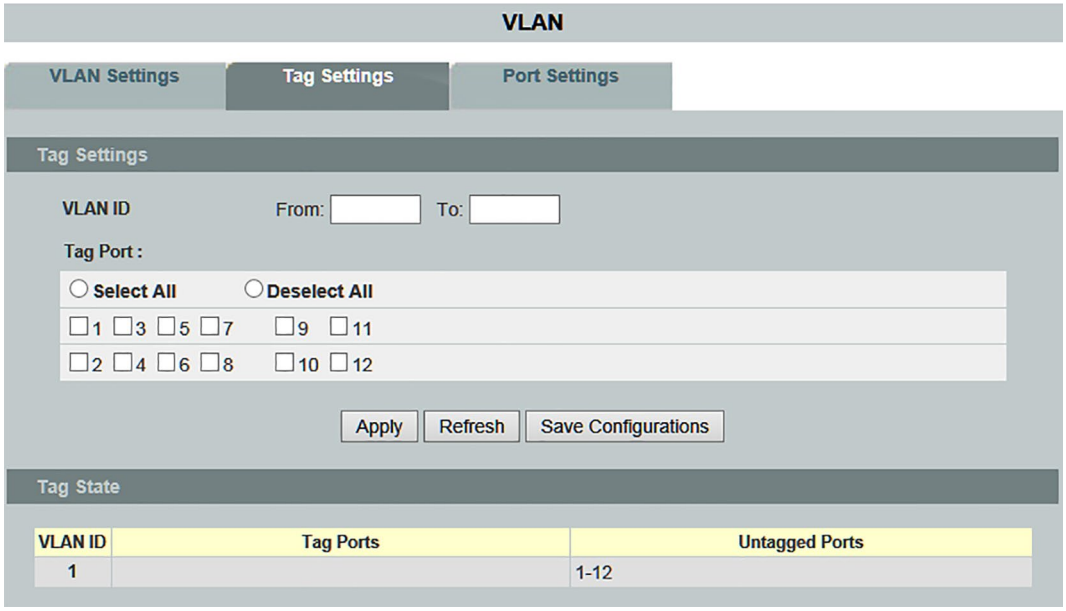


Figure 70: WBM “VLAN” Page – “Tag Settings” Tab

Table 86: WBM “VLAN” Page – “TAG Settings” Tab

Tag Settings				
Parameter		**Default**	**Description**	
VLAN ID	from:		Enter the VLAN ID for this entry in the input field. Valid range: 1 … 4094	
	to:		Enter the VLAN ID for this entry in the input field. Valid range: 1 … 4094	
Tag Port	Select All	○	○	No port is selected as a tagged port.
			◉	All ports are selected as tagged ports.
	Disable All	○	○	No tagged port is disabled.
			◉	All tagged ports are disabled.
	☐ 1 … ☐ 10 (12)	☐	☐	The port is not enabled.
			☑	The port is enabled.
Tag Status				
Parameter		**Default**	**Description**	
VLAN ID		1 … 4094	This column displays the VLAN ID.	
Tag Ports		1 … 7	This column displays the ports that have been assigned as tag ports.	
Untagged Ports		1 … 7	This column displays the ports that have been assigned as untagged ports.	

10.4.3.2.3 Port Settings

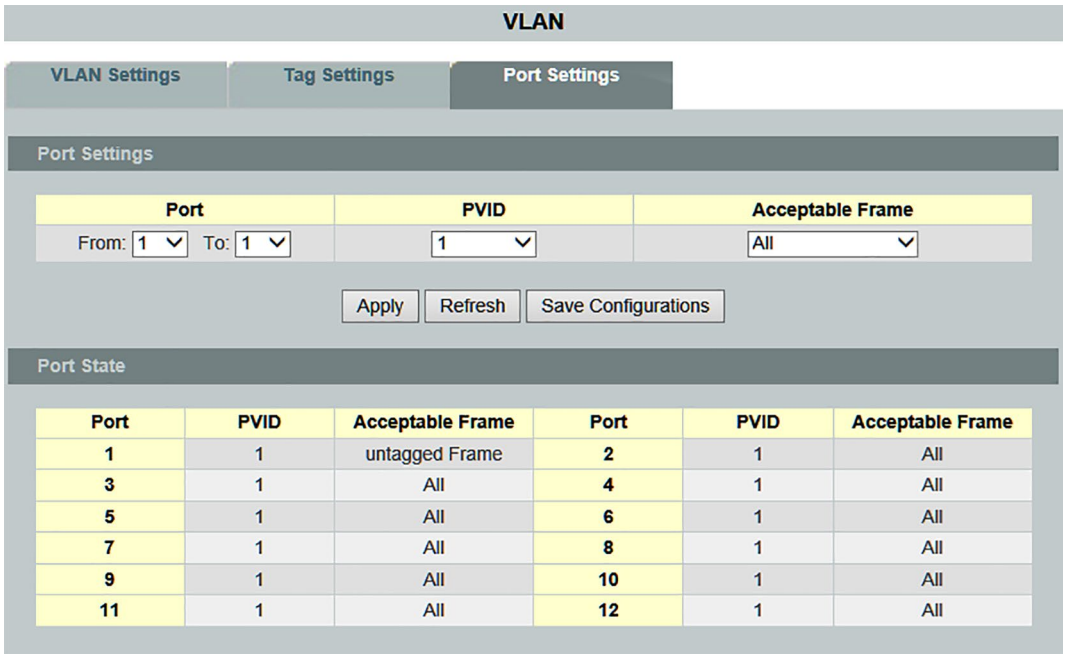


Figure 71: WBM “VLAN” Page – “Port Settings” Tab

Table 87: WBM “VLAN” Page – “Port Settings” Tab

Port Settings			
Parameter		**Default**	**Description**
Port	from:	**1**	Select a port or port range in the selection box to configure the “Port Settings”.
	to:	**1**	Select a port or port range in the selection box to configure the “Port Settings”.
PVID		**1**	Select the PVID (Port VLAN ID) in the selection box.
Acceptable Frame			You can specify the frame types allowed for a port in this selection box.
		All	Select “All” in the selection box if all frames (tagged and untagged) should be accepted on this port.
		Only Untagged VLANs	Select “Only Untagged VLANs” in the selection box if only untagged frames should be accepted on this port. All tagged frames are dropped.
		Only Tagged VLANs	Select “Only Tagged VLANs” in the selection box if only tagged frames should be accepted on this port. All untagged frames are dropped.
Port Status			
Parameter		**Default**	**Description**
Port		1 … 10 (12)	This column shows the port numbers.
PVID			This column displays the VLAN ID numbers.
Acceptable Frame		All Only Untagged VLANs Only Tagged VLANs	This column displays the type of frames allowed on the port.

10.4.3.3 MAC VLAN

Note

Additional Information

Please refer to the section “Function Description” for more information on “MAC VLAN” (**M**edia **A**ccess **C**ontrol-**V**irtual **L**ocal **A**rea **N**etwork).

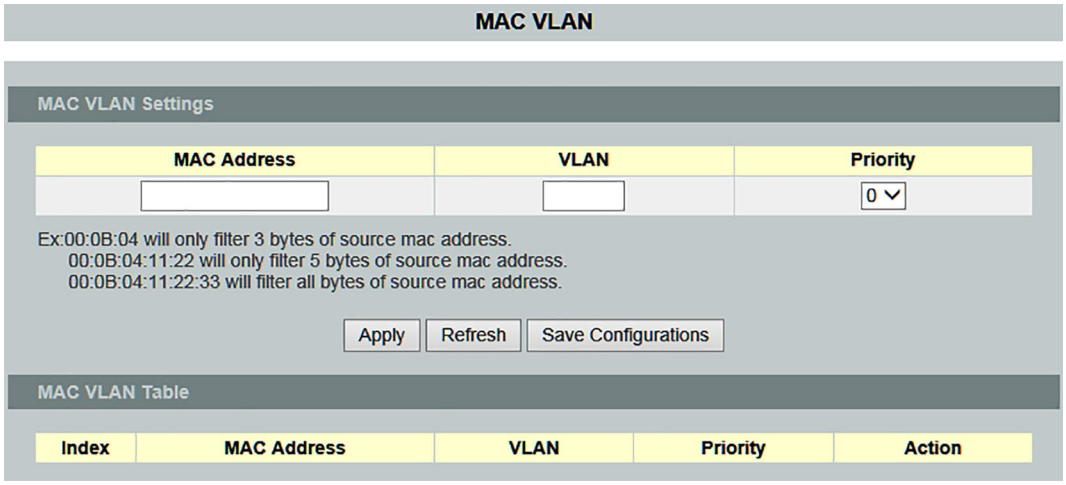


Figure 72: WBM “MAC VLAN” Page

Table 88: WBM “MAC VLAN” Page

MAC VLAN Settings		
Parameter	**Default**	**Description**
MAC Address		Enter the first three or more bytes of the MAC address in the input field.
VLAN		Enter the value for the MAC VLAN for the instance in the input field. Valid range: 1 … 4094 One or more data VLANs can be configured.
Priority	**0** … 7	Select the respective priority for the specific port in the selection box. 0 = lowest priority 7 = highest priority
MAC VLAN Table		
Parameter	**Default**	**Description**
Index	1 … 10	This column displays the number of entries.
MAC Address		This column displays the MAC address.
VLAN		This column displays the VLAN ID for the specific port.
Priority	0 … 7	This column displays the priority for the specific port.
Action		Click **[Delete]** to delete the multicast addresses.

10.4.4 LLDP

Note

Additional Information

Please refer to the section “Function Description” for more information on “LLDP” (**L**ink **L**ayer **D**iscovery **P**rotocol).

10.4.4.1 Settings

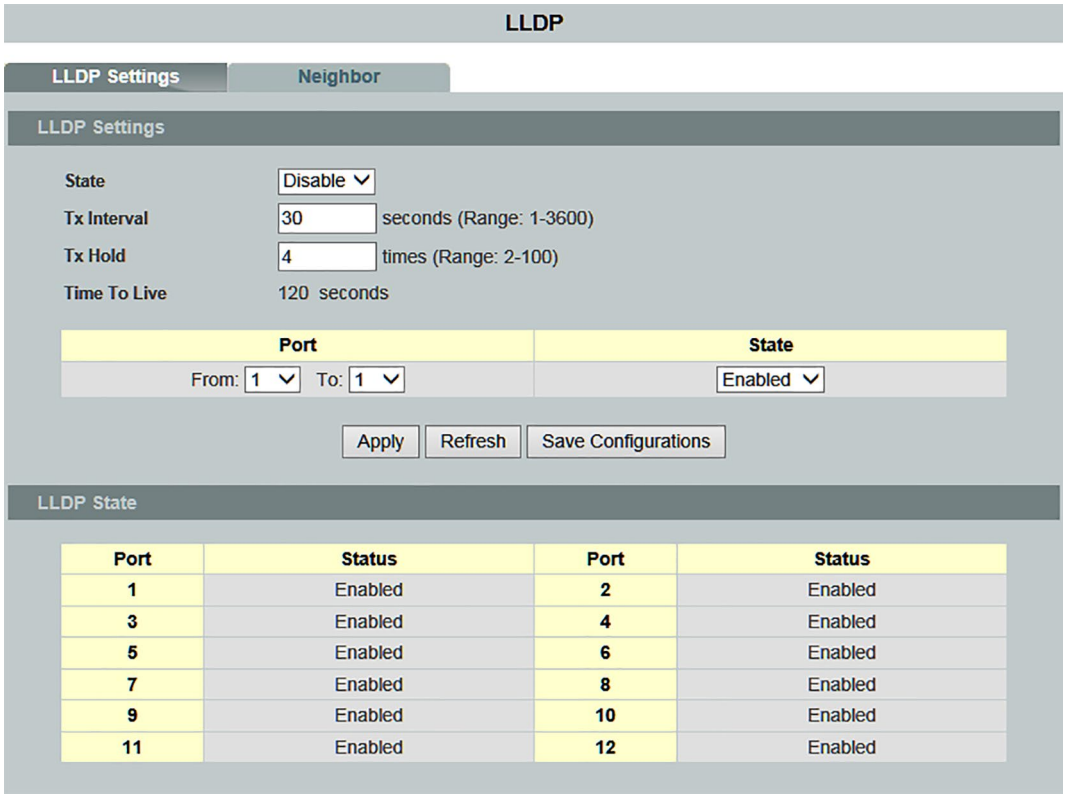


Figure 73: WBM “LLDP” Page – “LLDP Settings” Tab

Table 89: WBM “LLDP” Page – “LLDP Settings” Tab

LLDP Settings			
Parameter		**Default**	**Description**
Status		**Disable**	Select “Disable” in the selection box to disable the LLDP function for the switch globally.
		Enable	Select “Enable” in the selection box to enable the LLDP function for the switch globally.
TX Interval		**30**	Enter the value for the “TX Interval” (transmission interval) for the LLDP packets in the input field.
TX Hold		**4**	Enter the value for the “TX Hold Time” in the input field that determines the TTL of the switch’s message. (TTL = tx-hold * tx-interval)
Time to Live		**120**	This field displays the lifespan for the switch’s information.
Port	from:	**1**	Select a port or port range in the selection box for which you want to configure the “LLDP” setting.
	to:	**1**	Select a port or port range in the selection box for which you want to configure the “LLDP” setting.
Status		**Turn ON**	In this selection box, select “Enable” to enable the LLDP function on individual ports.
		Rx Only	Select the “Rx Only” setting in the selection box if “Rx Interval” is always used as the transmission interval for the switch or ports.
		Tx Only	Select the “Tx Only” setting in the selection box if “Tx Interval” is always used as the transmission interval for the switch or ports.
		Disable	In this selection box, select “Disable” to disable the “LLDP” function on individual ports.
LLDP Status			
Parameter		**Default**	**Description**
Port		1 … 10 (12)	This column shows the port numbers.
Status		Disable Enable	This column indicates whether “LLDP” is enabled or disabled.

10.4.4.2 Neighboring Detection

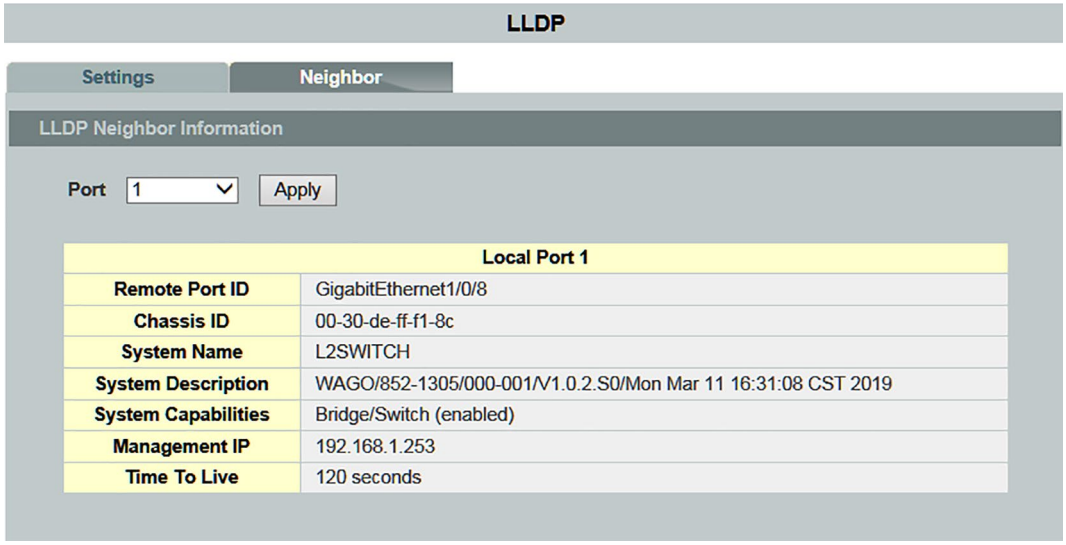


Figure 74: WBM “LLDP” Page – “Neighboring Detection” Tab

Table 90: WBM “LLDP” Page – “Neighboring Detection” Tab

LLDP Neighbor Information		
Parameter	**Default**	**Description**
Port	**All**	Select “All” in the selection box if you want to display information from all neighboring ports.
	1 … 10 (12)	Select the port in the selection box for whose neighbor port you want to display information.
Local Port	1 … 10 (12)	This field displays the port numbers.
Remote Port ID		This field displays the ID of the connected port.
Chassis ID		This field displays the neighbor port’s chassis ID.
System Name		This field displays the neighbor port’s system name.
System Description		This field displays the neighbor port’s system description.
System Capabilities		This field displays the system capabilities of the neighbor port.
Management IP		This field displays the neighbor port’s management address.
Time to Live		This field displays the validity period of the information of the neighbor port.

10.4.5 Loop Detection

Note

Additional Information

Please refer to the section “Function Description” for more information on “Loop Detection.”

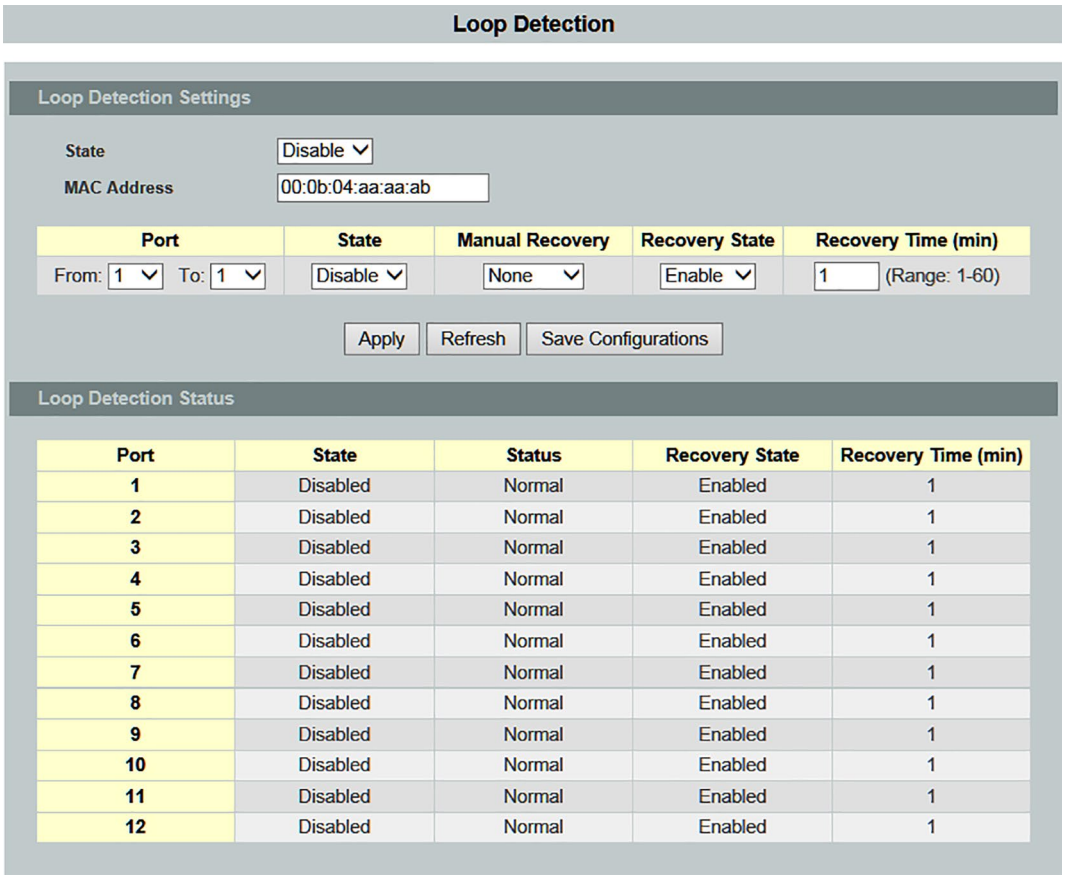


Figure 75: WBM “Loop Detection” Page

Table 91: WBM “Loop Detection” Page

Loop Detection Settings			
Parameter		**Default**	**Description**
State		**Disable**	Select “Disable” in the selection box to disable this function.
		Enable	Select “Enable” in the selection box to enable this function.
MAC Address			Enter the destination MAC address in the input field to which the probe packets should be sent. If the port receives the same packets, it is shut down.
Port	from:	**1**	Select a port or port range in the selection box for which you want to configure the “Loop Guard Protection” settings.
	to:	**1**	Select a port or port range in the selection box for which you want to configure the “Loop Guard Protection” settings.
Status		**Disable**	Select “Disable” in the selection box to disable the “Loop Guard” function for the switch.
		Enable	Select “Enable” in the selection box to enable the “Loop Guard” function for the switch.
Action		**None**	Select “None” in the selection box if you want to disable loop detection on the port.
		Activate	Select “Activate” in the selection box if you do not want to change the “Status” and “Loop Correction” functions.
Loop Recovery		**Enable**	Select “Enable” in the selection box to automatically re-enable the port after the designated “Recovery Time” has elapsed.
		Disable	Select “Disable” in the selection box to disable this function.
Recovery Time (min) (range: 1–60)		**1**	In the input field, enter the value for the “Recovery Time” (in minutes) that the switch waits before re-enabling the port. Time: 1 … 60 min
Loop Detection Status			
Parameter		**Default**	**Description**
Port		1 … 10 (12)	This column shows the port numbers.
State		Enable Disable	This column indicates whether the “Loop Guard” function is enabled or disabled.
Status		None Normal	This column indicates whether a port is blocked.
Loop Recovery		Enable Disable	This column indicates whether the “Loop Recovery” function is enabled or disabled.
Recovery Time (min)		1 … 50	This column displays the “Recovery Time” for the “Loop Recovery” function.

10.4.6 MRP

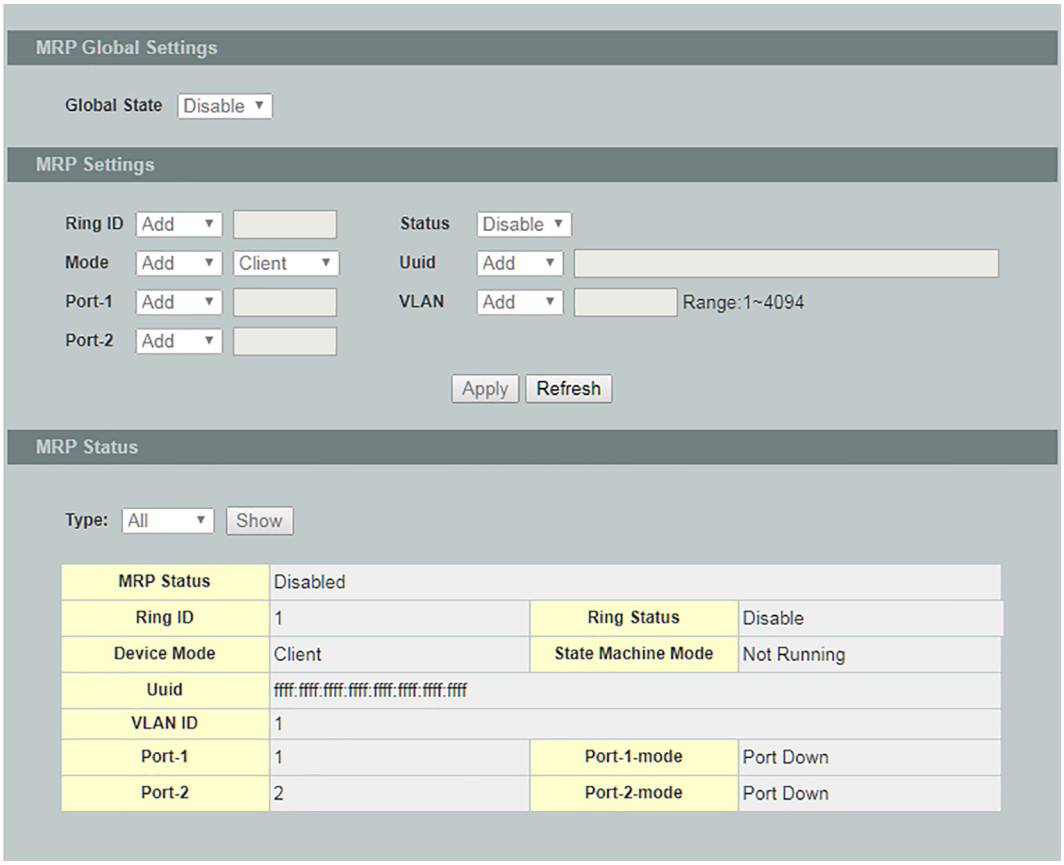


Figure 76: WBM “ MRP Global Settings” Page

Table 92: WBM Page “MRP”

MRP Global Settings		
Parameter	**Default**	**Description**
Global State	**Disable**	Select “Disable” in the selection box to disable the ring function of the global MRP.
	Enable	Select “Enable” in the selection box to enable the ring function of the global MRP.
MRP Settings		
Parameter	**Default**	**Description**
Ring ID	**Add**	Select “Add” in the selection box to add a (new) Ring ID.
	Delete	Select “Delete” in the selection box to delete a Ring ID.
Mode	**Add**	Select “Add” in the selection box to configure the switch either as a Client (MRC) or Manager (MRM).
	Delete	Select “Delete” in the selection box to delete the configure the switch either as a Client (MRC) or Manager (MRM).
Port 1	**Add**	Select “Add” in the selection box to add the primary port for the MRP ring.
	Delete	Select “Delete” in the selection box to delete the primary port for the MRP ring.
Port 2	**Add**	Select “Add” in the selection box to add the secondary port for the MRP ring.
	Remove	Select “Delete” in the selection box to delete the secondary port for the MRP ring.
Status	**Disable**	Select “Disable” in the selection box to switch on the respective ring.
	Enable	Select “Enable” in the selection box to switch off the respective ring.
UUID	**Add**	Configures the “Universal Unique Identifier” (UUID) for the MRP ring. This is a string of characters in hexadecimal format representing the ring to which this switch belongs. **Example:** 1a1b:225c:ef34:5671:9bcd:a018:ba34:5679
	Remove	
VLAN	**Add**	Select “Add” in the selection box and enter the VLANs which this ring should be enabled. Valid range of VLAN IDs: 1 … 4094. Use a comma (,) or hyphen (-) to specify individual VLANs or VLAN ranges.
	Delete	Select “Delete” in the selection box and enter the VLANs on which the switch should not enabled.

Table 92: WBM Page “MRP”

MRP Status (current state of the respective MRP ring)		
Parameter	**Default**	**Description**
Type	**All**	Select “All” in the selection box if you want display all ring statuses.
	Ring_1 … Ring_4	Select the Ring-ID in the selection box for whose MRP status of the selected ring ID to display.
MRP Status	–	This field displays the current state of the respective MRP ring.
Ring ID	–	This field displays the ID number of the MRP ring.
Device Mode	–	This field displays the switch mode: Client (CRM)/Manager (MRM)
Uuid	–	This field displays the assigned UUID.
Vlan ID	–	This field displays the VLAN to which this ring belongs.
Port-1	–	This field displays the assigned port of the switch.
Port-2	–	This field displays the assigned port of the switch.
Ring Status	–	This field displays the current status of the MRP ring: (switched on/switched off).
State Machine Mode	–	This field displays, whether or not the MRP state machine is running.
Port-1 Mode	–	This field displays the port status: (port down/port up).
Port-2 Mode	–	This field displays the port status: (port down/port up).

10.4.7 Spanning Tree Protocol

Note

Additional Information

Please refer to the section “Function Description” for more information on “**S**panning **T**ree **P**rotocol” (STP).

10.4.7.1 General Settings

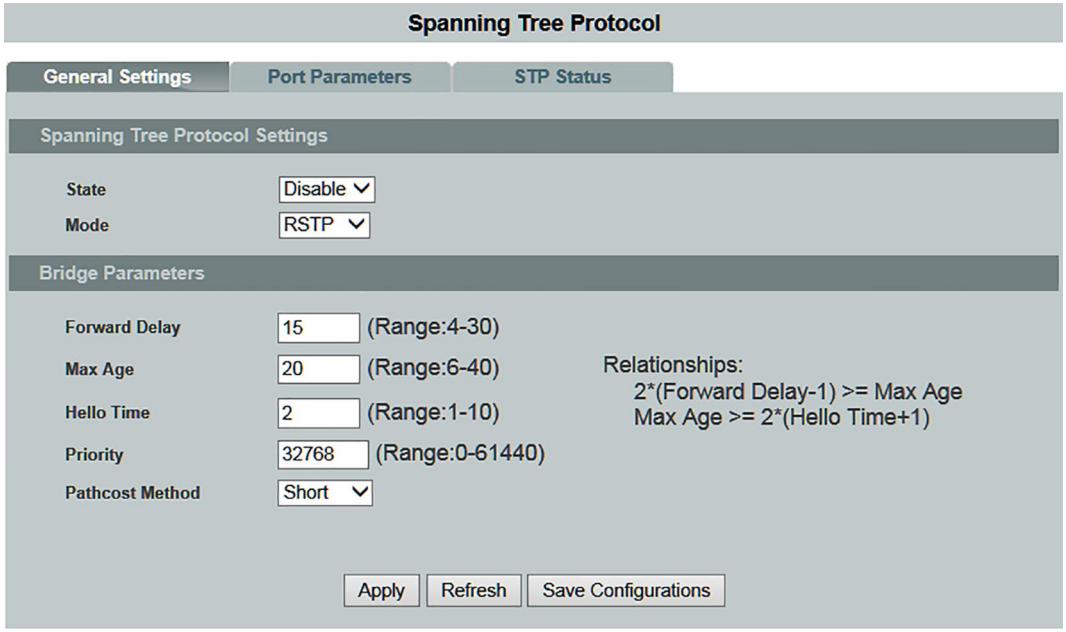
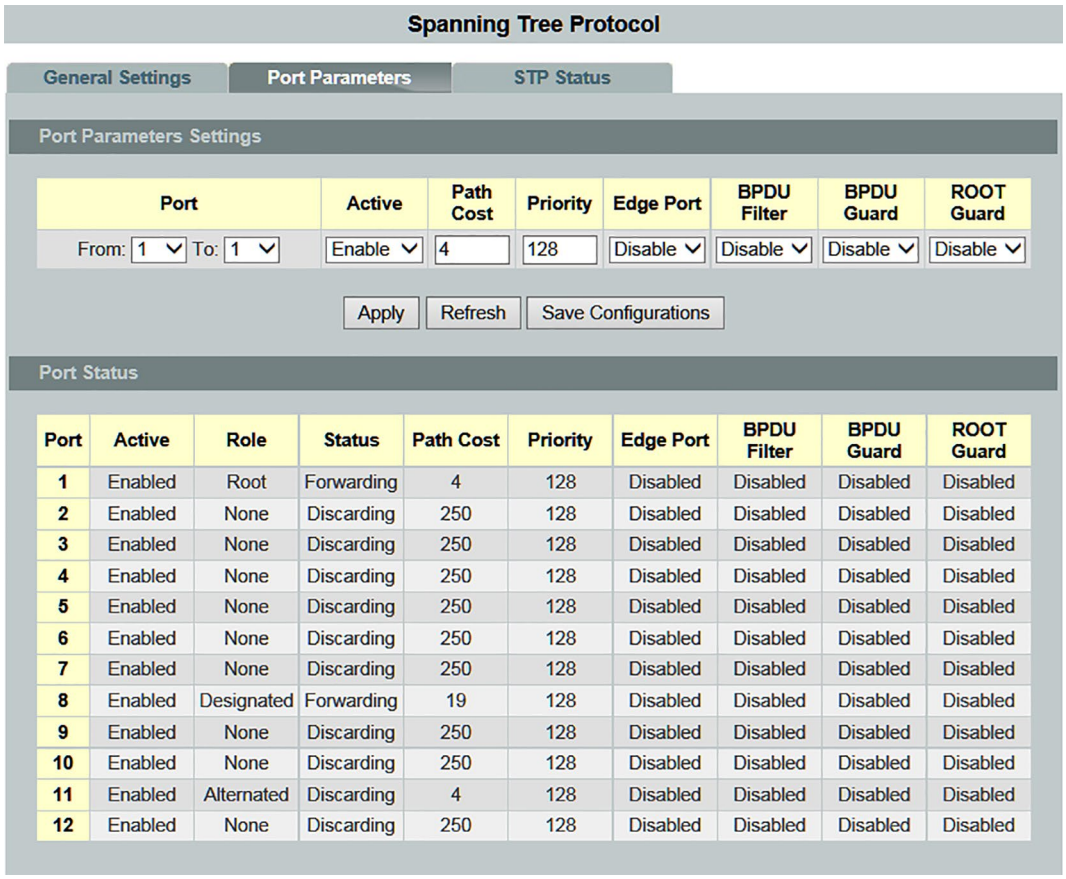


Figure 77: WBM “Spanning Tree Protocol” Page – “General Settings” Tab

Table 93: WBM “Spanning Tree Protocol” Page – “General Settings” Tab

Spanning Tree Protocol Settings		
Parameter	**Default**	**Description**
State	**Disable**	Select “Disable” in the selection box to disable this function.
	Enable	Select “Enable” in the selection box to use the “Spanning Tree Protocol” (STP) or “Rapid Spanning Tree Protocol” (RSTP).
Mode	**RSTP**	Select “RSTP” in the selection box if you want to use the faster “Rapid Spanning Tree Protocol.”
	MSTP	Select “MSTP” in the selection box if you want to use the “Multiple Spanning Tree Protocol.”
	STP	Select “STP” in the selection box if you want to use the “Spanning Tree Protocol.”
Bridge Parameters		
Parameter	**Default**	**Description**
Forward Delay (Range: 4~30)	**15**	Enter the “Forward Delay” time in the input field. Valid range: 4 … 30 s
Max Age (Range: 6~40)	**20**	Enter the “Max Age” time in the input field. Valid range: 6 … 40 s
Hello Time (Range: 1~10)	**2**	Enter the “Hello Time” in the input field. Valid range: 1 … 10 s
Priority (Range: 0~61440)	**32768**	Enter a value for the priority in the input field. The lower the numerical value you assign is, the higher the priority of this bridge is. Valid range: 0 … 61440
Path Cost Method	**Short**	Select “Short” in the selection box if you want to select a size of 16 bits and a transmission rate of up to 10 GBit. 10 MBit = 100 100 MBit = 19 1 GBit = 4 10 GBit = 2
	Long	Select “Long” in the selection box if you want to select a size of 32 bits and a transmission rate of up to 10 TBit. 10 MBit = 2000000 100 MBit = 200000 1 GBit = 20000 10 GBit = 2000 100 GBit = 200 1 TBit = 20

10.4.7.2 Port Parameters



Port	Active	Role	Status	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
1	Enabled	Root	Forwarding	4	128	Disabled	Disabled	Disabled	Disabled
2	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
3	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
4	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
5	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
6	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
7	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
8	Enabled	Designated	Forwarding	19	128	Disabled	Disabled	Disabled	Disabled
9	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
10	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
11	Enabled	Alternated	Discarding	4	128	Disabled	Disabled	Disabled	Disabled
12	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled

Figure 78: WBM “Spanning Tree Protocol” Page – “Port Parameters” Tab

Table 94: WBM “Spanning Tree Protocol” Page – “Port Parameters” Tab

Port Parameter Settings			
Parameter		**Default**	**Description**
Port	From:	**1**	Select a port or port range in the selection box to configure the “STP Function”.
	To:	**1**	Select a port or port range in the selection box to configure the “STP Function”.
Active		**Turn ON**	Select “Enable” in the selection box if you want to enable the “STP” function for the specific port.
		Disable	Select “Disable” in the selection box if you want to disable the STP function for the specific port.
Path Costs		**250**	Enter the value for the path costs for the specific port in the input field.
Priority		**128**	Enter the value for the priority for the specific port in the input field.
Edge Port		**Disable**	Select “Disable” in the selection box to disable the “Edge Port” type for the specific port.
		Enable	Select “Enable” in the selection box to enable the “Edge Port” type for the specific port.
BPDU Filter		**Disable**	Select “Disable” in the selection box to disable the BPDU filter function for the specific port.
		Enable	Select “Enable” in the selection box to enable the BPDU filter function for the specific port.
BPDU Guard		**Disable**	Select “Disable” in the selection box to disable the “BPDU Guard” function for the specific port.
		Enable	Select “Enable” in the selection box to enable the “BPDU Guard” function for the specific port.
ROOT Guard		**Disable**	Select “Disable” in the selection box to disable the “ROOT Guard” function for the specific port.
		Enable	Select “Enable” in the selection box to enable the “ROOT Guard” function for the specific port.

Table 94: WBM “Spanning Tree Protocol” Page – “Port Parameters” Tab

Port Status		
Parameter	**Default**	**Description**
Port	1 … 10 (12)	This column shows the port numbers.
Active	**Enable** Disable	This column displays the status of the “STP” function.
Role	Alternated Designated Root Backup None	This column displays the role of the port.
Status	Discarding Blocking Listening Learning Forwarding Disabled	This column displays the port status.
Path Costs	0 … 65535	This column displays the path cost of the port.
Priority	0 … 61440	This column displays the port priority.
Edge Port	Disable Enable	This column displays the status of the “Edge Port” function.
BPDU Filter	Disable Enable	This column displays the status of the BPDU filter function.
BPDU Guard	Disable Enable	This column displays the status of the “BPDU Guard” function.
ROOT Guard	Disable Enable	This column displays the status of the “Root Guard” function.

10.4.7.3 STP Status

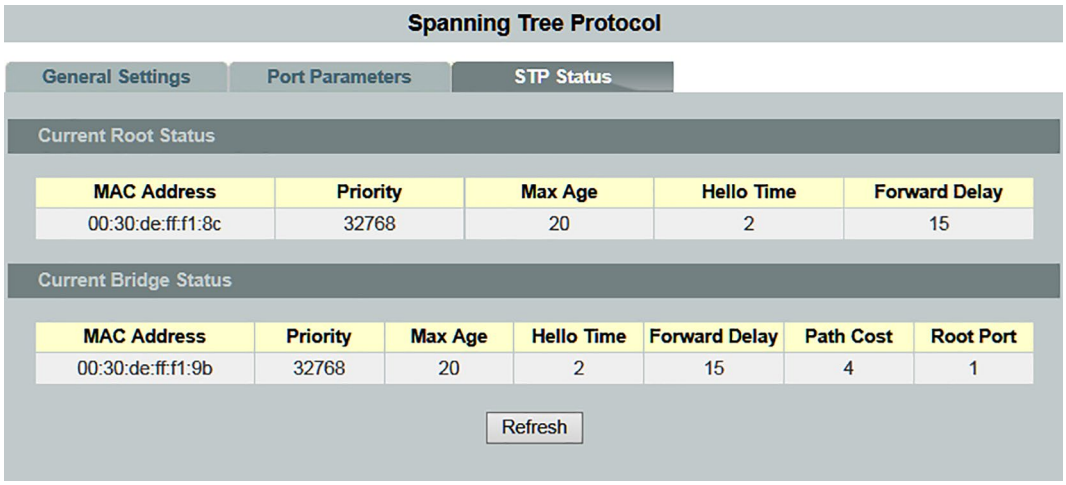


Figure 79: WBM “Spanning Tree Protocol” Page – “STP Status” Tab

Table 95: WBM “STP” Page – “STP Status” Tab

Current Root Status		
Parameter	**Default**	**Description**
MAC Address		This field displays the MAC address of the “Root Bridge.”
Priority		This field displays the priority of the “Root Bridge.” This switch can also be the “Root Bridge.”
Max Age		This field displays the “Max Age” of the “Root Bridge.”
Hello Time		This field displays the “Hello Time” of the “Root Bridge.” The “Root Bridge” determines the “Hello Time,” “Max Age and “Forwarding Delay.”
Forward Delay		This field displays the maximum time (in seconds) that the root switch waits before changing states.
Current Bridge Status		
Parameter	**Default**	**Description**
MAC Address		This field displays the MAC address of the current bridge.
Priority		This field displays the priority.
Max Age		This field displays the “Max Age.”
Hello Time		This field displays the “Hello Time.”
Forward Delay		This field displays the “Forward Time.”
Path Costs		This field displays the path cost.
ROOT Port		This field displays the number of the port on the switch through which the switch has to communicate with the root of the “Spanning Tree.”

10.5 Security

10.5.1 Access Control List

Note

Additional Information

Please refer to the section “Function Description” for more information on the “Access Control List.”

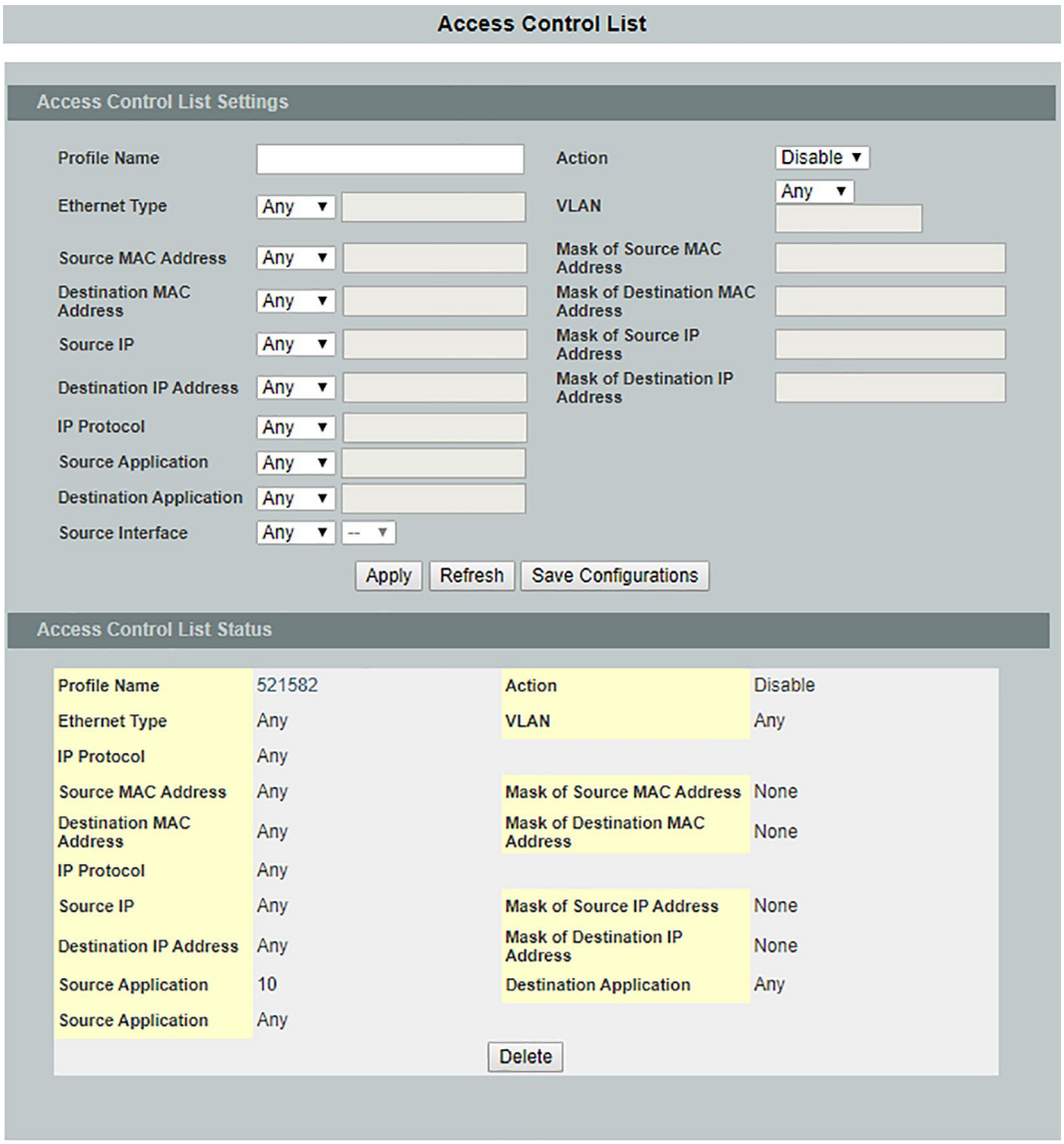


Figure 80: WBM Page “Access Control List”

Table 96: WBM Page “Access Control List”

Access Control List Settings		
Parameter	**Default**	**Description**
Profile Name		Enter the name of the profile in the input field.
Action	**Disable**	Select “Disable” from the drop-down list to disable access control.
	Permission	Select “Permission” from the drop-down list to forward data packets that match the information.
	Discard	Select “Discard” from the drop-down list to drop data packets that match the information.
ETHERNET Type	**Any**	Select “Any” from the drop-down list to make every ETHERNET type valid.
	Other	Select “Other” from the drop-down list to specify an ETHERNET type for which access control is valid.
VLAN	**Any**	Select “Any” from the drop-down list to make every VLAN ID valid.
	Other	Select “Other” from the drop-down list to enter a specific VLAN ID in the access control list.
Source MAC Address	**Any**	Select “Any” from the drop-down list to make every MAC address valid.
	Other	Select “Other” from the drop-down list to enter the MAC address for the source in the access control list.
Mask of the Source MAC Address		In the input field, enter the source MAC ID of the bitmap mask for source MAC addresses of packets to be filtered. If you selected “Source MAC Address” from the drop-down list, this field remains empty. The profile then only filters the MAC address entered in the Source MAC Address field.
Destination MAC Address	**Any**	Select “Any” from the drop-down list to make every MAC address valid.
	Other	Select “Other” from the drop-down list to enter the MAC address for the destination in the access control list.
Mask of the Destination MAC Address		In the input field, enter the destination MAC address of the bitmap mask for destination MAC addresses of packets to be filtered. If you selected “Destination MAC Address” from the drop-down list, this field remains empty. The profile then only filters the MAC address entered in the destination MAC address field.
Source IP	**Any**	Select “Any” from the drop-down list to make every IP address valid.
	Other	Select “Other” from the drop-down list to enter the IP address for the source in the access control list.
Mask of the Source IP Address		In the input field, enter the source IP address of the bitmap mask for source IP addresses of packets to be filtered. If you selected “Source IP” from the drop-down list, this field remains empty. The profile then only filters the IP address entered in the source IP address field.
Destination IP Address	**Any**	Select “Any” from the drop-down list to make every IP address valid.
	Other	Select “Other” from the drop-down list to enter the IP address for the destination in the access control list.

Table 96: WBM Page “Access Control List”

Mask of the Destination IP Address		In the input field, enter the destination IP address of the bitmap mask for IP destination addresses of packets to be filtered. If you selected “Destination IP Address” from the drop-down list, this field remains empty. The profile then only filters the IP address entered in the destination IP address field.	
IP Protocol	**Any**	Select “Any” from the drop-down list to make every IP protocol for the access control list valid.	
	Other	Enter “Other” from the drop-down list to enter the protocol.	
Source Application	**Any**	Select “Any” from the drop-down list to make every application valid.	
	Other	Select “Other” from the drop-down list to enter the source port (e.g., 2234).	
Destination Application	**Any**	Select “Any” from the drop-down list to make every destination application valid.	
	Other	Select “Other” from the drop-down list to enter the port (e.g., 502) for the destination in the access control list.	
Source Interface	**Any**	Select “Any” from the drop-down list if every physical port is valid.	
	Other	1 … 10 (12)	Enter the physical port in the input field for which this entry is valid in the access control list.

Table 96: WBM Page “Access Control List”

Access Control List Status		
Parameter	**Default**	**Description**
IP Type	IPv4 IPv6	This field displays the selected IP type.
Profile Name		This field displays the selected name of the profile.
Action	Disable Permission Discard DSCP	This field displays the status of the access control. (DSCP only with IPv4)
ETHERNET Type	Any Other	This field displays the ETHERNET type.
VLAN	Any Other	This field displays the VLAN ID.
IP Protocol	Any Other	This field displays the IP protocol.
Source MAC Address	Any Other	This field displays the source MAC address.
Mask of the Source MAC Address		This field displays the source MAC ID of the bitmap mask.
Destination MAC Address	Any Other	This field displays the destination MAC address.
Mask of the Destination MAC Address		This field displays the destination MAC ID of the bitmap mask.
IP Protocol	Any Other	This field displays the IP protocol.
Source IP	Any Other	This field displays the source IP.
Mask of the Source IP Address		This field displays the source MAC ID of the bitmap mask.
Destination IP Address	Any Other	This field displays the destination IP.
Mask of the Destination IP Address		This field displays the destination IP ID of the bitmap mask.
Source Application	Any Other	This field display the source application.
Destination Application	Any Other	This field displays the destination application.
Source Interface	1 … 10 (12)	This field displays the source interface.

10.6 Monitor

10.6.1 Alarm Information

Note

Additional information

Please refer to the section “Function Description” for more information on the “Alarm.”

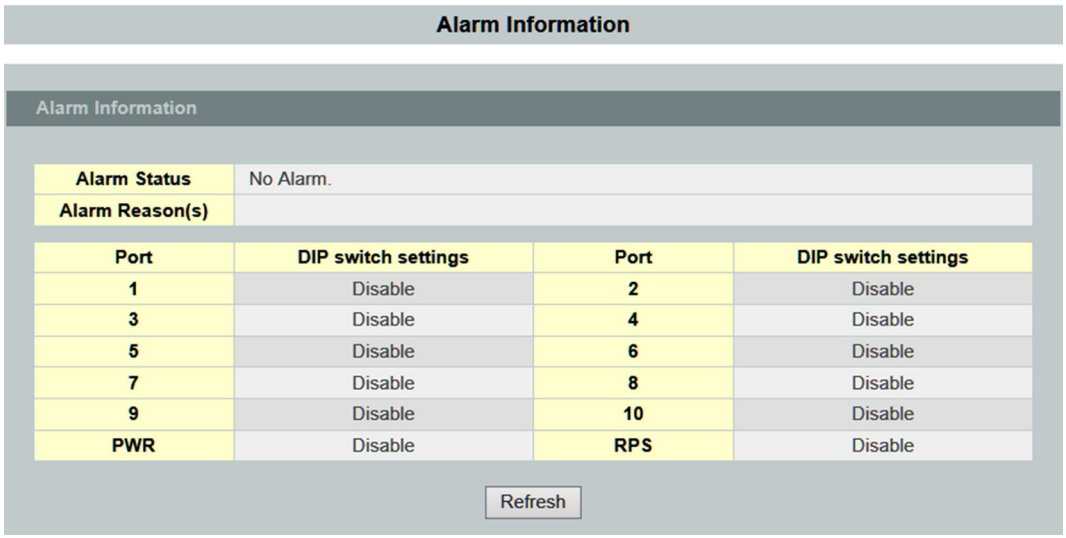


Figure 81: WBM “Alarm Information” Page

Table 97: WBM “Alarm Information” Page

Alarm Information		
Parameter	**Default**	**Description**
Alarm Status		This display field shows if there are any alarm events.
Alarm Reason		This display field shows details about the alarm events.
Port	0 … 10 PWR RPS	This column displays the DIP switch name.
DIP Switch Settings	Enable Disable	This column displays the current status of the DIP switch.

10.6.2 System Information

Note

Additional information

Please refer to the section “Function Description” for more information on “System Information.”

Monitor Information

Temperature unit: Celsius(C)

Hardware-Monitor Alarm: Enable

Hardware Information:

Temperature(C)	Current	MAX	MIN	Threshold	Status
BOARD	52.0	52.0	49.0	80.0	Normal
CPU	51.8	51.8	48.8	80.0	Normal
PHY	51.0	51.0	48.0	80.0	Normal
Voltage(V)	**Current**	**MAX**	**MIN**	**Threshold**	**Status**
1.0V IN	0.998	0.998	0.988	+/-6%	Normal
1.8V IN	1.784	1.810	1.777	+/-6%	Normal
5.0V IN	5.002	5.048	4.970	+/-6%	Normal

Apply Refresh Save Configurations

Figure 82: WBM “System Information” Page

Table 98: WBM “System Information” Page

Hardware Information		
Parameter	**Default**	**Description**
Temperature Unit	**Celsius (C)**	Select “Celsius (C)” in the selection box if you want to display the temperature in Celsius.
	Fahrenheit (F)	Select “Fahrenheit (F)” in the selection box if you want to display the temperature in Fahrenheit.
Hardware Information		
Parameter	**Default**	**Description**
Temperature (C)		
Current		This column displays the current temperature of the “BOARD,” “CPU” and “PHY” MAC chip.
MAX		This column displays the maximum temperature of the “BOARD,” “CPU” and “PHY” MAC chip.
MIN		This column displays the minimum temperature of the “BOARD,” “CPU” and “PHY” MAC chip.
Threshold		This column displays the threshold setting.
Status		This column displays the status.
Voltage [V]		
Current		This column displays the current voltage for the “1.0 V IN,” “2.5 V IN” and “3.3 V IN” inputs.
MAX		This column displays the maximum voltage for the “1.0 V IN,” “2.5 V IN” and “3.3 V IN” inputs.
MIN		This column displays the minimum voltage for the “1.0 V IN,” “2.5 V IN” and “3.3 V IN” inputs.
Threshold		This column displays the threshold setting.
Status		This column displays the status.

10.6.3 Port Statistics

Hinweis

Additional information

Please refer to the section “Function Description” for more information on the “Port Statistics.”

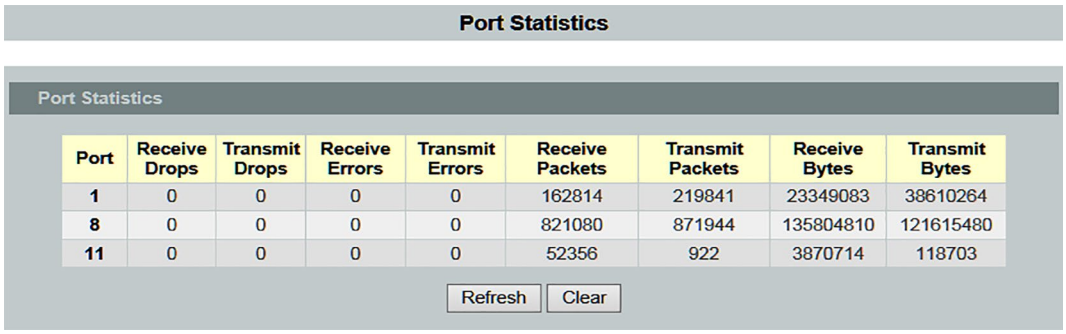


Figure 83: WBM “Port Statistics” Page

Table 99: WBM “Port Statistics” Page

Port Statistics		
Parameter	**Default**	**Description**
Port		This column shows the port numbers.
Transmit Drops		This column displays the number of dropped data packets on the transmission line.
Receive Drops		This column displays the number of dropped data packets on the receiving line.
Transmit Errors		This column displays the errors on the transmission line.
Receive Errors		This column displays the errors on the receiving line.
Transmit Packets		This column displays the number of data packets transmitted since power ON.
Receive Packets		This column displays the number of data packets received since power ON.
Transmit Byte		This column displays the number of bytes sent on the port since power ON.
Receive Bytes		This column displays the number of bytes received on the port since power ON.

10.6.4 Port Utilization

Note

Additional information

Please refer to the section “Function Description” for more information on the “Port Utilization.”

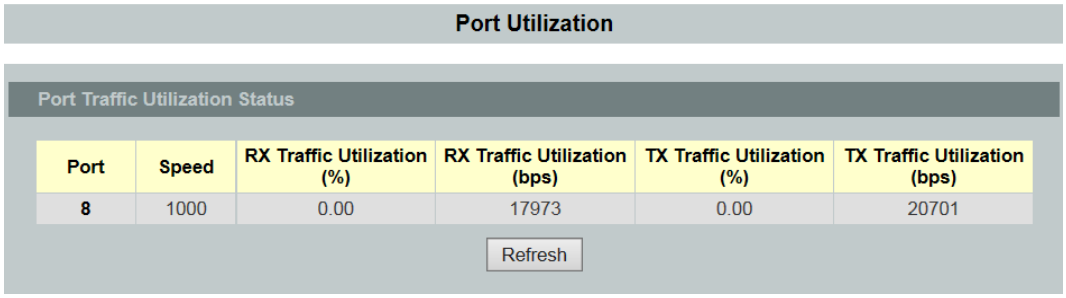


Figure 84: WBM “Port Utilization” Page

Table 100: WBM “Port Utilization” Page

Port Utilization Status		
Parameter	**Default**	**Description**
Port		This column shows the port numbers.
Speed		This column displays the transfer rate.
RX Port Utilization (%)		This column displays the RX bandwidth utilization as a percentage.
RX Port Utilization (bps)		This column displays the RX bandwidth utilization in bps.
TX Port Utilization (%)		This column displays the TX bandwidth utilization as a percentage.
RX Port Utilization (bps)		This column displays RX bandwidth utilization in bps.

10.6.5 RMON Statistics

Note

Additional information

Please refer to the section “Function Description” for more information on “RMON Statistics.”

RMON Statistics

RMON Statistics

Port 8 Show Clear

Port 8 (active)				
Inbound	Total Octets	138137205		
	BroadcastPkts	358	UnicastPkts	834746
	Non-unicastPkts	934	MulticastPkts	576
	FragmentsPkts	0	UndersizePkts	0
	OversizePkts	0	DiscardsPkts	0
	ErrorPkts	0	UnknownProtos	0
	AlignError	0	CRCAlignErrors	0
	Jabbers	0	DropEvents	0
Outbound	Total Octets	124304365		
	BroadcastPkts	0	UnicastPkts	834417
	Non-unicastPkts	52636	Collisions	0
	LateCollision	0	SingleCollision	0
	MultipleCollision	0	DiscardsPkts	0
	ErrorPkts	0		
#of packets received with a length of	64 Octets	1009822	65to127 Octets	356498
	128to255 Octets	134735	256to511 Octets	144291
	512to1023 Octets	37586	1024toMax Octets	39802

Figure 85: WBM “RMON Statistics” Page

Table 101: WBM “RMON Statistics” Page

RMON Statistics			
Parameter		**Default**	**Description**
Port		-	Select “-” in the selection box if you do not want to view any statistics.
		1 … 10 All	In the selection box, select a port, or all ports, for which you want to display RMON statistics.
Selected Port x (active)			
Parameter		**Default**	**Description**
Incoming	Total Octets		This display field shows the number of data packets received on the port.
	Broadcast Packets		This display field shows the number of broadcast packets received on the port.
	Unicast Packets		This display field shows the number of unicast packets received on the port.
	Non Unicast Packets		This display field shows the total number of broadcast and multicast packets received on the port.
	Multicast Packets		This display field shows the number of multicast packets received on the port.
	Fragmented Packets		This display field shows the number of fragmented data packets received on the port.
	Undersized Packets		This display field shows the number of data packets received on the port that are too small.
	Oversized Packets		This display field shows the number of data packets received on the port that are too large.
	Discards Packets		This display field shows the number of data packets received on the port that were dropped.
	Error Packets		This display field shows the number of data packets received on the port that were faulty.
	Unknown Protos		This display field shows the number of packets received by this port that contain an unknown or unsupported protocol as the destination.
	Align Error		This display field shows the number of data packets received where the total number of bits of a received frame is not divisible by eight.
	CRC Align Error		This display field shows the number of data packets received with a checksum error.
	Jabbers		This display field shows the number of jabbers received by this port.
	Drop Events		This display field shows the number of dropped data packets.

Table 101: WBM “RMON Statistics” Page

Outgoing	Total Octets		This display field shows the number of data packets sent from the port.
	Broadcast Packets		This display field shows the number of broadcast packets sent from the port.
	Unicast Packets		This display field shows the number of unicast packets sent from the port.
	Non Unicast Packets		This display field shows the number of unicast packets sent from the port.
	Collisions		This display field shows the number of data packets that were to be sent, have collided and were discarded.
	Late Collision		This display field shows the number of data packets that were to be sent, have collided and were discarded.
	Single Collisions		This display field shows the number of single collisions of the data packets sent.
	Multiple Collisions		This display field shows the number of multiple collisions of the data packets sent.
	Discards Packets		This display field shows the number of data packets sent from the port that were dropped.
	Error Packets		This display field shows the number of data packets sent from the port that were faulty.
#(number) of packets received with a length of ?.	64 Octets		This display field shows the number of data packets received that had a length of 64 octets.
	65 to 127 Octets		This display field shows the number of data packets received that had a length of 65 to 127 octets.
	128 to 255 Octets		This display field shows the number of data packets received that had a length of 128 to 255 octets.
	256 to 511 Octets		This display field shows the number of data packets received that had a length of 256 to 511 octets.
	512 to 1023 Octets		This display field shows the number of data packets received that had a length of 512 to 1023 octets.
	1024 to Max. Octets		This display field shows the number of data packets received that had a length of more than 1024 octets.

10.6.6 SFP Information

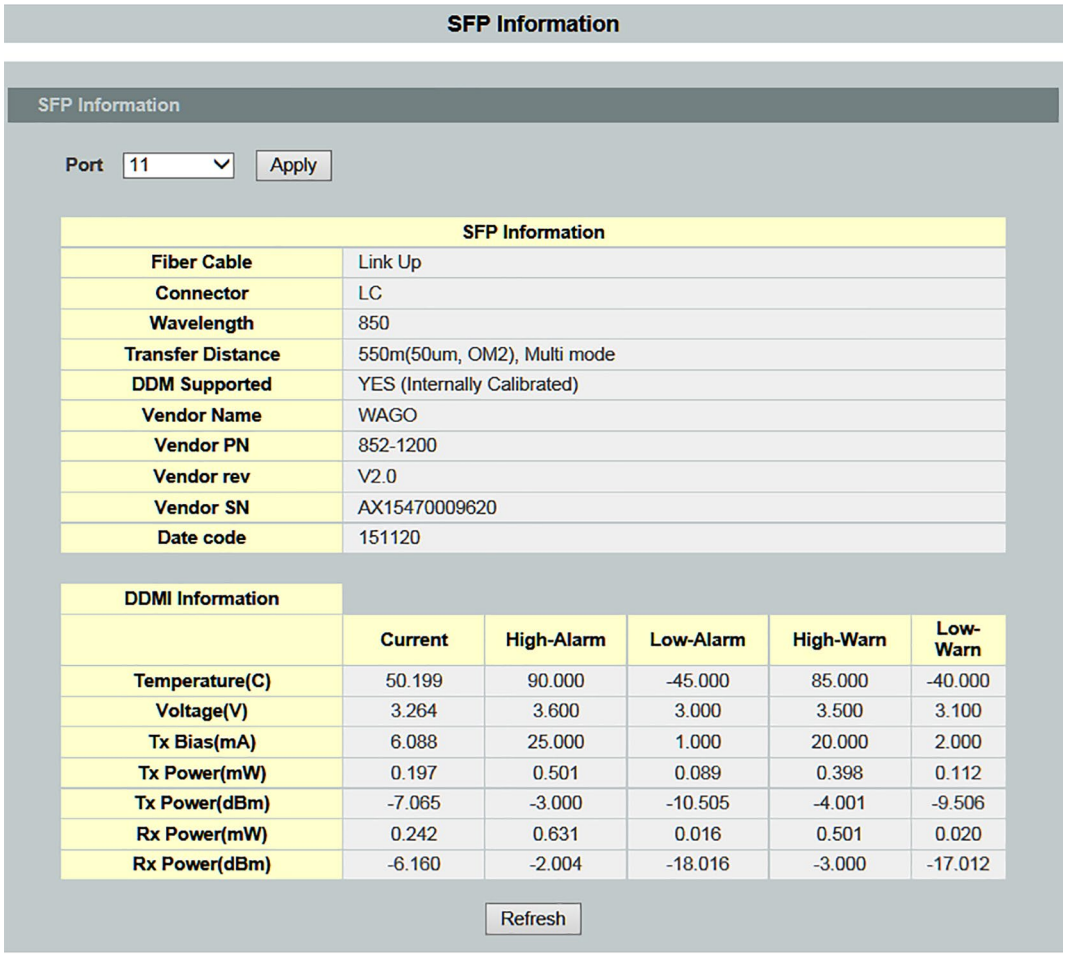


Figure 86: WBM “SFP Information” Page

Table 102: WBM “SFP Information” Page

SFP Information		
Parameter	**Default**	**Description**
Port	**-**	Select “-” in the selection box if you have not inserted an SFP module
	9, 10	In the selection box, select the port in which you have inserted an SFP module.
SFP Information		
Parameter	**Default**	**Description**
Fiber Cable		This display field shows if a fiber optic cable is connected.
Connector		This display field shows the code for the optical connector type.
Wavelength (nm)		This display field shows the wavelength.
Transfer Distance (nm)		This field displays the transmission distance.
DDM Support (nm)		This display field shows if the SFP module supports DDM (“**D**ynamic **D**evice **M**apping”).
Vendor Name (nm)		This display field shows the name of the SFP provider.
Vendor Part Number (nm)		This display field shows the part number.
Vendor Revision Status (nm)		This display shows the revision status of the part number.
Vendor Serial Number (nm)		This display field shows the serial number (ASCII).
Date code (nm)		This field displays the version date.

Table 102: WBM “SFP Information” Page

DDMI Information (nm)		
Parameter	**Default**	**Description**
Current (nm)		This column displays the following current values: - Temperature (C) - Voltage (V) - Tx bias (mA) - Tx power (mW) - Tx power (dBm) - Rx power (mW) - Rx power (dBm)
High-Alarm (nm)		This column displays the “Alarm High” values of the following values: - Temperature (C) - Voltage (V) - Tx bias (mA) - Tx power (mW) - Tx power (dBm) - Rx power (mW) - Rx power (dBm)
Low-Alarm (nm)		This column displays the “Alarm Low” values of the following values: - Temperature (C) - Voltage (V) - Tx bias (mA) - Tx power (mW) - Tx power (dBm) - Rx power (mW) - Rx power (dBm)
High-Warn (nm)		This column displays the “Warning High” values of the following values: - Temperature (C) - Voltage (V) - Tx bias (mA) - Tx power (mW) - Tx power (dBm) - Rx power (mW) - Rx power (dBm)
Low-Warn (nm)		This column displays the “Warning Low” values of the following values: - Temperature (C) - Voltage (V) - Tx bias (mA) - Tx power (mW) - Tx power (dBm) - Rx power (mW) - Rx power (dBm)

10.6.7 Traffic Monitor

Note

Additional information

Please refer to the section “Function Description” for more information on the “Traffic Monitor.”

Traffic Monitor

Traffic Monitor Settings

State: Disable

Port	State	Action	Packet Type	Packet Rate (pps)	Recovery State	Recovery Time	Quarantine times
From: 1 To: 1	Disable	None	Broadcast	100	Enable	1	3

Apply Refresh Save Configurations

Traffic Monitor Status

Port	State	Status	Packet Type	Packet Rate(pps)	Recovery State	Recovery Time	Quarantine times
1	Disable	Normal	Broadcast	100	Enable	1	3
2	Disable	Normal	Broadcast	100	Enable	1	3
3	Disable	Normal	Broadcast	100	Enable	1	3
4	Disable	Normal	Broadcast	100	Enable	1	3
5	Disable	Normal	Broadcast	100	Enable	1	3
6	Disable	Normal	Broadcast	100	Enable	1	3
7	Disable	Normal	Broadcast	100	Enable	1	3
8	Disable	Normal	Broadcast	100	Enable	1	3
9	Disable	Normal	Broadcast	100	Enable	1	3
10	Disable	Normal	Broadcast	100	Enable	1	3
11	Disable	Normal	Broadcast	100	Enable	1	3
12	Disable	Normal	Broadcast	100	Enable	1	3

Figure 87: WBM “Traffic Monitor” Page

Table 103: WBM “Traffic Monitor” Page

Traffic Monitor Settings			
Parameter		**Default**	**Description**
State		**Disable**	Select “Disable” in the selection box to disable the “Traffic Monitor” function globally.
		Enable	Select “Enable” in the selection box to enable the “Traffic Monitor” function globally.
Port	From:	**1**	Select a port or port range in the selection box which you want to configure.
	To:	**1**	Select a port or port range in the selection box which you want to configure.
State		**Disable**	Select “Disable” in the selection box if you want to disable the “Traffic Monitor” function for the port or port range.
		Enable	Select “Enable” in the selection box if you want to enable the “Traffic Monitor” function for the port or port range.
Action		**None**	Select “None” in the selection box if you do not want to cancel port blocking.
		Unblock	Select “Unblocked” in the selection box if you want to cancel port blocking.
Packet Type		**Broadcast**	Select “Broadcast” in the selection box if you want to monitor this as the packet type.
		Multicast	Select “Multicast” in the selection box if you want to monitor this as the packet type.
		Bcast+Mcast	Select “Bcast+Mcast” in the selection box if you want to monitor both as the packet types.
Packet Rate (pps)			In the input field, enter the packet rate that you want to monitor.
Recovery State		**Enable**	Select “Enable” in the selection box if you want to enable the recovery function with the “Traffic Monitor” function for the port or port range.
		Disable	Select “Disable” in the selection box if you want to disable the recovery function with the “Traffic Monitor” function for the port or port range.
Recovery Time		**1**	In the input field, enter the recovery time that you want to monitor.
Quarantine Time		**3**	Enter a value in the input field for the “Quarantine Time” for the “Traffic Monitor” function.

Table 103: WBM “Traffic Monitor” Page

Traffic Monitor Status		
Parameter	**Default**	**Description**
Port	1 … 10	This column shows the port numbers.
State	Disable Enable	This column displays the status of the specific port.
Status	Normal	This column displays the status of the operational state.
Packet Type	Broadcast Multicast Bcast+Mcast	This column displays the type of data packet.
Packet Rate (pps)		This column displays the selected packet rate.
Recovery Status	Enable Disable	This column displays the status of the selected recovery function.
Recovery Time (min)	1 … 60	This column displays the selected recovery time.
Quarantine Time	3	This column displays the selected quarantine time.

10.7 Management

10.7.1 SNMP

10.7.1.1 SNMP

10.7.1.1.1 SNMP Settings

Note

Additional Information
Please refer to the section “Function Description” for more information on “SNMP” (**S**imple **N**etwork **M**anagement **P**rotocol).

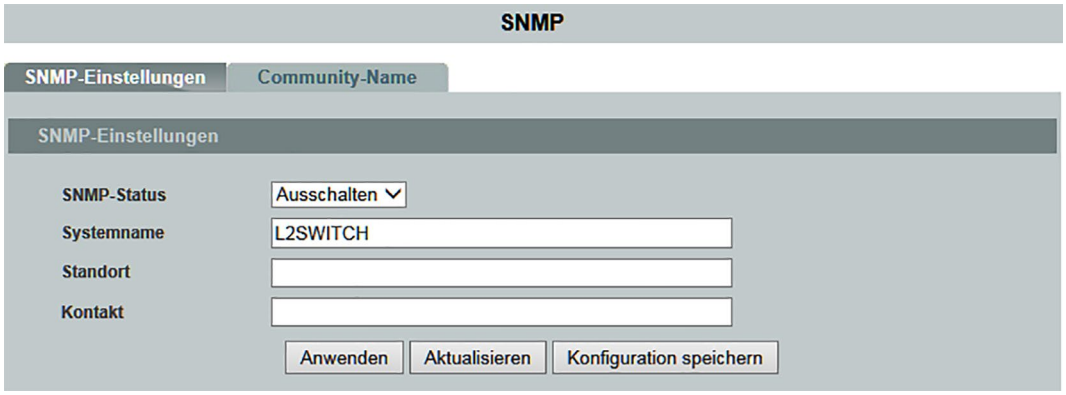


Figure 88: WBM “SNMP” Page – “SNMP Settings” Tab

Table 104: WBM “SNMP” Page – “SNMP Settings” Tab

SNMP Settings		
Parameter	**Default**	**Description**
SNMP Status	**Disable**	Select “Disable” from the drop-down list to disable SNMP on the switch.
	Enable	Select “Enable” from the drop-down list to enable SNMP on the switch.
System Name	**L2SWITCH**	Enter the system name for the switch in the input field (the system name and host name are identical).
Location	**–**	Enter the IP address (location information) of the switch in decimal-point notation.
Contact	**–**	Enter the IP subnet mask of the switch in decimal-point notation.

10.7.1.1.2 Community Name

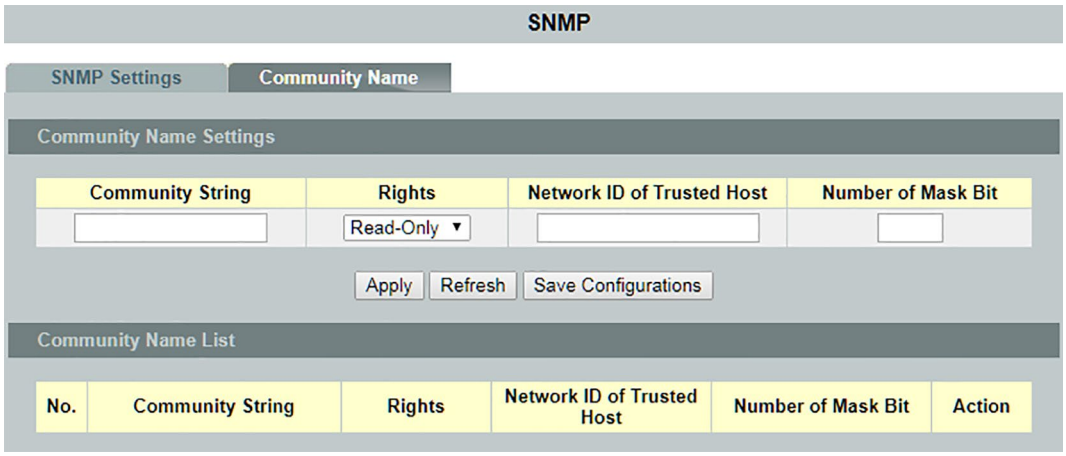


Figure 89: WBM “SNMP” Page – “Community Name” Tab

Table 105: WBM SNMP" Page – "Community Name" Tab

Community Name Settings		
Parameter	**Default**	**Description**
Community String		Enter the "Community String" that acts as a password for requests from the management station.
Rights	**Read Only**	Select "Read Only" from the drop-down list so that the SNMP manager can use this string to receive information from the switch.
	Read/ Write	Select "Read/Write" from the drop-down list so that the SNMP manager can use this string to configure settings on the switch.
Network ID of the Trusted Host		Enter the IP address of the remote SNMP management station in decimal-point notation (e.g., 192.168.1.0).
Number of Mask Bit		Enter the IP address of the subnet mask for the remote SNMP management station in decimal-point notation (e.g., 255.255.255.0).
Community Name List		
Parameter	**Default**	**Description**
No.		This column displays the "Community" number. It is for identification only. Click a number to modify the setting for a specific "Community."
Community String		This column displays the "SNMP Community String." This is a text element that acts as a password.
Rights	Read Only, Read/ Write	This column displays the rights for the "SNMP Community String."
Network ID of the Trusted Host		This column displays the IP address of the remote SNMP management station after it has been modified by the subnet mask.
Number of Mask Bit		This column displays the subnet mask for the IP address of the remote SNMP management station.
Action		Click **[Delete]** to delete a specific "Community String."

10.7.1.2 SNMP Trap

10.7.1.2.1 Trap Receiver Settings

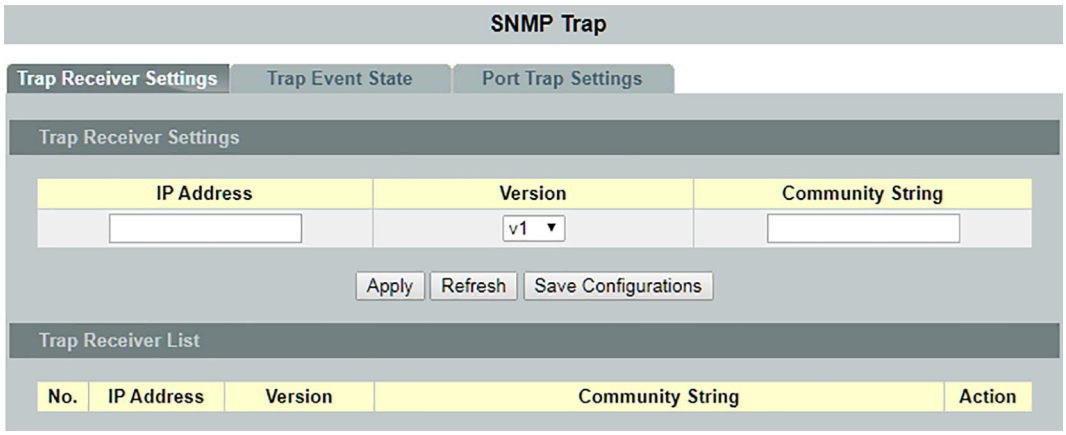


Figure 90: WBM “SNMP Trap” Page – “Trap Receiver Settings” Tab

Table 106: WBM “SNMP Trap” Page – “Trap Receiver Settings” Tab

Trap Receiver Settings		
Parameter	**Default**	**Description**
IP Address		Enter the IP address of the remote trap station in decimal-point notation.
Version	**v1**	Select “v1” from the drop-down list if you want to use SNMP Version v1.
	v2c	Select “v2c” from the drop-down list if you want to use SNMP Version v2c.
Community String		Enter the IP address of the remote SNMP management station in decimal-point notation (e.g., 192.168.1.0).
Trap Receiver List		
Parameter	**Default**	**Description**
No.		This column displays the “Community” number. It is for identification only. Click a number to modify the setting for a specific “Community.”
IP Address		This column displays the IP address of the remote trap station.
Version	v1 v2c	This column displays the SNMP version used.
Community String		This column displays the “Community String” used by the remote trap station.
Action		Click the **[Delete]** button to delete a configured trap receiver station.

10.7.1.2.2 Trap Event Status

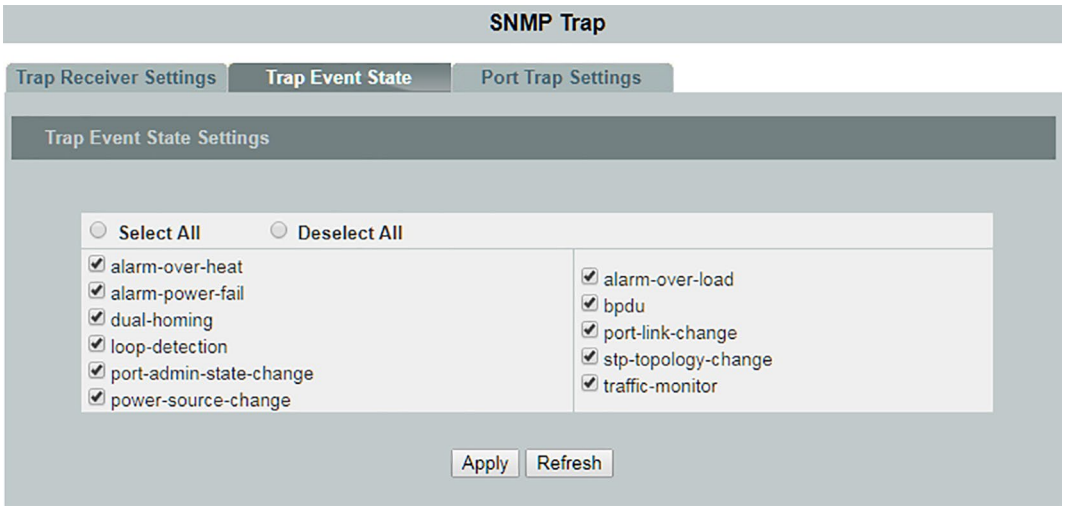


Figure 91: WBM “SNMP Trap” Page – “Trap Event State” Tab

Table 107: WBM “SNMP Trap” Page – “Trap Event State” Tab

Trap Event State Settings		
Parameter	**Default**	**Description**
alarm-over-heat	☑	Enables/disables the SNMP trap when the system temperature is too high.
alarm-power-fail	☑	Enables/disables the SNMP trap when system capacity is overvoltage/undervoltage. RPS overvoltage / RPS voltage
dual-homing	☑	Enables/disables the SNMP trap when the port is blocked by dual homing.
loop-detection	☑	Enables/disables the SNMP trap when the port is blocked by loop detection.
port-admin-state-change	☑	Enables/disables the SNMP trap when the port is enabled/disabled by the Administrator.
power-source-change	☑	Enables/disables the SNMP trap when the power source is changed (AC to DC or DC to AC).
alarm-over-load	☑	Enables/disables the SNMP trap when the system is overloaded.
bpdu	☑	Enables/disables the SNMP trap when the port is blocked by BPDU Guard/BDPU Root. The Guard/BPDU connection status is changed.
port-link-change	☑	Enables/disables the SNMP trap when the port switches between upward and downward.
stp-topology-change	☑	Enables/disables the SNMP trap when the STP topology changes.
traffic-monitor	☑	Enables/disables the SNMP trap when the port is blocked by the traffic monitor.

10.7.1.2.3 Port Trap Settings

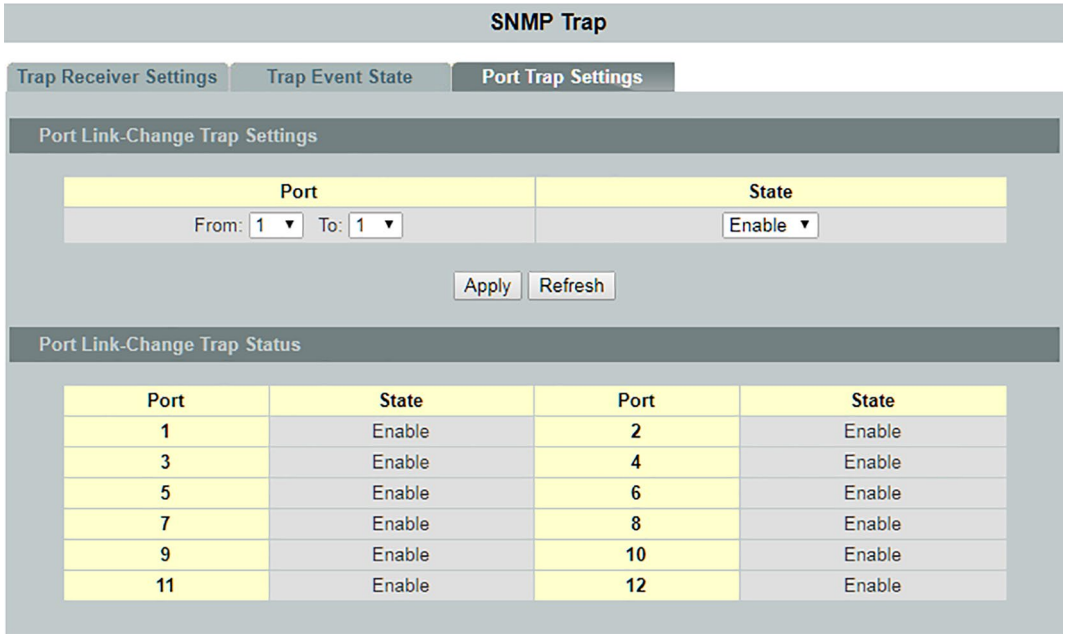


Figure 92: WBM “SNMP Trap” Page – “Port Trap Settings” Tab

Table 108: WBM “SNMP Trap” Page – “Port Trap Settings” Tab

Port Link Change Trap Settings			
Parameter		**Default**	**Description**
Port	von:	**1**	Select a port or port range to configure in the selection box.
	an:	**1**	Select a port or port range to configure in the selection box.
State		**Disable**	Select “Enable” in the selection box to enable the port status.
		Enable	Select “Disable” in the selection box to disable the port status.
Port Link Change Trap Status			
Parameter		**Default**	**Description**
Port		1 … 10 (12)	This column displays the port range.
State		Enable Disable	This field displays the port status.

10.7.1.3 SNMPv3 Configuration

10.7.1.3.1 SNMPv3 User

Note

Additional Information
Please refer to the section “Function Description” for more information on “SNMPv3.”

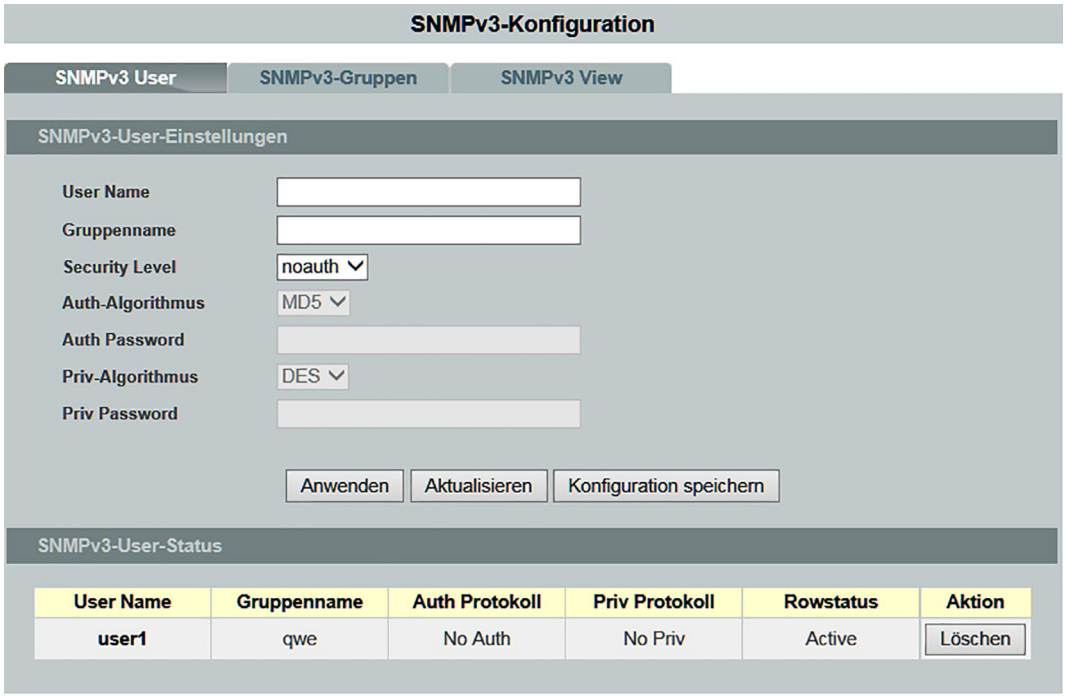


Figure 93: WBM “SNMPv3 Configuration” Page – “SNMPv3 User” Tab

Table 109: WBM “SNMPv3 Configuration” Page – “SNMPv3 User” Tab

SNMPv3 User Settings		
Parameter	**Default**	**Description**
Username		Enter a new username in the input field, or modify an existing username.
Group Name		Enter the group name for the SNMPv3 in the input field.
Security Level		This selection box is used to select he security level.
	noauth	If you selected “noauth” from the drop-down list, you then cannot change the “Auth Algorithm” or the “Priv Algorithm.”
	auth	If you selected “auth” from the drop-down list, you then can change the “Auth Algorithm” and the “Auth Password.”
	priv	If you selected “priv” from the drop-down list, you then can change the “Auth Algorithm,” “Priv Algorithm” and “Priv Password.”
Auth Algorithm	**MD5**	If you selected “auth” or “priv” from the drop-down list, you then can select “Auth Algorithm” “MD5.”
	SHA	If you selected “auth” or “priv” from the drop-down list, you then can select “Auth Algorithm” “SHA.”
Auth Password		If you selected “auth” from the drop-down list, you can enter a password in the input field (consisting of at least eight alphanumeric characters).
Priv Algorithm	**DES**	If you selected “priv” from the drop-down list, you can then select “DES” from the drop-down list.
	AES	If you selected “priv” from the drop-down list, you can then select “AES” from the drop-down list.
Priv Password		If you selected “priv” from the drop-down list, you can enter a password in the input field (consisting of at least eight alphanumeric characters).
SNMPv3 User Status		
Parameter	**Default**	**Description**
Username		This column displays the username.
Group Name		This column displays the group name.
Auth Protocol		This column displays the selected “Auth Algorithm.”
Priv Protocol		This column displays the selected “Priv Algorithm.”
Row Status		This column displays the row status.
Action		Click **[Delete]** to delete a specific entry.

10.7.1.3.2 SNMPv3 Groups

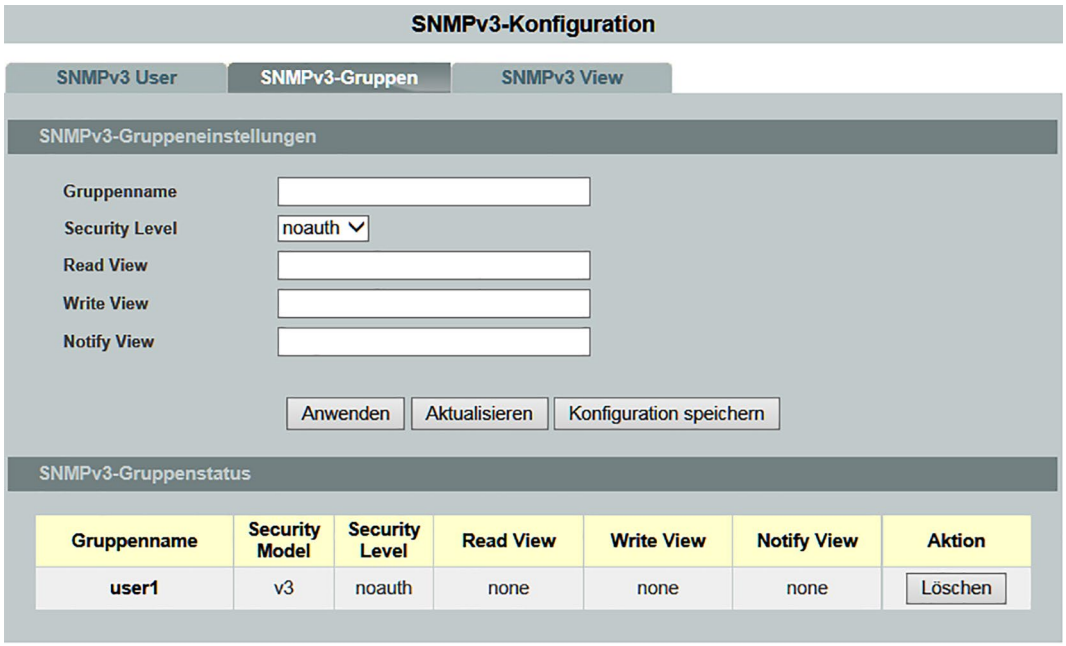


Figure 94: WBM “SNMPv3 Configuration” Page – “SNMPv3 Groups” Tab

Table 110: WBM “SNMPv3 Configuration” Page – “SNMPv3 Groups” Tab

SNMPv3 Group Settings		
Parameter	**Default**	**Description**
Group Name		Enter the group name for the SNMPv3 group in the input field.
Security Level		This selection box is used to select he security level.
	Noauth auth priv	Select the respective security level from the drop-down list.
Read View		In the input field, enter the name of the objects that should be available in the Read view. If you do not enter an object, all objects will be readable.
Write View		In the input field, enter the name of the objects to which you want to grant write access.
Notify View		In the input field, enter the name of the object that can receive user notifications.
SNMPv3 Group Status		
Parameter	**Default**	**Description**
Group Name		This column displays the group name.
Security Model		This column displays the selected security level.
Security Level		This column displays the selected security level.
Read View		This column displays the Read view
Write View		This column displays the Write view
Notify View		This column displays the Notify view
Action		Click **[Delete]** to delete a specific entry.

10.7.1.3.3 SNMPv3 View

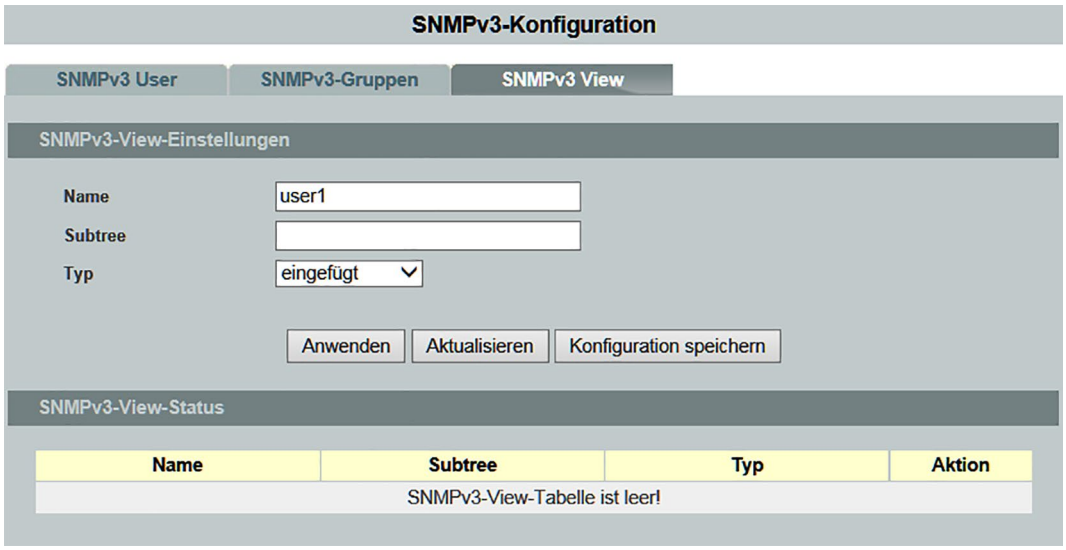


Figure 95: WBM “SNMPv3 Configuration” Page – “SNMPv3 View” Tab

Table 111: WBM “SNMPv3 Configuration” Page – “SNMPv3 View” Tab

SNMPv3 View Settings		
Parameter	**Default**	**Description**
Name		Enter the name for the SNMPv3 view in the input field.
Subtree		Enter the name for the subtree in the input field.
Type	**Inserted**	If you selected “Inserted” from the drop-down list, the subtree is inserted
	Removed	If you selected “Removed” from the drop-down list, the subtree is not inserted.
SNMPv3 View Status		
Parameter	**Default**	**Description**
Name		This column displays the name of the SNMPv3 view.
Subtree		This column displays the name of the subtree.
Type	Inserted Removed	This column displays the selected type.
Action		Click **[Delete]** to delete a specific entry.

10.7.2 Maintenance

10.7.2.1 Configuration

Figure 96: WBM “Maintenance” Page – “Configuration” Tab

Save Configuration

- Click the **[Save]** button to save the current settings in NV-RAM (Flash).

Upload and Download of the Configuration

Execute the following steps to save the configuration file to your PC.

1. Select “Press Download to save the configuration file to your PC.”
2. Click the **[Download]** button to start the download.

Execute the following steps to upload the configuration file from your PC to the switch.

1. Select “Upload the configuration file to the switch.”
2. Click the **[Select file]** button.
   Select the configuration file by specifying the full path.
3. Click the **[Upload]** button to begin uploading the file.

Reset Configuration

- Click the **[Reset]** button to reset the switch configuration to the factory default.

Configuration Status

“The configurations have been changed” indicates that changes have been made to the configurations.

If no changes were made to the configurations, the following message appears: “The user configuration file is the default. The configurations are default values.”

10.7.2.2 Firmware

Figure 97: WBM “Maintenance” Page – “Firmware” Tab

Firmware Upgrade

Execute the following steps to update the switch’s firmware.

1. Click the **[Select file]** button.
   The file selection dialog opens. Select the respective firmware file.

2. Click the **[Upgrade]** button to load the new firmware.

10.7.2.3 Reboot

Figure 98: WBM “Maintenance” Page – “Reboot” Tab

Reboot

The “Reboot” function allows you to restart the switch without physically turning the power off.

Follow the steps below to reboot the switch.

1. Click the **[Reboot]** button in the “Reboot” menu. The following window opens:

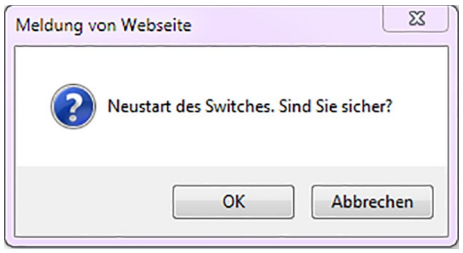


Figure 99: WBM “Maintenance” Page – “Reboot” Tab – Message

2. Click **[OK]** and wait for the switch to restart. The process can take up to two minutes. This process does not change the switch configuration.

10.7.2.4 Protocols

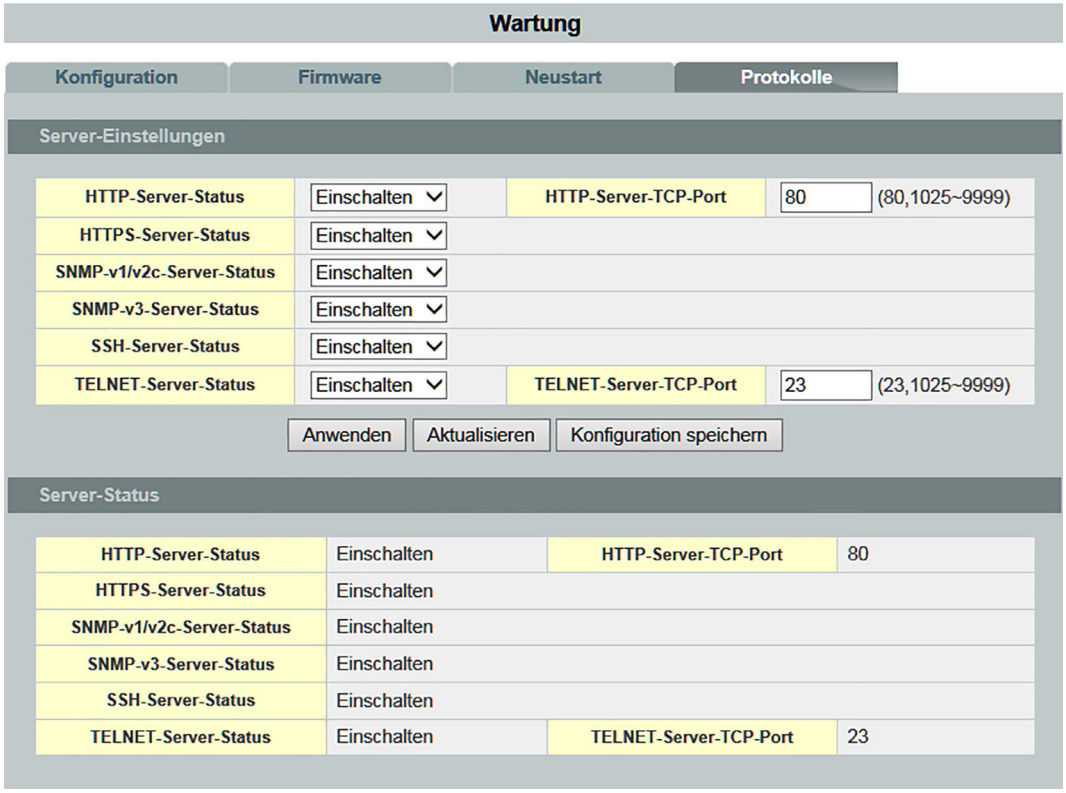


Figure 100: WBM “Maintenance” Page – “Protocols” Tab

Table 112: WBM “Maintenance” Page – “Protocols” Tab

Server Settings		
Parameter	**Default**	**Description**
HTTP Server Status	**Turn ON**	Select “Enable” to enable the HTTP server.
	Disable	Select “Disable” to disable the HTTP server.
HTTP Server TCP Port (80, 1025–9999)	**80** 1025 … 9999	Enter the “HTTP Server TCP Port” in the input field.
HTTP Server Status	**Turn ON**	Select “Enable” to enable the HTTPS server.
	Disable	Select “Disable” to disable the HTTPS server.
SNMP v1/v2c Server Status	**Turn ON**	Select “Enable” to enable the SNMP v1/v2c server.
	Disable	Select “Disable” to disable the SNMP v1/v2c server.
SNMP v3 Server Status	**Turn ON**	Select “Enable” to enable the SNMP v3 server.
	Disable	Select “Disable” to disable the SNMP v3 server.
SSH Server Status	**Turn ON**	Select “Enable” to enable the SSH server.
	Disable	Select “Disable” to disable the SSH server.
Telnet Server Status	**Turn ON**	Select “Enable” to enable the Telnet server.
	Disable	Select “Disable” to disable the Telnet server.
Telnet Server TCP Port (23, 1025–9999)	**23** 1025 … 9999	Enter the “Telnet Server TCP Port” in the input field.
Server Status		
Parameter	**Default**	**Description**
HTTP Server Status	Enable Disable	This field displays the status of the HTTP server.
HTTP Server TCP Port	80 1025 … 9999	This field displays the status of the HTTP server TCP port.
HTTP Server Status	Enable Disable	This field displays the status of the HTTPS server.
SNMP v1/v2c Server Status	Enable Disable	This field displays the status of the SNMP v1/v2c server.
SNMP v3 Server Status	Enable Disable	This field displays the status of the SNMP v3 server.
SSH Server Status	Enable Disable	This field displays the status of the SSH server.
Telnet Server Status	Enable Disable	This field displays the status of the Telnet server.
Telnet Server TCP Port	23 1025 … 9999	This field displays the status of the Telnet server TCP port.

10.7.3 System Log

The “syslog” function records various system information for debugging.
Each log entry records one of the following levels:
- Alert
- Critical
- Error
- Warning
- Notice
- Information

The syslog function can be enabled or disabled. The default setting is “disabled.”
The log message is recorded in the switch’s file system. If the IP address of the syslog server has been configured, the switch sends a copy to it.

Note

Size of the Log Message File
The size of the log message file is limited to 4 KB. If the file is full, the oldest message is replaced.

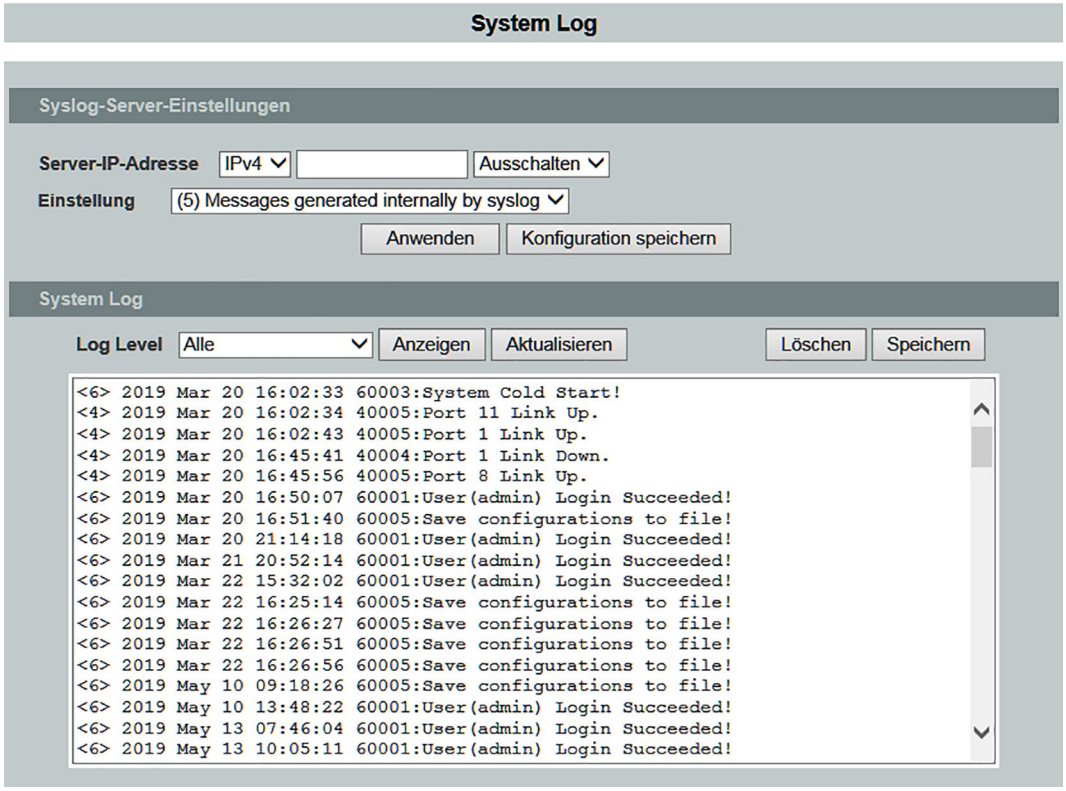


Figure 101: WBM “System Log” Page

Table 113: WBM “System Log” Page

Syslog Server Settings		
Parameter	**Default**	**Description**
Server IP Address	**IPv4**	Select “IPv4” in the selection field if you want to select this version of the Internet protocol.
	IPv6	Select “IPv6” from the drop-down list to enable this Internet protocol version.
		Enter the IP address in decimal-point notation (e.g., 192.168.1.1).
	Disable	Select “Disable” from the drop-down list to prevent the switch from sending all new log messages to the syslog server.
	Enable	Select “Enable” from the drop-down list to allow the switch to send all new log messages to the syslog server.
Setting	(1) User-level messages	Select “(1) User-level messages” from the drop-down list if you want to display user-specific messages.
	(5) Messages generated internally by syslogd	Select “(5) Messages generated internally by syslogd” from the drop-down list if you want to display messages generated by syslog internally.
	(14) Log alert	
	(16) Local use 0	
	(17) Local use 1	
	(18) Local use 2	
	(19) Local use 3	
	(20) Local use 4	
	(21) Local use 5	
	(22) Local use 6	
	(23) Local use 7	
System Log		
Parameter	**Default**	**Description**
Log Level	**All**	Select “All” from the drop-down list if you want to display all log messages.
	1:Alarm	Select “Alarm” from the drop-down list if you want to display the log messages.
	2:Critical	Select “Critical” from the drop-down list if you want to display critical log messages.
	3:Error	Select “Error” from the drop-down list if you want to display the errors.
	4:Warning	Select “Warning” from the drop-down list if you want to display the warnings.
	5:Notice	Select “Notice” from the drop-down list if you want to display the notices.
	6:Information	Select “Information” from the drop-down list if you want to display all information.

10.7.4 Upload File

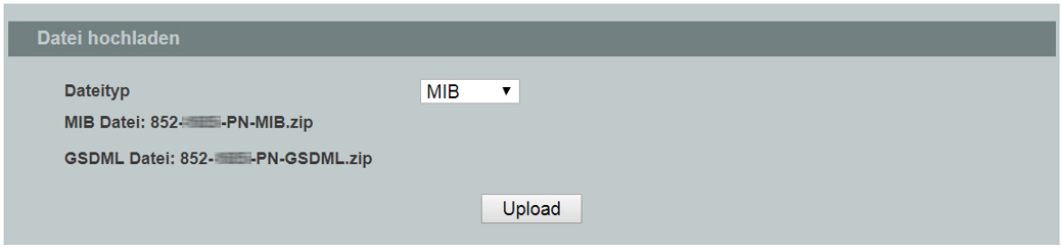


Figure 102: WBM Page “Upload File”

Table 114: WBM Page “Upload File”

Parameter	Default	Description
File Type	**MIB**	Specifies whether the MIB or GSDML file should be loaded into WBM

10.7.5 Ping

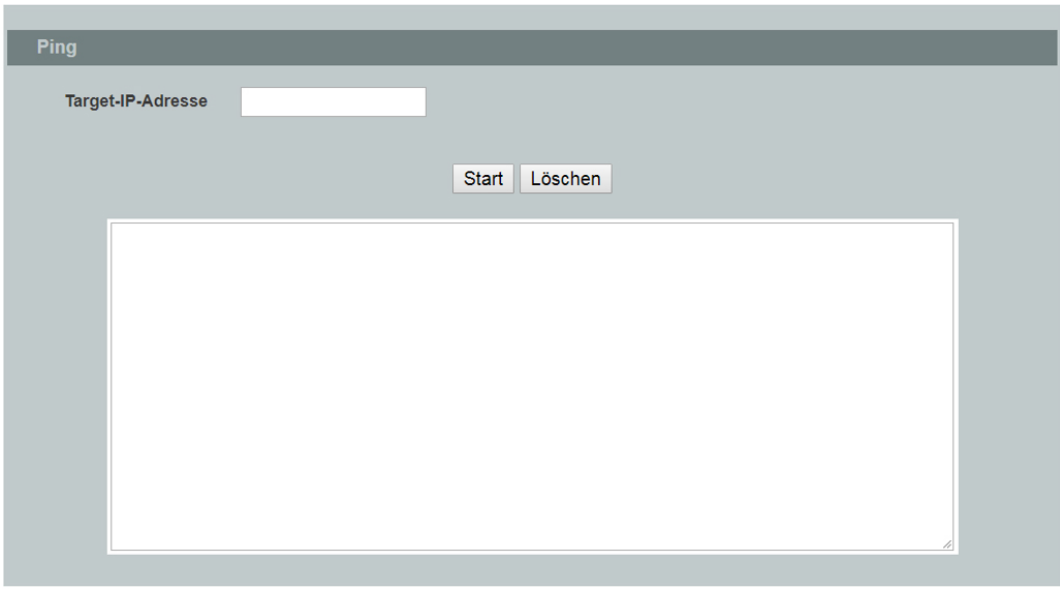


Figure 103: WBM “Ping” Page

Table 115: WBM “Ping” Page

Parameter	Default	Description
Target IP address	–	Inputting the destination address

10.7.6 User Account

The switch allows users to create up to six user accounts. The username and password must be combinations of numbers and letters. The last admin account cannot be deleted. To use the CLI or Web-Based Management, a user has to be logged into a valid user account.

User Permissions

The switch support two types of user accounts:

The default user accounts have the following credentials:
Firmware version 01: Username = “admin”
User password = “wago

1. Admin account — Read/Write permissions

2.. Normal user account — Read permission only
- Use of the privileged mode in the CLI is not possible.
- Configurations cannot be changed in the Web-Based Management.

The switch also supports a “backdoor” user account. If a user has forgotten his or her username or password, the switch can create a “backdoor” account with the MAC address of the system. A user can then log into the switch and create a new account.

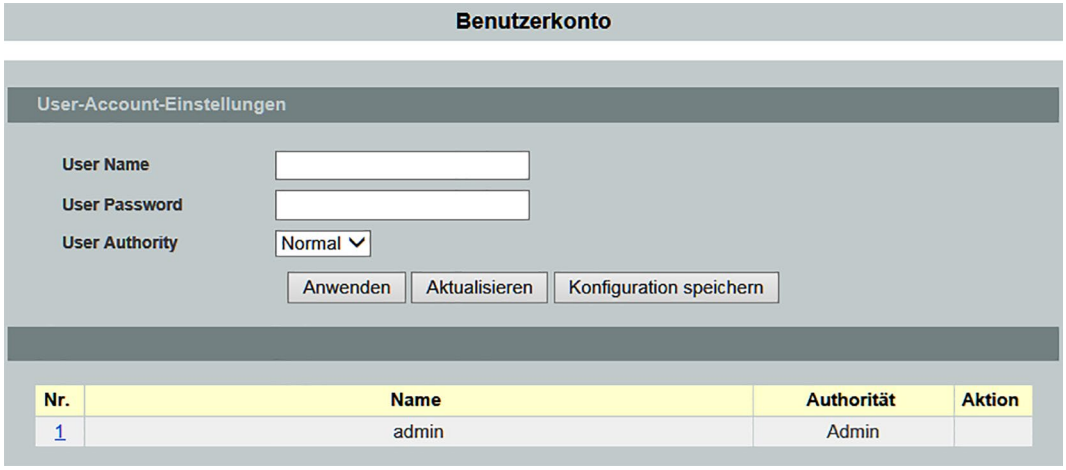


Figure 104: WBM “User Account” Page

Table 116: WBM “User Account” Page

User Account Settings		
Parameter	**Default**	**Description**
Username		Enter a new username in the input field, or modify an existing username.
User Password		Enter a new password in the input field, or modify an existing password. You can enter up to 32 alphanumeric characters or digits.
User Role		In this box, select the type of user account.
	Normal	Select “Normal” from the drop-down list if you need only read permission for this user account.
	Admin	Select “Admin” from the drop-down list if you need read and write permission for this user account.
No.		
Parameter	**Default**	**Description**
No.		This column displays the index number of an entry.
Name		This column displays the name of the user account.
User Role		This column displays the type of user account.
Action		Click the **[Delete]** button to delete a user account.
		Note  **Deleting an Administrator Account** The last admin account cannot be deleted.

11 Appendix

11.1 Console Port (RJ-45 to DB9)

Use the included console cable to connect the console port of the industrial managed switch to the COM port. The connector pin assignment is:

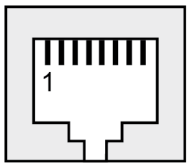


Figure 105: RJ-45 Connector Pin Assignment

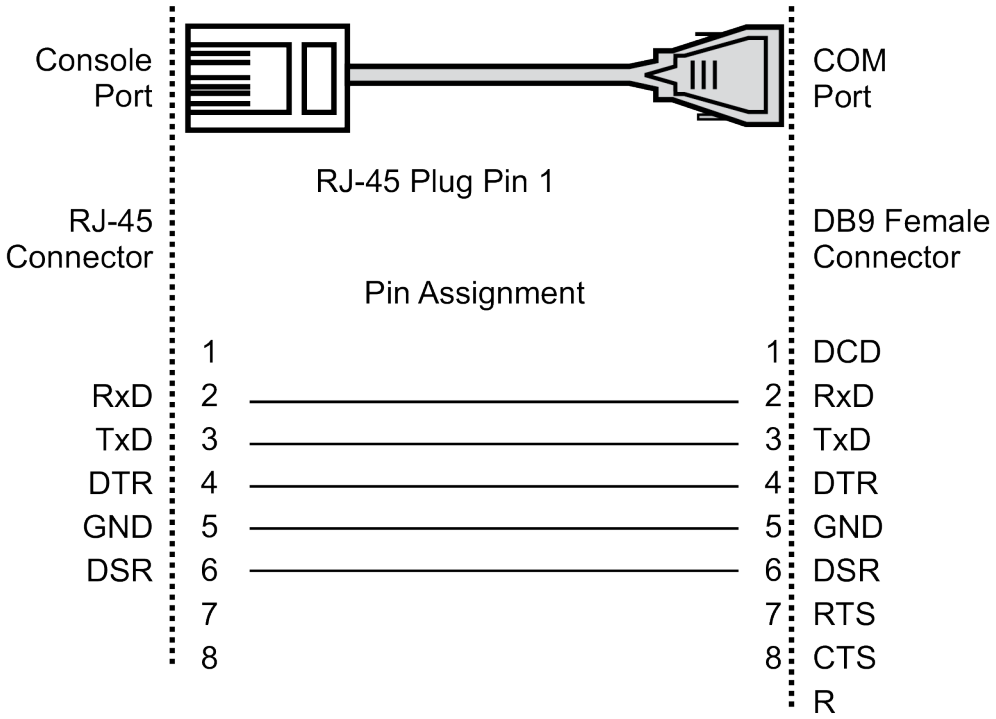


Figure 106: Connector Pin Assignment RJ-45 to DB9

11.2 RJ-45 Cable

Always use category 5e cables to connect your network devices. The pin assignment is given below:

Table 117: RJ-45 Cable

Contact	Description		Pair	Color (acc. EIA/TIA 568B)
	4-wire	8-wire		
1	TD	D1+	2	White/Orange
2	TD-	D1-	2	Orange
3	RX+	D2+	3	White/Green
4	Not assigned	D3+	1	Blue
5	Not assigned	D3-	1	White/Blue
6	RX-	D2-	3	Green
7	Not assigned	D4+	4	White/Brown
8	Not assigned	D4-	4	Brown

Note

Functions on the RJ45 connector

The industrial managed switch offers the functions autocrossing und autonegotiation to the RJ-45 connection.

11.3 Configuring in the Command Line Interface (CLI) (Zugriff über Konsole (CLI))

11.3.1 System Status

11.3.1.1 System Information

Table 118: CLI “System Information” Configuration

Node	Command	Description
enable	show hostname	This command displays the system’s network name.
configure	reboot	This command reboots the system.
eth0	ip address A.B.C.D/M	This command configures the static IP and subnet mask for the system.
interface	show	This command displays the current port configuration.
acl	show	This command displays the current access control list.
vlan	show	This command displays the current VLAN configuration.
enable	show interface eth0	This command displays the current Eth0 configurations.
enable	show model	This command displays the system information.
enable	show running-config	This command displays the current operating configurations.
enable	show system-info	This command displays the system’s CPU utilization and memory information.
enable	show uptime	This command displays the system uptime.

11.3.2 Default Settings

11.3.2.1 System

Table 119: CLI “System” Configuration

Node	Command	Description
enable	ping IPADDR [–c COUNT]	
enable	ping IPADDR [–s SIZE]	
enable	ping IPADDR [–c COUNT –s SIZE]	
enable	ping IPADDR [-s SIZE –c COUNT]	
configure	Reboot	
configure	hostname STRINGS	This command sets the system’s network name.
configure	interface eth0	This command enters the eth0 interface node to configure the system IP.
configure	configure terminal	
configure	interface eth0	
eth0	Show	
eth0	ip address A.B.C.D/M	
eth0	ip address default-gateway A.B.C.D	This command configures the system’s default gateway.
eth0	ip dhcp client (disable|enable|renew)	This command configures a DHCP client function for the system. “Disable”: Use a static IP address for the switch. “Enable & Renew”: Use the DHCP client to get an IP address from the DHCP server.
eth0	management vlan VLAN_ID	This command configures the management VLAN.

11.3.2.1.1 Jumbo Frame

Table 120: CLI “Jumbo Frame” Configuration

Node	Command	Description
enable	show jumboframe	This command displays the current jumbo frame settings.
configure	jumboframe (10240|1522|1536|1552|9216)	This command configures the maximum number of bytes for frame sizes.
configure	interface IFNAME	This command starts configuration mode.
interface	jumboframe(10240|1522|1536|1552|9010|9216)	This command configures the maximum number of bytes per frame.
configure	interface range gigabitethernet1/0/PORTLISTS	This command starts configuration mode.
if-range	jumboframe(10240|1522|1536|1552|9010|9216)	This command configures the maximum number of bytes per frame.

11.3.2.1.2 SNTP

Table 121: CLI “SNTP” Configuration

Node	Command	Description
enable	show time	This command displays the current time and date configuration.
configure	time HOUR:MINUTE:SECOND	This command sets the current time of the switch. hour: 0 ... 23 min: 0 ... 59 sec: 0 ... 59 Note: If you do not configure daylight saving time until after the date and time, the switch uses daylight saving time.
configure	time date YEAR/MONTH/DAY	This command sets the current date of the switch. year: 1970– month: 1 ... 12 day: 1 ... 31
configure	time daylight-saving-time	This command enables daylight saving time.
configure	no time daylight-saving-time	This command disables daylight saving time on the switch.
configure	time daylight-saving-time start-date (first | second | third | fourth | last) (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH HOUR	This command sets the start date of daylight saving time.
configure	time daylight-saving-time end-date (first | second | third | fourth | last) (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH HOUR	This command sets the end date of daylight saving time.
configure	time ntp-server (disable|enable)	This command disables/enables the NTP server settings.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of the time server.
configure	time ntp-server domain-name STRING	This command sets the domain names of the time server.
configure	time timezone STRING	This command sets the time difference between UTC (formerly GMT) and the time zone. Valid range: −1200 … +1200

Example

L2SWITCH(config)*#time ntp-server 192.5.41.41*

L2SWITCH(config)*#time timezone +0800*

L2SWITCH(config)*#time ntp-server enable*

L2SWITCH(config)*#time daylight-saving-time start-date first Monday 6 0*

L2SWITCH(config)*#time daylight-saving-time end-date last Saturday 10 0*

11.3.2.1.3 Management Host

Table 122: CLI “Management Host” Configuration

Node	Command	Description
enable	show interface eth0	The command displays all eth0 interface configurations.
eth0	Show	The command displays all eth0 interface configurations.
eth0	management host A.B.C.D	The command adds a management host address.
eth0	no management host A.B.C.D	The command deletes a management host address.

Example

L2SWITCH*#configure terminal*

L2SWITCH(config)*#interface eth0*

L2SWITCH(config-if)*#management host 192.168.200.106*

11.3.2.2 MAC Management

Table 123: CLI “MAC Management” Configuration

Node	Command	Description
enable	show mac-address-table aging-time	This command displays the current “Age Time” for the MAC address table.
enable	show mac-address-table (static|dynamic)	This command displays the current static/dynamic unicast address entries.
enable	show mac-address-table mac MACADDR	This command displays information on a specific MAC address table.
enable	show mac-address-table port PORT_ID	This command displays the current unicast address entries recognized by the specific port.
configure	mac-address-table static MACADDR vlan VLANID port PORT_ID	This command configures a static unicast entry.
configure	no mac-address-table static MACADDR vlan VLANID	This command deletes a static unicast entry from the address table.
configure	mac-address-table aging-time VALUE	This command configures the MAC table “Age Time.”
configure	clear mac address-table dynamic	This command deletes the dynamic address entries.

Example

L2SWITCH(config)*#mac-address-table static 00:11:22:33:44:55 vlan 1 port 1*

11.3.2.3 Blackhole MAC

Table 124: CLI “Blackhole MAC” Configuration

Node	Command	Description
enable	show mac-address-table refusal	This command displays the current rejected MAC address only.
configure	mac-address-table refusal MACADDR vlan VLANID	This command configures the rejection of a MAC address in a specific VLAN.
configure	mac-address-table refusal MACADDR	This command configures the rejection of a MAC address.

Example

L2SWITCH(config)*#mac-address-table refusal 00:11:22:33:44:55*

L2SWITCH(config)*#mac-address-table refusal 00:11:22:33:44:55 vlan 1*

11.3.2.4 Port Mirroring

Table 125: CLI “Port Mirroring” Configuration

Node	Command	Description
enable	show mirror	This command displays the current “Port Mirroring” configurations.
configure	mirror (disable|enable)	This command disables/enables “Port Mirroring” on the switch.
configure	mirror destination port PORT_ID	This command specifies the monitor port for the “Port Mirroring.”
configure	mirror source ports PORT_LIST mode (both|ingress|egress)	This command adds a port or port range as the source port(s) for the “Port Mirroring.”
configure	no mirror source ports PORT_LIST	This command removes a port or port range as the source port(s) for the “Port Mirroring.”

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*mirror enable*

L2SWITCH(config)#*mirror destination port 2*

L2SWITCH(config)#*mirror source ports 3-11 mode both*

11.3.3 Port Settings

Table 126: CLI “Port Settings” Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
configure	interface IFNAME	This command is used to enter the “interface configure node.”
interface	Show	This command displays the current port configurations.
interface	loopback (none | phy)	This command specifies the “Loopback” mode for a specific port.
interface	flowcontrol (off | on)	This command disables/enables “Flow Control” for a port.
interface	speed (auto|10-full||10-half100-full|100-half)	This command configures the speed and duplex mode for a port.
interface	shutdown	This command disables a specific port.
interface	no shutdown	This command enables a specific port.
interface	description STRINGs	This command configures a description for the respective port.
interface	no description	This command is used to configure the standard description of the port.
interface	cable test	This command performs diagnostics on the ETHERNET cable and displays the cable break.
interface	clean cable-test result	This command deletes the ETHERNET cable test results.
interface	show cable-test result	This command displays the ETHERNET cable test results.
configure	interface range gigabitethernet1/0/PORTLISTS	This command is used to enter the interface configure node.
if-range	description STRINGs	This command configures a description for the specific port.
if-range	no description	This command is used to configure the standard port description for the individual ports.
if-range	shutdown	This command disables specific ports.
if-range	no shutdown	This command enables specific ports.
if-range	speed (auto|10-full||10-half| 100-full|100-half|1000-full)	This command configures the speed and duplex for the port.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*interface fa1/0/1*

L2SWITCH(config-if)#*speed auto*

11.3.3.1 Advanced Settings

11.3.3.1.1 Bandwidth Control

11.3.3.1.2 QoS

Table 127: CLI “QoS” Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the “Service Queue.”
enable	show qos mode	This command displays the current IEEE 802.1p QoS mode.
configure	queue cos-map PRIORITY QUEUE_ID	This command configures the 802.1p priority mapping of the “Service Queue.”
configure	no queue cos-map	This command configures the default settings for the 802.1p priority mapping of the “Service Queue.”
configure	qos mode high-first	This command sets the QoS mode to “high_first” so every “Hardware Queue” transmits all packets in its buffer before permitting the next lower priority queue to transmit its packets.
configure	qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE	This command sets the QoS mode to “Weighted Round Robin.”
interface	default-priority	This command allows the user to specify which priority is assigned by default to the untagged packets received by the switch. The priority value entered with this command is used to determine which of the “Hardware Priority Queues” the packet is forwarded to (default value:0).
interface	no default-priority	This command sets the default priority for the specific port to 0.
enable	show diffserv	This command displays the DiffServ configurations.
configure	diffserv (disable|enable)	This command configures the DiffServ function.
configure	diffserv dscp VALUE priority VALUE	This command sets the associations between DSCP and IEEE 802.1q.

11.3.3.1.2.1 Rate Limitation

Table 128: CLI “Rate Limitation” Configuration

Node	Command	Description
enable	show bandwidth-limit	This command displays the current “Rate Limitation” configurations.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	This command enables bandwidth limitation for outgoing packets and sets the limit.
configure	no bandwidth-limit egress ports PORTLISTS	This command disables bandwidth limitation for outgoing packets.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	This command enables bandwidth limitation for incoming packets and sets the limit.
configure	no bandwidth-limit ingress ports PORTLISTS	This command disables bandwidth limitation for incoming packets.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*bandwidth-limit egress 1 ports 1-8*

L2SWITCH(config)#*bandwidth-limit ingress 1 ports 1-8*

11.3.3.2 Storm Control

Table 129: CLI “Storm Control” Configuration

Node	Command	Description
enable	show storm-control	This command displays the current “Storm Control” configurations.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command enables bandwidth limitation for broadcast, multicast or DLF packets and sets it for a specified type.
configure	no storm-control type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command disables bandwidth limitation for broadcast, multicast or DLF packets.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*storm-control rate 1 type broadcast ports 1-6*

L2SWITCH(config)#*storm-control rate 1 type multicast ports 1-6*

L2SWITCH(config)#*storm-control rate 1 type DLF ports 1-6*

11.3.3.2.1 IGMP Snooping

Table 130: CLI “IGMP Snooping” Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current “IGMP Snooping” configurations.
enable	show igmp-snooping counters	This command displays the current IGMP snooping counters.
enable	show igmp-snooping querier	This command displays the “IGMP Snooping Querier” function.
enable	show multicast	This command displays the multicast group in IP format.
configure	clear igmp-snooping counters	This command clears the IGMP snooping counters.
configure	igmp-snooping (disable | enable)	This command disables/enables “IGMP Snooping” on the switch.
configure	igmp-snooping vlan VLAN_ID	This command enables “IGMP Snooping” on a VLAN or VLAN range.
configure	no igmp-snooping vlan VLAN_ID	This command disables “IGMP Snooping” on a VLAN or VLAN range.
configure	igmp-snooping unknown-multicast (drop|flooding)	This command configures the process for unknown multicast packets when the “IGMP Snooping” function is enabled. drop: All unknown multicast packets are dropped.
configure	igmp-snooping report-suppression (disable|enable)	This command disables/enables the “IGMP Snooping Report Suppression” function on the switch.
configure	clear igmp-counters	This command clears the IGMP snooping counters.
configure	clear igmp-counters (port|vlan)	This command clears the IGMP snooping counters for the port or VLAN.
interface	igmp-querier-mode (auto | fixed | edge)	This command specifies whether the ports are “IGMP Query Ports” and, if so, under what conditions. The switch forwards the “IGMP Join/Leave” packets to an “IGMP Query Port,” treating the port as if it were connected to an IGMP multicast router (or server). “IGMP Snooping” must also be enabled (default: “Auto”).
interface	igmp-immediate-leave	The command enables the “Immediate Leave” function for “IGMP Snooping” for a specific interface.
interface	no igmp-immediate-leave	The command disables the “Immediate Leave” function for “IGMP Snooping” for a specific interface.
interface	igmp-snooping group-limit VALUE	This command configures maximum groups for the respective interface.
interface	no igmp-snooping group-limit	This command removes the restriction on the maximum groups for the specific interface.
configure	interface range gigabitethernet1/0/PORTLISTS	This command executes the node interface configuration.
if-range	igmp-immediate-leave	This command enabling the IGMP snooping function for immediately leaving the port.
if-range	no igmp-immediate-leave	This command disables the IGMP “Snooping immediate leave” function for the specific port.
if-range	igmp-snooping group-limit VALUE	This command configures the maximum groups for the individual ports.
if-range	no igmp-snooping group-limit	This command removes the restriction on the maximum groups for the individual ports.

Table 130: CLI “IGMP Snooping” Configuration

Node	Command	Description
if-range	igmp-querier-mode (auto|fixed|edge)	This command specifies whether and, if so, under what conditions the ports are IGMP query ports. The switch forwards IGMP Join or Leave packets to an IGMP query port, treating the port as if it were connected to an IGMP multicast router (or server). The “IGMP-Snooping” function must be enabled.

Example

L2SWITCH(config)*#igmp-snooping enable*

L2SWITCH(config)*#igmp-snooping vlan 1*

L2SWITCH(config)*#igmp-snooping querier enable*

L2SWITCH(config)*#igmp-snooping querier vlan 1*

L2SWITCH(config)*#interface 1/0/1*

L2SWITCH(config-if)*#igmp-immediate-leave*

L2SWITCH(config-if)*# igmp-querier-mode fixed*

L2SWITCH(config-if)*# igmp-snooping group-limit 20*

11.3.3.2.2 Multicast-Adresse

Table 131: CLI “Multicast Address” Configuration

Node	Command	Description
enable	show mac-address-table multicast	This command displays the current static/dynamic multicast address entries.
configure	mac-address-table multicast MACADDR vlan VLAN_ID ports PORTLIST	This command configures a static multicast entry.
configure	no mac-address-table multicast MACADDR	This command deletes a static multicast entry from the address table.

11.3.3.3 VLAN

11.3.3.4 Port Isolation

Table 132: CLI “Port Isolation” Configuration

Node	Command	Description
enable	show port-isolation	This command displays the current “Port Isolation” configurations. “V” indicates that the port’s packets can be sent to this port. “-” indicates that the port’s packets cannot be sent to this port.
interface	port-isolation ports PORTLISTS	This command configures a port or port range to forward data packets from a specific port.
interface	no port-isolation	This command configures all ports to forward data packets from a specific port.

Example

L2SWITCH(config)*#interface 1/0/2*

L2SWITCH(config-if)*#port-isolation ports 3-10*

11.3.3.4.1 VLAN Settings

Table 133: CLI “VLAN Settings” Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1–4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1–4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	name STRING	This command assigns a name to the specific VLAN. The VLAN name should be a combination of numbers, letters, hyphens (-) and underscores (_). The maximum length of the name is 16 characters.
vlan	no name	This command resets the VLAN name to the default setting. Note: The default VLAN name comprises the following: : “VLAN”+VLAN_ID, VLAN1, VLAN2, …
vlan	fixed PORT_LIST	This command assigns ports to a VLAN group as fixed subscribers.
vlan	no fixed	This command deletes all fixed ports from a VLAN.
vlan	tagged PORT_LIST	This command assigns fixed ports to a VLAN group as tagged subscribers. The port(s) should be a fixed subscriber of the VLAN group.
vlan	no tagged	This command deletes all tagged fixed ports from a VLAN.
vlan	untagged PORT_LIST	This command assigns fixed ports to a VLAN group as untagged subscribers. The port(s) should be a fixed subscriber of the VLAN group.
vlan	no untagged	This command deletes all untagged ports from a VLAN.
vlan	acceptable frame type (all | tagged | untagged)	This command configures the permissible frame type.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*vlan 2*

L2SWITCH(config-vlan)#*fixed 1*-6

L2SWITCH(config-vlan)#*untagged 1-3*

11.3.3.4.2 GARP/GVRP

Table 134: CLI “GARP/GVRP” Configuration

Node	Command	Description
enable	show gvrp configuration	This command displays the GVRP configurations.
enable	show gvrp statistics	This command displays the GVRP configurations for one port or all ports.
enable	show garp timer	This command displays the timers for GARP.
configure	gvrp (disable | enable)	This command disables/enables GVRP on the switch.
configure	no gvrp configuration	This command resets the GVRP configuration to the default setting.
interface	gvrp (disable | enable)	This command disables/enables GVRP on a specific port.
interface	gvrp registration (normal | forbidden)	This command configures the registration mode for GVRP on a specific port.
interface	no gvrp configuration	This command resets the GVRP configuration for a specific port to the default setting.
interface	garp join-time VALUE leave-time VALUE leaveall-time VALUE	This command configures the “Join Time,” “Leave Time” and “Leaveall Time” for GVRP on a specific port.
interface	no garp time	This command resets the Join, Leave and Leaveall times for GVRP on a specific port to the default settings.

11.3.3.4.3 Q-in-Q

11.3.3.5 VLAN-Stacking

Table 135: CLI “VLAN Stacking” Configuration

Node	Command	Description
enable	show vlan-stacking	This command displays the current “VLAN Stacking” type.
enable	show vlan-stacking selective-qinq	This command displays the selective Q-in-Q configurations.
enable	show vlan-stacking portbased-qinq	This command displays the port-based Q-in-Q configurations.
enable	show vlan-stacking tpid-inform	This command displays the TPID configurations.
config	vlan-stacking (disable | port-based | selective)	This command disables “VLAN Stacking” or enables port-based or selective “VLAN Stacking” on the switch.
config	vlan-stacking selective-qinq STRINGS	This command creates a selective Q-in-Q profile by name.
config	no vlan-stacking selective-qinq STRINGS	This command deletes a selective Q-in-Q profile by name.
config	vlan-stacking tpid-table index <2-6> value STRINGS	This command configures the TPID table.
interface	vlan-stacking port-based priority <0–7>	This command sets the priority in the port based Q-in-Q.
interface	vlan-stacking port-based role (tunnel | access | normal)	This command sets the “VLAN Stacking” port role.
interface	vlan-stacking port-based spvid <1–4096>	This command sets the service provider VID of the specified port.
interface	vlan-stacking tunnel-tpid index <1-6>	This command sets the TPID for a “Q-in-Q Tunnel Port.”
qinq	active	This command enables the selective Q-in-Q profile.
qinq	inactive	This command disables the selective Q-in-Q profile.
qinq	cvid VLANID	This command specifies the service provider’s VLAN range for incoming packets.
qinq	spvid VLANID	This command specifies the service provider’s VLAN range for outgoing packets in the selective Q-in-Q.
qinq	priority <0–7>	This command sets the priority in the selective Q-in-Q.
qinq	access-ports PORTLISTS	This command specifies the “Access Ports” that should apply the rules.
qinq	tunnel-ports PORTLISTS	This command specifies the “Tunnel Ports” that should apply the rules.
qinq	end	The command exits the “CLI Q-in-Q” node and enables the “CLI enable” node.
qinq	exit	The command exits the “CLI Q-in-Q” node and enables the “CLI configure” node.
qinq	show	The command displays the current configurations of the Q-in-Q profile.

11.3.3.6 LLDP

Table 136: CLI “LLDP” Configuration

Node	Command	Description
enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all information of port neighbors.
configure	lldp (disable | enable)	This command globally enables/disables the LLDP function on the switch.
configure	lldp tx-interval	This command configures the transmission interval for LLDP packets.
configure	lldp tx-hold	This command configures the “tx-Hold Time” that determines the TTL of the switch message (TTL = tx-hold * tx-interval).
interface	lldp-agent (disable | enable | rx-only | tx-only)	This command configures the Agent function for LLDP. “disable”: LLDP is disabled for a specific port. “enable”: The LLDP packet is transmitted from a specific port and received. “tx-only”:The LLDP packet is only transmitted from a specific port. “rx-only”: The LLDP packet is only received on a specific port.

11.3.3.7 Loop Detection

Table 137: CLI “Loop Detection” Configuration

Node	Command	Description
enable	show loop-detection	This command displays the current configuration for “Loop Detection.”
configure	loop-detection (disable | enable)	This command disables/enables “Loop Detection” on the switch.
configure	loop-detection address MACADDR	This command configures the destination MAC address for special “Loop Detection” packets.
configure	no loop-detection address	This command resets the destination MAC address to the default setting (00:0b:04:AA:AA:AB).
interface	loop-detection (disable | enable)	This command disables/enables “Loop Detection” for a specific port.
interface	no shutdown	This command enables a specific port. The command can enable a port blocked by “Loop Detection.”
interface	loop-detection recovery (disable | enable)	This command enables/disables the “Recovery” function on a port.
interface	loop-detection recovery time VALUE	This command configures the “Recovery Time” period.

Example

L2SWITCH(config)#*loop-detection enable*

L2SWITCH(config)#*interface 1/0/1*

L2SWITCH(config-if)#*loop-detection enable*

L2SWITCH(config-if)#*loop-detection recovery enable*

L2SWITCH(config-if)#*loop-detection recovery time 10*

11.3.3.8 STP

Table 138: CLI “STP” Configuration

Node	Command	Description
enable	show spanning-tree active	This command only displays STP information for active ports.
enable	show spanning-tree blockedports	This command only displays STP information for blocked ports.
enable	show spanning-tree port detail PORT_ID	This command displays STP information for the interface port.
enable	show spanning-tree statistics PORT_ID	This command displays STP information for the interface port.
enable	show spanning-tree summary	This command displays a summary of port states and configurations.
enable	clear spanning-tree counters	This command clears the STP statistics for all ports.
enable	clear spanning-tree counters PORT_ID	This command clears the STP statistics for a specific port.
configure	spanning-tree (disable | enable)	This command disables/enables the STP function in the system.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	This command configures the bridge times (“Forward Delay,” “Max Age” and “Hello Time”).
configure	no spanning-tree algorithm-timer	This command configures the default values for “Forward Delay,” “Max Age” and “Hello Time.”
configure	spanning-tree forward-time <4–30>	This command configures the “Forward Delay” period (in seconds) for the bridge.
configure	no spanning-tree forward-time	This command configures the default values for “Forward Delay.”
configure	spanning-tree hello-time <1–10>	This command configures the “Hello Time” period (in seconds) for the bridge.
configure	no spanning-tree hello-time	This command configures the default values for the “Hello Time.”
configure	spanning-tree max-age <6-40>	This command configures the “Max Age” period (in seconds) for bridge messages.
configure	no spanning-tree max-age	This command configures the default values for the “Max Age.”
configure	spanning-tree mode (rstp | stp)	This command configures the STP mode.
configure	spanning-tree pathcost method (short | long)	This command configures the path cost method.
configure	spanning-tree priority <0-61440>	This command configures the priority for the system.
configure	no spanning-tree priority	This command configures the default values for the system priority.
interface	spanning-tree bpdufilter (disable | enable)	This command configures enables/disables the “BPDU Filter” function.
interface	spanning-tree bpduguard (disable | enable)	This command configures enables/disables the “BPDU Guard” function.
interface	spanning-tree edge-port (disable | enable)	This command enables/disables the “Edge Port” setting.

Table 138: CLI “STP” Configuration

Node	Command	Description
interface	spanning-tree cost VALUE	This command configures the costs for the specific port. Cost range: 16-bit-based value range from 1 to 65,535, 32-bit-based value range from 1 to 200,000,000.
interface	no spanning-tree cost	This command sets the path cost of the specific port to the default value.
interface	spanning-tree port-priority <0-240>	This command configures the priority for the specific port (default value: 128).
interface	no spanning-tree port-priority	This command sets the priority of the specific port to the default value.

11.3.4 Security

11.3.4.1 Access Control List

Table 139: CLI “Access Control List” Configuration

Node	Command	Description
enable	show access-list	This command displays all access control profiles.
configure	access-list STRING	This command creates a new access control profile, where “STRING” is the profile name.
configure	no access-list STRING	This command deletes an access control profile.
acl	show	This command displays the current access control profile.
acl	action (disable | drop | permit)	This command processes the profile. “disable”: The profile is disabled. “drop”: If packets match the profile, they are dropped. “permit”: If packets match the profile, they are forwarded.
acl	destination mac host MACADDR	This command configures the destination MAC address and the mask for the profile.
acl	destination mac MACADDR	This command configures the destination MAC address and the mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC address and the mask for the profile. The second “MACADDR” parameter is the mask (e.g., ffff.ffff.0000) for the profile.
acl	no destination mac	This command deletes the destination MAC address from the profile.
acl	ethertype STRING	This command configures the ETHERNET type for the profile, where the “STRING” is a hexadecimal value, e.g., 08AA.
acl	no ethertype	This command deletes the ETHERNET type limit from the profile.
acl	source mac host MACADDR	This command configures the source MAC address and the mask for the profile.
acl	source mac MACADDR MACADDR	This command configures the source MAC address and the mask for the profile.
acl	no source mac	This command deletes the source MAC and the mask from the profile.
acl	source ip host IPADDR	This command configures the source IP address for the profile.
acl	source ip IPADDR IPMASK	This command configures the source IP address and the mask for the profile.
acl	no source ip	This command deletes the source IP address from the profile.
acl	destination ip host IPADDR	This command configures a specific destination IP address for the profile.
acl	destination ip IPADDR IPMASK	This command configures the destination IP address and the mask for the profile.
acl	no destination ip	This command deletes the destination IP address from the profile.
acl	l4-source-port IPADDR	This command configures the UDP/TCP source port for the profile.
acl	no l4-source-port IPADDR	This command removes the UDP/TCP source port from the profile.

Table 139: CLI “Access Control List” Configuration

Node	Command	Description
acl	L4-destination-port PORT	This command configures the UDP/TCP destination port for the profile.
acl	no l4-destination-port	This command removes the UDP/TCP destination port from the profile.
acl	vlan VLANID	This command configures the VLAN for the profile.
acl	no vlan	This command deletes the VLAN limit from the profile.
acl	source interface PORT_ID	This command configures the source interface for the profile.
acl	no source interface PORT_ID	This command deletes the source interface from the profile.

11.3.5 Monitor

11.3.5.1 Alarm

Table 140: CLI “Alarm” Configuration

Node	Command	Description
enable	show alarm-info	This command displays alarm information.

11.3.5.2 Monitor Information

Table 141: CLI “Monitor Information” Configuration

Node	Command	Description
enable	show hardware-monitor (C|F)	This command displays hardware operation information.

11.3.5.3 RMON Statistics

Table 142: CLI “RMON Statistics” Configuration

Node	Command	Description
enable	show rmon statistics	This command displays the RMON statistics.
configure	clear rmon statistics [IFNAME]	This command clears the RMON statistics for one or all ports.

11.3.5.4 SFP Information

Table 143: CLI “SFP Information” Configuration

Node	Command	Description
enable	show sfp info port PORT_ID	This command displays the SFP information.
enable	show sfp ddmi port PORT_ID	This command displays the SFP DDMI status.

11.3.5.5 Traffic Monitor

Table 144: CLI “Traffic Monitor” Configuration

Node	Command	Description
enable	show traffic-monitor	This command displays the “Traffic Monitor” configurations and current status.
configure	traffic-monitor (disable | enable)	This command enables/disables the “Traffic Monitor” on the switch.
interface	traffic-monitor rate RATE_LIMIT type (bcast | mcast | bcast+mcast)	This command configures the packet rate and type for the “Traffic Monitor” on a specific port. mcast: broadcast packet mcast: multicast packet The rate should be greater than 50 pps.
interface	traffic-monitor (disable | enable)	This command enables/disables the “Traffic Monitor” on a specific port.
interface	traffic-monitor recovery (disable | enable)	This command enables/disables the “Recover” function of the “Traffic Monitor” on a specific port.
interface	traffic-monitor recovery time VALUE	This command configures the “Recovery Time” of the “Traffic Monitor” on a specific port.

11.3.5.6 Management

11.3.5.7 SNMP

Table 145: CLI “SNMP” Configuration

Node	Command	Description
enable	show snmp	This command displays the SNMP configurations.
configure	snmp community STRING (ro | rw) trusted-host IPADDR	This command configures the “SNMP Community” name.
configure	snmp (disable | enable)	This command disables/enables SNMP on the switch.
configure	snmp system-contact STRING	This command configures contact information for the system.
configure	snmp system-location STRING	This command configures the location information for the system.
configure	snmp system-name STRING	This command assigns a name to the system.
configure	snmp trap-receiver IPADDR VERSION COMMUNITY	This command sets up the trap receiver’s configurations, including the IP address, version (v1 or v2c) and “Community.”

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*snmp enable*

L2SWITCH(config)#*snmp community public rw trusted-host 192.168.200.106/24*

L2SWITCH(config)#*snmp trap-receiver 192.168.200.106 v2c public*

L2SWITCH(config)#*snmp system-contact IT engineer*

L2SWITCH(config)#*snmp system-location Wago*

11.3.6 Auto Provision

Table 146: CLI “Auto Provision” Configuration

Node	Command	Description
auto-provision	show	This command displays the current configurations for the “Auto Provision.”
auto-provision	active (enable | disable)	This command enables/disables the “Auto Provision” function.
auto-provision	server-address IPADDR	This command sets the IP address of the server for the “Auto Provision.”
auto-provision	protocol (tftp | http | ftp)	The command configures the update protocol.
auto-provision	FTP-user username STRING password STRING	The command configures the username and password for the FTP server.
auto-provision	folder STRING	The command sets the folder for the “Auto Provision” server.
auto-provision	version <0-65535>	The command configures the version for “Auto Provision” of the switch.
auto-provision	no folder	The command resets the folder to the default setting.
auto-provision	no FTP-user	The command resets the username and password to default setting.

11.3.6.1 Mail Alarm

Table 147: CLI “Mail Alarm” Configuration

Node	Command	Description
enable	show mail-alarm	This command displays the “Mail Alarm” configurations.
configure	mail-alarm (disable | enable)	This command disables/enables the “Mail Alarm” function.
configure	mail-alarm mail-from	This command configures the email sender.
configure	mail-alarm mail-to	This command configures the email receiver.
configure	mail-alarm server-ip IPADDR server-port VALUE	This command configures the IP address and TCP port for the mail server.
configure	mail-alarm server-ip IPADDR server-port Default	This command configures the IP address of the mail server and sets its TCP port to 25.
configure	mail-alarm trap-event (reboot | link-change | config. | firmware | login | port-blocked) (disable|enable)	This command disables/enables mail trap events.

11.3.6.1.1 Maintenance

Table 148: CLI “Maintenance” Configuration

Node	Command	Description
configure	reboot	This command reboots the system.
configure	reload default-config	This command resets the system configuration to the default settings. Note: The system automatically reboots to apply the configurations.
configure	write memory	This command writes the current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	This command downloads an updated configuration file from the TFTP server, where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	This command uploads the current configurations file to the TFTP server.
configure	archive download-fw <URL PATH>	This command downloads an updated firmware file from the TFTP server, where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*interface eth0*

L2SWITCH(config-if)#*ip address 172.20.1.101/24*

L2SWITCH(config-if)#*ip address default-gateway 172.20.1.1*

L2SWITCH(config-if)#*management vlan 1*

11.3.6.1.2 System Log

Table 149: CLI “System Log” Configuration

Node	Command	Description
enable	show syslog	The command displays all log messages recorded in the switch.
enable	show syslog level LEVEL	This command displays the log messages with the “LEVEL” recorded in the switch.
enable	show syslog server	The command displays the syslog server configurations.
configure	syslog (disable | enable)	The command disables/enables the syslog function.
configure	syslog ip IPADDR	The command configures the IP address of the syslog server.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*syslog-server ip 192.168.200.106*

L2SWITCH(config)#*syslog-server enable*

11.3.6.1.2.1 USB Functions

Table 150: CLI “USB Functions” Configuration

Node	Command	Description
enable	show usb status	This command displays the current USB function configurations.
configure	usb auto-upgrade-fw (disable|enable)	This command automatically disables/enables the USB firmware upgrade.
configure	usb auto-download-config (disable|enable)	This command automatically disables/enables the configuration file for the USB download.
configure	usb auto-download-syslog (disable|enable)	This command disables/enables the USB download syslog file.

Example

L2SWITCH#*show usb status*

USB auto upgrade firmware State : Enabled

USB auto download config State : Enabled

USB auto download syslog State : Enabled

L2SWITCH#*configure terminal*

L2SWITCH(config)#*usb auto-upgrade-fw enable*

L2SWITCH(config)#*usb auto-download-config enable*

L2SWITCH(config)# *usb auto-download-syslog enable*

11.3.6.1.3 User Account

Table 151: CLI “System Log” Configuration

Node	Command	Description
enable	show user account	This command displays the current user accounts.
configure	add user USER_ACCOUNT PASSWORD (normal | admin)	This command adds a new user account.
configure	delete user USER_ACCOUNT	The command deletes an existing user account.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)*#add user q admin*

L2SWITCH(config)*#add user 1 1 normal*

List of Figures

List of Tables

WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 • D - 32385 Minden
Hansastraße 27 • D - 32423 Minden
Phone: +49 571 887 – 0
Fax: +49 571 887 – 844169
E-Mail: info@wago.com
Internet: www.wago.com