TECHDOCS

Manual

WAGO Industrial Switches

852-1812

Lean Managed Switch

8 Ports 1000BASE-T

Version 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 “Lean Managed Switch” (852-1812).

1.2 Copyright

This Manual, including all figures and illustrations, is copyright-protected. Any further use of this Manual by third parties that violate pertinent copyright provisions is prohibited. Reproduction, translation, electronic and phototechnical filing/archiving (e.g., photocopying) as well as any amendments require the written consent of WAGO Kontakttechnik GmbH & Co. KG, Minden, Germany. Non-observance will involve the right to assert damage claims.

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.
- 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 Lean Managed Switch with CAGE CLAMP® connection (Item. No. 2231-103/026-000)
- Protective covers for unused ports
- Operating and Assembly instructions

3.2 Industrial ETHERNET Technology

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

- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX/FX
- IEEE 802.3ab 1000BASE-T Ethernet
- IEEE 802.3x Flow Control
- IEEE 802.1d Spanning Tree Protocol (STP)
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- IEEE 802.1Q VLAN Tagging
- IEEE 802.1p Prioritization
- IEEE 802.1x Port Authentication
- IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
- IEEE 802.1AB LLDP-MED
- IEEE 802.3az Energy Efficient Ethernet (EEE)
- ITU-T G8032v1/v2 Ethernet Ring Protection Switching (ERPS)

The switches have a power supply with a supply voltage range of 24 … 48 V.

Features such as autonegotiation and auto MDI/MDIX (crossover) on all 10/100/1000 BASE-T ports are also implemented.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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 852-1812 is a configurable industrial ETHERNET switch with eight 10/100/1000BASE-T ports.
Enclosed in a rugged housing, this switch offers both a redundant power supply and relay-based function monitoring. This device also streamlines network management: Commissioning and diagnostics are intuitive and can be performed without extensive IT knowledge.
The topology map clearly displays the switch and connected devices. Key diagnostic information is displayed on the diagnostics dashboard.

The following functions increase the robustness, availability and security of the network:

Security:

- Network segmentation per IEEE802.1Q (max. 5 VLANs),
- authentication of network participants per IEEE802.1X,
- firewall functions using access-control list (max. 32 entries)
- service control,
- port security

Availability:

- Rapid Spanning Tree Protocol (RSTP) for meshed and ring networks,
- ETHERNET Ring Protection Switching (ERPS) for up to two rings per switch,
- loop detection and
- storm control on each port

Configuration/Diagnostics/Maintenance:

- Port mirroring,
- Modbus® registers,
- SNMP v3,
- SNMP trap events,
- alarm threshold,
- port statistics,
- backup and restore,
- system log,
- syslog server,
- command line interface with SSH/Telnet,
- topology map and
- dashboard

4.1 View

4.1.1 Front View

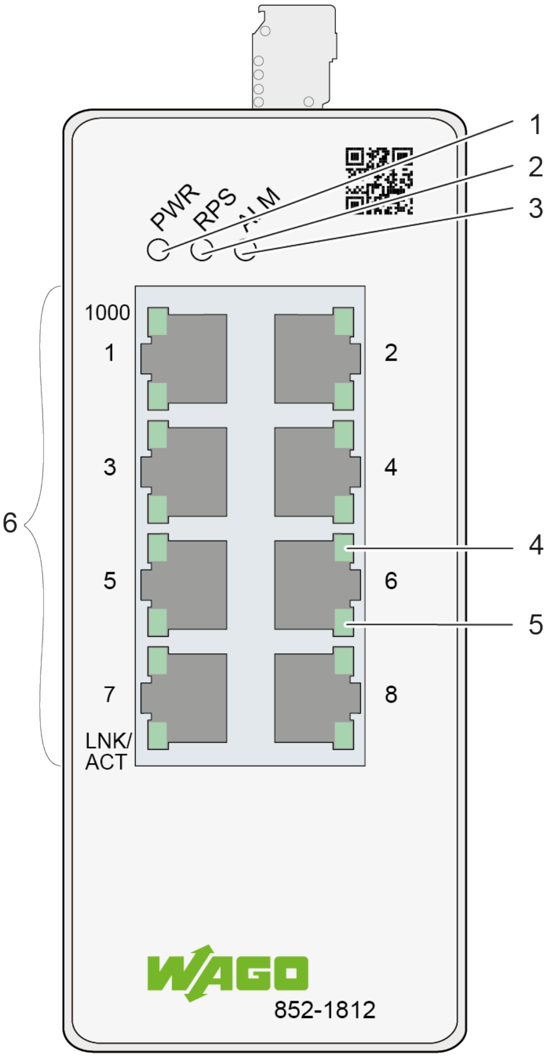


Figure 1: Front View of the Lean Managed Switch

Table 3: Legend for the Figure “Front View of the Lean Managed Switch”

Pos.	Description	Meaning	For Details, see Section
1	PWR	Status LED, supply voltage	“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	-	Status LED TX port 1000 Mbit/s (1 LED for each port)	“Device Description” > “Display Elements”
5	-	Status LED TX port LNK/ACT (1 LED for each port)	“Device Description” > “Display Elements”
6	-	Port RJ-45 (10/100M/1000BASE-T) (8)	“Device Description” > “Connections”

4.1.2 Top View

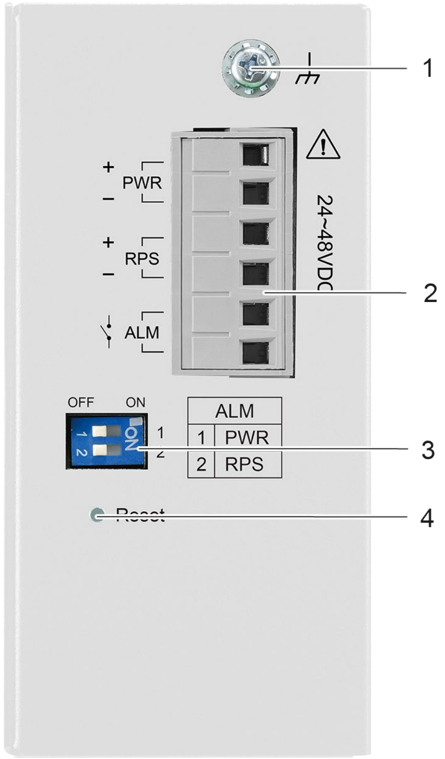


Figure 2: Top View of the Lean Managed Switch

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

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

4.2 Connectors

4.2.1 Grounding screw

The switch must be grounded.
Connect the grounding screw to the ground potential.
Do not operate the switch without an appropriately installed protective earth conductor.

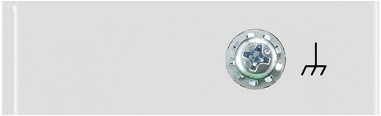


Figure 3: Grounding screw

4.2.2 Power Supply (PWR/RPS)

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

The male connector shows the following pin assignment:

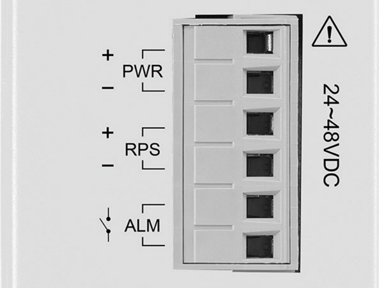


Figure 4: Power Supply (PWR/RPS)

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

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

NOTICE

Warning: Damage to property caused by electrostatic discharge (ESD)!
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.

4.2.3 Network Connections

The Lean Managed Switch uses ports with copper connectors and supports ETHERNET and/or Fast ETHERNET.

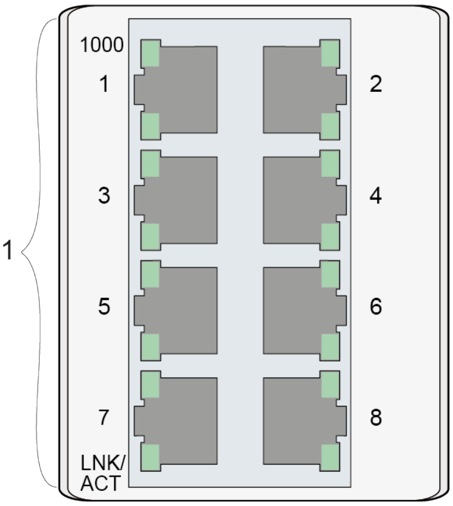


Figure 5: Network Connections

Table 6: Legend for Figure “Network Connections”

No.	Desig- nation	Meaning	For Details, see Section:
1	-	8 RJ-45 connections (10/100/1000BASE-T)	“Device Description” > … “10/100/1000BASE-T Ports”

4.2.3.1 RJ45 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).

4.2.3.2 10/100/1000BASE-T-Ports

The 10/100/1000BASE-T ports support networks speeds of 10 Mbit/s, 100 Mbit/s and 1000 Mbit/s and can be operated in half- and full-duplex transmission modes. These ports also provide automatic crossover detection (Auto-MDI/MDI-X), with plug-and-play capabilities. Simply plug the network cables into the ports; they then adapt to the end node devices. We recommend the following cable for the RJ-45 ports:

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

4.3 Display Elements

The Lean Managed Switch is equipped with device LEDs and port LEDs. You can see the status quickly with the device LEDs, while the port LEDs provide information about connection actions.

4.3.1 Device LEDs

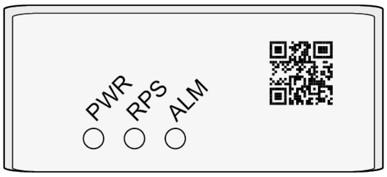


Figure 6: Device LEDs

Table 7: Legend for “Device LEDs” Figure

LED	Name	Status	Description
PWR	Primary Power LED	Green	Use the primary power supply.
		Off	Primary power off or failure.
RPS	Redundant Power System LED	Green	Use the redundant power supply.
		Off	Redundant power off or failure.
ALM	Alarm LED	Red	Failure of a port connection; miscellaneous alarm.
		Off	No alarm to report.

4.3.2 Port LEDs

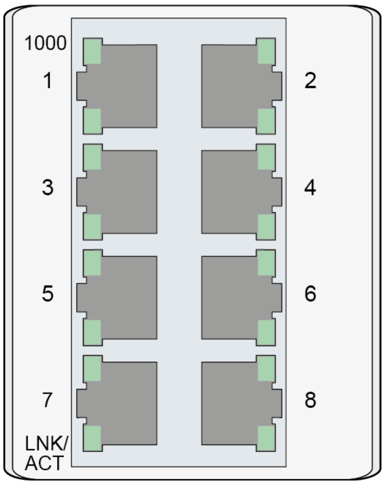


Figure 7: Port LEDs

Table 8: Legend for “Port LEDs” Figure

LED	Name	Status	Description
1000	1000BASE T-Ports LED (1 LED for each port)	Green	1000 Mbit/s connection in operation.
		Off	Port disconnected or link failed.
LNK/ACT	10/100BASE T-Ports LED (1 LED for each port)	Green	10/100/1000 Mbit/s connection in operation.
		Flashes	Data traffic via connection.
		Off	Port disconnected or link failed.

4.4 Operating elements

4.4.1 DIP Switches

There is a DIP switch for alarm configuration on the top of the Lean Managed Switch. When the alarm reporting function is active, the alarm contact is switched when an alarm event occurs.

The meaning of the DIP switch settings are described below:

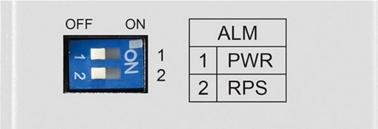


Figure 8: DIP Switches

Table 9: Legend for Figure "DIP Switches"

No.	Name	Status	Description
1	PWR	ON	The alarm reporting function for the primary power supply is activated.
		OFF	The alarm reporting function for the primary power supply is deactivated.
2	RPS	ON	The alarm reporting function for the secondary power supply is activated.
		OFF	The alarm reporting function for the secondary power supply is deactivated.

The user can manually switch the alarm function for the primary or redundant power supply on and off through the DIP switches.

The DIP switch must be "ON" to activate the port alarm function. The default setting is "OFF".

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

1 Turn all DIP switches to "OFF".

2 Install the Lean Managed Switch in your network.

3 Select the port(s) to be monitored or the alarm to be activated.

4 Set the DIP switch of the corresponding port to "ON".

5 Turn the Lean Managed Switch ON.

4.4.2 Reset Button

Figure 9: Reset Button

Table 10: Legend for Figure “Reset Button”

Name	Status	Description
Reset	Press the Reset button for 2 seconds and release.	The system is restarted.
Delivery state	Press the Reset button for 10 seconds and release.	The system is reset to the switches factory default settings.

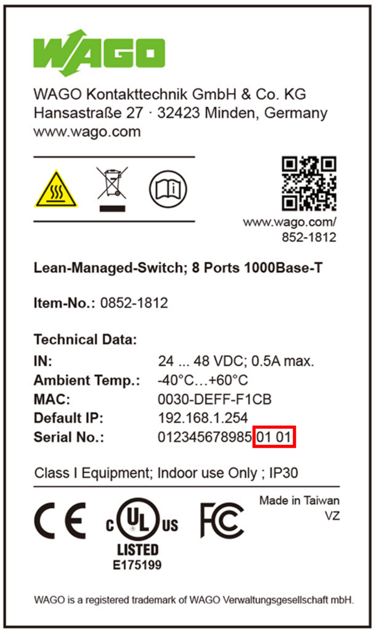
Note

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

4.5 Label

4.5.1 Hardware and Software Version

There is a label with the “MAC Address” and “Serial NO” on the back of the Lean Managed Switch.



WAGO Kontakttechnik GmbH & Co. KG
Hansastraße 27 · 32423 Minden, Germany
www.wago.com

www.wago.com/
852-1812

Lean-Managed-Switch; 8 Ports 1000Base-T

Item-No.: 0852-1812

Technical Data:
IN: 24 ... 48 VDC; 0.5A max.
Ambient Temp.: -40°C…+60°C
MAC: 0030-DEFF-F1CB
Default IP: 192.168.1.254
Serial No.: 012345678985 01 01

Class I Equipment; Indoor use Only ; IP30

Made in Taiwan
VZ

c UL us
LISTED
E175199

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Figure 10: Label

Table 11: Legend for Figure “Label”

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	116 mm (from the top edge of the carrier rail)
Depth	100 mm
Weight	550 g
Degree of protection	IP30

4.6.2 System Data

Table 13: Technical Data – System Data

MAC table	Up to 8000 addresses
VLAN	Port based and tag based (max. 5 VLANs)
Jumbo Frame Size	10 kB
Maximum lengths	10/100/ 1000BASE-TX: 100 m

4.6.3 Power Supply

Table 14: Technical Data – Power Supply

Supply voltage	24 … 48 VDC (± 15 %) 24 … 48 VDC (UL)

4.6.4 Communication

Table 15: Technical Data – Communication

Ports (copper; RJ-45)	8 x 10/100/1000BASE-T
Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/FX IEEE 802.3ab 1000BASE-T Ethernet IEEE 802.3x Flow Control IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1Q VLAN Tagging IEEE 802.1p Prioritization IEEE 802.1x Port Authentication IEEE 802.1ab Link Layer Discovery Protocol (LLDP) IEEE 802.1AB LLDP-MED IEEE 802.3az Energy Efficient Ethernet (EEE) ITU-T G8032v1/v2 Ethernet Ring Protection Switching (ERPS)

4.6.5 Environmental Conditions

Table 16: Technical Data – Environmental Conditions

Surrounding air temperature (operation)	-40 … +60 °C
Surrounding air temperature (storage)	-40 °C … +85 °C
UL 61010 Use Pollution degree	Indoor 2
Relative humidity (operation)	10 … 95 % (without condensation)
Relative humidity (storage)	5 … 95 % (without condensation)
Vibration resistance	Acc. IEC 60068-2-6
Shock resistance	Acc. IEC 60068-2-27
EMC-1 immunity to interference	EN 55024 IEC 61000-4-2 IEC 61000-4-3 IEC 61000-4-4 IEC 61000-4-5 IEC 61000-4-6 IEC 61000-4-8 EN 61000-6-2
EMC-1 Emission of interference	FCC Part 15 Subpart B Class A EN 55011: Class A EN 55032: Class A EN 61000-6-4

4.7 Approvals

The following approvals have been granted for the WAGO ETHERNET accessory product “Lean Managed Switch” (852-1812):

CE	Conformity Marking	
c UL us	Ordinary Locations	UL61010-2-201 (E175199)

5 Mounting

5.1 Installation Site

The location selected to install the Lean Managed Switch may greatly affect its performance. When selecting a site, we recommend considering the following rules:

- Install the Lean 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 Lean Managed Switch and ventilation around it is adequate. Do not place any heavy objects on the Lean Managed Switch.

5.2 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 Lean Managed Switch onto the DIN rail from the top and snap it into position.

5.3 Removal from Carrier Rail

To remove the Lean 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.

6 Connect Devices

6.1 Power Supply

The switch uses direct current power supply for 24 … 48 V.

The primary and secondary network link is established via a 6-pin plug-in connection located on the top of the Lean Managed Switch.

The female connector (Item No. 2231-106/026-000) is composed of six 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 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.

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.

6.2 External Alarm Contact Port

The Lean Managed Switch has an alarm contact connection 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)” (it is the same procedure).

You can connect the alarm circuit to any warning device already installed in the user's control room or factory floor. When a fault occurs, the Lean Managed Switch sends a signal through 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 PWR/RPS:
   a Power failure (power cord is disconnected, power supply malfunction, etc.)
   b Input power falls outside specification
   (24 … 48 V)

6.3 10/100/1000BASE-T Ports

The 10/100/1000BASE-T ports (RJ-45 ETHERNET ports) of the industrial 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 switch and the other end to the port of the selected network node.

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

7 Configuration

7.1 Overview of Configuration Options

The Lean Managed Switch provides three options for advanced management features:

7.1.1 Web Based Management

A menu-driven user interface can be called up from the WBM (“**W**eb **B**ased **M**anagement”) via the protocols “http” or “https”.

➔ **Note**

Standard setting
By default, the Lean Managed Switch is set to the "http" protocol.

➔ **Note**

Using Protocol “https”
If you use the protocol “https”, you must activated this service (see Section “Service Control”.).

➔ **Note**

Additional Information
Please refer to the section “Configuration in the Web Based Management” for a detailed description.

7.1.2 Telnet or SSH Connection

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

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

Table 17: Default Settings for the Telnet Port

Setting	Default Value
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Management VLAN	1
Default Username	admin
Default Password	wago

3. Make sure your computer IP address is in the same subnet, unless you are accessing the switch through one or more routers.

Note

Using Protocol “Telnet”
If you use the protocol “telnet”, you must activated this service (see Section “Configuration in the Web Based Management” > …> “Service Control”).

7.1.3 Access via Console Port (CLI)

The following describes how to view the device configuration using the command line interface.

1. Connect the computer over SSH or Telnet to the Command Line Interface (CLI) of the switch.

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

   ```
   L2SWITCH login:
   ```

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

   ```
   L2SWITCH login: admin
   L2SWITCH>
   ```

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

   ```
   L2SWITCH>enable
   user:admin
   password: wago
   ```

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

   ```
   L2SWITCH#show running-config
   ```

Note

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

8 Diagnostics

Diagnostic will help user and network administrators for quick reference, diagnosing and identifying problems within a system and network. It is a type of network management that helps in finding network connectivity, performance and other related problems in a dashboard.

Note

Changing the colors of the tiles when the threshold value changes
For easy diagnosis, you can set a change in the colors (red, yellow, green) of the tiles when the threshold values are exceeded or not reached (see Section "Dashboard Configuration".

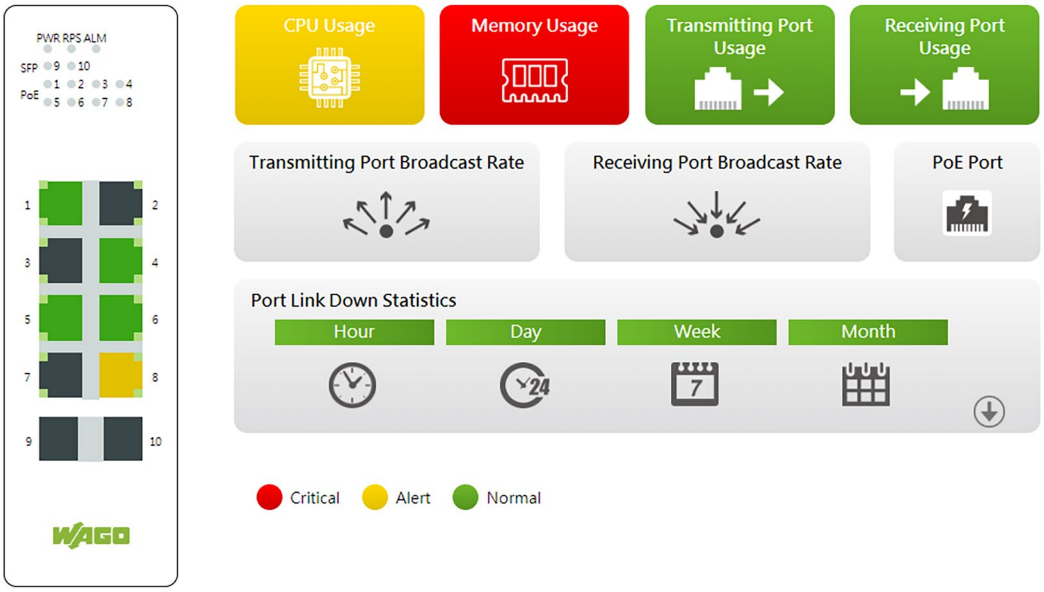


Figure 11: Dashboard - Example

8.1 Web Based Management for Diagnostic Function

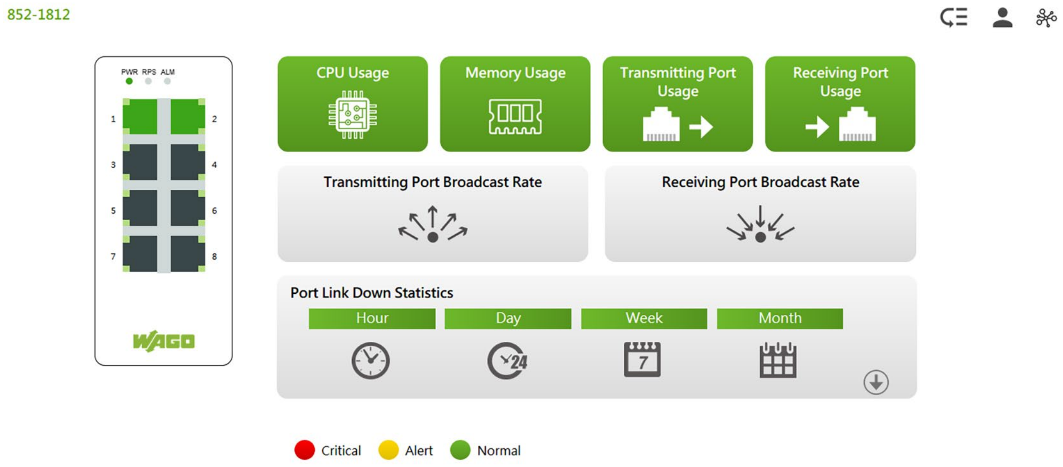


Figure 12: Dashboard

8.1.1 CPU Usage

User can get the switch CPU usage information in % by just one click shown below.

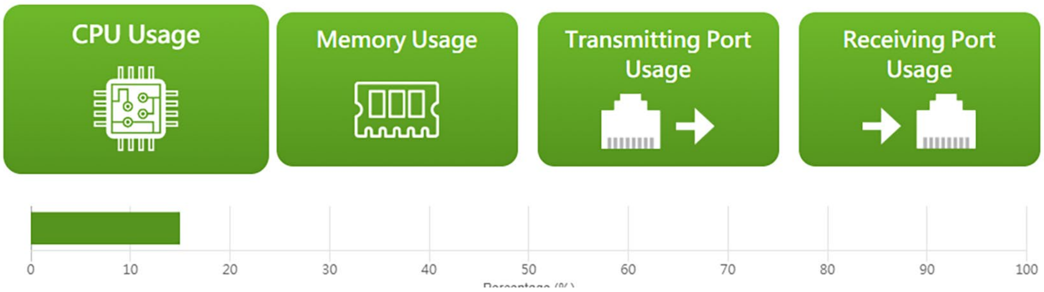


Figure 13: CPU Usage

8.1.2 Memory Usage

User can get the switch memory usage information in % by just one click shown below.

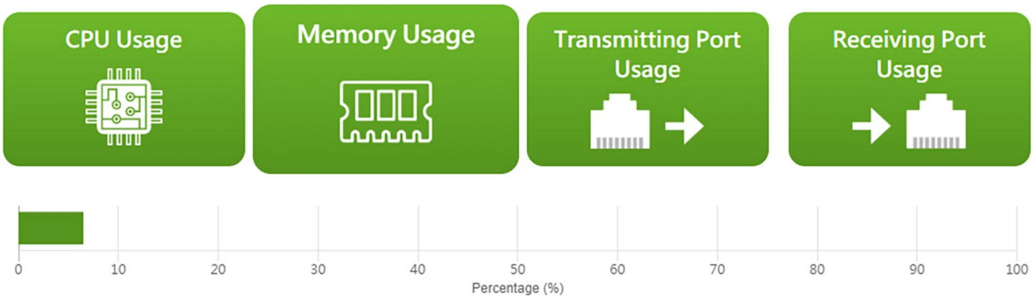


Figure 14: Memory Usage

8.1.3 Transmitting Port Usage

User can get the switch port Tx utilization information in % by just one click shown below.

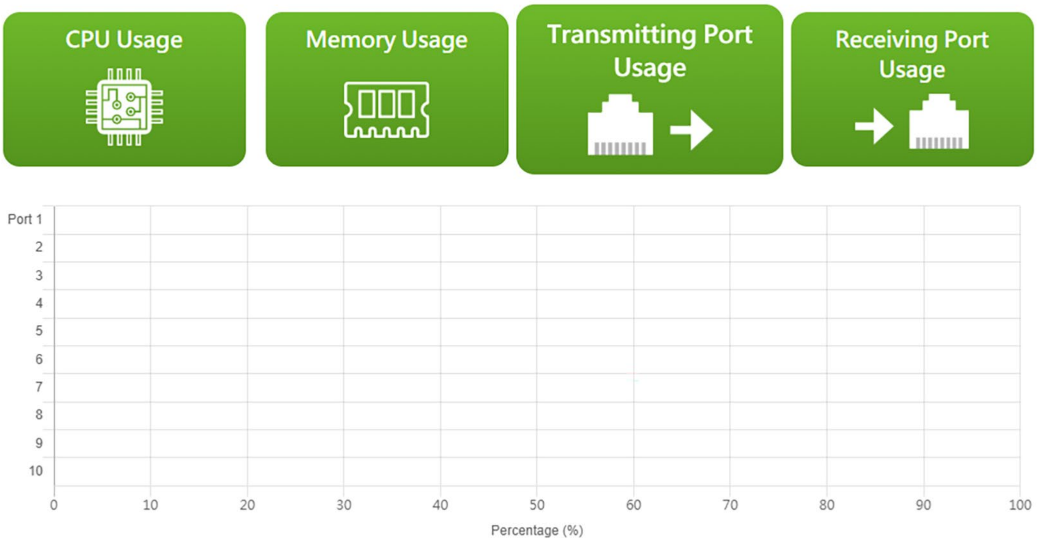


Figure 15: Transmitting Port Usage (Example)

8.1.4 Receiving Port Usage

User can get the switch port Rx utilization information in % by just one click shown below.

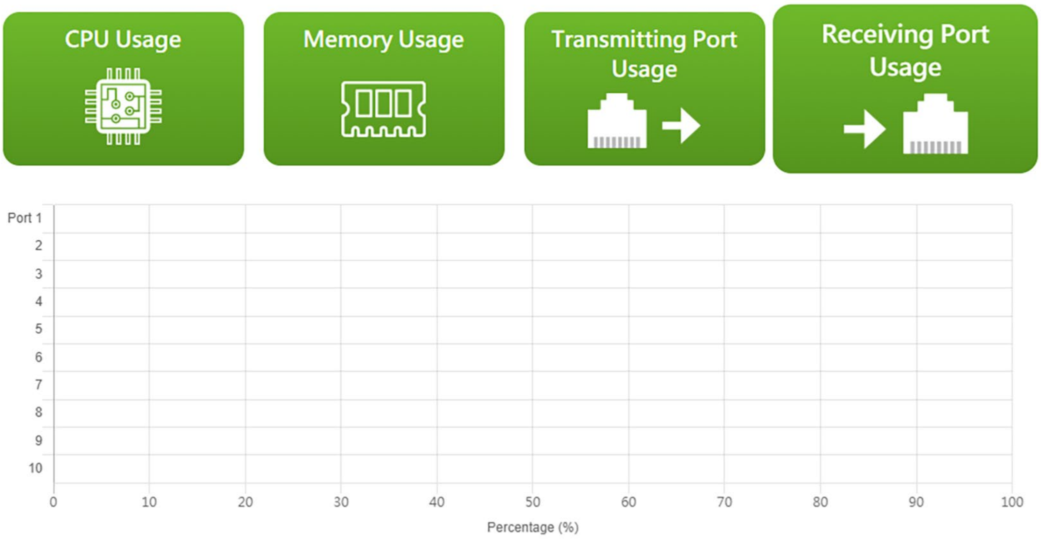


Figure 16: Receiving Port Usage (Example)

8.1.5 Transmitting Port Broadcast Rate

The user can get the Transmitting Port Broadcast Rate for every port.

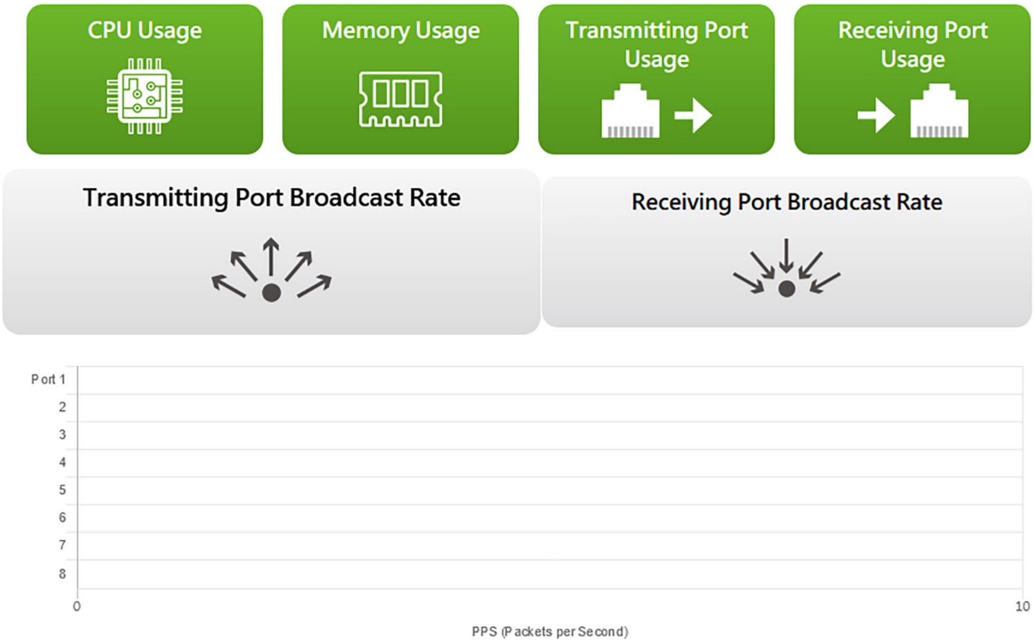


Figure 17: Transmitting Port Broadcast Rate (Example)

8.1.6 Receiving Port Broadcast Rate

The user can get the Receiving Port Broadcast Rate for every Port.

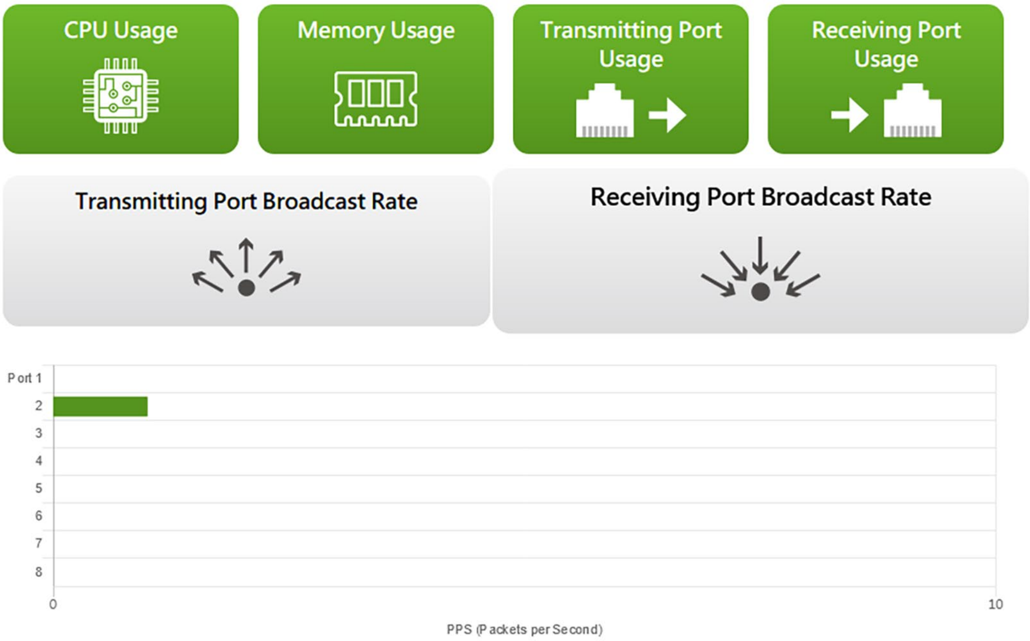
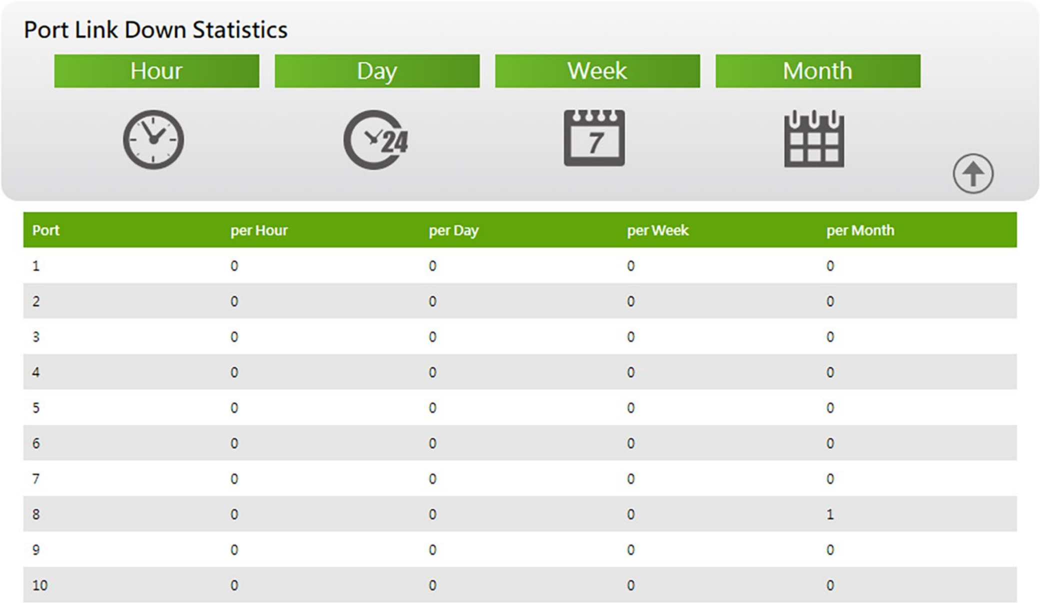


Figure 18: Receiving Port Broadcast Rate (Example)

8.1.7 Port Link Down Statistics

User can get the summary of the port link down statistics per hour, day, week and month wise information in just one click shown below.

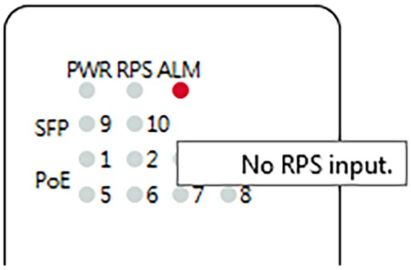


Port	per Hour	per Day	per Week	per Month
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	1
9	0	0	0	0
10	0	0	0	0

Figure 19: Port Link Down Statistics (Example)

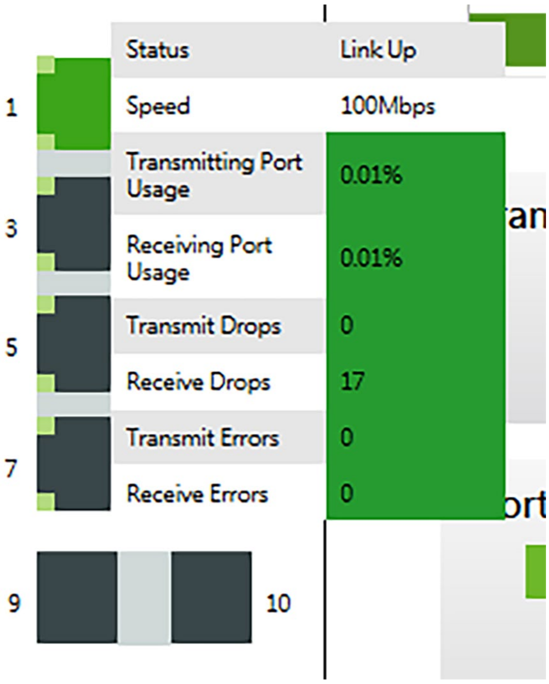
8.2 Mouse pointer

User can get the detailed information of the Alarm, Alert, utilization by just pointing the curser on specified as shown below.



No RPS input.

Figure 20: LED Information



Status	Link Up
Speed	100Mbps
Transmitting Port Usage	0.01%
Receiving Port Usage	0.01%
Transmit Drops	0
Receive Drops	17
Transmit Errors	0
Receive Errors	0

Figure 21: Port Information - Example

8.3 Collapse, User Login, Topology Map

Collapse option	is used for the user to get back to home in the dash board.
User Login option	is to login to the device for further configuration and maintenance.
Topology Map	will show the user about the connectivity.

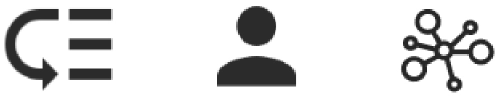
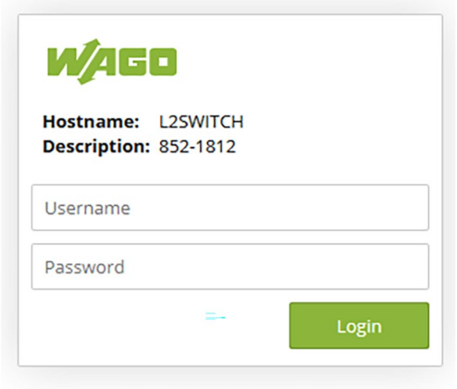


Figure 22: Collapse, User Login, Topology Map

Once user select login it will redirect to switch login window and below screen will appear.



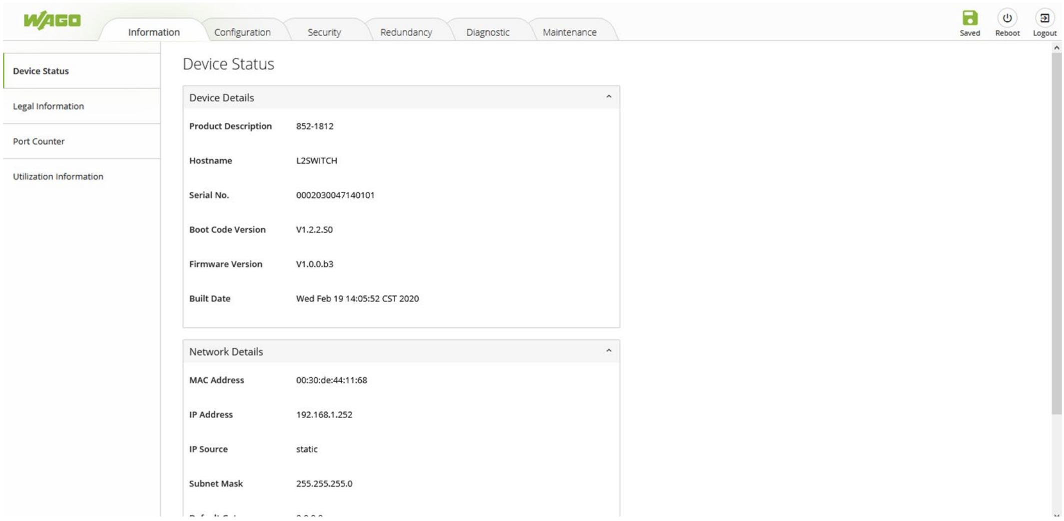
WAGO

Hostname: L2SWITCH
Description: 852-1812

Figure 23: Log in

Table 18: Login Screen

Setting	Default Value
Default username	admin
Default password	wago



Device Status

Device Details

Product Description	852-1812
Hostname	L2SWITCH
Serial No.	0002030047140101
Boot Code Version	V1.2.2.S0
Firmware Version	V1.0.0.b3
Built Date	Wed Feb 19 14:05:52 CST 2020

Network Details

MAC Address	00:30:de:44:11:68
IP Address	192.168.1.252
IP Source	static
Subnet Mask	255.255.255.0

Figure 24: Tab “Information” – Menu “Device Status”

Note

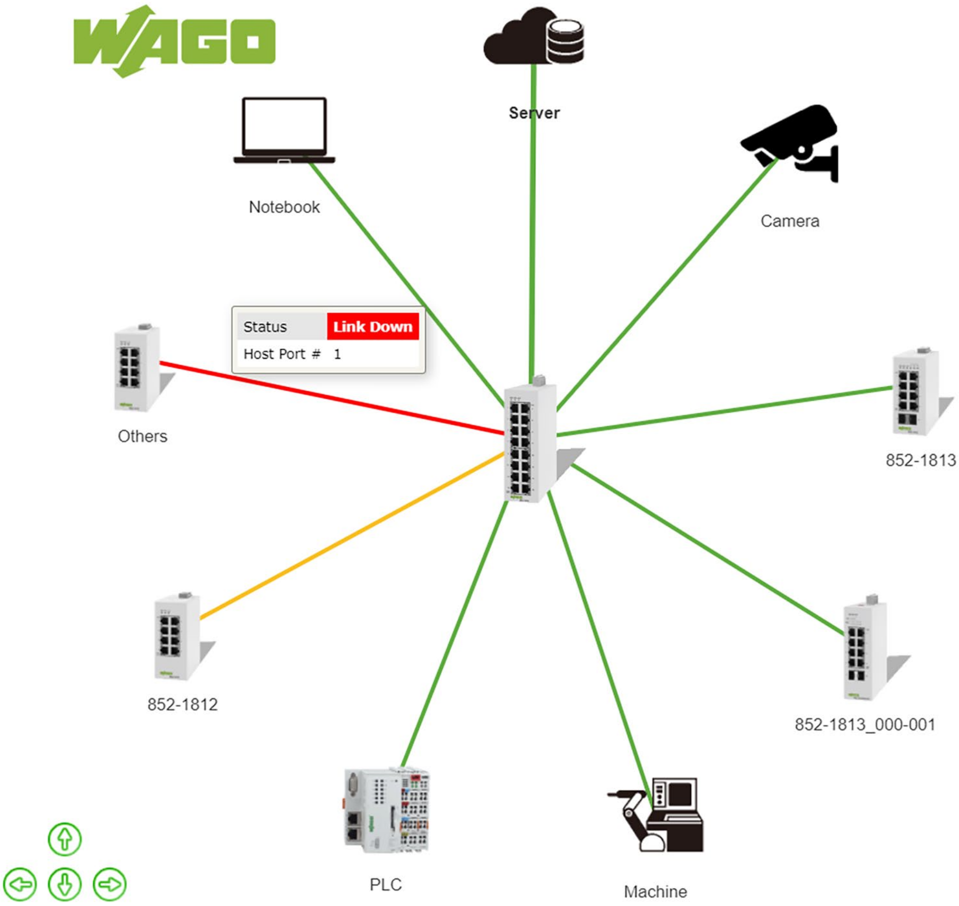
The Web Based Management (WBM)
For a detailed description of the configuration in Web Based Management (WBM), see Section "Configuration in the Web Based Management (WBM)”.

Once user select Topology map option it will appear get to network connectivity connected to this device as shown below.

The switch offers lean network management:

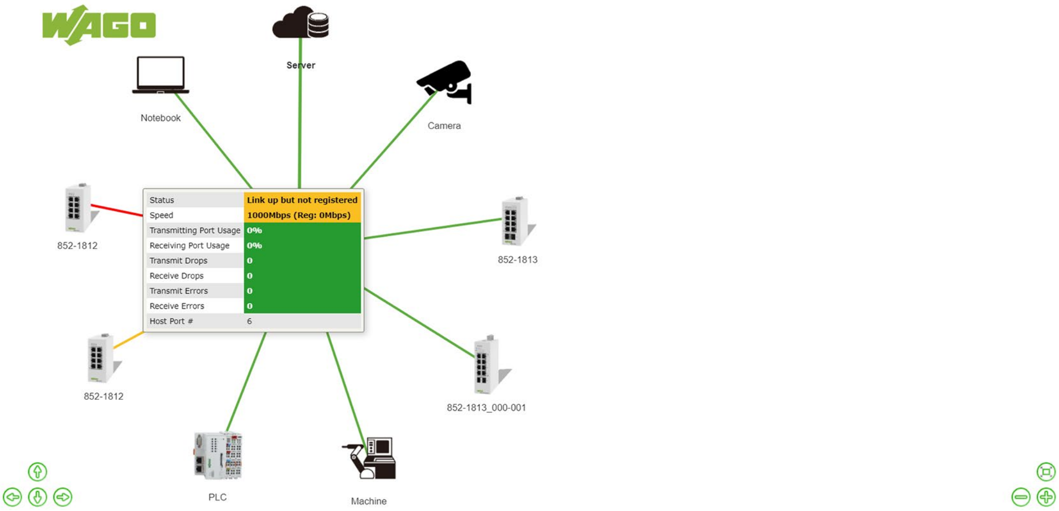
Diagnostics are intuitive and can be performed without IT knowledge. The topology map clearly displays the switch and the connected nodes. Important diagnostic information is visualized.

If the connection is interrupted at a port, the connection line changes color to red.



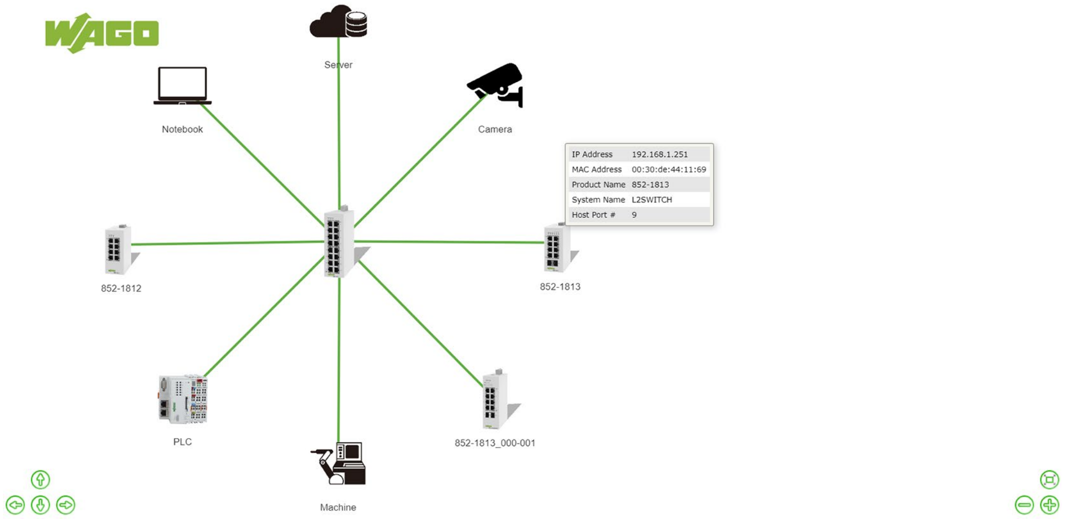
Status	Link Down
Host Port #	1

Figure 25: Topology Map – Link Down Port 1



Status	Link up but not registered
Speed	1000Mbps (Reg: 0Mbps)
Transmitting Port Usage	0%
Receiving Port Usage	0%
Transmit Drops	0
Receive Drops	0
Transmit Errors	0
Receive Errors	0
Host Port #	6

Figure 26: Topology Map – Link not registered



IP Address	192.168.1.251
MAC Address	00:30:de:44:11:69
Product Name	852-1813
System Name	L2SWITCH
Host Port #	9

Figure 27: Topology Map – Link Information

9 Configuration in the Web Based Management

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.

The HTML pages saved 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 the WBM, launch a Web browser (e. g. Google Chrome or Mozilla Firefox).

➔ **Note**

Standard setting
By default, the Lean Managed Switch is set to the "http" protocol.

➔ **Note**

Using Protocol "https"
If you use "https", you must activated this service (see Section "Service Control".).

2. Enter the IP address of the switch.

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

4. Enter your user name and password in the query dialog:

   User = "admin"
   Password = "wago"

5. The start page of WBM loads.

6. Make the desired settings.

7. Click **[Submit]** to confirm your changes, or click **[Delete]** to discard your changes.

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

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

Table 19: Overview – Navigation Links and WBM Pages

Navigation Links and WBM Pages
▶ **[Information]** **[Device Status]** • Device Details • Network Details • Operating Time **[Legal Information]** • WAGO Licenses • Open Source Licenses • WBM Licenses **[Port Counter]** • Port Counter **[Utilization Information]** • Utilization Information
▶ **[Configuration]**
[Device Discovery] • LLDP   • LLDP Settings   • LLDP Neighbor Information • Manual Registration   • Manual Registration Settings   • Manual Registration Information **[Interface]** • Loop Detection   • Configuration Settings   • Configuration Status • Mirror   • Port Mirror Settings • Port Setup   • Port Setup   • Port Status • Port Priority   • Port Priority Settings   • Port Priority Status

[**SNMP**]

- Event Settings
  - Trap Event State Settings

- Port Event Settings
  - Port Link-Change Trap Settings
  - Port Link-Change Trap Status

- SNMP Setup
  - SNMP Setup
  - Community Name List

- SNMP Trap
  - Trap Receiver Settings
  - Trap Receiver List

- SNMPv3 Group
  - SNMPv3 Group Settings
  - SNMPv3 Group Status

- SNMPv3 User
  - SNMPv3 User Settings
  - SNMPv3 User Status

- SNMPv3 View
  - SNMPv3 View Settings
  - SNMPv3 View Status

[System Management]

- General Setup
  - TCP/IP Configuration
  - Hostname
  - Management VLAN

- SNTP
  - Current Time and Date
  - Time and Date Settings

- User Account
  - Add New User
  - User Account List

[Storm Control]

- Storm Control Settings
- Storm Control Status

▶ **[Security]**

[802.1X]

- Global Setup
    - Global Setup
    - Global Status
- Port Setup
    - Port Setup
    - Port Status

[ACL]

- Access Control List Settings
- Access Control List Status

[Port Security]

- Port Security Settings
- Port Security Status

[Service Control]

- Service Settings

[VLAN]

- Port Isolation
    - Port Isolation Settings
    - Egress Port
- VLAN Setup
    - VLAN Setup

▶ **[Redundancy]**

[ERPS]

- ERPS Setup
- Configuration Status

[STP/RSTP]

- STP/RSTP Setup
    - Spanning Tree Protocol Settings
- STP/RSTP Port Setup
    - Port Parameter Settings
    - Port Status

▶ **[Diagnostic]**

[Alarm]

- Information
  - Alarm Information

- DIP Status
  - DIP Switch Status

- Traffic Flooding
  - Traffic Flooding Settings
  - Traffic Flooding Status

- Port Utilization
  - Port Utilization Settings
  - Port Utilization Status

[Dashboard Configuration

- Port Registration Learn
- Port Link Down Statistics
- Critical/Alert Thresholds

[Modbus]

- Modbus TCP Setting
- Modbus TCP Information

[**SNMP**]

- Event Settings
  - Trap Event State Settings

- Port Event Settings
  - Port Link-Change Trap Settings
  - Port Link-Change Trap Status

- SNMP Setup
  - SNMP Setup
  - Community Name List

- SNMP Trap
  - Trap Receiver Settings
  - Trap Receiver List

- SNMPv3 Group
  - SNMPv3 Group Settings
  - SNMPv3 Group Status

- SNMPv3 User
  - SNMPv3 User Settings
  - SNMPv3 User Status

- SNMPv3 View
  - SNMPv3 View Settings
  - SNMPv3 View Status

[System Log]

- Syslog Server Settings

▶ **[Maintenace]**

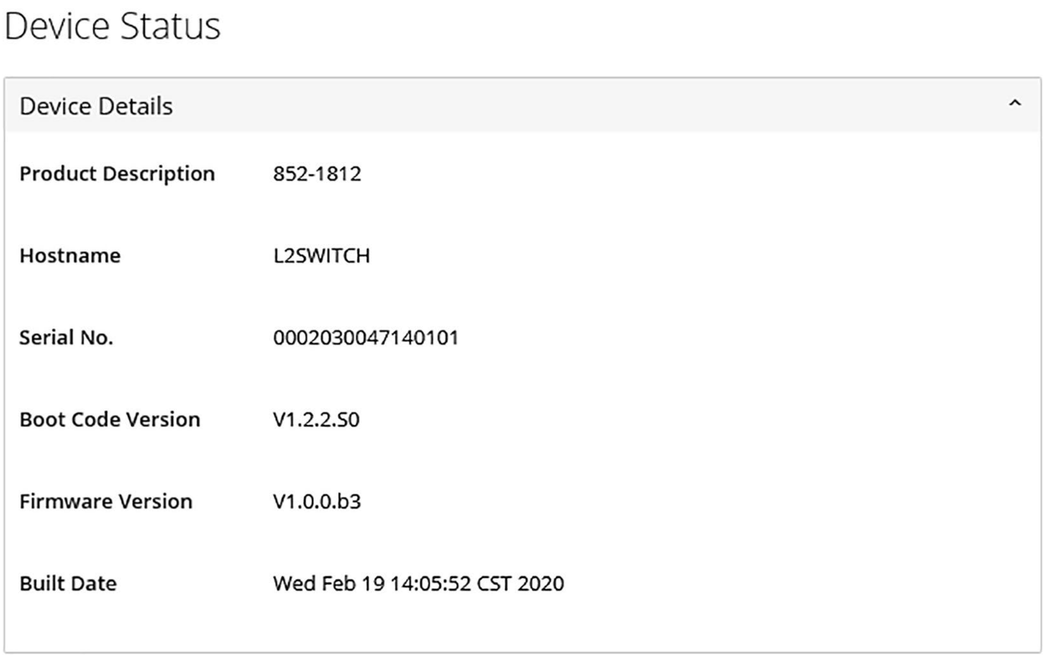
- Reboot
- Upgrade Firmware
- Upload Configuration
- Download Configuration
- Reset Configuration

The settings/configuration of the Lean 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 displayed in **bold**.

9.1 Information

9.1.1 Device Status



Device Status

Device Details

Product Description 852-1812

Hostname L2SWITCH

Serial No. 0002030047140101

Boot Code Version V1.2.2.S0

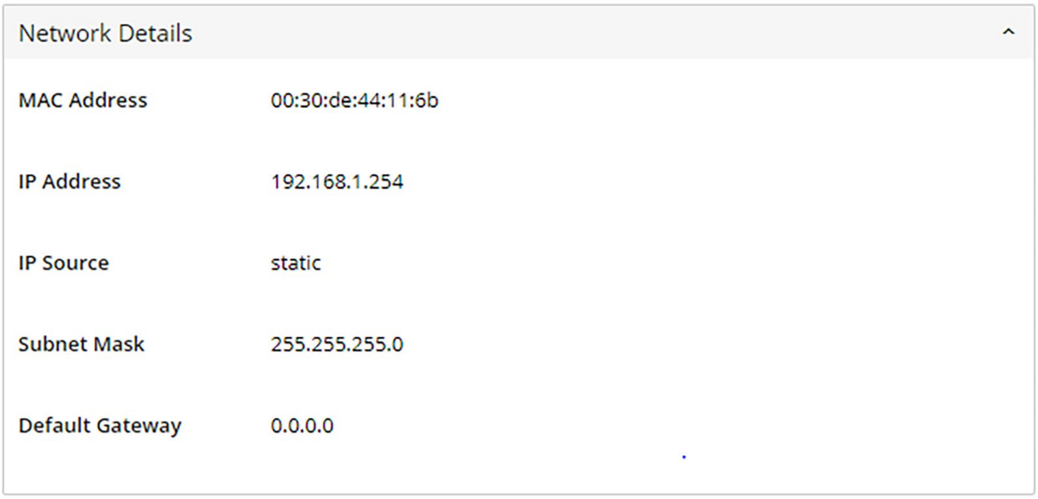
Firmware Version V1.0.0.b3

Built Date Wed Feb 19 14:05:52 CST 2020

Figure 28: Tab “Information” – Menu “Device Status” – “Device Details”

Table 20: Tab “Information” – Menu “Device Status” – “Device Details”

Parameter	Description
Product Description	This display field shows the model name of the switch.
Host Name	This display field shows the host name of the switch.
Serial No.	This display field shows the serial number.
Boot Code Version	This display field shows the boot code version.
Built Date	This display field shows the create date of the primary firmware currently installed.



Network Details

MAC Address 00:30:de:44:11:6b

IP Address 192.168.1.254

IP Source static

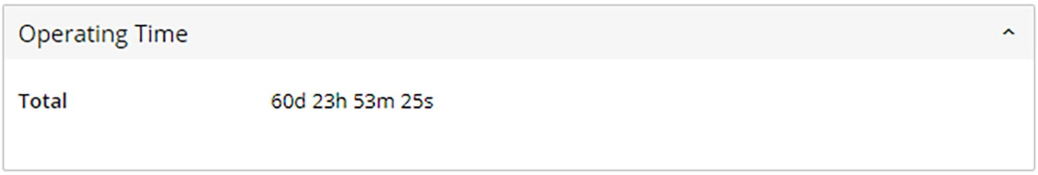
Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

Figure 29: Tab “Information” – Menu “Device Status” – “Network Details”

Table 21: Tab “Information” – Menu “Device Status” – “Network Details”

Parameter	Description
MAC Address	This display field shows the MAC (Media Access Control) address of the switch.
IP Address	This display field shows the IP address of the switch.
IP Source	This display field shows the Static IP or DHCP.
Subnet Mask	This display field shows the subnet mask of the switch.
Default Gateway	This display field shows the default gateway of the switch.



Operating Time

Total 60d 23h 53m 25s

Figure 30: Tab “Information” – Menu “Device Status” – “Operating Time”

Table 22: Tab “Information” – Menu “Device Status” – “Operating Time”

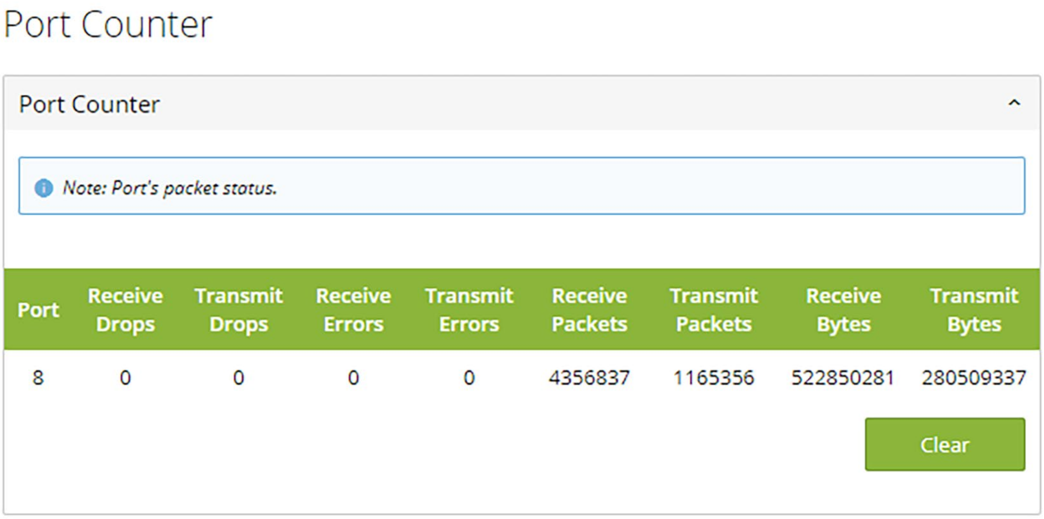
Parameter	Description
Total	This display field shows the operating time (dd:hh:mm:ss).

9.1.2 Legal Information

In this menu, you can find informations about:

- WAGO Licenses
- Open Source Licenses and
- WBM Licenses

9.1.3 Port Counter



Port Counter

Port Counter

Note: Port's packet status.

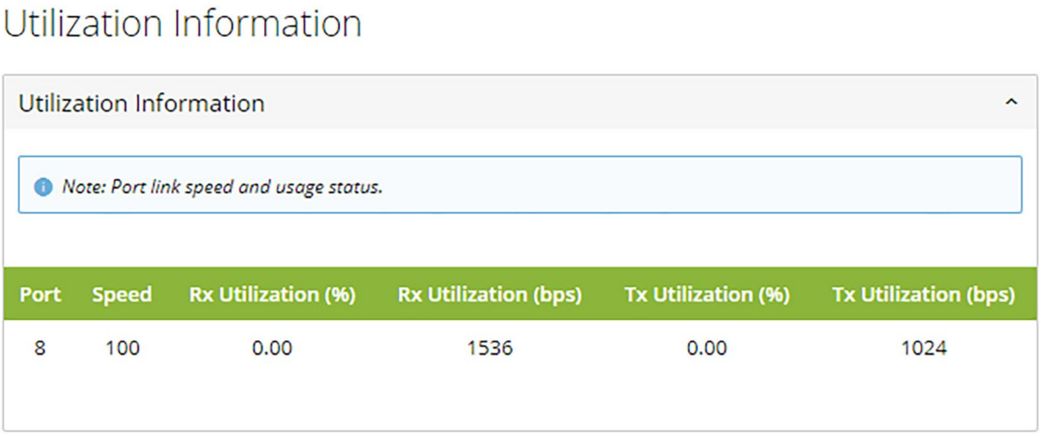
Port	Receive Drops	Transmit Drops	Receive Errors	Transmit Errors	Receive Packets	Transmit Packets	Receive Bytes	Transmit Bytes
8	0	0	0	0	4356837	1165356	522850281	280509337

Figure 31: Tab “Information” – Menu “Port Counter”

Table 23: Tab “Information” – Menu “Port Counter”

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

9.1.4 Utilization Information



Utilization Information

Utilization Information

Note: Port link speed and usage status.

Port	Speed	Rx Utilization (%)	Rx Utilization (bps)	Tx Utilization (%)	Tx Utilization (bps)
8	100	0.00	1536	0.00	1024

Figure 32: Tab “Information” – Menu “Utilization Information”

Table 24: Tab “Information” – Menu “Utilization Information”

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.

9.2 Configuration

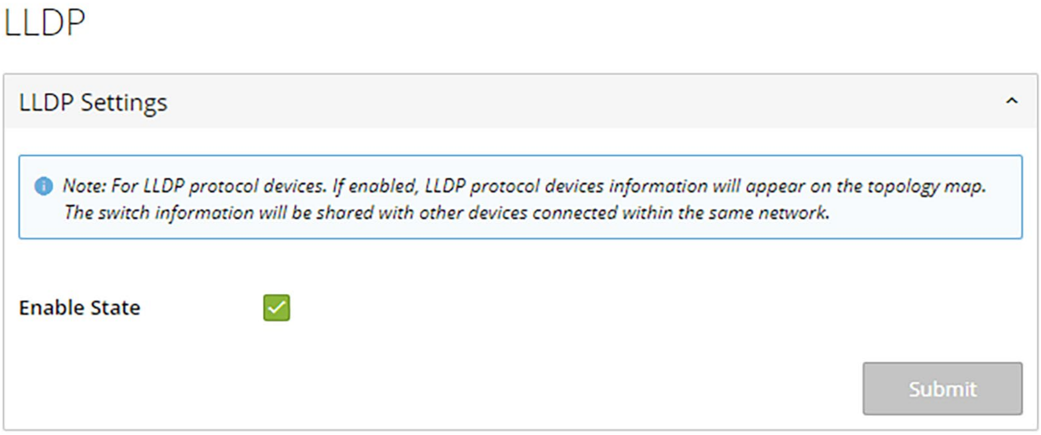
9.2.1 Device Discovery

9.2.1.1 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 includes 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.

Note

For LLDP protocol devices.
If enabled, LLDP protocol devices information will appear on the topology map. The switch information will be shared with other devices connected within the same network



LLDP

LLDP Settings

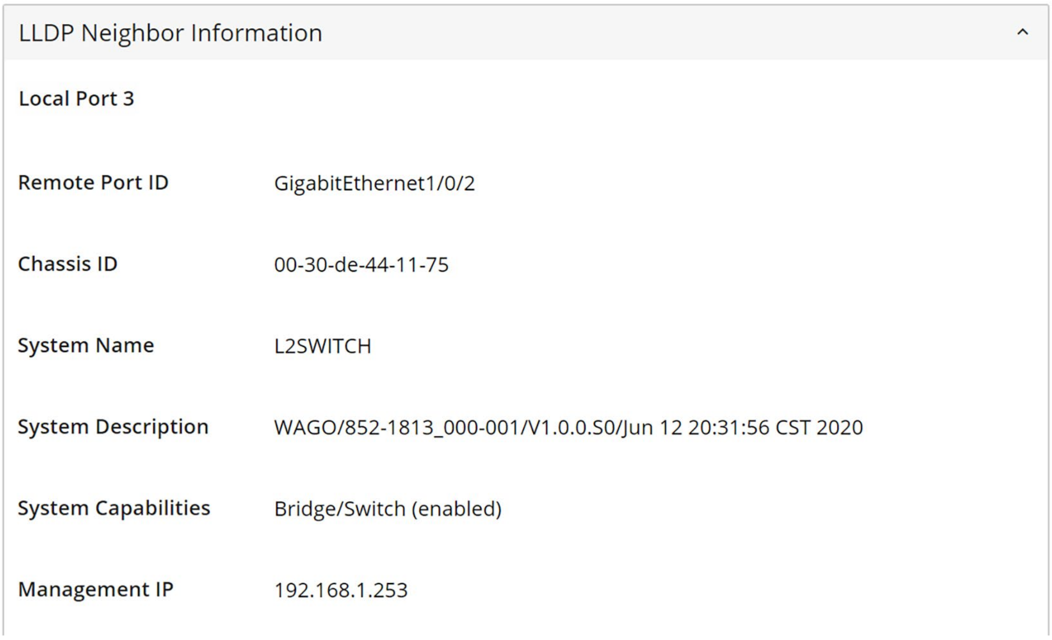
Note: For LLDP protocol devices. If enabled, LLDP protocol devices information will appear on the topology map. The switch information will be shared with other devices connected within the same network.

Enable State ☑

Figure 33: Tab “Configuration” – Menu “LLDP Settings”

Table 25: Tab “Configuration – Menu “LLDP Settings”

LLDP Settings			
Parameter	**Default**	**Description**	
State	☑	☐	The LLDP function is globally not enabled for the switch.
		☑	The LLDP function is globally enabled for the switch.



LLDP Neighbor Information

Local Port 3

Remote Port ID GigabitEthernet1/0/2

Chassis ID 00-30-de-44-11-75

System Name L2SWITCH

System Description WAGO/852-1813_000-001/V1.0.0.S0/Jun 12 20:31:56 CST 2020

System Capabilities Bridge/Switch (enabled)

Management IP 192.168.1.253

Figure 34: Tab “Configuration” – Menu “LLDP Neighbor Information”

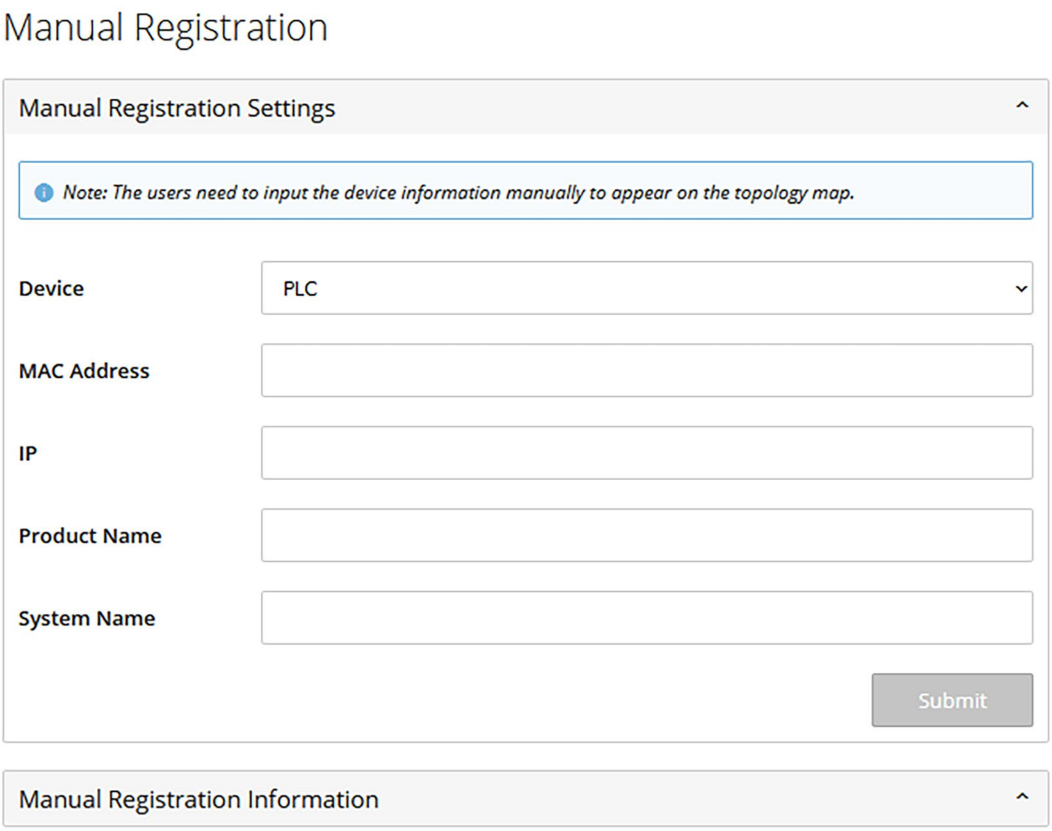
Table 26: Tab “Configuration” – Menu “LLDP Neighbor Information”

LLDP Neighbor Information		
Parameter	**Default**	**Description**
Local Port X		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.

9.2.1.2 Manual Registration

Note

Manual input of the device information
The users need to input the device information manually to appear on the topology map.



Manual Registration

Manual Registration Settings

Note: The users need to input the device information manually to appear on the topology map.

Device: PLC

MAC Address:

IP:

Product Name:

System Name:

Figure 35: Tab “Configuration” – Menu “Manual Registration”

Table 27: Tab “Configuration” – Menu “Manual Registration”

Manual Registration Settings		
Parameter	**Default**	**Description**
Device	**PLC** Switch Camera Computer Display Machine Notebook Others Router Server Wireless	Select the suitable device name in the selection box.
MAC Address		In the input field, enter the MAC address of the device.
IP		In the input field, enter the IP address of the device.
Product Name		In the input field, enter the product name of the device.
System Name		In the input field, enter the system name of the device.

9.2.2 Interface

9.2.2.1 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 with 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 Traffic flooding.”

The “Loop Detection” function sends probe 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 probe packets looping back to the same port.

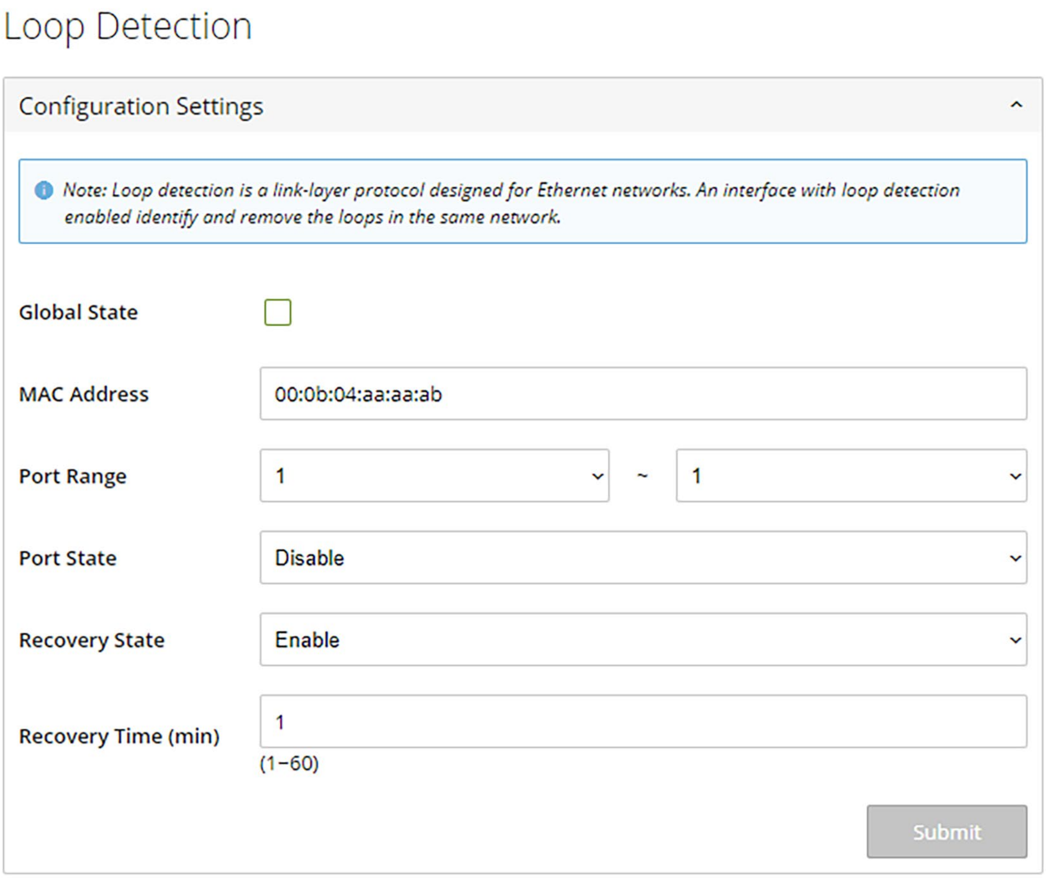
9.2.2.1.1 Loop Recovery

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 re-enables the port and executes “Loop Detection” again.

The switch generates a “Syslog” (system log), internal log messages and “SNMP Traps” if it disables a port after “Loop Detection.”

Note

Loop detection
Loop detection is a link-layer protocol designed for Ethernet networks. An interface with loop detection enabled identify and remove the loops in the same network.



Loop Detection

Configuration Settings

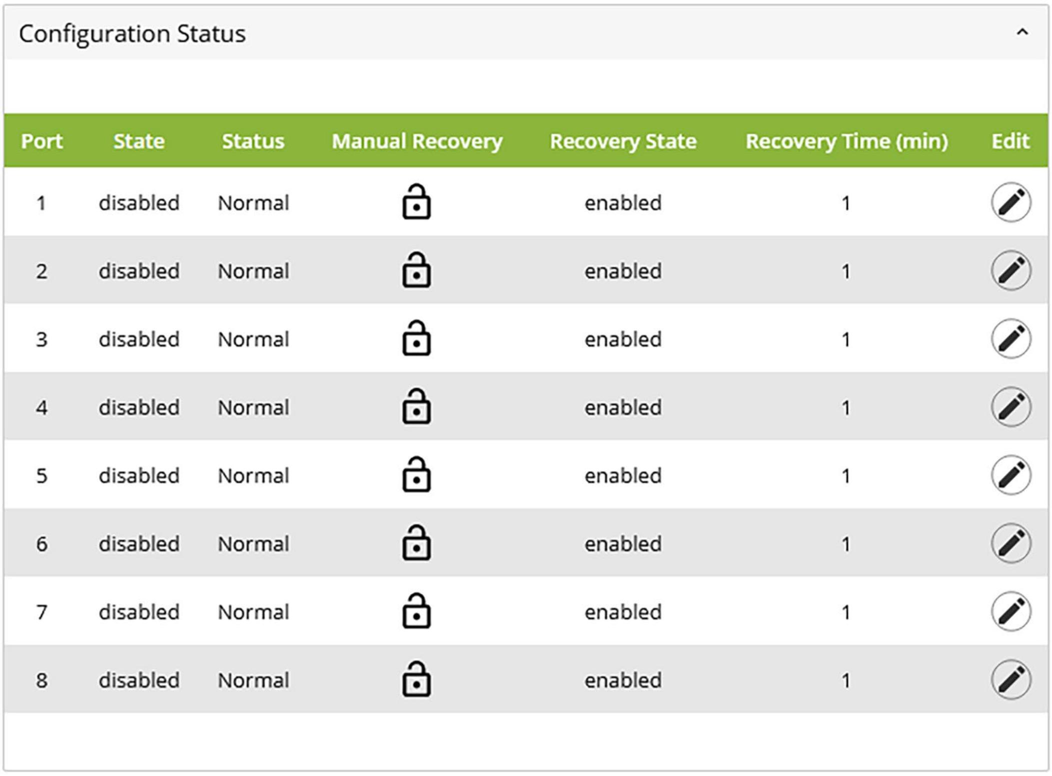
Note: Loop detection is a link-layer protocol designed for Ethernet networks. An interface with loop detection enabled identify and remove the loops in the same network.

Global State	□
MAC Address	00:0b:04:aa:aa:ab
Port Range	1 ~ 1
Port State	Disable
Recovery State	Enable
Recovery Time (min)	1 (1–60)

Figure 36: Tab “Configuration” – Menu “Loop Detection” – “Configuration Settings”

Table 28: Tab “Configuration” – Menu “Loop Detection” – “Configuration Settings”

Configuration Settings		
Parameter	**Default**	**Description**
Global State	☑	□ The Loop Detection function is not enabled for the switch.
		☑ The Loop Detection function is enabled for the switch.
MAC Address		In the input field, enter the destination MAC address to which the probe packets should be sent. If the port receives the same packets, it is shut down.
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Loop Detection” settings.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Loop Detection” settings.
Port State	**Disable**	Select “Disable” in the selection box to disable the “Loop Detection” function for the switch.
	Enable	Select “Enable” in the selection box to enable the “Loop Detection” function for the switch.
Recovery State	**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



Configuration Status

Port	State	Status	Manual Recovery	Recovery State	Recovery Time (min)	Edit
1	disabled	Normal	🔓	enabled	1	✎
2	disabled	Normal	🔓	enabled	1	✎
3	disabled	Normal	🔓	enabled	1	✎
4	disabled	Normal	🔓	enabled	1	✎
5	disabled	Normal	🔓	enabled	1	✎
6	disabled	Normal	🔓	enabled	1	✎
7	disabled	Normal	🔓	enabled	1	✎
8	disabled	Normal	🔓	enabled	1	✎

Figure 37: Tab “Configuration” – Menu “Loop Detection” – “Configuration Status” (Example)

Table 29: Tab “Configuration” – Menu “Loop Detection” – “Configuration Status” (Example)

Loop Detection Status		
Parameter	**Default**	**Description**
Port	1 … 8 (16)	This column shows the port numbers.
State	Enable Disable	This column indicates whether the “Loop Detection” function is enabled or disabled.
Status	None Normal	This column indicates whether a port is blocked.
Manual Recovery		This column indicates whether the manual recovery is complete.
Recovery State	Enable Disable	This column indicates whether the “Loop Recovery” function is enabled or disabled.
Recovery Time (min)	1 … 60	This column displays the “Recovery Time” for the “Loop Detection” function.
Edit		Preselection for editing.

9.2.2.2 Mirror

Port mirroring is used on switches to send a copy of network packets sent/received on one switch port or a range of switch ports to a network monitoring connection on another switch port (Monitor Port).

Port mirroring is used in network systems that require monitoring of network traffic, such as an IDS (“Intrusion Detection System”).

Port mirroring, together with an NTA (“Network Traffic Analyzer”), can help to monitor network traffic. Users can monitor the selected ports (“Source Ports”) for egress and/or ingress packets.

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.

Note

Important Note!

1. The monitor port cannot be a trunk member port.
2. The monitor port cannot be an ingress or egress port.
3. If a port has been configured as a source port and the user configures the port as a destination port, the port will be removed from the source ports automatically.

9.2.2.2.1 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 replying.

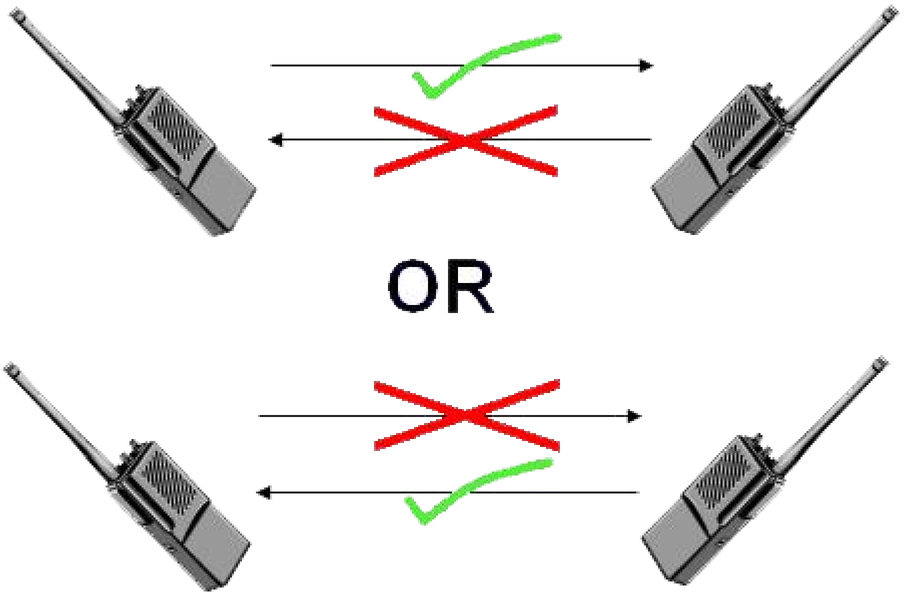


Figure 38: Half-Duplex Mode

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 39: Full-Duplex Mode

Auto MDI/MDIX

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

Auto-MDIX (“**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-MDIX to work properly, the speed must be set to “Auto” for the interface and in the duplex settings.

Auto-Negotiation

Auto-negotiation 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.
Auto-negotiation only applies to twisted-pair cables – not to WLAN, fiber optic or coaxial cable connections.

If the port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode.
If auto-negotiation is enabled on the switch, a port uses its pre-configured settings for speed and duplex mode when establishing the connection.
This should 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 adjusting them to the bandwidth on the input port.
Higher data traffic on the port decreases the bandwidth and can overflow the buffer memory, which can lead to packet and frame loss.

According to IEEE 802.3x, the switch uses “Flow Control” in full-duplex mode and “Backpressure Flow Control” in half-duplex mode.

With flow control, the switch is used in full-duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.

For “Backpressure Flow Control“, the switch sends a collision signal to the sending port in half-duplex mode (mimicking a state of packet collision), causing the sending port to temporarily stop sending signals and to resend the signals later.

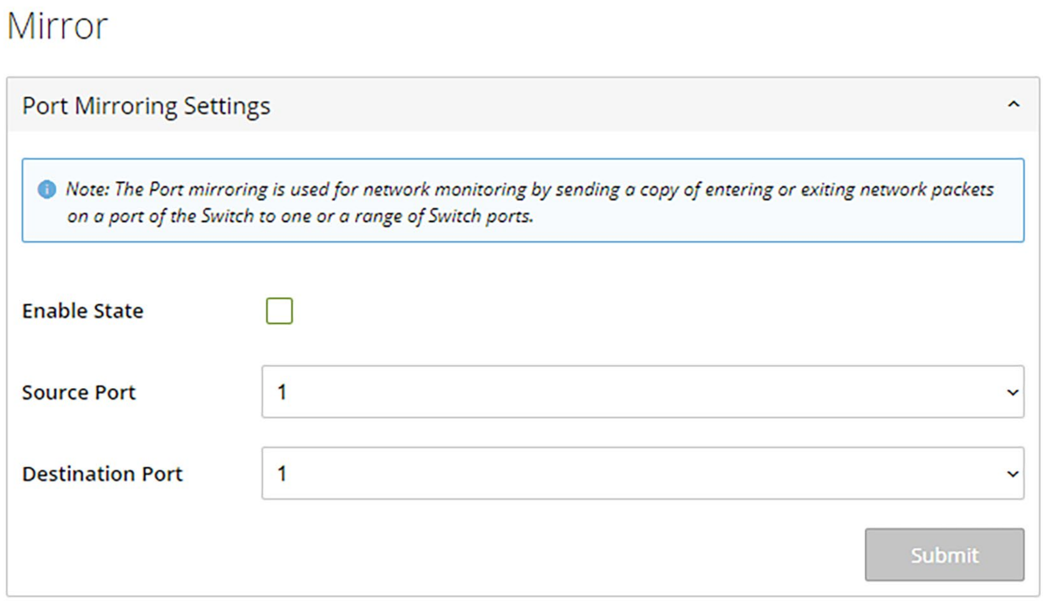
Note

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

Note

Using the Port Mirroring

The Port Mirroring is used for network monitoring by sending a copy of entering or existing network packets on a port of the switch to one or a range of switch ports.



Note: The Port mirroring is used for network monitoring by sending a copy of entering or exiting network packets on a port of the Switch to one or a range of Switch ports.

Enable State □

Source Port 1

Destination Port 1

Figure 40: Tab “Configuration” – Menu “Mirror” – “Port Mirroring Settings”

Table 30: Tab “Configuration” – Menu “Mirror” – “Port Mirroring Settings”

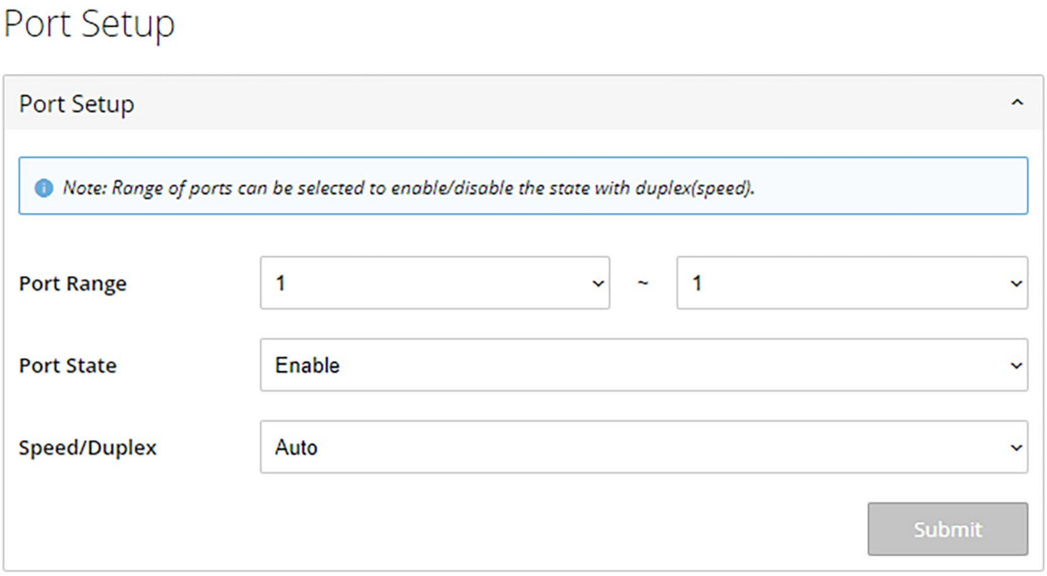
Port Mirror Settings			
Parameters	**Default**	**Description**	
Enable State	□	□	The mirror function is not enabled for the switch.
		☑	The mirror function is enabled for the switch.
Source Port	1 … 8 (16)	Select the source port for the mirror function in the selection field.	
Destination Port	1 … 8 (16)	Select the destination port for the mirror function in the selection field.	

9.2.2.3 Port Setup

Note

Select a range of ports

Range of ports can be selected to enable/disable the state with duplex (speed).



Port Setup

Port Setup

Note: Range of ports can be selected to enable/disable the state with duplex(speed).

Port Range: 1 ~ 1

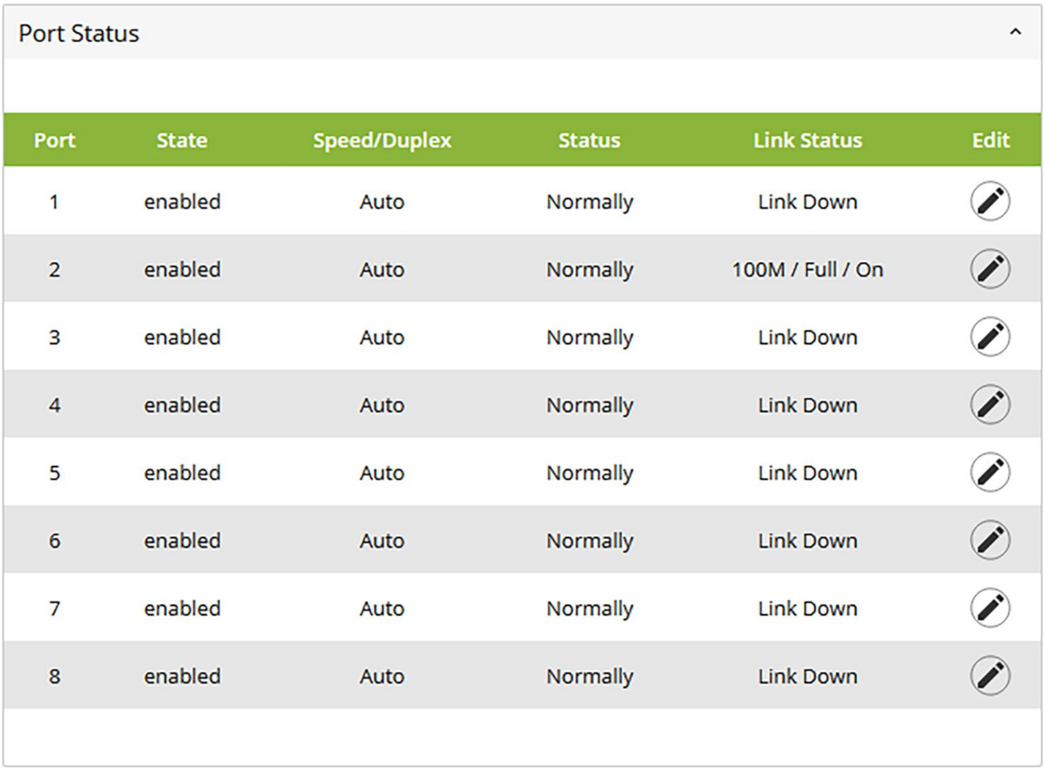
Port State: Enable

Speed/Duplex: Auto

Figure 41: Tab “Configuration” – Menu “Port Setup” – “Port Setup”

Table 31: Tab “Configuration” – Menu “Port Setup” – “Port Setup”

Port Setup		
Parameters	**Default**	**Description**
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Mirror” settings.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Mirror” settings.
Port 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. Nway means Autonegotiation in the Ethernet.
	10 Mbit/s / Full	
	10 Mbit/s / Half	
	100 Mbit/s / Full	
	100 Mbit/s / Half	
	1000 Mbit/s / Full	



Port Status ⌃

Port	State	Speed/Duplex	Status	Link Status	Edit
1	enabled	Auto	Normally	Link Down	✎
2	enabled	Auto	Normally	100M / Full / On	✎
3	enabled	Auto	Normally	Link Down	✎
4	enabled	Auto	Normally	Link Down	✎
5	enabled	Auto	Normally	Link Down	✎
6	enabled	Auto	Normally	Link Down	✎
7	enabled	Auto	Normally	Link Down	✎
8	enabled	Auto	Normally	Link Down	✎

Figure 42: Tab “Configuration” – Menu “Port Setup” – “Port Status” (Example)

Table 32: Tab “Configuration” – Menu “Port Setup” – “Port Status” (Example)

Port Status		
Parameters	**Default**	**Description**
Port	1 … 8	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.
Status		This column displays the deviations.
Link Status		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.
Edit		Preselection for editing.

9.2.2.4 Port Priority

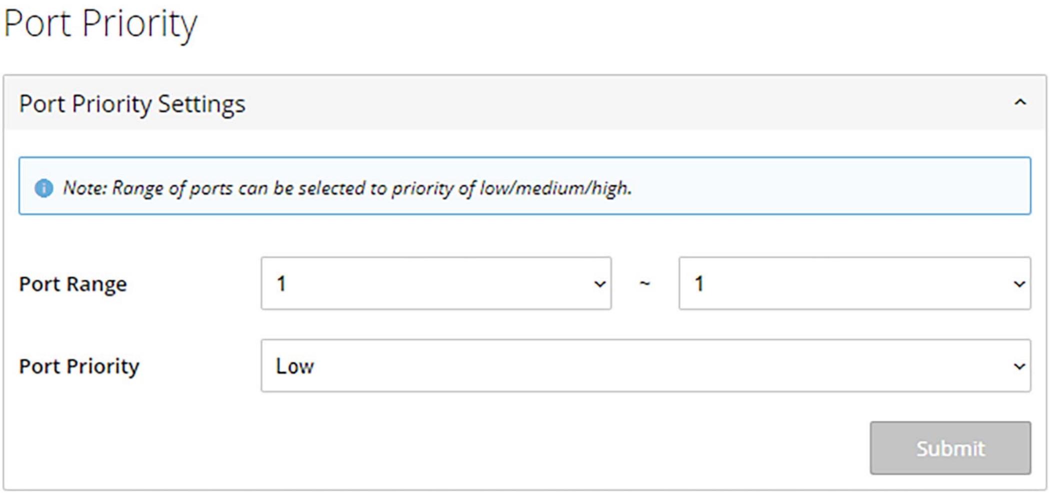
Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

Using Port Priority feature, you can select specific network traffic, and prioritize it according to its relative importance. Implementing Port Priority in your network makes network performance more predictable and bandwidth utilization more effective.

Note

Select the priority of ports

Range of ports can be selected to priority of low/medium/high.



Port Priority

Port Priority Settings

Note: Range of ports can be selected to priority of low/medium/high.

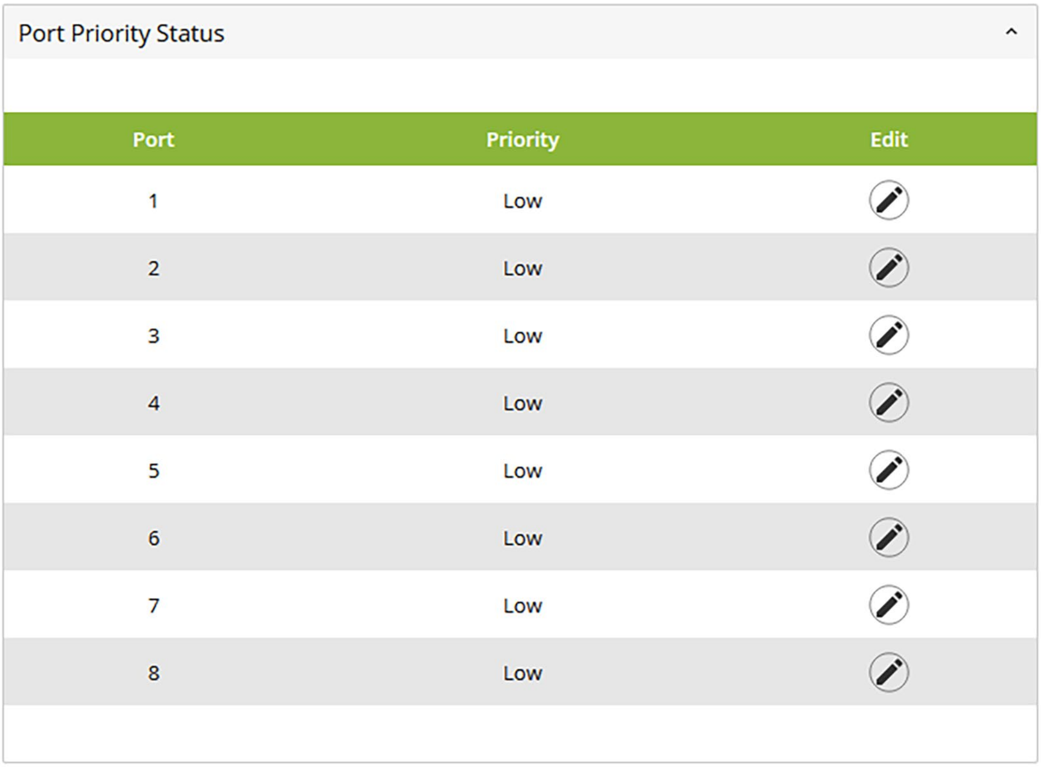
Port Range: 1 ~ 1

Port Priority: Low

Figure 43: Tab “Configuration” – Menu “Port Priority” – “Port Priority Settings”

Table 33: Tab “Configuration” – Menu “Port Priority” – “Port Priority Settings”

Port Priority Settings		
Parameter	**Default**	**Description**
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Port Setup” settings.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Port Setup” settings.
Port Priority	Low	In this selection box, select “Low” for applications with high data transfer.
	Medium	In this selection box, select “Medium” for normal applications.
	High	In this selection box, select “High” for time critical applications.



Port Priority Status ˄

Port	Priority	Edit
1	Low	✎
2	Low	✎
3	Low	✎
4	Low	✎
5	Low	✎
6	Low	✎
7	Low	✎
8	Low	✎

Figure 44: Tab “Configuration” – Menu “Port Priority” – “Port Priority Status” (Example)

Table 34: Tab “Configuration” – Menu “Port Priority” – “Port Priority Status” (Example)

Port Priority Status		
Parameters	**Default**	**Description**
Port	1 … 8 (16)	This column displays the port numbers.
Priority	Low Medium High	This column displays the priority of the port.
Edit		Preselection for editing.

9.2.3 SNMP

SNMP (“**S**imple **N**etwork **M**anagement **P**rotocol”) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). 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 exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

SNMP community act like passwords and are used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default SNMP community is “public” for both SNMP v1 and SNMP v2c..

Network ID of Trusted Host:

The IP address is a combination of the Network ID and the Host ID.

Network ID = (Host IP & Mask).

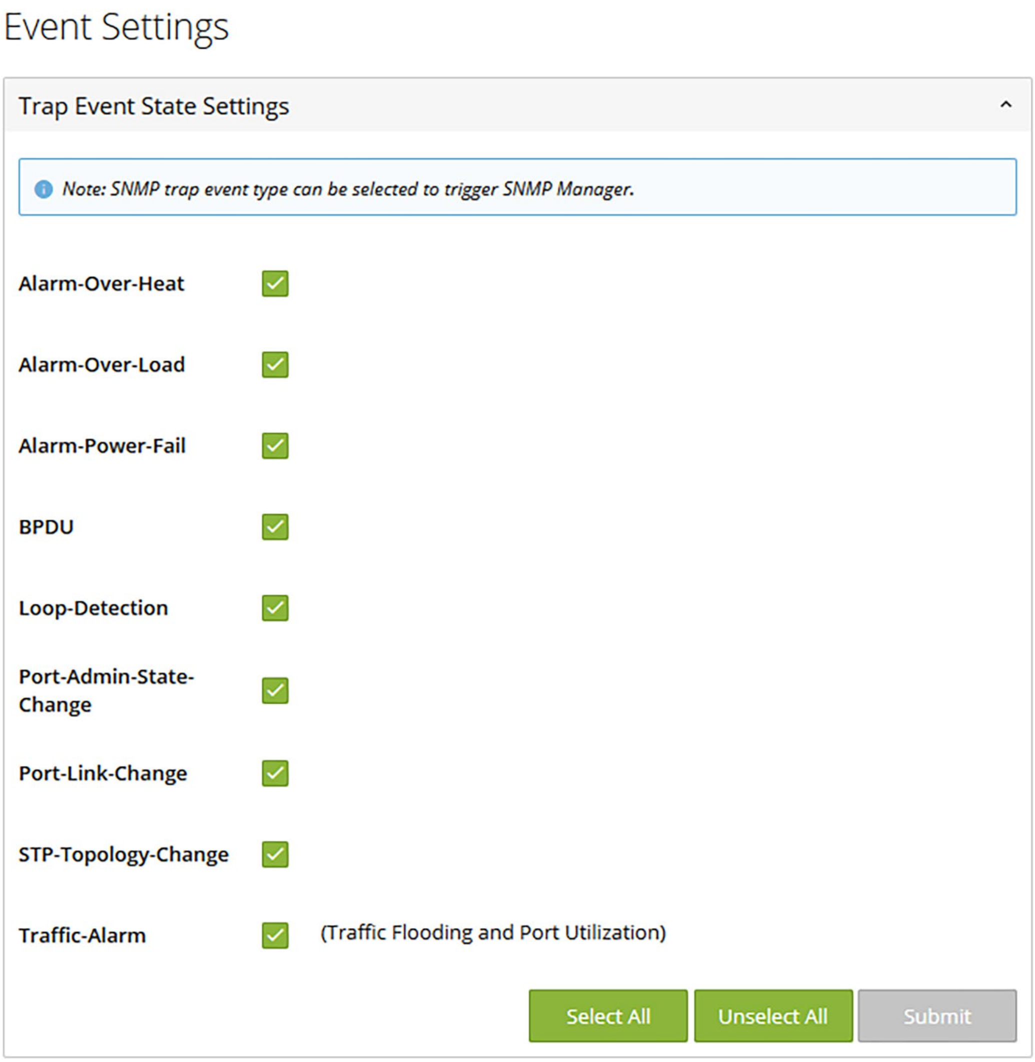
User need only input the network ID and leave the host ID to 0. If user has input the host ID, such as 192.168.1.102, the system will reset the host ID, such as 192.168.1.0.

9.2.3.1 Event Settings

Note

Select the type of SNMP trap event

SNMP trap event type can be selected to trigger SNMP Manager.



Event Settings

Trap Event State Settings

Note: SNMP trap event type can be selected to trigger SNMP Manager.

Alarm-Over-Heat ☑

Alarm-Over-Load ☑

Alarm-Power-Fail ☑

BPDU ☑

Loop-Detection ☑

Port-Admin-State-Change ☑

Port-Link-Change ☑

STP-Topology-Change ☑

Traffic-Alarm ☑ (Traffic Flooding and Port Utilization)

Figure 45: Tab “Configuration” – Menu “SNMP” – “Event Settings” – “Trap Event State Settings”

Table 35: Tab “Configuration” – Menu “SNMP” – “Event Settings” – “Trap Event State Settings”

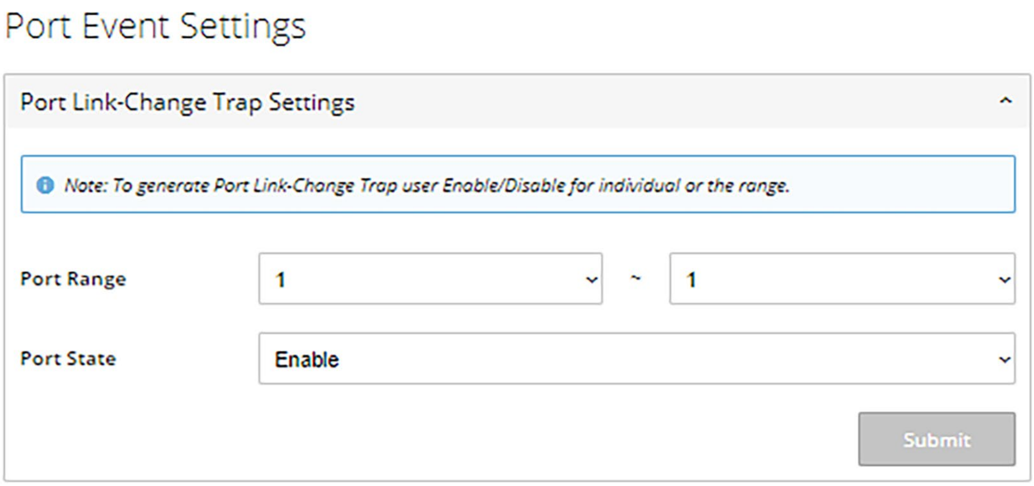
Trap Event State Settings		
Parameter	**Default**	**Description**
Alarm-Over-Heat	☑	Enables/disables the SNMP trap when the system temperature is too high.
Alarm-Over-Load	☑	Enables/disables the SNMP trap when the system is over load.
Alarm-Power-Fail	☑	Enables/disables the SNMP trap when system capacity is - overvoltage - undervoltage - RPS overvoltage - RPS undervoltage
BPDU	☑	Enables/disables the SNMP trap when the port is blocked by - BPDU Guard - BDPU Root - BPDU port state changed
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.
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-Alarm (Traffic Flooding and Port Utilization)	☑	Enables/disables the SNMP trap when the port is blocked by the traffic monitor.

9.2.3.2 Port Event Settings

Note

Generate port link-change trap

To generate port link-change trap user enable/disable for individual or the range.


Port Event Settings

Port Link-Change Trap Settings

Note: To generate Port Link-Change Trap user Enable/Disable for individual or the range.

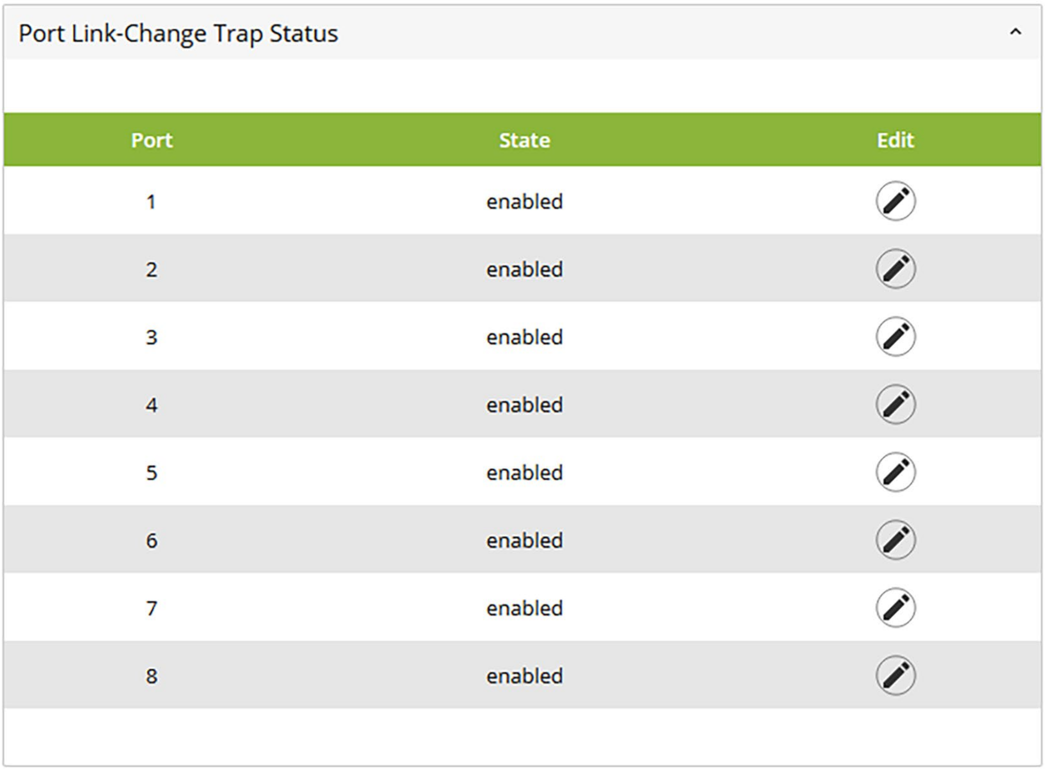
Port Range: 1 ~ 1

Port State: Enable

Figure 46: Tab “Configuration” – Menu “SNMP” – “Port Event Settings” – “Port Link-Change Trap Settings”

Table 36: Tab “Configuration” – Menu “SNMP” – “Port Event Settings” – “Port Link-Change Trap Settings”

Port Link-Change Trap Settings		
Parameter	**Default**	**Description**
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Port Event Settings” settings.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Port Event Settings” settings.
Port State	**Disable**	Select “Disable” in the selection box to disable the “Port Event Settings” function for the switch.
	Enable	Select “Enable” in the selection box to enable the “Port Event Settings” function for the switch.



Port Link-Change Trap Status

Port	State	Edit
1	enabled	✎
2	enabled	✎
3	enabled	✎
4	enabled	✎
5	enabled	✎
6	enabled	✎
7	enabled	✎
8	enabled	✎

Figure 47: Tab “Configuration” – Menu “SNMP” – “Port Event Settings” – “Port Link-Change Trap Status” (Example)

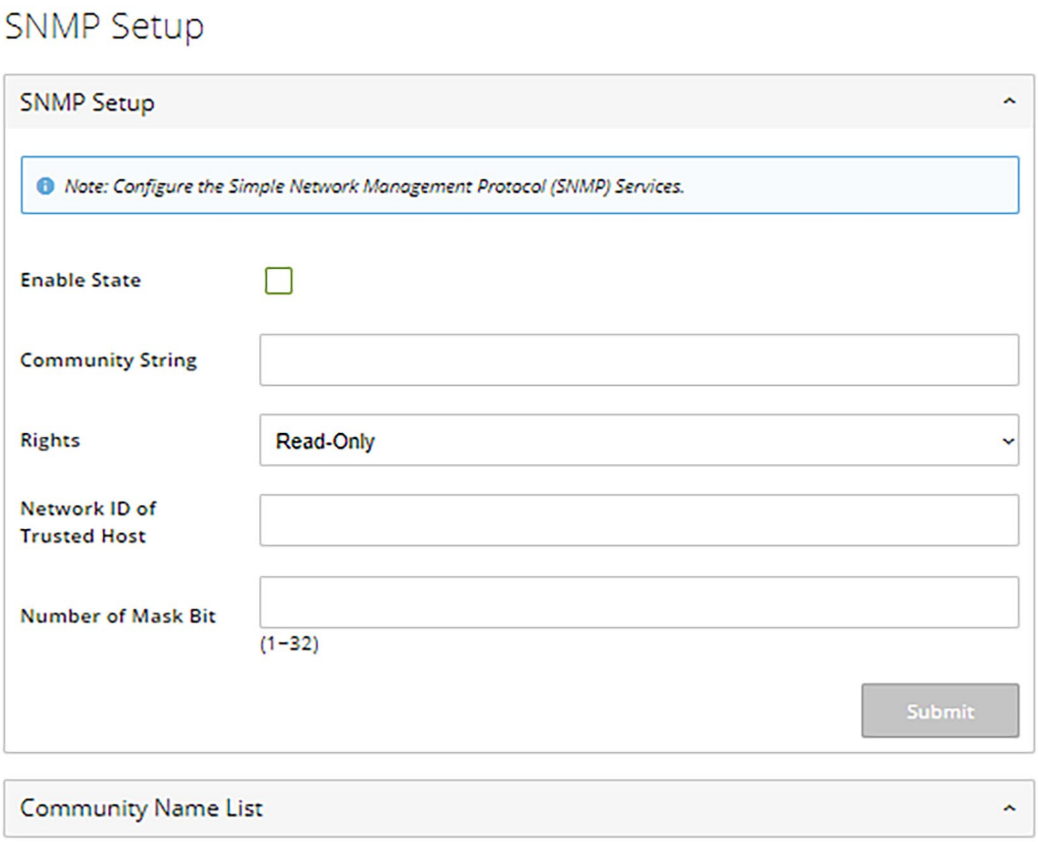
Table 37: Tab “Configuration” – Menu “SNMP” – “Port Event Settings” – “Port Link-Change Trap Status” (Example)

Port Link-Change Trap Status		
Parameter	**Default**	**Description**
Port	1 … 8 (16)	This column displays the port range.
State	Enable Disable	This field displays the port status.
Edit		Preselection for editing.

9.2.3.3 SNMP Setup

Note

Simple Network Management Protocol (SNMP)
Configure the Simple Network Management Protocol (SNMP) services.



SNMP Setup

SNMP Setup

Note: Configure the Simple Network Management Protocol (SNMP) Services.

Enable State □

Community String

Rights Read-Only

Network ID of Trusted Host

Number of Mask Bit (1~32)

Figure 48: Tab “Configuration” – Menu “SNMP” – “SNMP Setup” – “SNMP Setup”

Table 38: Tab “Configuration” – Menu “SNMP” – “SNMP Setup” – “SNMP Setup”

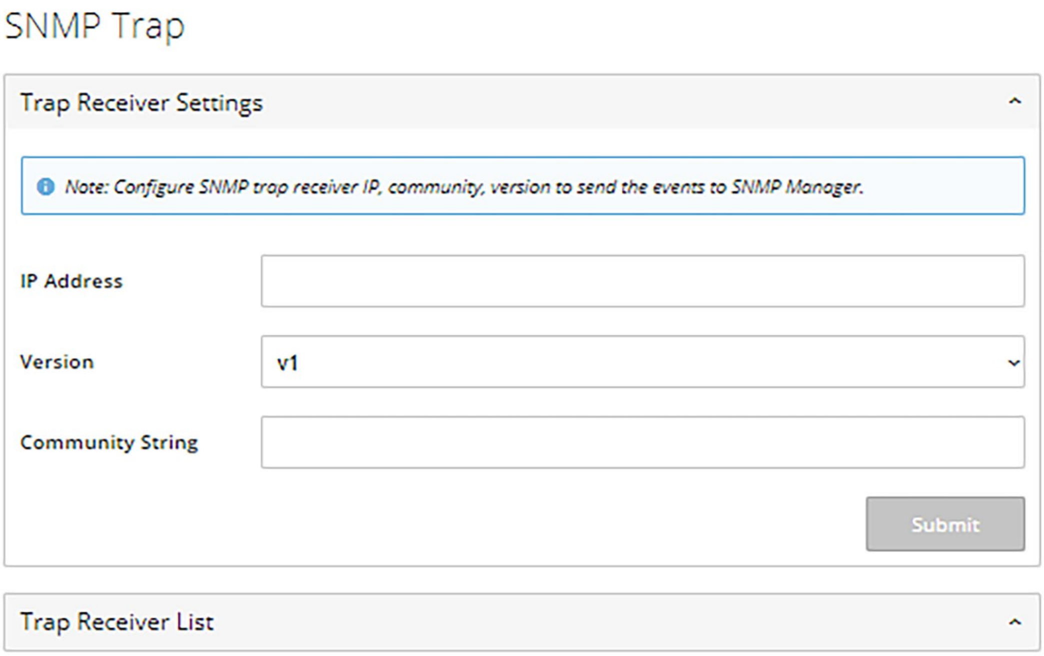
SNMP Setup			
Parameter	**Default**	**Description**	
Enable State	□	□	The “SNMP Setup” function is not enabled for the switch.
		☑	The “SNMP Setup” function is enabled for the switch.
Community String		Enter a “Community string”; this will act as a password for requests from the management station. An 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 “Community String” is included in every packet that is transmitted between the SNMP manager and the SNMP agent.	
Rights	**Read-Only**	Select “Read-Only” in the selection box to allow the SNMP manager using this string to collect information from the switch.	
	Read/ Write	Select “Read/Write” in the selection box to allow the SNMP manager using this string to create or edit MIBs (configure settings on the switch).	
Network ID of 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 (1-32)		Select the length of the subnet mask bits in the selection field.	
Community Name List			
Parameter	**Default**	**Description**	
No.		This column displays the “Community” number. It is used 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.”	

9.2.3.4 SNMP Trap

Note

Trap Receiver Settings

Configure SNMP trap receiver IP, community, version to send the events to SNMP Manager.



SNMP Trap

Trap Receiver Settings

Note: Configure SNMP trap receiver IP, community, version to send the events to SNMP Manager.

IP Address

Version: v1

Community String

Figure 49: Tab “Configuration” – Menu “SNMP” – “SNMP Trap” – “Trap Receiver Settings”

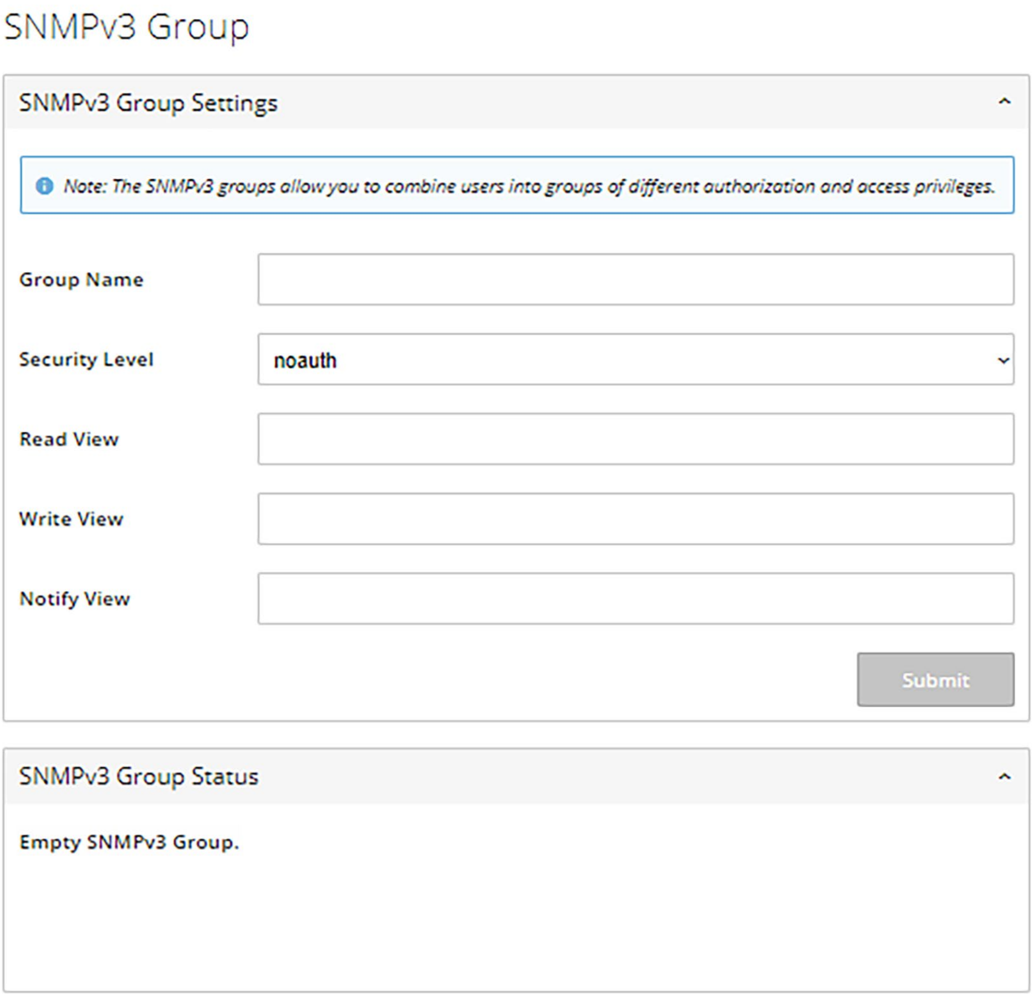
Table 39: Tab “Configuration” – Menu “SNMP” – “SNMP Trap” – “Trap Receiver Settings”

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” in the selection box if you want to use SNMP Version v1.
	v2c	Select “v2c” in the selection box 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 used 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 in use.
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.

9.2.3.5 SNMPv3 Group

Note

Possibilities of SNMPv3 groups
The SNMPv3 groups allow you to combine users into groups of different authorization and access privileges.



SNMPv3 Group

SNMPv3 Group Settings

Note: The SNMPv3 groups allow you to combine users into groups of different authorization and access privileges.

Group Name	
Security Level	noauth
Read View	
Write View	
Notify View	

SNMPv3 Group Status

Empty SNMPv3 Group.

Figure 50: Tab “Configuration” – Menu “SNMP” – “SNMPv3 Group”

Table 40: Tab “Configuration” – Menu “SNMP” – “SNMPv3 Group”

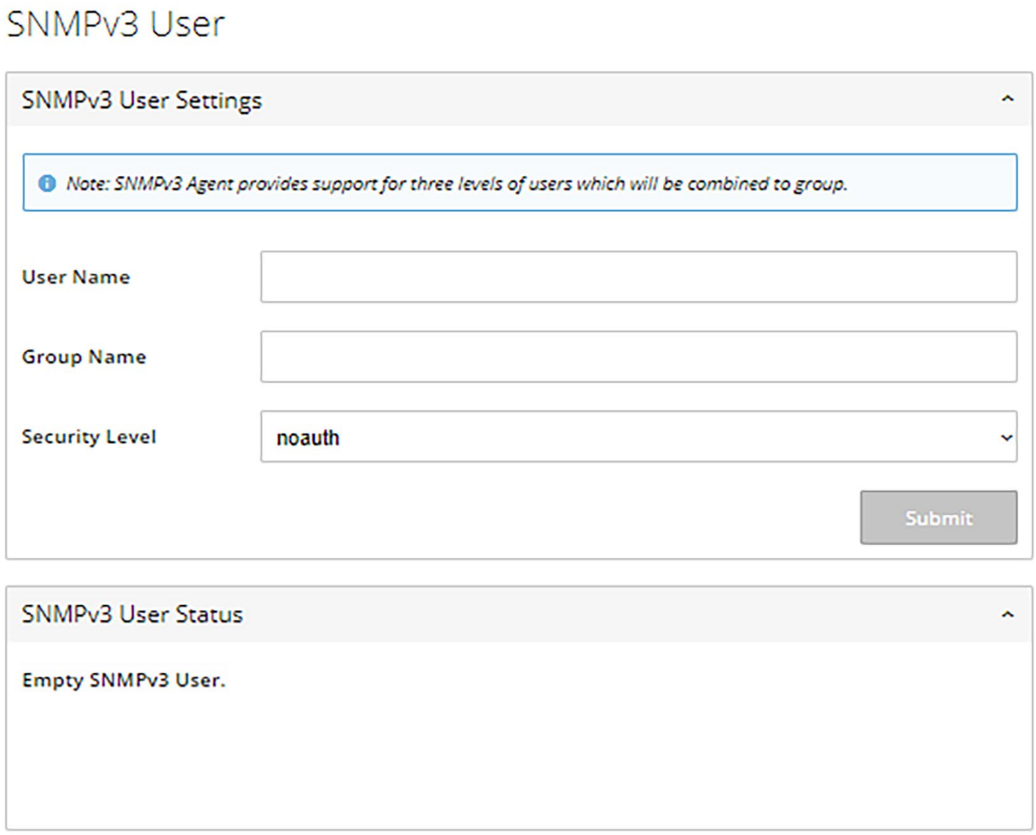
SNMPv3 Group Settings		
Parameter	**Default**	**Description**
Group Name		In the input field, enter the group name for the SNMPv3 group.
Security Level		This selection box is used to select the security level.
	noauth auth priv	Select the respective security level in the selection box.
Read View	**None**	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	**None**	In the input field, enter the name of the objects to which you want to grant write access. If no write or notify view is defined, no write access is granted and no objects can send notifications to members of the group.
Notify View	**None**	In the input field, enter the name of the object that can receive user notifications. By using a notify view, a group determines the list of notifications its users can receive.
SNMPv3 Group Status		
Parameter	**Default**	**Description**
Group Name		This column displays the group name.
Security Model		This column displays the selected security level. Always displayed v3: User-based Security Model (USM)
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.

9.2.3.6 SNMPv3 User

Note

SNMPv3 Agent support

SNMPv3 Agent provides support for three levels of users, which will be combined to group.



SNMPv3 User

SNMPv3 User Settings

Note: SNMPv3 Agent provides support for three levels of users which will be combined to group.

User Name	
Group Name	
Security Level	noauth

SNMPv3 User Status

Empty SNMPv3 User.

Figure 51: Tab “Configuration” – Menu “SNMP” – “SNMPv3 User”

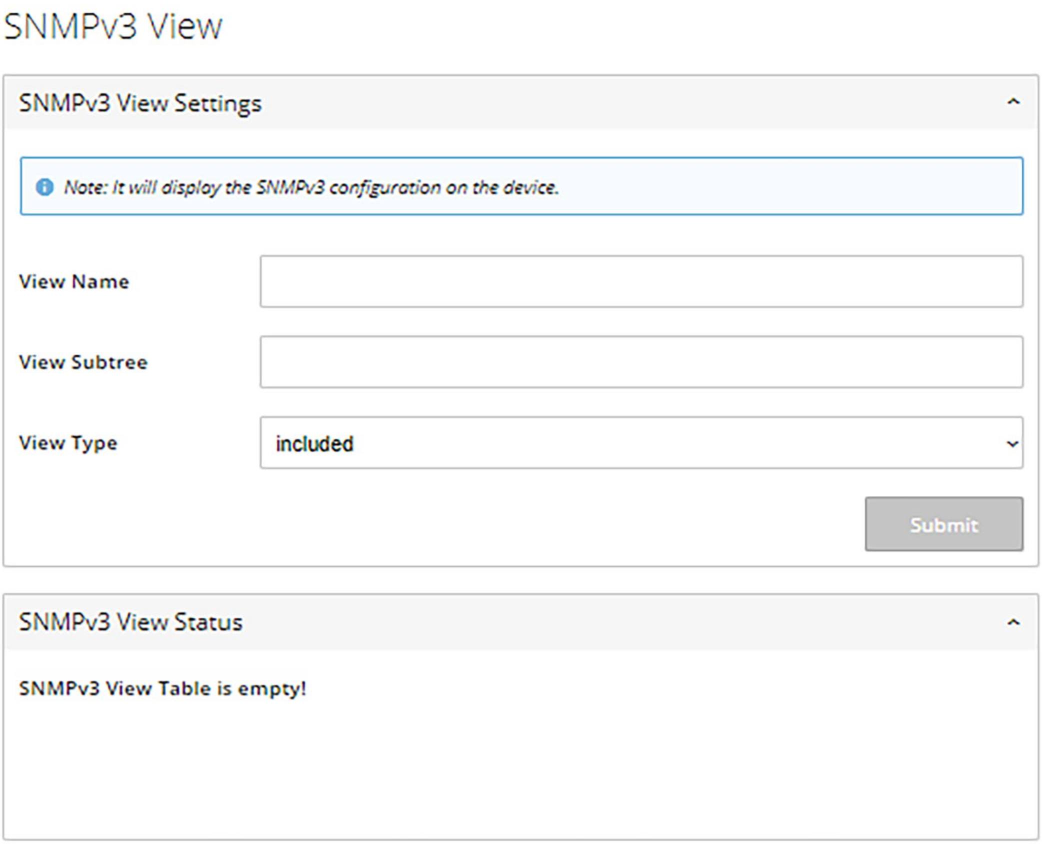
Table 41: Tab “Configuration” – Menu “SNMP” – “SNMPv3 User”

SNMPv3 User Settings		
Parameter	**Default**	**Description**
User Name		In the input field, enter a new user name, or modify an existing user name.
Group Name		In the input field, enter the group name for the SNMPv3.
Security Level		This selection box is used to select the security level.
	noauth	If you selected “noauth” in the selection box, you then cannot change the “Auth Algorithm” or the “Priv Algorithm.”
	auth	If you selected “auth” in the selection box, you then can change the “Auth Algorithm” and the “Auth Password.”
	priv	If you selected “priv” in the selection box, you then can change the “Auth Algorithm,” the “Priv Algorithm” and the “Priv Password.”
SNMPv3 User Status		
Parameter	**Default**	**Description**
User Name		This column displays the user name.
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.”
Action		Click **[Delete]** to delete a specific entry.

9.2.3.7 SNMPv3 View

Note

Display SNMPv3 configuration
It will display the SNMPv3 configuration on the device.



SNMPv3 View

SNMPv3 View Settings

Note: It will display the SNMPv3 configuration on the device.

View Name

View Subtree

View Type: included

SNMPv3 View Status

SNMPv3 View Table is empty!

Figure 52: Tab “Configuration” – Menu “SNMP” – “SNMPv3 View”

Table 42: Tab “Configuration” – Menu “SNMP” – “SNMPv3 View”

SNMPv3 View Settings		
Parameter	**Default**	**Description**
View Name		In the input field, enter the name for the SNMPv3 view.
View Subtree		In the input field, enter the name for the subtree.
View Type	**included**	If you selected “included” in the selection box, the subtree is inserted
	excluded	If you selected “excluded” in the selection box, the subtree is not inserted.
SNMPv3 View Status		
Parameter	**Default**	**Description**
View Name		This column displays the name of the SNMPv3 view.
View Subtree		This column displays the name of the subtree.
View Type	Inserted Removed	This column displays the selected type.
Action		Click **[Delete]** to delete a specific entry.

9.2.4 System Management

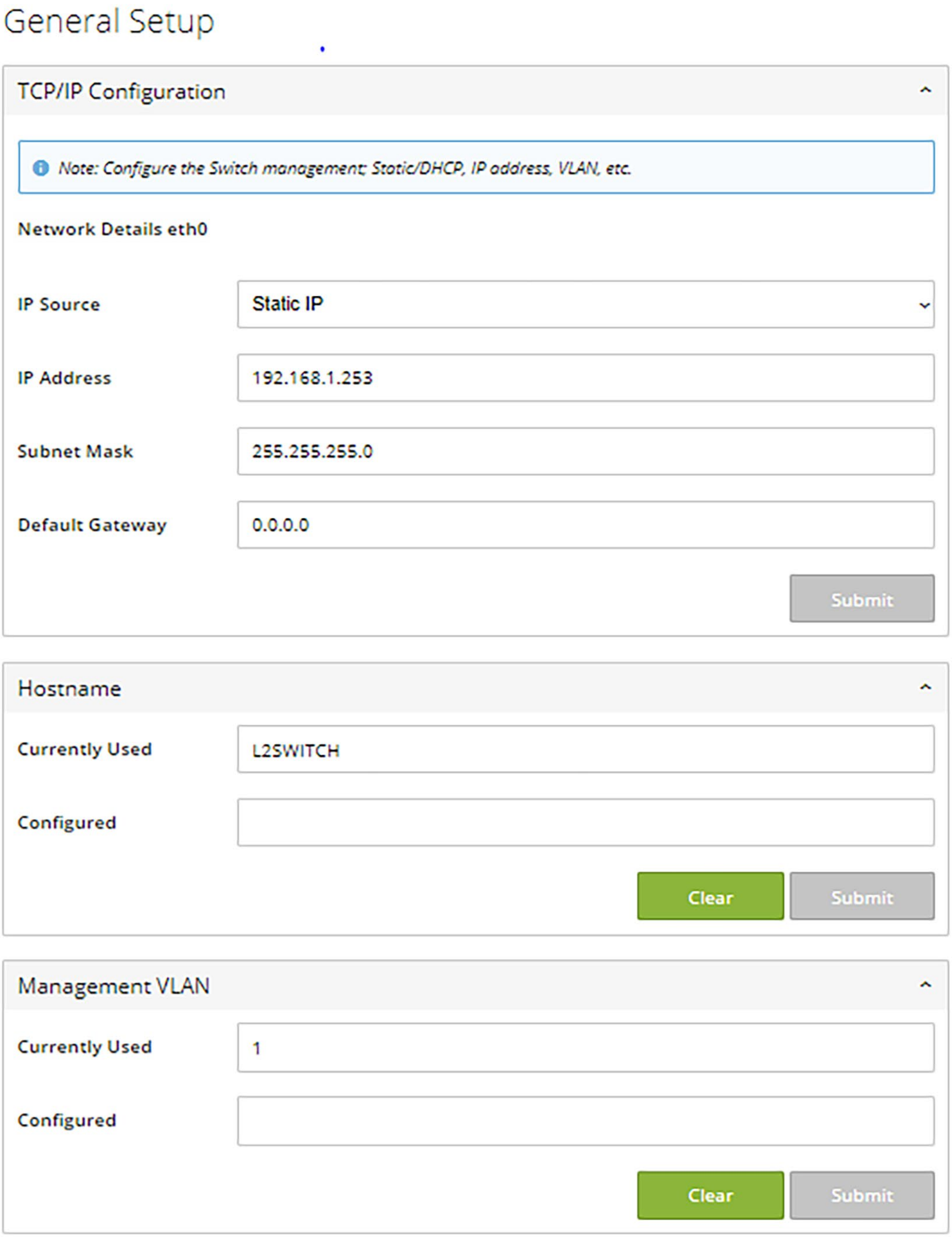
9.2.4.1 General Setup

Host Name

The hostname is same as the SNMP system name. Its length is up to 64 characters.

Note

Configure the switch management
Configure the switch management, static/DHCP, IP address, VLAN etc.



General Setup

TCP/IP Configuration

Note: Configure the Switch management: Static/DHCP, IP address, VLAN, etc.

Network Details eth0

IP Source	Static IP
IP Address	192.168.1.253
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

Hostname

Currently Used	L2SWITCH
Configured	

Management VLAN

Currently Used	1
Configured	

Figure 53: Tab “Configuration” – Menu “System Management” – “General Setup”

Table 43: Tab “Configuration” – Menu “System Management” – “General Setup”

TCP/IP Configuration		
Parameters	**Default**	**Description**
IP Source	**Static IP** DHCP	This selection box is used to select the option for the IP source.
IP Address	**192.168.1.254**	Enter the IP address of the switch in decimal-point notation.
Subnet Mask	**255.255.255.0**	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.
Hostname		
Parameters	**Default**	**Description**
Currently Used	**L2SWITCH**	This column displays the host name.
Configured		In the input field, enter the host name.
Management VLAN		
Parameters	**Default**	**Description**
Currently Used	**1**	This column displays the management VLAN.
Configured		In the input field, enter the management VLAN.

9.2.4.2 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 **Universel Coordonné**”). 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.

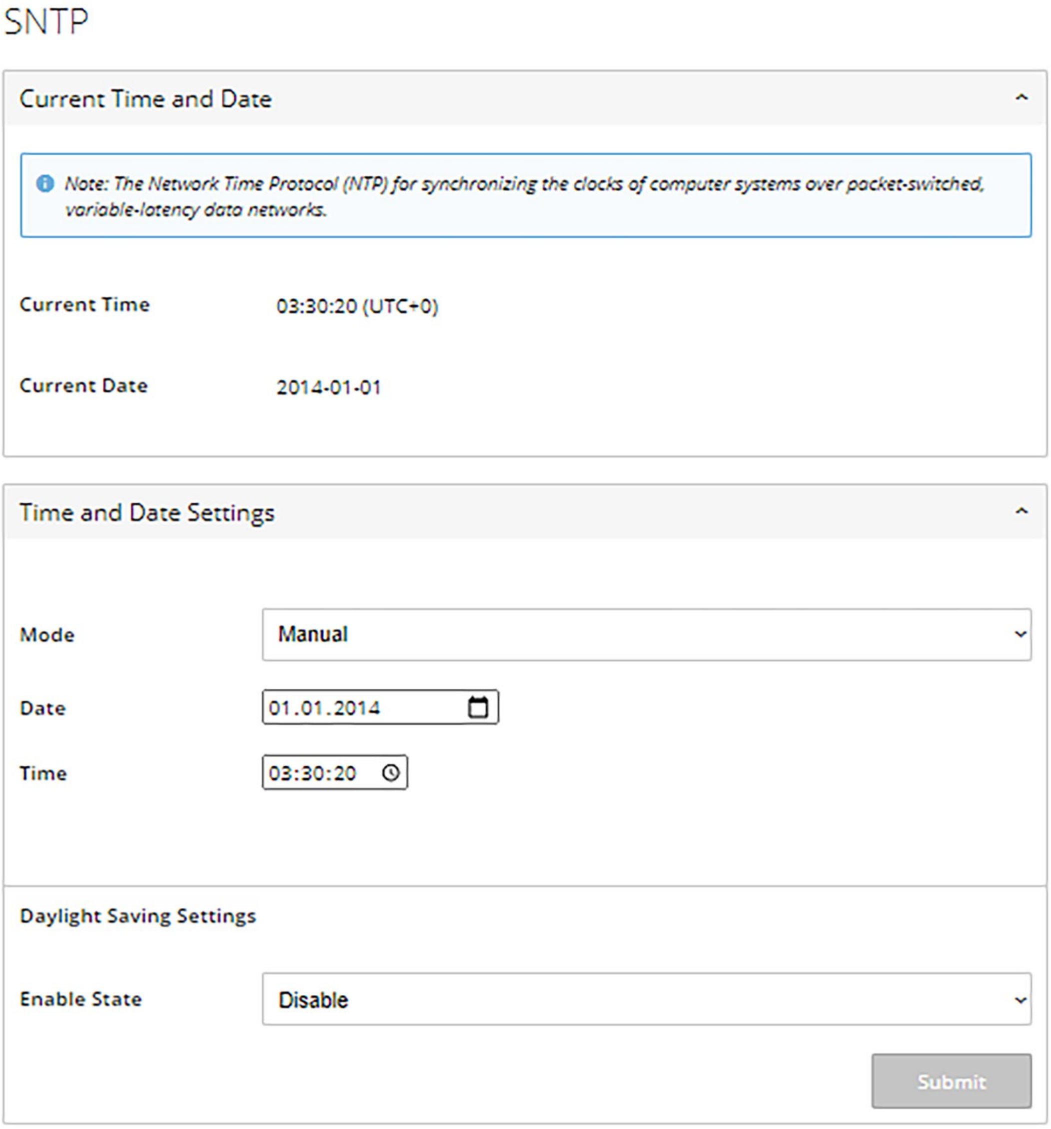
Note

Note!

1. The SNTP server always replies the current UTC time.
2. If the switch receives the SNTP reply time, it adjusts the 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 challenge 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 changes, the switch repeats the request process.
7. No default SNTP server.

Note

Synchronization of the clocks of computer systems
The Network Time Protocol (NTP) for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.



SNTP

Current Time and Date

Note: The Network Time Protocol (NTP) for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

Current Time 03:30:20 (UTC+0)

Current Date 2014-01-01

Time and Date Settings

Mode: Manual

Date: 01.01.2014

Time: 03:30:20

Daylight Saving Settings

Enable State: Disable

Figure 54: Tab “Configuration” – Menu “System Management” – “SNTP”

Table 44: Tab “Configuration” – Menu “System Management” – “SNTP”

<table>
<tr><th colspan="5">Current Time and Date</th></tr>
<tr><th>Parameters</th><th>Default</th><th colspan="3">Description</th></tr>
<tr><td>Current Time</td><td></td><td colspan="3">This field displays the current time if you open or refresh the menu.</td></tr>
<tr><td>Current Date</td><td></td><td colspan="3">The field displays the current date if you open or refresh the menu.</td></tr>
<tr><th colspan="5">Time and Date Settings</th></tr>
<tr><th>Parameters</th><th>Default</th><th colspan="3">Description</th></tr>
<tr><td rowspan="11">Mode</td><td rowspan="3">Manual</td><td colspan="3">Select this option if you want to manually set the time and date for the system.
Click <b>[Submit]</b> to display the “Current Time” and “Current Date”.</td></tr>
<tr><td>Date</td><td colspan="2">Enter the new date in the format day//month/ year format.
TT.MM.JJJJ</td></tr>
<tr><td>Time</td><td colspan="2">Enter the new time in the format hour/minute/second.
--:--:--</td></tr>
<tr><td>Network Time Protocol</td><td colspan="3">Select this option to use NTP (“Network Time Protocol”) for the time service.</td></tr>
<tr><td rowspan="6">NTP Server
<b>0.0.0.0</b></td><td rowspan="3">Public</td><td colspan="2">Select this option if you want to use a public server.</td></tr>
<tr><td>ntp0.fau.de - Europe</td><td></td></tr>
<tr><td>ntps1-1.cs.tu-berlin.de - Europe</td><td></td></tr>
<tr><td rowspan="3">Manual</td><td colspan="2">Select this option if you want to use manually settings.</td></tr>
<tr><td>IP</td><td>Enter the IP address of the NTP server in decimal-point notation.</td></tr>
<tr><td>Domain Name</td><td>Enter the domain address of the switch.</td></tr>
<tr><td>Time Zone
<b>+0000</b></td><td colspan="3">Enter the time difference between UTC (“Universal Time Coordinated”, formally GMT “Greenwich Mean Time”) and the time zone in hh.mm.</td></tr>
</table>

Table 44: Tab “Configuration” – Menu “System Management” – “SNTP”

Daylight Saving Settings		
Parameters	**Default**	**Description**
Enable 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).

9.2.4.3 User Account

The switch allows users to create up to six user accounts. The user name and password must be a combination of numbers or 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 supports two types of user accounts:

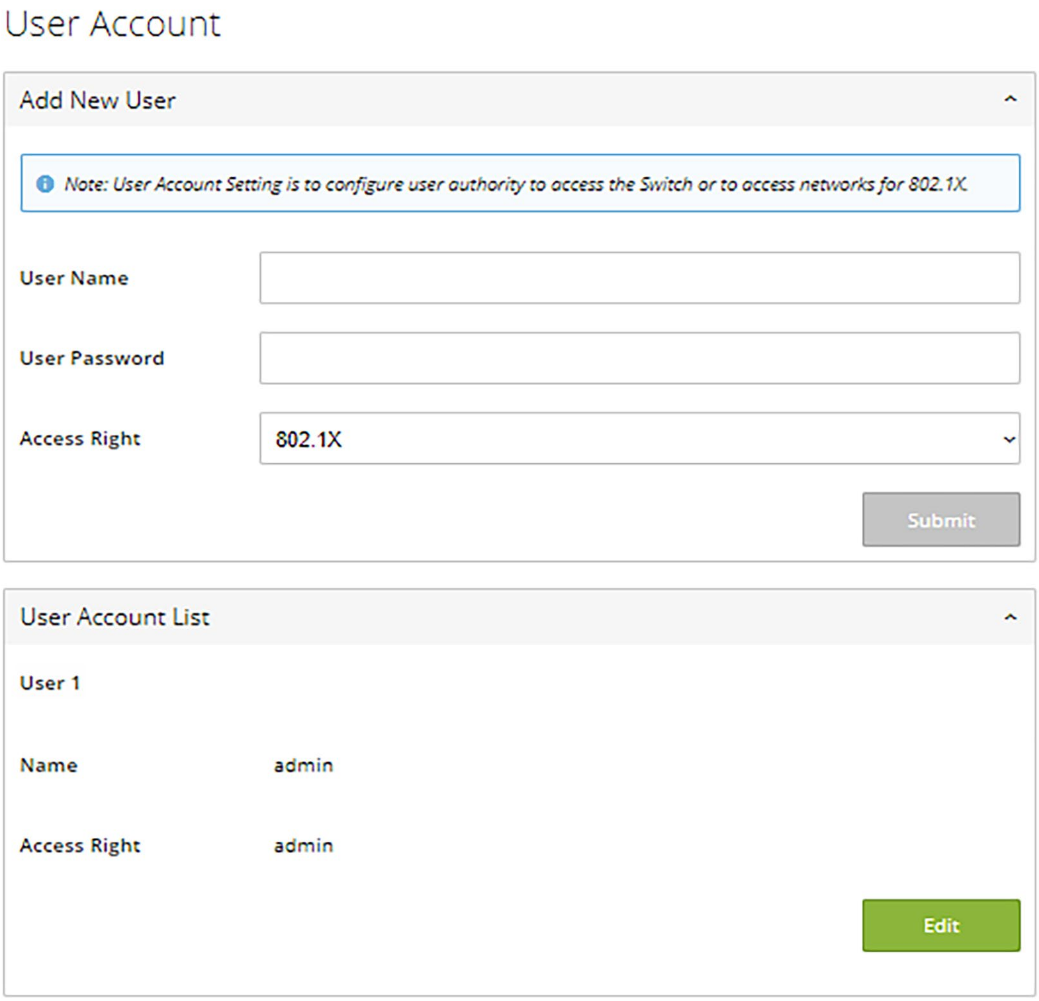
The default user accounts have the following credentials:
User Name = “admin”
User Password = “wago”

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.

Note

User Account Setting

User Account Setting is to configure user authority to access the switch or to access networks for 802.1X.



User Account

Add New User

Note: User Account Setting is to configure user authority to access the Switch or to access networks for 802.1X.

User Name

User Password

Access Right: 802.1X

User Account List

User 1

Name: admin

Access Right: admin

Figure 55: Tab “Configuration” – Menu “System Management” – “User Account”

Table 45: Tab “Configuration” – Menu “System Management” – “User Account”

User Account Settings		
Parameter	**Default**	**Description**
User Name		In the input field, enter a new user name, or modify an existing user name.
User Password		In the input field, enter a new password, or modify an existing password. You can enter up to 32 alphanumeric characters or digits.
User Authority		In this box, select the type of user account.
	802.1X	Select “802.1X” in the selection box if you need this users for authentication.
	Normal (Read Only)	Select “Normal (Read Only)” in the selection box if you need only read permission for this user account.
	Admin	Select “Admin” in the selection box if you need read and write permission for this user account.
User Account List		
Parameter	**Default**	**Description**
No.		This column displays the index number of an entry.
Name		This column displays the name of the user account.
Access Right		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.

9.2.5 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.

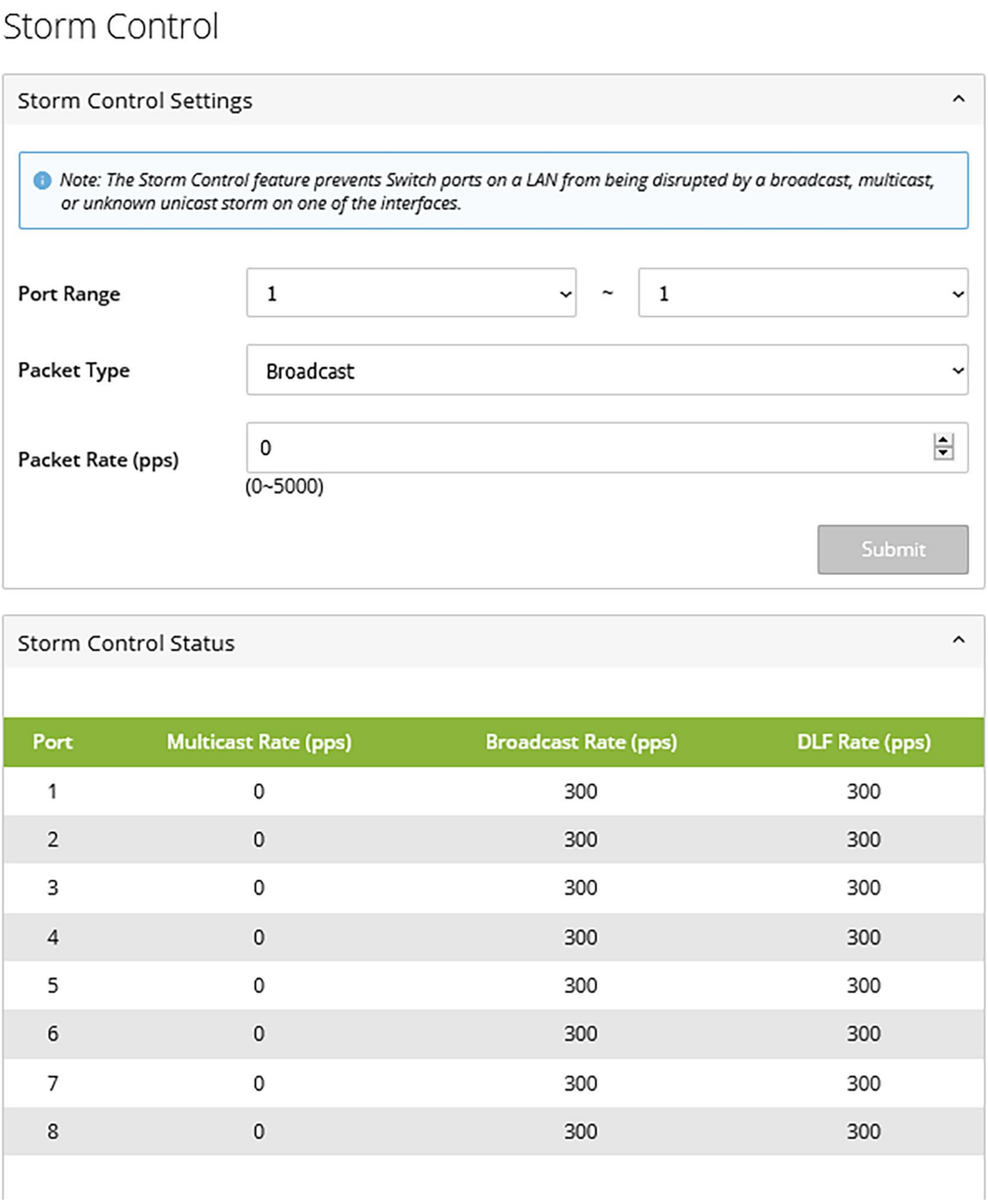
“Broadcast Storm Control” limits the number of broadcast, multicast and unknown unicast (also referred to as “Destination Lookup Failure” or DLF) packets the switch receives per second on the ports. If the maximum number of packets per second is reached, all subsequent packets are discarded. Enable this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

The default rate is 300 Mbit/s for Broadcast and DLF. You can set to maximum rate of 5000 Mbit/s for multicast, broadcast or DLF.

Note

Function of the Storm Control feature

The Storm Control feature prevents switch ports on a LAN from being disrupted by a broadcast, multicast or unknown unicast storm on one of the interfaces.



Storm Control

Storm Control Settings

Note: *The Storm Control feature prevents Switch ports on a LAN from being disrupted by a broadcast, multicast, or unknown unicast storm on one of the interfaces.*

Port Range: 1 ~ 1

Packet Type: Broadcast

Packet Rate (pps): 0
(0~5000)

Storm Control Status

Port	Multicast Rate (pps)	Broadcast Rate (pps)	DLF Rate (pps)
1	0	300	300
2	0	300	300
3	0	300	300
4	0	300	300
5	0	300	300
6	0	300	300
7	0	300	300
8	0	300	300

Figure 56: Tab “Configuration” – Menu “Storm Control” (Example)

Table 46: Tab “Configuration” – Menu “Storm Control” (Example)

Storm Control Settings		
Parameter	**Default**	**Description**
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Loop Detection” settings.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Loop Detection” settings.
Packet Type	Broadcast	Choose “Broadcast” in the selection box to specify a limiting value for the number of broadcast packets received per second.
	Multicast	Choose “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.
Packet Rate (0-5000)	300 = Broadcast/DLF Rate 0 = Multicast	In the selection box, choose the number of packets (of the type specified in the “Type” field) that the switch can receive per second.
Storm Control Status		
Parameter	**Default**	**Description**
Port	1 … 8	This column shows the port numbers.
Multicast Rate (pps)		This column displays the multicast traffic flooding control state on the port.
Broadcast Rate (pps)		This column displays the broadcast traffic flooding control state on the port.
DLF Rate (pps)		This column displays the DLF traffic flooding control state on the port.

9.3 Security

9.3.1 802.1X

9.3.1.1 IEEE 802.1X Communication Standard

IEEE 802.1X is an IEEE standard for port-based Network Access Control ("port" meaning a single point of attachment to the LAN infrastructure). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism for devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. It is used for most wireless 802.11 access points and is based on EAP ("**E**xtensible **A**uthentication **P**rotocol").

IEEE 802.1X provides port-based authentication, which involves communications between a so-called supplicant, authenticator and authentication server. The supplicant is often software on a client device, such as a laptop, the authenticator is a wired ETHERNET switch or wireless access point, and the authentication server is generally a RADIUS ("**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice") database.

The authenticator acts like a security guard for the protected network. The supplicant (e.g., client device) is not allowed access the protected side of the network through the authenticator until the supplicant's identity is authenticated. With 802.1X port-based authentication, the supplicant provides credentials, such as a user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the credentials are valid (in the authentication server database), the supplicant (client device) is allowed to access resources located on the protected side of the network.

Upon detection of a new client ("supplicant"), the port on the switch ("authenticator") is enabled and set to the "unauthorized" state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is blocked on the network layer (Layer 3). The authenticator sends out the EAP identity request to the supplicant, the supplicant responds with the EAP response packet, which the authenticator forwards to the authenticating server. If the authenticating server accepts the request, the authenticator sets the port to the "authorized" mode, and normal traffic is allowed. If the supplicant logs off, it sends an EAP logoff message to the authenticator. The authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.

RADIUS Server

The RADIUS server ("**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice") is a client/server-based security protocol for authentication and control of network access permissions.
The RADIUS server operates using the Challenge/Response process and supports central administration of user data, such as user ID, passwords, phone numbers, access rights and account data, and consists of an accounting and authentication protocol.
In combination with DHCP and PPP, configuration of dial-in systems can occur automatically with RADIUS.

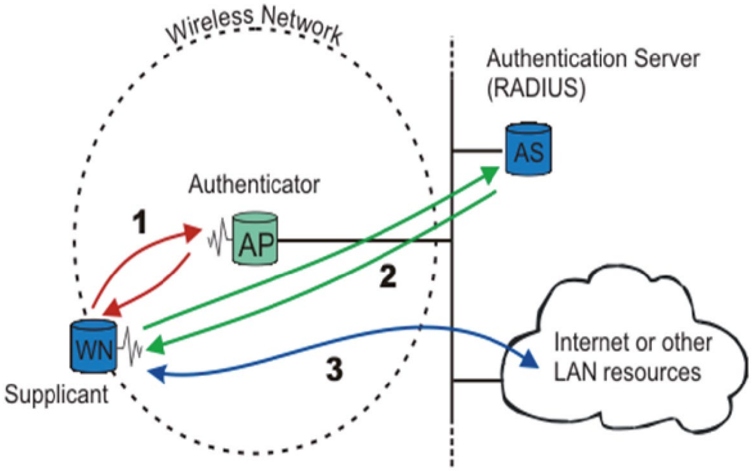


Figure 57: IEEE 802.1X

The following figure illustrates how a client connecting to an IEEE 802.1X-authentication-enabled port goes through the validation process. The switch prompts the client for login information in the form of a user name and password.

Once the client provides the login credentials, the switch sends an authentication request to the RADIUS server. The RADIUS server checks whether this client is allowed access to the port.

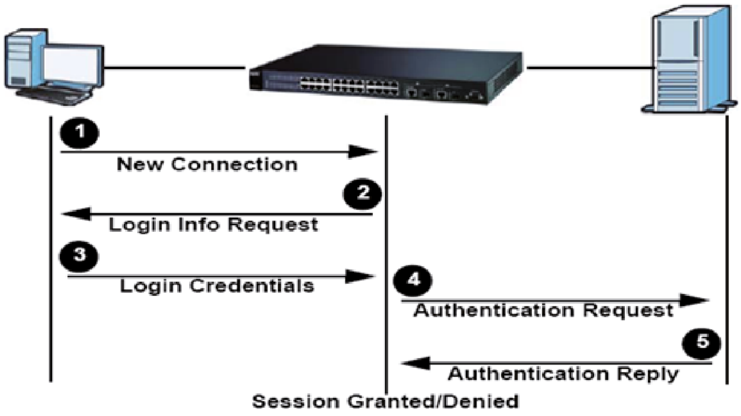


Figure 58: RADIUS Server

Local User Accounts

By storing user profiles locally on the switch, the switch can authenticate users without interacting with the network authentication server. However, there is a limit to six users that can be authenticated in this way.

Guest VLAN

The Guest VLAN function in IEEE 802.1X port-based authentication on the switch provides limited services to clients, such as downloading the IEEE 802.1X client. These clients can update their system for IEEE 802.1X authentication.

If you enable a guest VLAN on an IEEE 802.1X port, the switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL (“EAP over LAN”) packets are not sent by the client.

Port Parameters

- **Admin Control Direction**
  Both - If 802.1X port authentication for a user has failed, incoming and outgoing packets on the port are dropped.
  Incoming - If 802.1X port authentication for a user has failed, only incoming packets on the port are dropped.

- **Re-Authentication**
  This function specifies whether a subscriber must periodically re-enter his or her user name and password to stay connected to the port.

- **Reauth Period**
  The “Reauth Period” function is used to specify how often a client has to re-enter his or her username and password to stay connected to the port. The permissible range for this field is 0 to 65535 seconds.

- **Port Control Mode**

“Auto”	Users can access the network after authentication.
“Force-authorized”	Users can access the network without authentication.
“force-unauthorized”	Users cannot access the network.

- **Quiet Period**
  The “Quiet Period” function is used to specify the time a client has to wait before the next authentication attempt. This prevents the switch from becoming overloaded with continuous authentication attempts from the client. The permissible range for this field is 0 to 65535 seconds.

- **Server Timeout**
  The “Server Timeout” value is used for timing out the authentication server.

- **Supp Timeout**
  The “Supp Timeout” value is the initialization value used for timing out a supplicant.

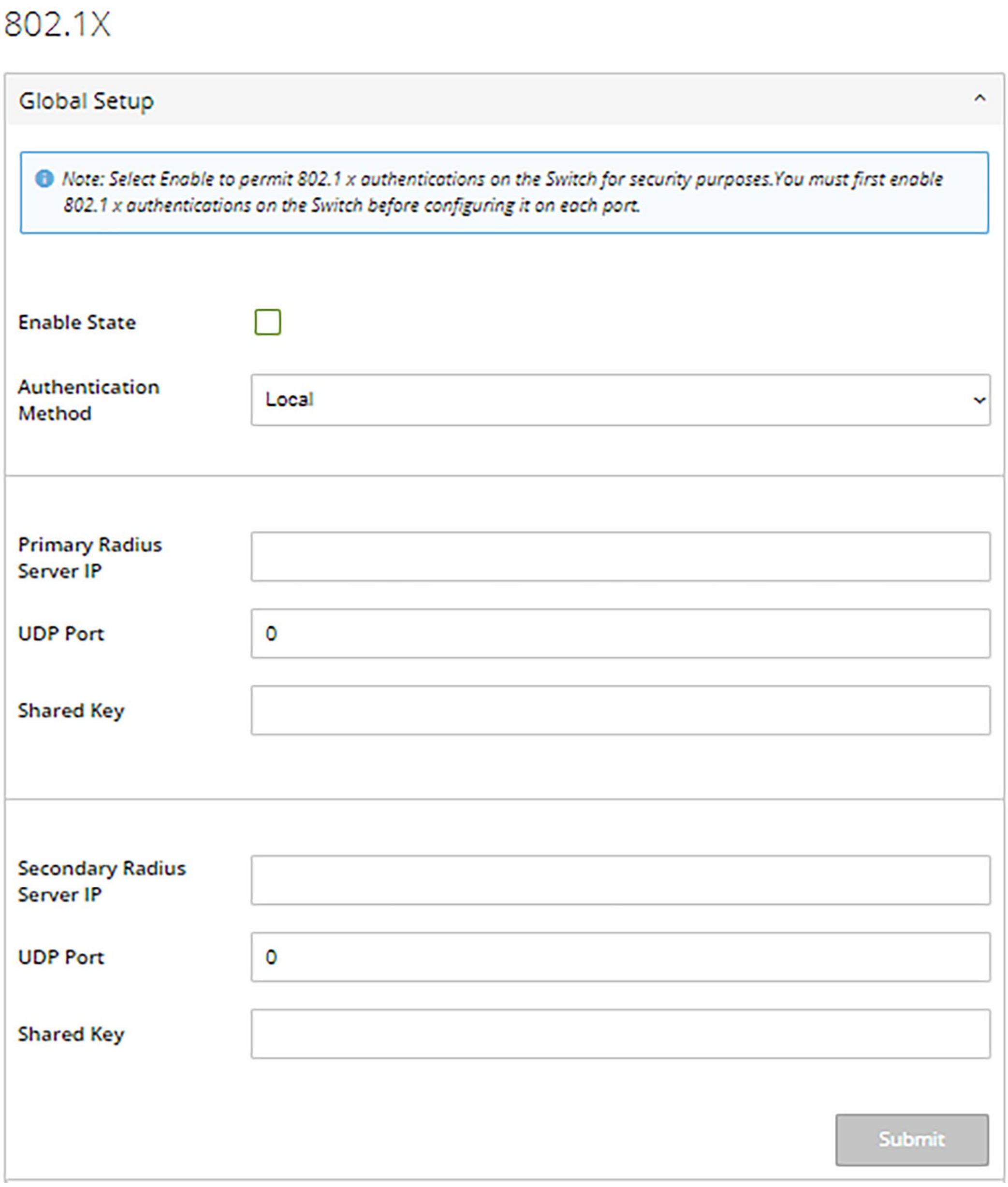
- **Max Req Time**
  The “Max Req Time” specifies how often the switch attempts to connect to the authentication server before determining that the server is down. The permissible range for this field is 1 to 10 attempts.

9.3.1.2 Global Setup

Note

Activate 802.1X authentication

Select enable to permit 802.1X authentications on the switch for security purposes. You must first enable 802.1X authentications on the switch before configuring it on each port.



802.1X

Global Setup

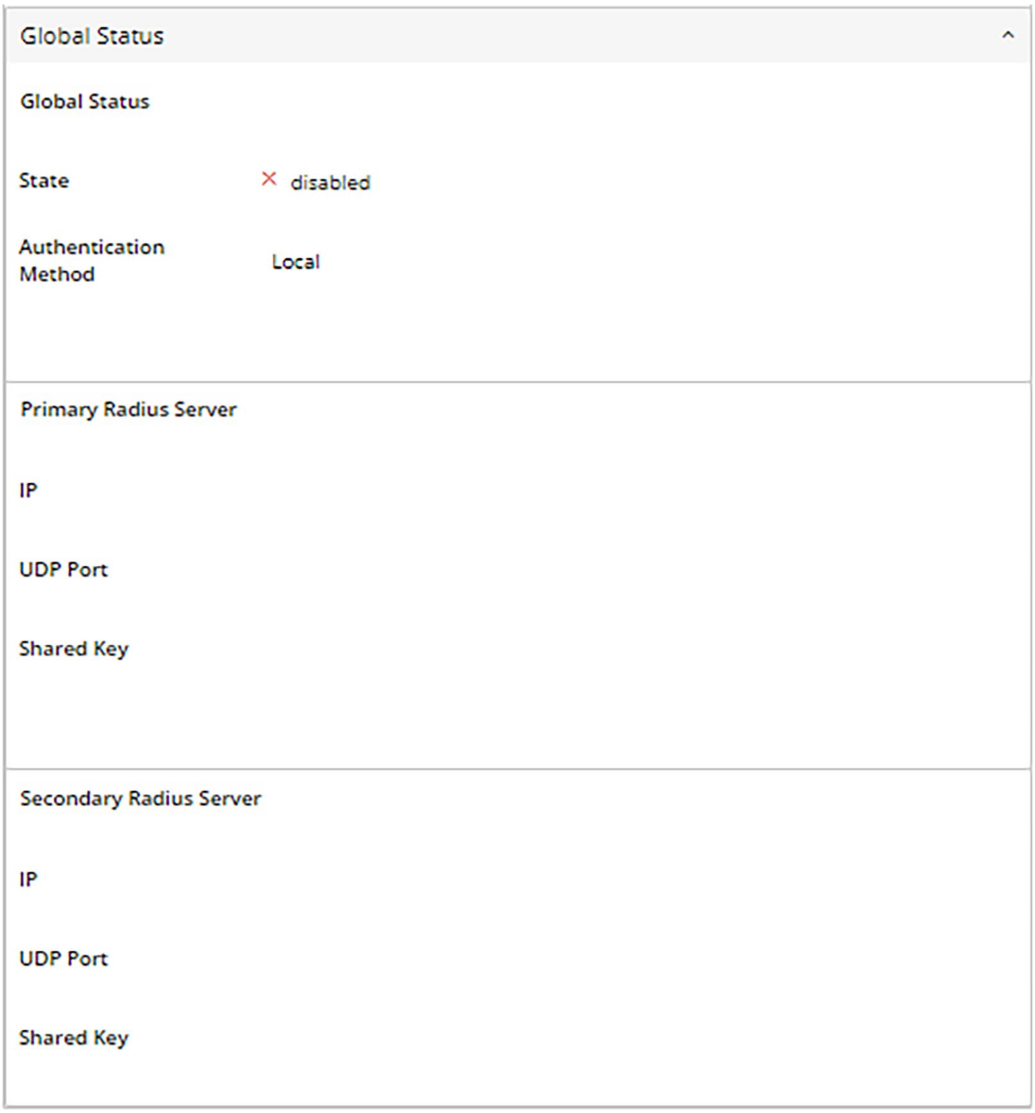
Note: Select Enable to permit 802.1 x authentications on the Switch for security purposes.You must first enable 802.1 x authentications on the Switch before configuring it on each port.

Enable State	□
Authentication Method	Local
Primary Radius Server IP	
UDP Port	0
Shared Key	
Secondary Radius Server IP	
UDP Port	0
Shared Key	

Figure 59: Tab “Security” – Menu “802.1X” – “Global Setup”

Table 47: Tab “Security” – Menu “802.1X” – “Global Setup”

Global Setup		
Parameter	**Default**	**Description**
Enable State	□	□ The function “802.1X” is not enabled.
		☑ The function “802.1X” port is not enabled.
		Note **IEEE 802.1X Authentication** You must first enable IEEE 802.1X authentication on the switch before you can configure this function for individual ports.
Authentication Method	**Local**	Select “Local” in the selection box to use the “Guest” and “User” user groups from the user account database on the switch for authentication. However, the number of nodes that can exist at the same time is limited.
	Radius	Select “Radius” in the selection box to enable the security protocol that uses an external server for user authentication, in contrast to the internal user database, in devices with limited storage. In general, “RADIUS” allows validation of an unlimited number of users from a central location.
Primary Radius Server IP		If you selected “Radius” for the authentication method, the primary Radius server is used for all authentication requests. In the input field, enter the IP address of the external Radius server in decimal-point notation.
UDP Port	**0**	In the input field, enter the UDP port.
Shared Key		In the input field, enter a password (up to 32 alphanumeric characters) to use as the common key for the connection between the external Radius server and the switch. This key must not be sent over the network. The key must be identical on the external RadiusADIUS server and the switch.
Secondary RADIUS Server IP		This is the back-up server that is only used if the primary Radius server fails.
UDP Port	**0**	In the input field, enter the IP address of the external RADIUS server in decimal-point notation.
Shared Key		In the input field, enter a password (up to 32 alphanumeric characters) to use as the common key for the connection between the external Radius server and the switch. This key must not be sent over the network. The key must be identical on the external RadiusADIUS server and the switch. Secondary RADIUS Server IP This is the back-up server



Global Status

Global Status

State ✕ disabled

Authentication Method Local

Primary Radius Server

IP

UDP Port

Shared Key

Secondary Radius Server

IP

UDP Port

Shared Key

Figure 60: Tab “Security” – Menu “802.1X” – “Global Status”

Table 48: Tab “Security” – Menu “802.1X” – “Global Status”

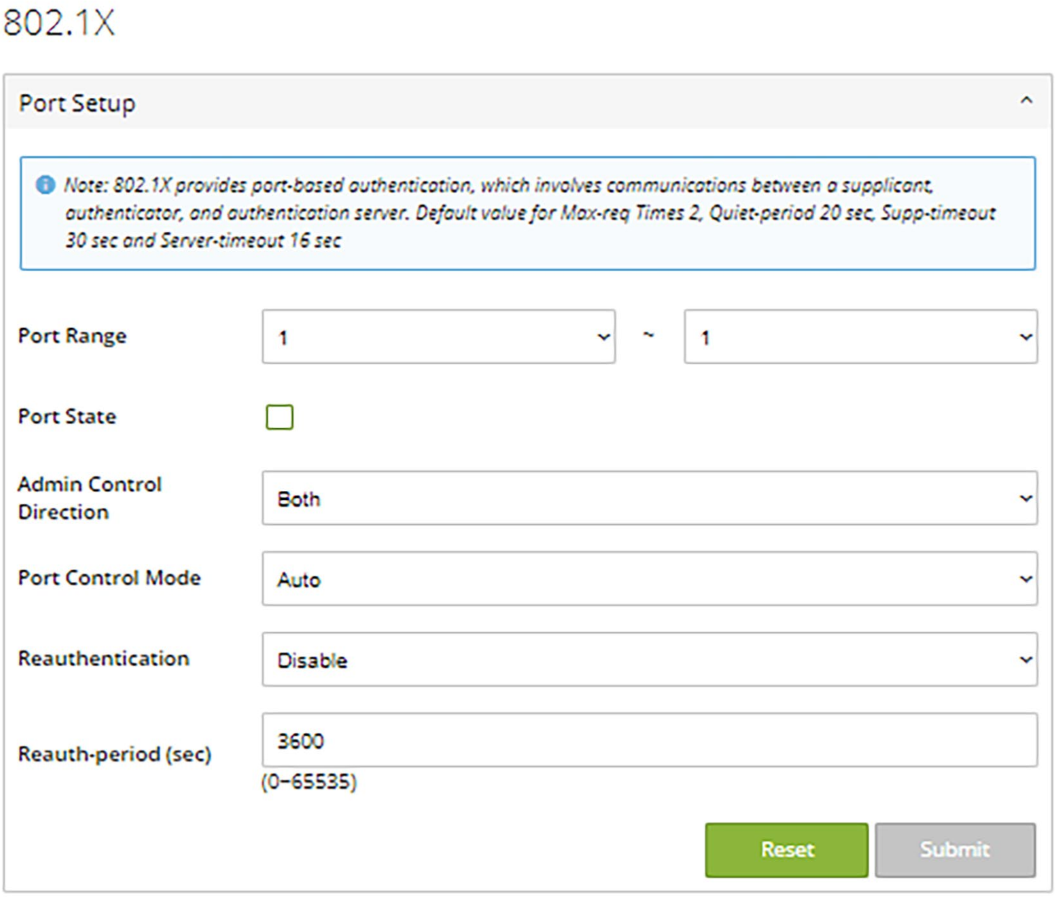
Global Status		
Parameter	**Default**	**Description**
State	Disable Enable	This field indicates whether IEEE 802.1X authentication is enabled or disabled.
Authentication Method	Local Radius	This field displays the authentication method.
Primary RADIUS Server	IP	This field displays the IP address, UDP port and common key for the primary Radius server. The fields are empty if no configuration is performed.
	UDP Port	
	Shared Key	
Secondary RADIUS Server	IP	This field displays the IP address, UDP port and common key for the secondary Radius server. The fields are empty if no configuration is performed.
	UDP Port	
	Shared Key	

9.3.1.3 Port Setup

Note

802.1X Authentication

802.1X provides port-based authentication, which involves communications between a supplicant authenticator and authentication server.
Default value for Max-req Times 2, Quiet-period 20 s, Supp-timeout 30 s and server-timeout 16 s.



802.1X

Port Setup

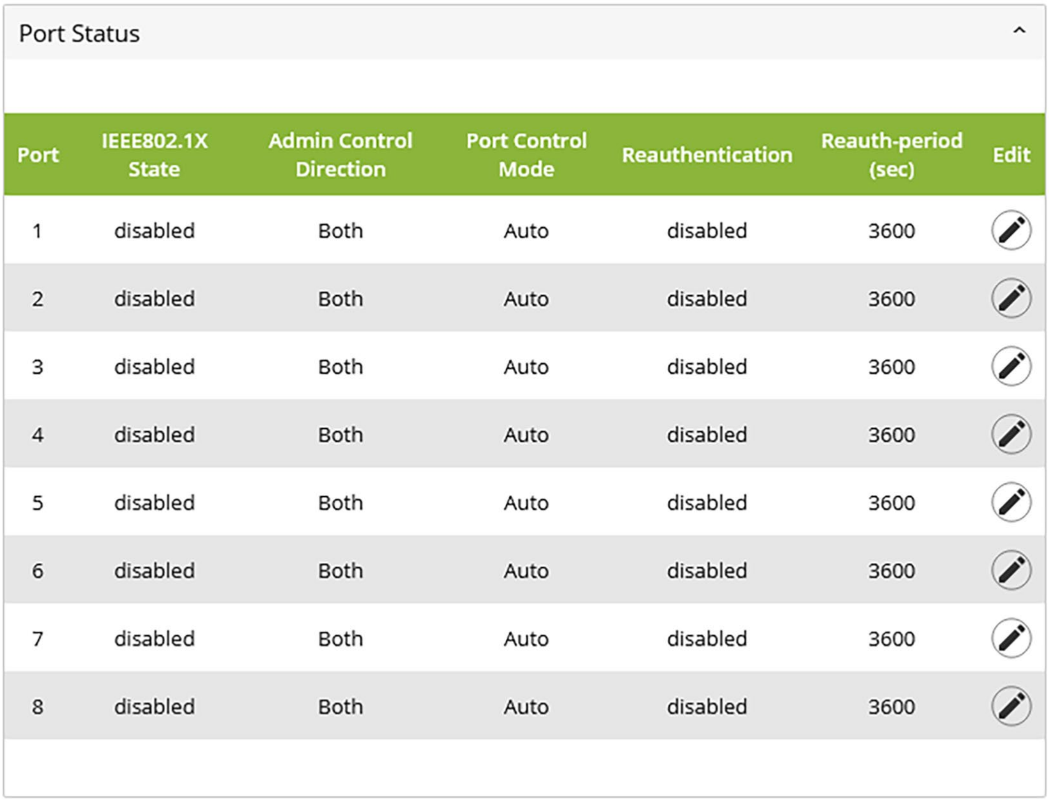
Note: 802.1X provides port-based authentication, which involves communications between a supplicant authenticator, and authentication server. Default value for Max-req Times 2, Quiet-period 20 sec, Supp-timeout 30 sec and Server-timeout 16 sec

Port Range	1 ~ 1
Port State	□
Admin Control Direction	Both
Port Control Mode	Auto
Reauthentication	Disable
Reauth-period (sec)	3600 (0~65535)

Figure 61: Tab “Security” – Menu “802.1X” – “Port Setup”

Table 49: Tab “Security” – Menu “802.1X” – “Port Setup”

Port Settup		
Parameter	**Default**	**Description**
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “802.1X” Setting.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “802.1X” Setting.
Port State	☐	☐ The function “802.1X” is not enabled. ☑ The function “802.1X” port is not enabled. ➔ **Note** **IEEE 802.1X Authentication** You must first enable IEEE 802.1X authentication on the switch before you can configure this function for individual ports.
Admin Control Direction	**Both**	In the selection box, select “Both” to drop incoming and outgoing packets on the port when a user has not passed IEEE 802.1X port authentication.
	In	In the selection box, select “In” to drop only incoming packets on the port when a user has not passed IEEE 802.1X port authentication.
Reauthentication	**Disable**	Select “Disable” in the selection box if a subscriber does not have to regularly reenter the user name and password to remain connected to the port.
	Enable	Select “Enable” in the selection box if a subscriber has to regularly reenter the user name and password to remain connected to the port.
Port Control Mode	**Auto**	Select “Auto” in the selection box to enable authentication for the port.
	Force Authorized	Select “Force Authorized” in the selection box to enable permanent authentication for the port.
	Force Unauthorized	Select “Force Unauthorized” in the selection box to enable permanent denial of authentication for the port. No packets can pass through this port.
Reauth-period (sec) (0-65535)	**3600**	In the input field, enter a value for interval at which a subscriber has to reenter the user name and password to remain connected to the port.



Port Status

Port	IEEE802.1X State	Admin Control Direction	Port Control Mode	Reauthentication	Reauth-period (sec)	Edit
1	disabled	Both	Auto	disabled	3600	✎
2	disabled	Both	Auto	disabled	3600	✎
3	disabled	Both	Auto	disabled	3600	✎
4	disabled	Both	Auto	disabled	3600	✎
5	disabled	Both	Auto	disabled	3600	✎
6	disabled	Both	Auto	disabled	3600	✎
7	disabled	Both	Auto	disabled	3600	✎
8	disabled	Both	Auto	disabled	3600	✎

Figure 62: Tab “Security” – Menu “802.1X” – “Port Status” (Example)

Table 50: Tab “Security” – Menu “802.1X” – “Port Status” (Example)

Port Status		
Parameter	**Default**	**Description**
Port	1 **…** 8 (16)	This column shows the port numbers.
IEEE 802.1X State	Disable Enable	This column indicates whether IEEE 802.1X authentication for a port is enabled or disabled.
Admin Control Direction	Both In	This column displays the “Control Direction.”
Port Control Mode	Automatic, Force Authorized, Force Unauthorized	This column displays the port control mode.
Reauthentication	Disable Enable	This column indicates whether the subscriber has to reenter the user name and password regularly to remain connected to the port.
Reauth Period (sec)	0 … 65535	This column displays the interval at which a subscriber must reenter the user name and password to remain connected to the port.
Edit		Preselection for editing.

9.3.2 ACL

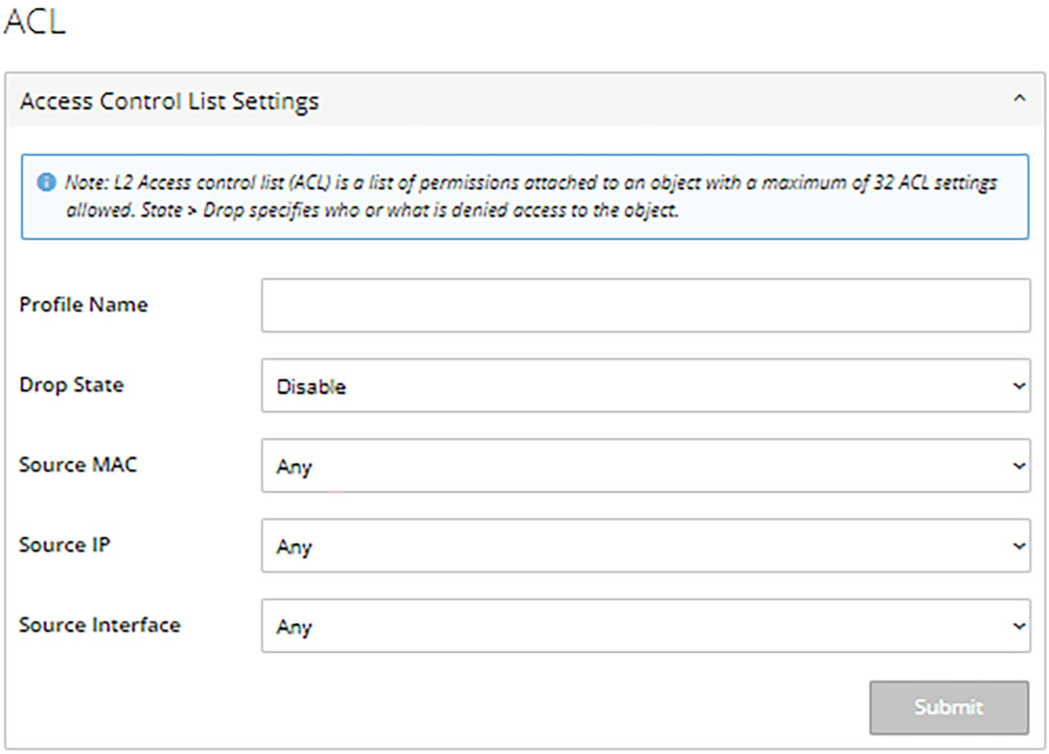
The ACL (“**A**ccess **C**ontrol **L**ist”) is a list of permissions attached to an object. The list specifies who or what is allowed to access an object and what operations are allowed to be performed on the object.

The ACL function allows users to configure a few rules to reject packets from the specific ingress ports or all ports. These rules check the source and destination MAC addresses of packets. If packets match these 32 rules, the system executes the “deny” action, meaning it rejects these packets.

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.

Note

Permissions of the Access Control List (ACL)
L2 Access Control List (ACL) is a list of permissions attached an object with an maximum of 32 ACL settings allowed. State > Drop specifies who or what is denied access to the object.



ACL

Access Control List Settings

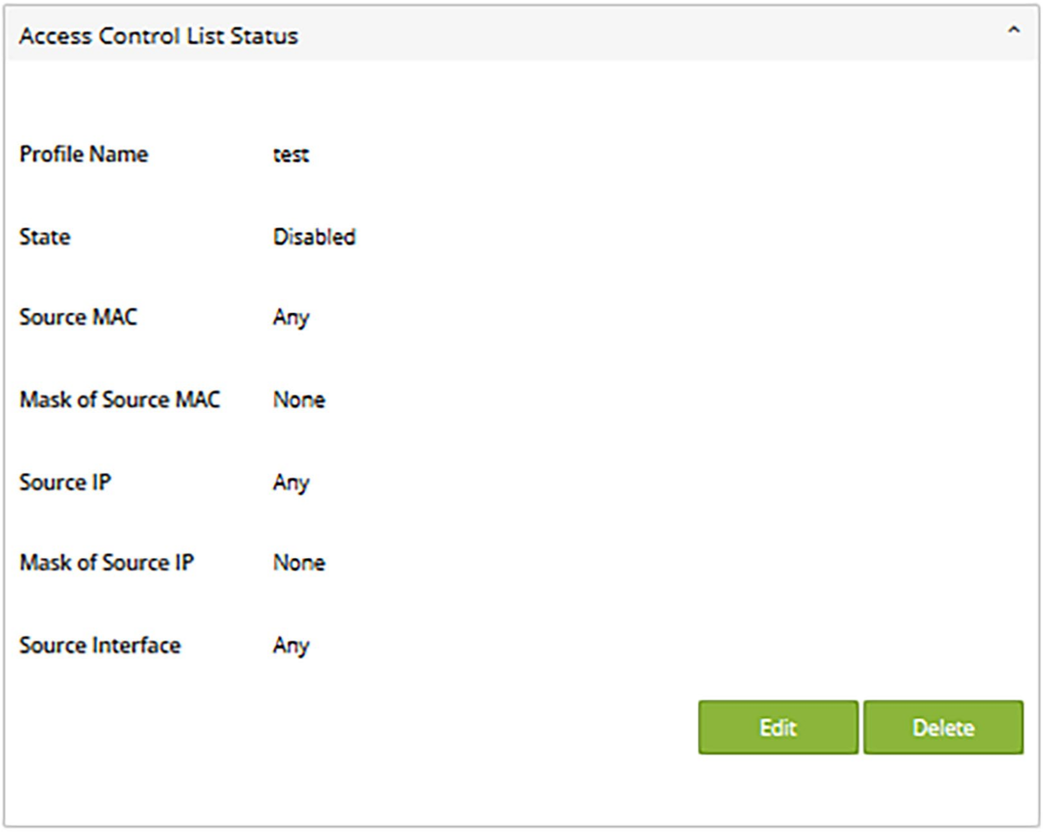
Note: L2 Access control list (ACL) is a list of permissions attached to an object with a maximum of 32 ACL settings allowed. State > Drop specifies who or what is denied access to the object.

Profile Name	
Drop State	Disable
Source MAC	Any
Source IP	Any
Source Interface	Any

Figure 63: Tab “Security” – Menu “ACL” – “Access Control List Settings”

Table 51: Tab “Security” – Menu “ACL” – “Access Control List Settings”

<table>
<tr><th colspan="4">Access Control List Settings</th></tr>
<tr><th>Parameter</th><th>Default</th><th colspan="2">Description</th></tr>
<tr><td>Profile Name</td><td></td><td colspan="2">In the input field, enter the name of the profile.</td></tr>
<tr><td rowspan="2">Drop State</td><td><b>Disable</b></td><td colspan="2">Select “Disable” in the selection if you will not the data packets are dropped.</td></tr>
<tr><td>Enable</td><td colspan="2">Select “enable” in the selection if you will the data packets are dropped.</td></tr>
<tr><td rowspan="2">Source MAC</td><td><b>Any</b></td><td colspan="2">Select “Any” in the selection box to make every MAC address valid.</td></tr>
<tr><td>Other</td><td colspan="2">Select “Other” in the selection box to enter the MAC address for the source in the access control list.</td></tr>
<tr><td rowspan="2">Source IP</td><td><b>Any</b></td><td colspan="2">Select “Any” in the selection box to make every IP address valid.</td></tr>
<tr><td>Other</td><td colspan="2">Select “Other” in the selection box to enter the IP address for the source in the access control list.</td></tr>
<tr><td rowspan="2">Source Interface</td><td><b>Any</b></td><td colspan="2">Select “Any” in the selection box if every physical port is valid.</td></tr>
<tr><td>Other</td><td>1 … 8</td><td>In the input field, enter the physical port for which this entry is valid in the access control list.</td></tr>
</table>



Access Control List Status

Profile Name test

State Disabled

Source MAC Any

Mask of Source MAC None

Source IP Any

Mask of Source IP None

Source Interface Any

Figure 64: Tab “Security” – Menu “ACL” – “Access Control List Status”

Table 52: Tab “Security” – Menu “ACL” – “Access Control List Status”

Access Control List Status		
Parameters	**Default**	**Description**
Profile Name		This field displays the selected name of the profile.
Drop State	Disable Enable	This field displays the Drop State.
Source MAC Address	Any Other	This field displays the source MAC address.
Source IP	Any Other	This field displays the source IP.
Source Interface	Any Other	This field displays the source interface.

9.3.3 Port Security

The switch receives the MAC address of a device that is connected to a specific port direction and allows data forwarding. The functions of the switch allow control over which and how many devices may be connected to a switch port.

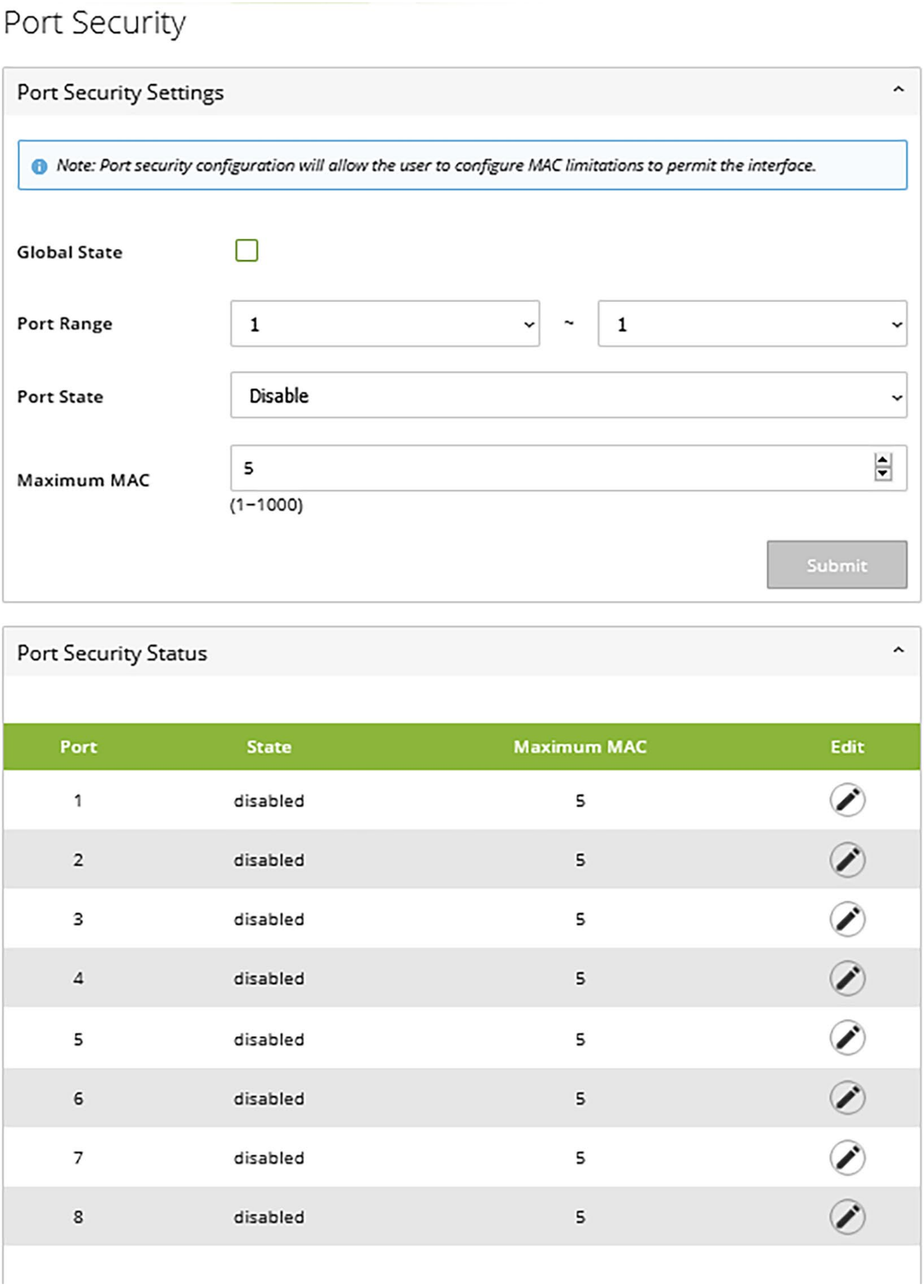
The "Port Security" functions can specify the maximum number of MAC addresses per interface. If this number is exceeded, incoming packets with new MAC addresses are dropped. A MAC address table can be used to check this. The static MAC addresses are included for this limit.

Note

State Change of a Port on the Switch
If the state of a port on the switch is changed from disabled to enabled, all MAC addresses captured by this port are dropped.

Note

Configuration of the Port Security
Port security configuration will allow the user to configure MAC limitations to permit the interface.



Port Security

Port Security Settings

Note: Port security configuration will allow the user to configure MAC limitations to permit the interface.

Global State □

Port Range 1 ~ 1

Port State Disable

Maximum MAC 5
(1–1000)

Port Security Status

Port	State	Maximum MAC	Edit
1	disabled	5	✎
2	disabled	5	✎
3	disabled	5	✎
4	disabled	5	✎
5	disabled	5	✎
6	disabled	5	✎
7	disabled	5	✎
8	disabled	5	✎

Figure 65: Tab “Security” – Menu “Port Security” (Example)

Table 53: Tab “Security” – Menu “Port Security” (Example)

Port Security Settings		
Parameter	**Default**	**Description**
Global State	□	□ The function “Port Security” is not enabled.
		☑ The function “Port Security” port is not enabled.
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Port Security” setting.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Port Security” setting.
Port State	**Disable**	Select “Disable” in the selection box to disable port security for a port or port range.
	Enable	Select “Enable” in the selection box to enable port security for a port or port range.
Maximum MAC (1–1000)	**5**	In the input field, enter the maximum number of MAC addresses per interface.
Port Security Status		
Parameter	**Default**	**Description**
Port	1 … 8 (16)	This column shows the port numbers.
State	Enable Disable	This field indicates whether port security is enabled or disabled.
Maximum MAC Address	0 … 1000	This column displays the maximum number of MAC addresses.
Edit		Preselection for editing.

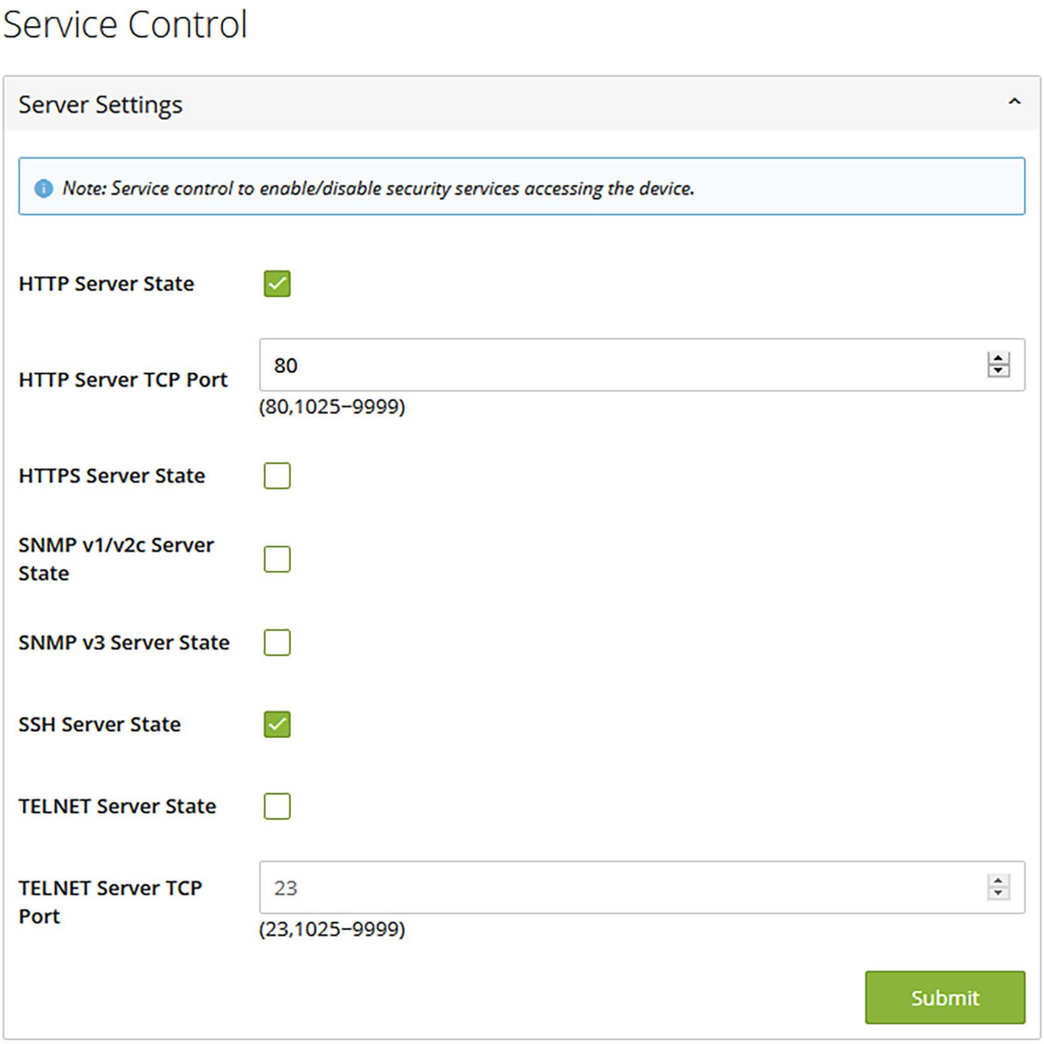
9.3.4 Service Control

The Service Control allow the user to configure security services accessing the device like HTTP, HTTPS, SNMP v1/v2c, SNMP v3, SSH.

Note

Function of the Service Control

Service Control to enable/disable security services accessing the device.



Service Control

Server Settings

Note: Service control to enable/disable security services accessing the device.

HTTP Server State ☑

HTTP Server TCP Port 80
(80,1025–9999)

HTTPS Server State □

SNMP v1/v2c Server State □

SNMP v3 Server State □

SSH Server State ☑

TELNET Server State □

TELNET Server TCP Port 23
(23,1025–9999)

Figure 66: Tab “Security” – Menu “Service Control”

Table 54: Tab “Security” – Menu “Service Control”

Server Settings		
Parameter	**Default**	**Description**
HTTP Server State	☑	Enables/disables the HTTP server.
HTTP Server TCP Port (80, 1025–9999)	**80** 1025 … 9999	In the input field, enter the “HTTP Server TCP Port”.
HTTPS Server State	□	Enables/disables the HTTPS server.
SNMP v1/v2c Server State	□	Enables/disables the SNMP v1/v2c server.
SNMP v3 Server State	□	Enables/disables the SNMP v3 server.
SSH Server State	☑	Enables/disables the SSH server.
Telnet Server State	□	Enables/disables the Telnet server.
Telnet Server TCP Port (23, 1025~9999)	**23** 1025 … 9999	In the input field, enter the “Telnet Server TCP Port”.
Server Status		
Parameter	**Default**	**Description**
HTTP Server State	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 State	Enable Disable	This field displays the status of the HTTPS server.
SNMP v1/v2c Server State	Enable Disable	This field displays the status of the SNMP v1/v2c server.
SNMP v3 Server State	Enable Disable	This field displays the status of the SNMP v3 server.
SSH Server State	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.

9.3.5 VLAN

9.3.5.1 Port Isolation

Port isolation is a port-based virtual LAN feature. 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.

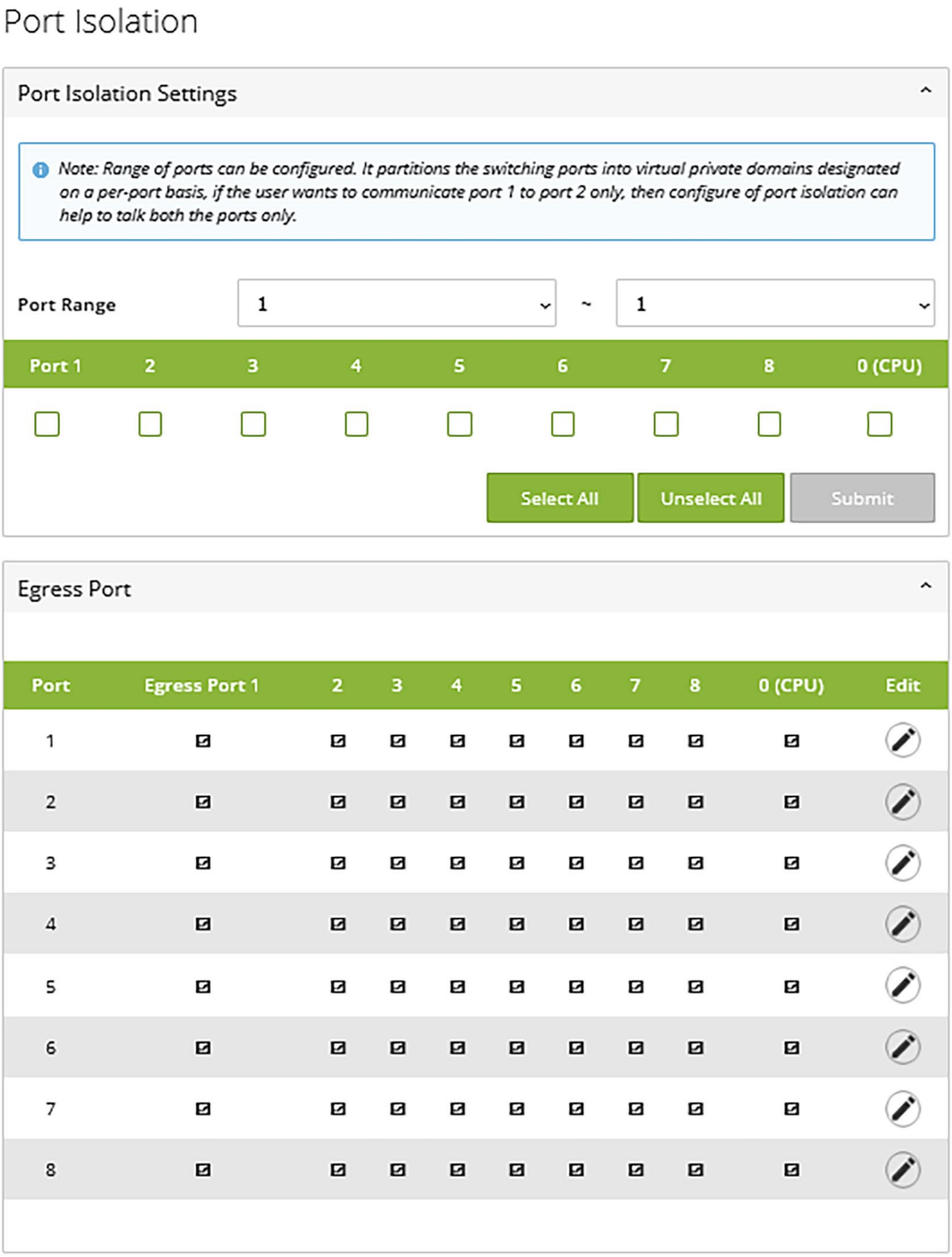
This feature is a per-port setting to configure the egress port(s) for the specific port to forward its received packets. If the CPU port (port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the switch.

If you wish to allow two subscriber ports to talk to each other, 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.

Note

Configure the ports

Range of ports can be configured. It partitions the switching ports into virtual private domains designated on a per-port basis, if the user wants to communicate port 1 to port 2 only, then configure of port isolation can help to talk both the port only.



Port Isolation

Port Isolation Settings

Note: Range of ports can be configured. It partitions the switching ports into virtual private domains designated on a per-port basis, if the user wants to communicate port 1 to port 2 only, then configure of port isolation can help to talk both the ports only.

Port Range: 1 ~ 1

Port 1	2	3	4	5	6	7	8	0 (CPU)
□	□	□	□	□	□	□	□	□

Egress Port

Port	Egress Port 1	2	3	4	5	6	7	8	0 (CPU)	Edit
1	☑	☑	☑	☑	☑	☑	☑	☑	☑	✎
2	☑	☑	☑	☑	☑	☑	☑	☑	☑	✎
3	☑	☑	☑	☑	☑	☑	☑	☑	☑	✎
4	☑	☑	☑	☑	☑	☑	☑	☑	☑	✎
5	☑	☑	☑	☑	☑	☑	☑	☑	☑	✎
6	☑	☑	☑	☑	☑	☑	☑	☑	☑	✎
7	☑	☑	☑	☑	☑	☑	☑	☑	☑	✎
8	☑	☑	☑	☑	☑	☑	☑	☑	☑	✎

Figure 67: Tab “Security” – Menu “VLAN” – “Port Isolation” (Example)

Table 55: Tab “Security” – Menu “VLAN” – “Port Isolation” (Example)

Port Isolation Settings				
Parameter		**Default**	**Description**	
Port Range		**1** … 8 (16) 0 (CPU)	Select a port or port range in the selection box for which you want to configure the “Port Isolation” setting.	
		1 … 8 (16) 0 (CPU)	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) … ☐ 8	☐	☐	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.
Edit			Preselection for editing.	

9.3.5.2 VLAN Setup

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 for 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 identification 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. But the Lean Managed Switch has 5 VLANs available.

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 the 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 output to an untagged port. The remaining 12 bits define the VLAN ID, giving a possible maximum number of 4096 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 bit	12 bits

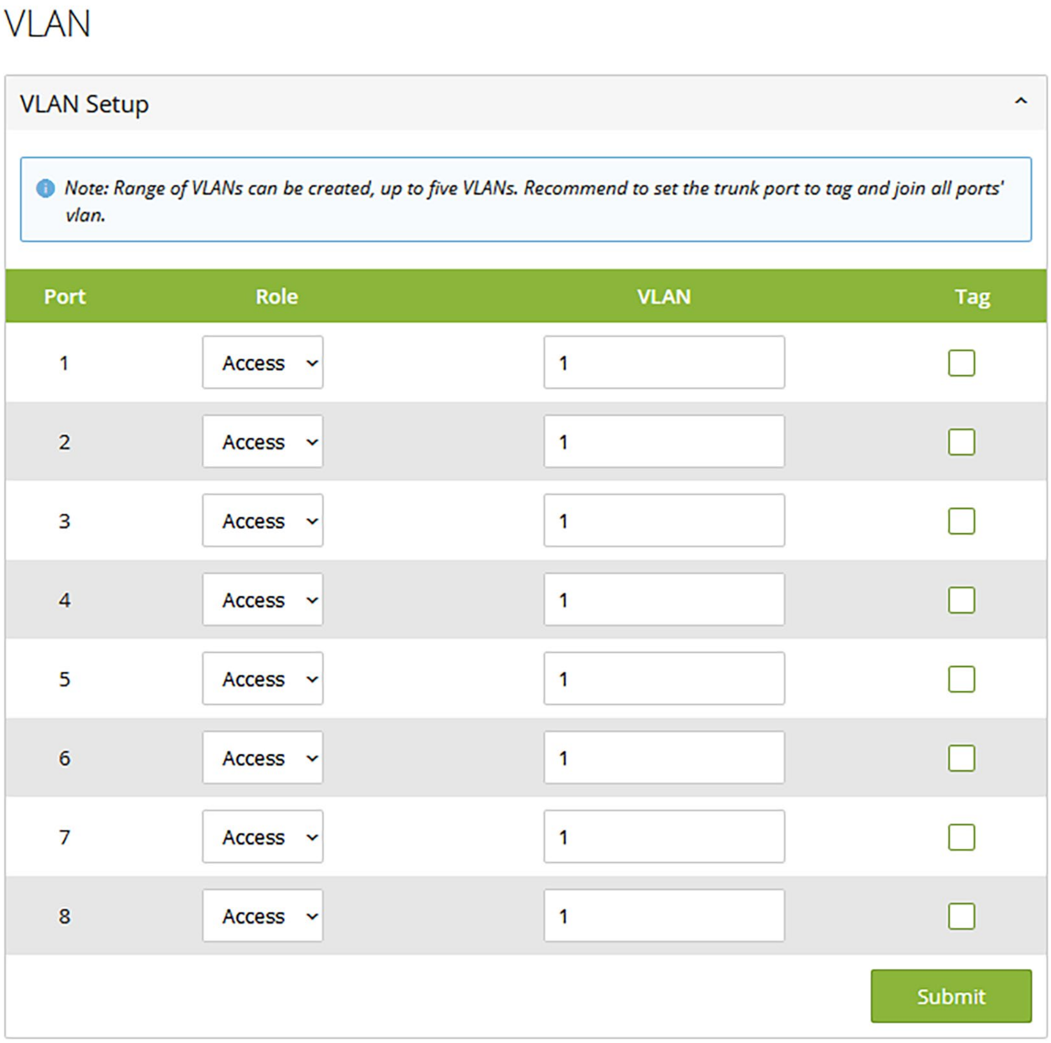
- **Forwarded Tagged and Untagged Frames**

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. When a frame is forwarded 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 members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

Note

Create VLANs
Range of VLANs can be created, up to five VLANs. Recommend to set the trunk port to tag and join all port´vlan.



VLAN

VLAN Setup

Note: Range of VLANs can be created, up to five VLANs. Recommend to set the trunk port to tag and join all ports' vlan.

Port	Role	VLAN	Tag
1	Access	1	□
2	Access	1	□
3	Access	1	□
4	Access	1	□
5	Access	1	□
6	Access	1	□
7	Access	1	□
8	Access	1	□

Figure 68: Tab “Security” – Menu “VLAN” – “VLAN Setup” (Example)

Table 56: Tab “Security” – Menu “VLAN” – “VLAN Setup” (Example)

VLAN Setup		
Parameter	**Default**	**Description**
Port	**Access**	Select “Access” in the selection box to access the port.
	Trunk	Select “Trunk” in the selection box to trunk the port.
VLAN		In the input field, select a VLAN ID from 1 zo 4094.

Note

Always one Port in the Management VLAN

There should always be one port in the Management VLAN.
Otherwise the switch can not be configured.

9.4 Redundancy

9.4.1 ERPS

The ERPS (“**E**THERNET **R**ing **P**rotection **S**witching”) function implements a protection switching mechanism for ETHERNET layer ring topologies according to ITU-T standard G.8032. The ERP (“**E**THERNET **R**ing **P**rotection”) protects ETHERNET traffic in a ring topology and ensures that no loops can arise within the ring in the ETHERNET layer. Looping is prevented by blocking traffic on either a predetermined link or a failed link.

The ETHERNET ring protection functionality includes the following:

- Loop avoidance
- Use of learning, forwarding and filter database (FDB) mechanisms

Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular ring link serves as a reserve connection and is called an RPL (“**R**ing **P**rotection **L**ink”). In normal operation, it is blocked and not used for service traffic. A specific ETHERNET ring node, the “RPL Owner” node, is responsible for blocking traffic at one end of the RPL. Under an ETHERNET ring failure condition, the “RPL Owner” node is responsible for unblocking its end of the RPL, unless the RPL has failed, allowing the RPL to be used for traffic. The ETHERNET ring node adjacent to the RPL, the “RPL Neighbor” node, may also participate in blocking or unblocking its end of the RPL.

The ETHERNET rings can support a multi-ring/ladder network that consists of ETHERNET rings linked through one or more interconnection points. The protection switching mechanisms and protocol defined in this recommendation can be used for a multi-ring/ladder network under the following conditions:

- R-APS channels are not shared across ETHERNET ring connections;
- On each ring port, all traffic channels and all R-APS channels are controlled (e.g., for blocking or flushing) by the ETHERNET ring protection control process (ERP control process) of only one ETHERNET ring;
- Each main ring or subring has its own RPL.

In an ETHERNET ring without congestion, with all ETHERNET ring nodes in the idle state (i.e., no detected failure, no active automatic or external command and receiving only R-APS (NR, RB) messages) and with less than 1,200 km of ring fiber circumference and fewer than 16 ETHERNET ring nodes, the switch completion time (transfer time as defined in [ITU-T G.8032]) for a failure on a ring link should be less than 800 ms.

The ring protection architecture relies on the existence of an APS protocol to coordinate ring protection actions in an ETHERNET ring.

The switch supports up to two rings.

Guard Timer

All ring subscribers use a “Guard Timer.” It prevents a closed loop from forming and prevents ring subscribers from using outdated R-APS messages. The “Guard Timer” is enabled if a ring subscriber received information on a local switching request, such as after SF (“**S**witch **F**ail”), MS (“**M**anual **S**witch”) or FS (“**F**orced **S**witch”) commands. When the timer expires, the ring subscriber begins executing the actions it received from the R-APS. This timer cannot be stopped manually.

WTR Timer

The “WTR Timer” (“**W**ait **T**o **R**estore **Timer**”) is used by the “RPL Owner.” The WTR timer applies to the revertive mode to prevent frequent triggering of the protection switching due to port flapping or intermittent signal failure defects. When the timer expires, the “RPL Owner” sends an R-APS (NR, RB) message through the ring.

WTB Timer

The “WTB Timer” (“**W**ait **T**o **B**lock **Timer**”) is enabled on the “RPL Owner.” The “RPL Owner” uses “WTB Timers” before initiating an RPL block and then reverting to the idle state after operator-initiated commands, such as for FS or MS conditions, are entered. Because multiple FS commands are allowed to co-exist in a ring, the “WTB Timer” ensures that clearing a single FS command does not trigger the re-blocking of the RPL. The “WTB Timer” should run five seconds longer than the “Guard Timer” – enough time to allow a reporting ring subscriber to receive two R-APS messages and to allow the ring to identify the latent state. When clearing a MS command, the “WTB Timer” prevents the formation of a closed loop, because the “RPL Owner” node does not respond to an outdated remote MS request during the recovery process.

Hold-off Timer

Each ring subscriber uses a “Hold-off Timer” to delay reporting a port failure. When the timer expires, the ring subscriber checks the port status. If the problem persists, a failure is reported. If the issue does not persist, nothing is reported.

ERPS Revertive and Non-Revertive Switching

ERPS uses revertive and non-revertive operation. In revertive operation, after the conditions causing a switch have cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. After an error condition is cleared, the traffic channel is switched back only after expiration of a “WTR Timer” to prevent protecting states from toggling due to intermittent errors. Without revertive operation, the traffic channel continues to use RPL after a switch condition is cleared if the RPL has not failed.

Control VLAN

The “Control VLAN” is a domain in which only ERPS control packets are transmitted. Because no other packets are transmitted in the VLAN, there are no delays for the ERPS. Therefore, when configuring a control VLAN for a ring, make sure it is a new VLAN. The ERPS creates this control VLAN and its member ports automatically. The member port should have a left right port only.

In ERPS, control packets and data packets are separated in different VLANs. The control packets are transmitted in a control VLAN.

Instance

For ERPS Version 2, an instance is a profile that specifies a control VLAN and one or more data VLANS for the ERPS. The control and data packets in ERPS are separated in different VLANs. The control packets are transmitted in the control VLAN and the data packets in one or more data VLANs. In this way, a user can easily assign an instance to an ERPS ring.

If a port is blocked by the ERPS in ERPS Version 1, all packets are blocked.

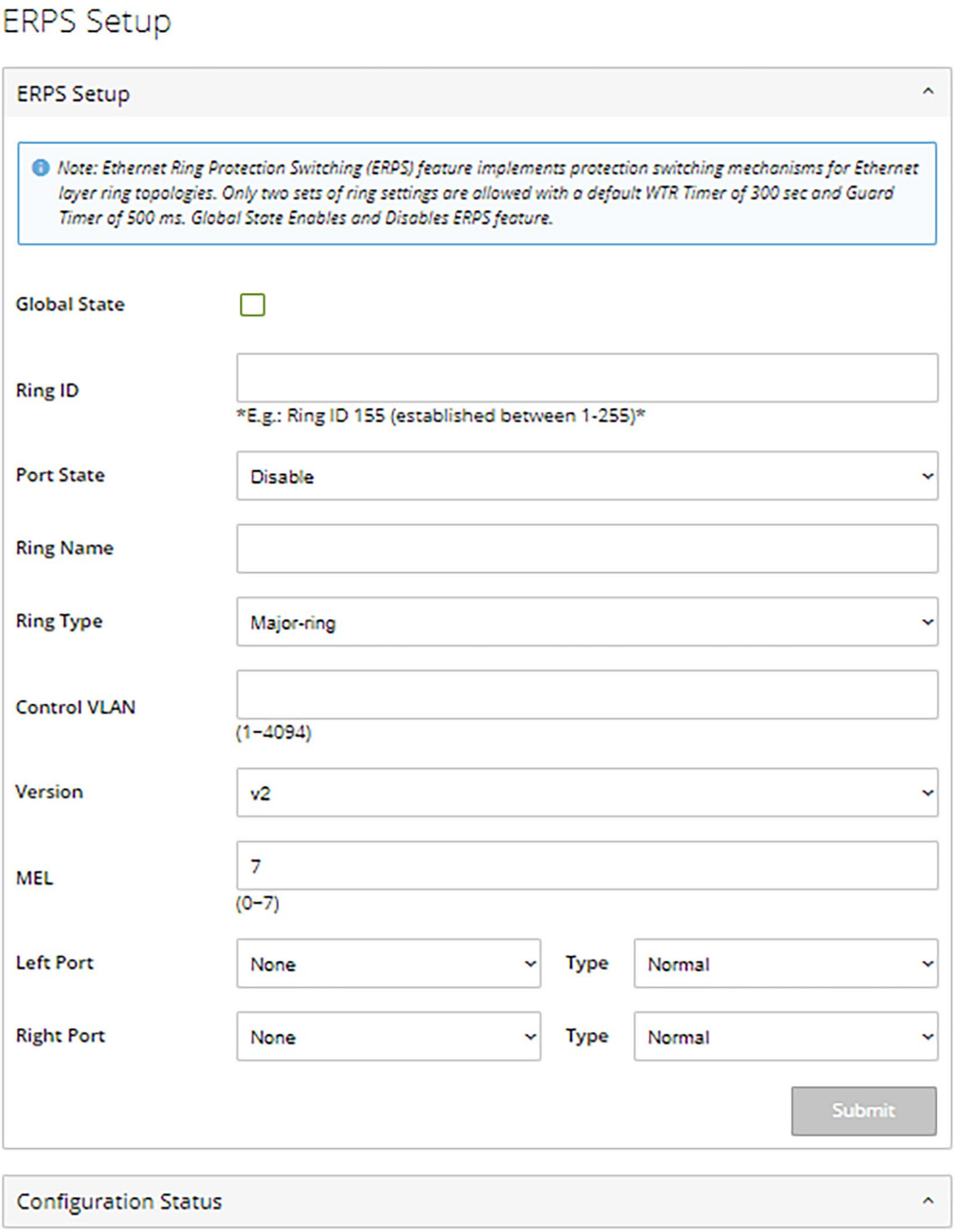
If a port is blocked by an ERPS ring in ERPS Version 2, only the packets belonging to the VLANs in this instance are blocked.

Note

Control VLAN and Instance
In CLI or Web configurations, there are settings for the control VLAN and the instance. If the control VLAN is configured for a ring and an instance is to be configured for the ring, the control VLAN must be the same for the instance as that of the ring. Otherwise, an error is displayed. If you still want to use this instance, you can first change the control VLAN so that it is the same as that of the instance. You can the configure the instance.

Note

Function of the Ethernet Ring Protection Switching (ERPS)
Ethernet Ring Protection Switching (ERPS) feature implements protection switching mechanisms for Ethernet layer ring topologies. Only two sets of ring settings are allowed with a default WTR Timer of 300 s and Guard Timer of 500 ms. Global State enables and disables ERPS feature (max. 2 rings per switch, max. 16 switches per ring, switching time < 800 ms).



ERPS Setup

ERPS Setup

Note: Ethernet Ring Protection Switching (ERPS) feature implements protection switching mechanisms for Ethernet layer ring topologies. Only two sets of ring settings are allowed with a default WTR Timer of 300 sec and Guard Timer of 500 ms. Global State Enables and Disables ERPS feature.

Global State	□		
Ring ID	*E.g.: Ring ID 155 (established between 1-255)*		
Port State	Disable		
Ring Name			
Ring Type	Major-ring		
Control VLAN	(1~4094)		
Version	v2		
MEL	7 (0~7)		
Left Port	None	Type	Normal
Right Port	None	Type	Normal

Figure 69: Tab “Redundancy” – Menu “ERPS”

Table 57: Tab “Redundancy” – Menu “ERPS”

ERPS Setup			
Parameter	**Default**	**Description**	
Global State	☑	☐	The “ERPS” function is not enabled for the switch.
		☑	The “ERPS” function is enabled for the switch.
Ring ID (*E.g.: Ring ID 155 (established between 1-255))		In the input field, enter the ring ID. Valid range: 1 … 255 But in the Lean Managed Switches we support 2 rings.	
Port State	**Disable**	Select “Disable” in the selection box to disable the state of the ring.	
	Enable	Select “Enable” in the selection box to enable the state of the ring.	
Ring Name		In the input field, enter the name of the ring (max. 32 characters). (e.g., Major Ring ID255)	
Ring Type	**Major-ring**	Select “Major Ring” in the selection box if the switch should operate in the major ring.	
	Sub-ring	Select “Subring” in the selection box if the switch should operate in the subring.	
Control VLAN (1-4094)	1 … 4094	In the input field, enter the VLAN ID that should serve as the domain for the ERPS control packets. Valid range: 1 … 4094	
Version	**v2**	Select “v2” in the selection box if you want to use Version 2 of the “ERPS” function.	
	v1	Select “v1” in the selection box if you want to use Version 1 of the “ERPS” function.	
MEL (0~7)	**7**	In the input field, enter the value for the “Control MEL” (**M**aintenance **E**ntity Group **L**evel) for the ring. The MEL specifies the priority. 0 = Lowest priority 7 = Highest priority	
Left Port		The selection box is used to configure the left port and its type for the ring.	
	None	Select “None” in the selection box if you do not want to select a port.	
	1 … 8 (16)	Select the corresponding port in the selection box.	
	Normal	Select “Normal” in the selection box if the port is not assigned any specific function in the ERPS ring.	
	Neighbor	Select “Neighbor” in the selection box if the neighboring port has the “Neighbor” function.	
	Owner	Select “Owner” in the selection box if the port should take on the “Owner” function in the ERPS ring.	
Right Port		This selection box is used to configure the right port and its type for the ring.	
	None	Select “None” in the selection box if you do not want to select a port.	
	1 … 8 (16)	Select the corresponding port in the selection box.	
	Normal	Select “Normal” in the selection box if the port is not assigned any specific function in the ERPS ring.	
	Neighbor	Select “Neighbor” in the selection box if the neighboring port has the “Neighbor” function.	
	Owner	Select “Owner” in the selection box if the port should take on the “Owner” function in the ERPS ring.	

Table 57: Tab “Redundancy” – Menu “ERPS”

ERPS Ring Status		
Parameter	**Default**	**Description**
Ring ID	1 … 255	This field displays the ring ID.
Port State	Disable Enable	This field displays the ring status.
Ring Name		This field displays the ring name.
Ring Type	Major Ring Subring	This field displays the ring type.
Control VLAN	1 … 4084	This field displays the VLAN of the controller.
Version	v2 v1	This field displays the version of the “ERPS” function.
MEL	0 … 7	This field displays the value for the “Control MEL.”
Left Port	None 1 … 8 (16)	This field displays the port number of the left port.
Right Port	None 1 … 8 (16)	This field displays the port number of the right port.
Left Port Type	Normal Neighbor Owner	This field displays the type of the left port.
Right Port Type	Normal Neighbor Owner	This field displays the type of the right port.
Left Port Status	Forwarding Blocking	This field displays the current status of the left port.
Right Port Status	Forwarding Blocking	This field displays the current status of the right port.
Ring Status	Protection Idle	This field displays the ring status.
Delete		Click **[Delete]** to delete this setting.

9.4.2 STP/RSTP

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.

- In STP, the port states are Blocking, Listening, Learning and Forwarding.
- In RSTP, the port states are Discarding, Learning and Forwarding.

STP Switch Port States

- **"Blocking"**
  If a port causes a "Switching Loop" (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"**
  It 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 is used 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 look 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 58: 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 (in 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

The “Hello Time” is the time interval in seconds between configuration messages (BDPU “Bridge Protocol Data Unit”) sent from 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 re-establish 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 transmissions of consecutive RSTP BPDUs. This function can only be enabled in RSTP mode. The valid range is from 1 to 10 seconds.

Bridge Priority

“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, however, the switch with the lowest MAC address becomes the root switch.

Port Priority

The port priority is configured in 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 the “BPDU Guard” are enabled, the “BPDU Filter” has the higher priority.

Note

BPDU Filter and BPDU Guard
If both the “BPDU Filter” and the “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 “Hello Times.”

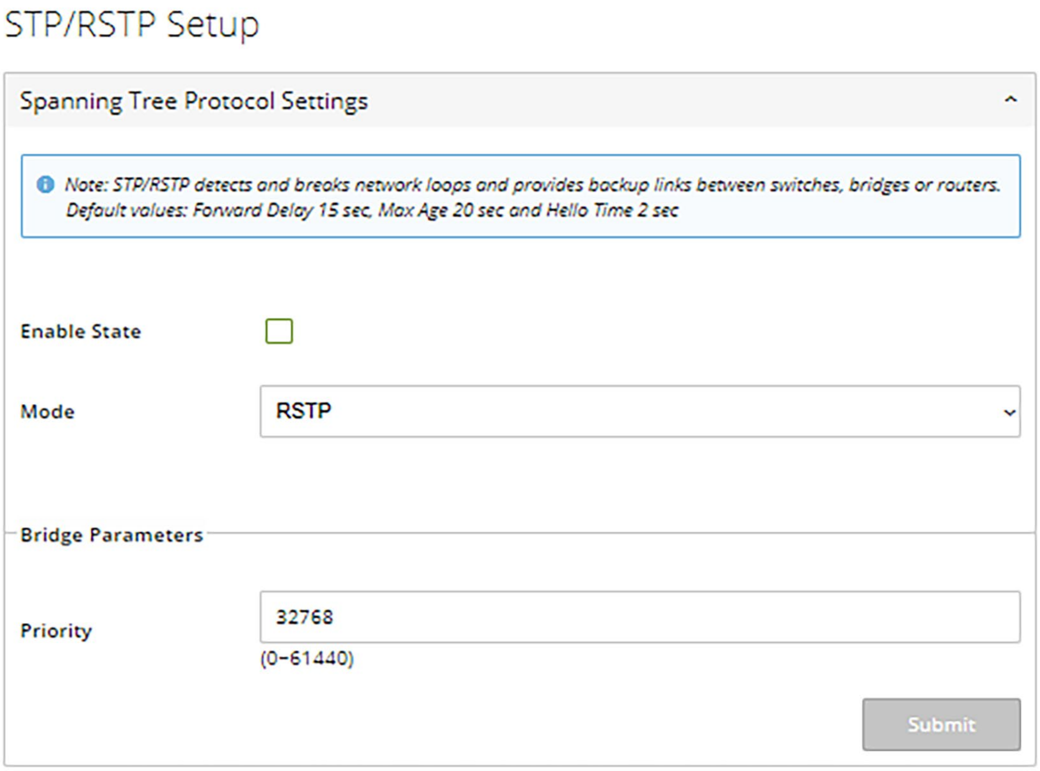
9.4.2.1 STP/RSTP Setup

Note

Functions of the STP/RSTP

STP/RSTP detects and breaks network loops provides backup links between switches, bridges or routers.

Default values: Forward Delay 15 s, Mag Age 20 s and Hello Time 2 s.



STP/RSTP Setup

Spanning Tree Protocol Settings

Note: STP/RSTP detects and breaks network loops and provides backup links between switches, bridges or routers. Default values: Forward Delay 15 sec, Max Age 20 sec and Hello Time 2 sec

Enable State □

Mode RSTP

Bridge Parameters

Priority 32768
(0~61440)

Figure 70: Tab “Redundancy” – Menu “STP/RSTP Setup”

Table 59: Tab “Redundancy” – Menu “STP/RSTP Setup”

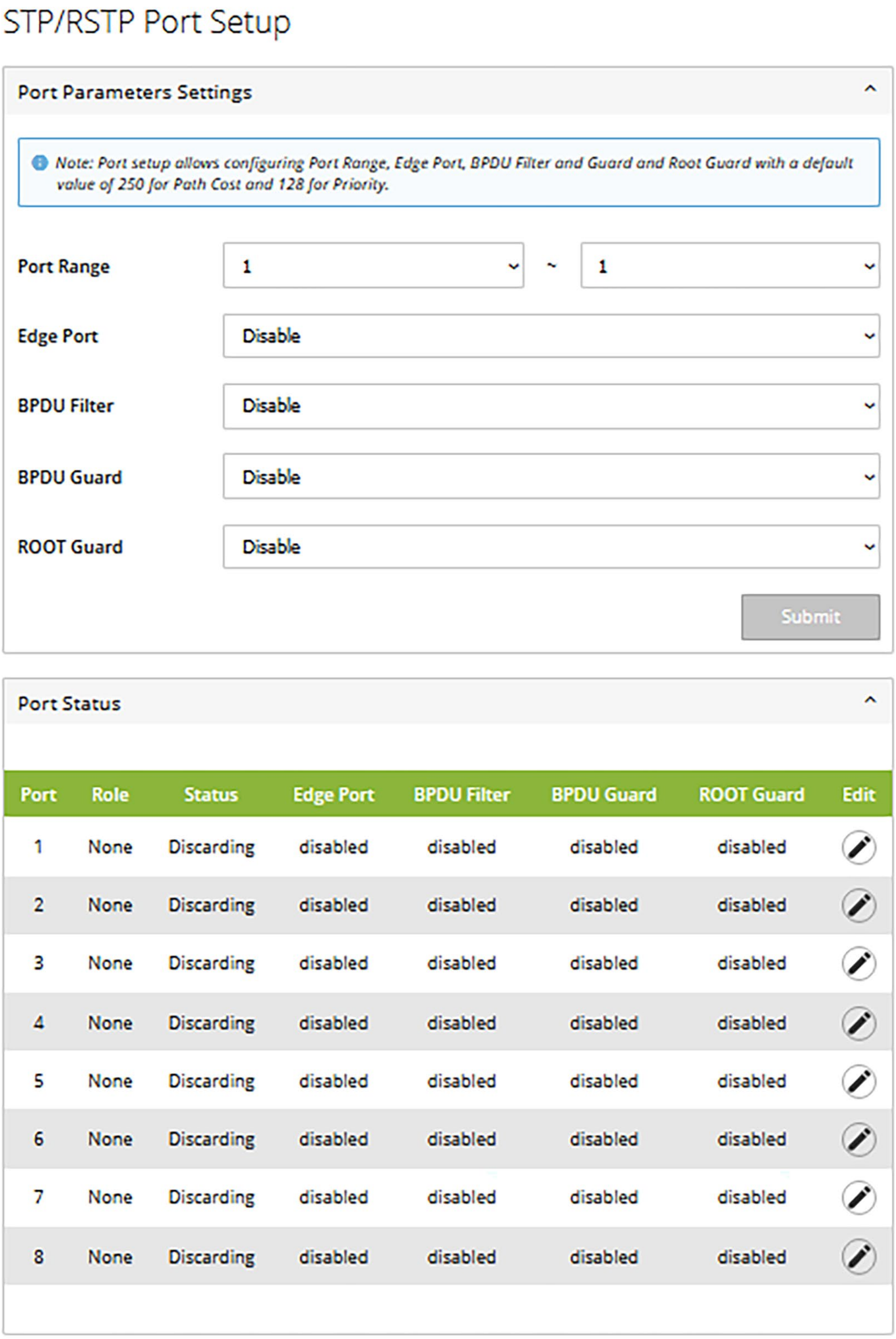
Spanning Tree Protocol Settings		
Parameter	**Default**	**Description**
Enable State	□	□ The “STP/RSTP” function is not enabled for the switch.
		☑ The “STP/RSTP” function is enabled for the switch.
Mode	**RSTP**	Select “RSTP” in the selection box if you want to use the faster “Rapid Spanning Tree Protocol.”
	STP	Select “STP” in the selection box if you want to use the “Spanning Tree Protocol.”
Bridge Parameters		
Parameter	**Default**	**Description**
Priority (Range: 0~61440)	**32768**	In the input field, enter a value for the priority. The lower the numerical value you assign, the higher the priority of this bridge is. Valid range: 0 … 61440

9.4.2.2 STP/RSTP Port Setup

Note

Functions of Port Setup

Port Setup allows configuring Port Range, Edge Port, BDU Filter and Guard and Root Guard with a default value of 250 for Path Costs and 128 for Priority.



STP/RSTP Port Setup

Port Parameters Settings

Note: Port setup allows configuring Port Range, Edge Port, BPDU Filter and Guard and Root Guard with a default value of 250 for Path Cost and 128 for Priority.

Port Range	1 ~ 1
Edge Port	Disable
BPDU Filter	Disable
BPDU Guard	Disable
ROOT Guard	Disable

Port Status

Port	Role	Status	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard	Edit
1	None	Discarding	disabled	disabled	disabled	disabled	✎
2	None	Discarding	disabled	disabled	disabled	disabled	✎
3	None	Discarding	disabled	disabled	disabled	disabled	✎
4	None	Discarding	disabled	disabled	disabled	disabled	✎
5	None	Discarding	disabled	disabled	disabled	disabled	✎
6	None	Discarding	disabled	disabled	disabled	disabled	✎
7	None	Discarding	disabled	disabled	disabled	disabled	✎
8	None	Discarding	disabled	disabled	disabled	disabled	✎

Figure 71: Tab “Redundancy” – Menu “STP/RSTP Port Setup” (Example)

Table 60: Tab “Redundancy” – Menu “STP/RSTP Port Setup” (Example)

Port Parameter Settings		
Parameter	**Default**	**Description**
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “STP/RSTP” settings.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “STP/RSTP” settings.
Edge Port	**Disable**	Select “Disable” in the selection box to disable the “Edge Port” port type for the specific port.
	Enable	Select “Enable” in the selection box to enable the “Edge Port” 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.
Port Status		
Parameter	**Default**	**Description**
Port	1 … 8 (16)	This column shows the port numbers.
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.
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.
Edit		Preselection for editing.

9.5 Diagnostic

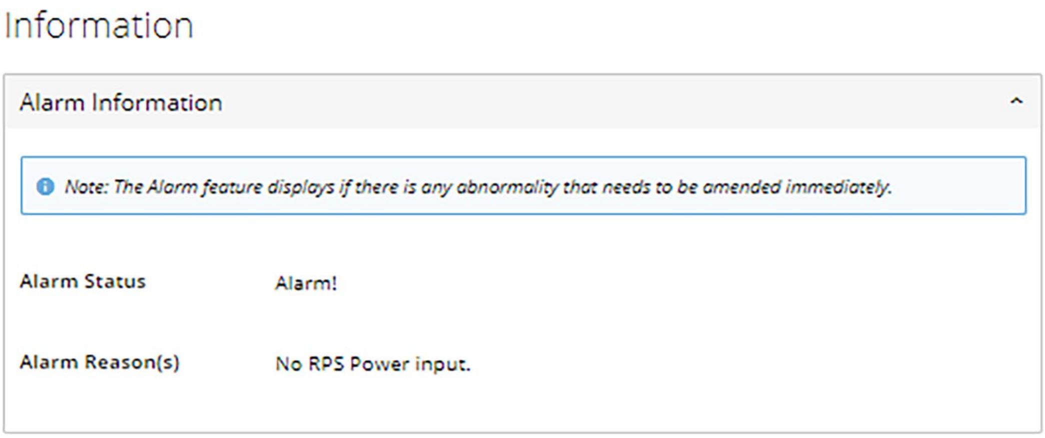
9.5.1 Alarm

9.5.1.1 Information

Note

Function of the Alarm function

The Alarm feature displays if there is any abnormality that needs to be amended immediately.



Information

Alarm Information

Note: The Alarm feature displays if there is any abnormality that needs to be amended immediately.

Alarm Status Alarm!

Alarm Reason(s) No RPS Power input.

Figure 72: Tab “Diagnostic” – Menu “Information”

Table 61: Tab “Diagnostic” – Menu “Information”

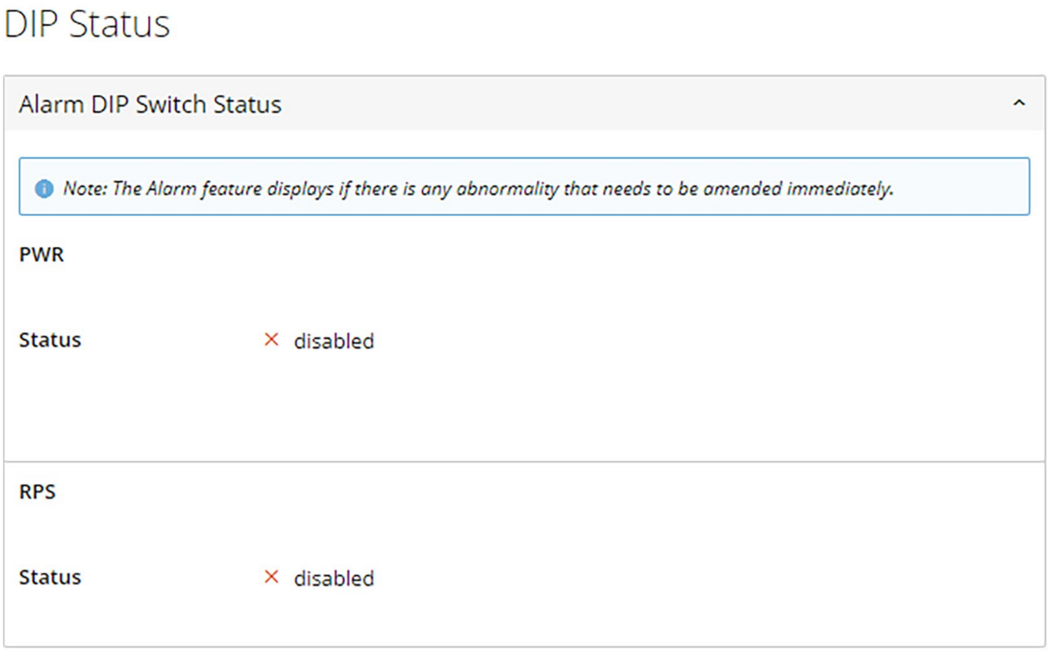
Alarm Information		
Parameter	**Default**	**Description**
Alarm Status		This display field shows if there are any alarm events.
Alarm Reason		This display field shows details about the alarm events.

9.5.1.2 DIP Status

Note

Displays of the DIP Status

It will display the status of the DIP for QoS, Traffic flooding, Port 9,10- 100Fx enabled or disabled


DIP Status

Alarm DIP Switch Status

Note: The Alarm feature displays if there is any abnormality that needs to be amended immediately.

PWR

Status ✕ disabled

RPS

Status ✕ disabled

Figure 73: Tab “Diagnostic” – Menu “DIP Status”

Table 62: Tab “Diagnostic” – Menu “DIP Status”

DIP switch Status		
Parameter	**Default**	**Description**
PWR	**Disable** Enable	This display field indicates whether “PWR” is enabled or disabled.
RPS	**Disable** Enable	This display field indicates whether “RPS” is enabled or disabled.

9.5.1.3 Traffic Flooding

A traffic flooding means that your network is over whelmed with constant broadcast or multicast traffic. Broadcast traffic flooding can eventually lead to a complete loss of network connectivity as the packets proliferate.

Traffic flooding Control protects the Switch bandwidth from flooding packets, including broadcast packets, multicast packets, and destination lookup failure (DLF). The Rate is a threshold that limits the total number of the selected type of packets. For example, if the broadcast and multicast options are selected, the total amount of packets per second for those two types will not exceed the limit value.

Broadcast traffic flooding 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. When the maximum number of allowable broadcast, multicast and unknown unicast packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and unknown unicast packets in your network.

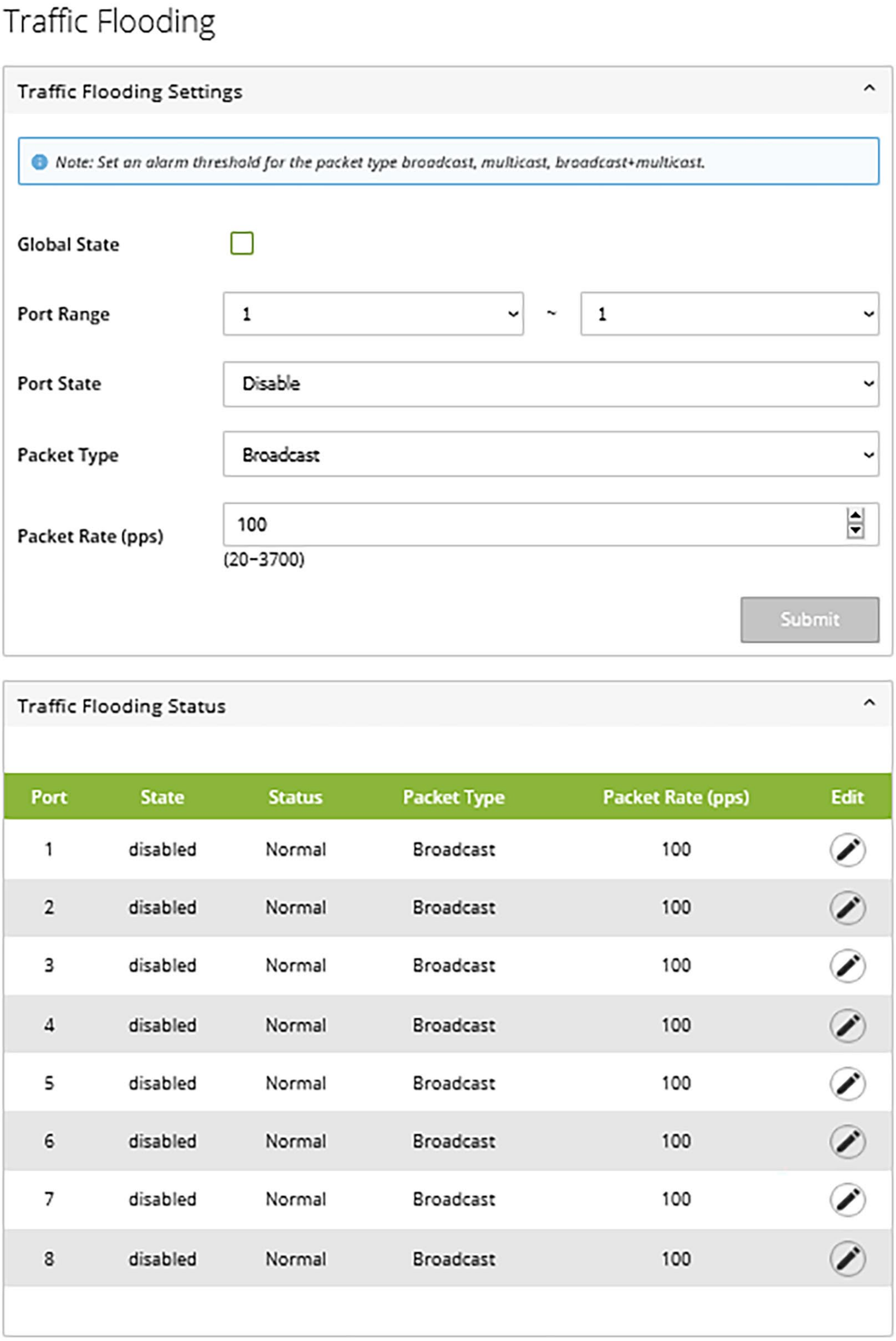
Traffic flooding Control unit: 3700 Mbit/s.

Default Settings

Broadcast Storm Control:	100 Mbit/s
Multicast Storm Control	None
DLF Storm Control	100 Mbit/s

Note

Set an alarm threshold
Set an alarm threshold for the packet type Broadcast, Multicast, Broadcast+Multicast.



Traffic Flooding

Traffic Flooding Settings

Note: Set an alarm threshold for the packet type broadcast, multicast, broadcast+multicast.

Global State	□
Port Range	1 ~ 1
Port State	Disable
Packet Type	Broadcast
Packet Rate (pps)	100 (20–3700)

Traffic Flooding Status

Port	State	Status	Packet Type	Packet Rate (pps)	Edit
1	disabled	Normal	Broadcast	100	✎
2	disabled	Normal	Broadcast	100	✎
3	disabled	Normal	Broadcast	100	✎
4	disabled	Normal	Broadcast	100	✎
5	disabled	Normal	Broadcast	100	✎
6	disabled	Normal	Broadcast	100	✎
7	disabled	Normal	Broadcast	100	✎
8	disabled	Normal	Broadcast	100	✎

Figure 74: Tab “Diagnostic” – Menu “Traffic Flooding” (Example)

Table 63: Tab “Diagnostic” – Menu “Traffic Flooding” (Example)

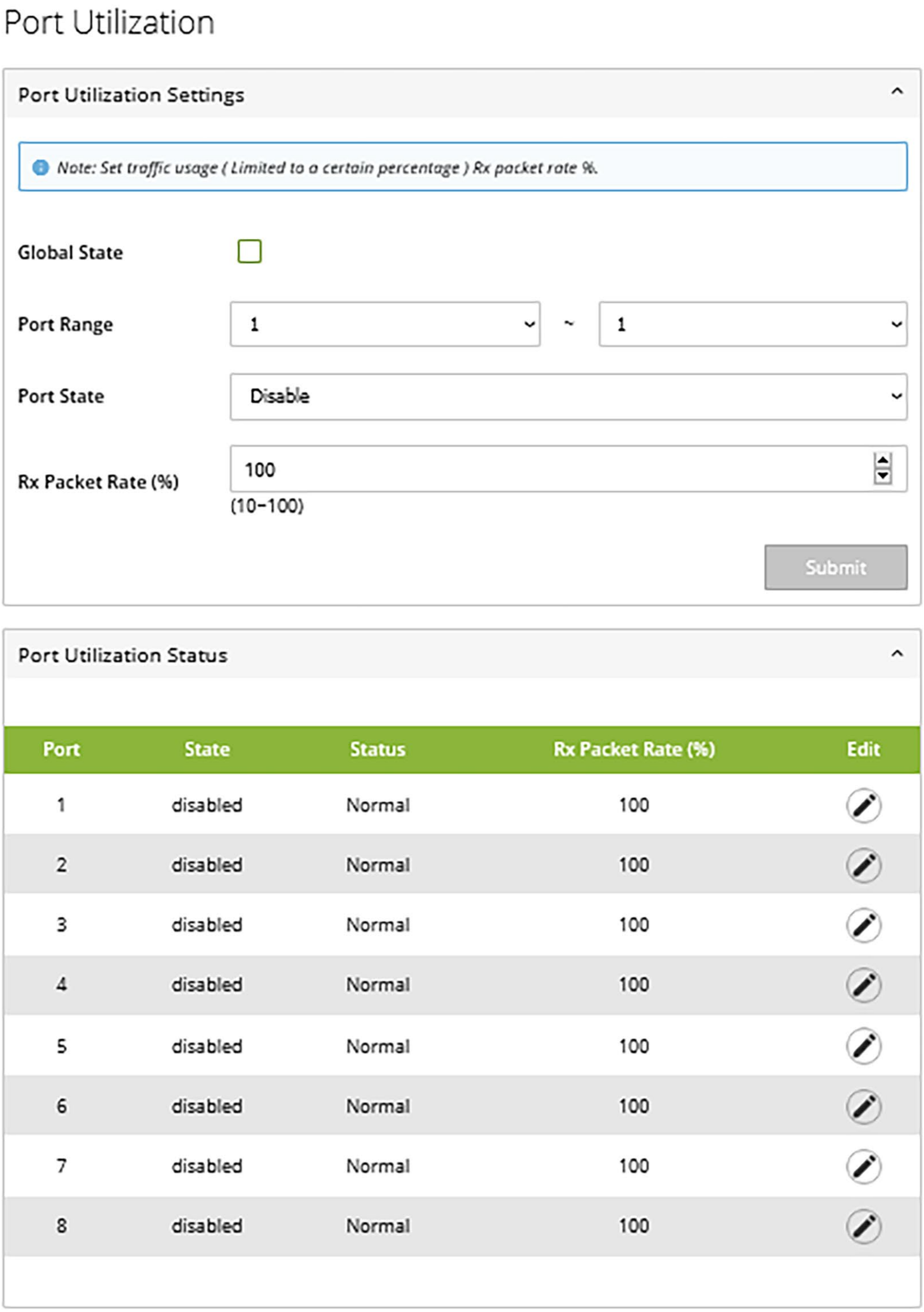
Traffic Flooding Settings		
Parameter	**Default**	**Description**
Global State	□	□ Global State is disable.
		☑ Global State is enable.
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Traffic Flooding” settings.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Traffic Flooding” settings.
Port State	**Disable**	Select “Disable” in the selection box to disable the “Traffic Flooding” function for the switch.
	Enable	Select “Enable” in the selection box to enable the “Traffic Flooding” function for the switch.
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) (20-3700)		User can configure allowable packets per second and the configurable range is 20 to 3700 Mbit/s
Traffic Flooding Status		
Parameter	**Default**	**Description**
Port	1 … 8 (16)	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.
Edit		Preselection for editing.

9.5.1.4 Port Utilization

This feature helps users to monitor the ports’ traffic utilization, to display the link up ports’ traffic utilization only.

Note

Set traffic usage
Set traffic usage (Limited to a certain percentage) Rx packet rate %.



Port Utilization

Port Utilization Settings

Note: Set traffic usage (Limited to a certain percentage) Rx packet rate %.

Global State	□
Port Range	1 ~ 1
Port State	Disable
Rx Packet Rate (%)	100 (10–100)

Port Utilization Status

Port	State	Status	Rx Packet Rate (%)	Edit
1	disabled	Normal	100	✎
2	disabled	Normal	100	✎
3	disabled	Normal	100	✎
4	disabled	Normal	100	✎
5	disabled	Normal	100	✎
6	disabled	Normal	100	✎
7	disabled	Normal	100	✎
8	disabled	Normal	100	✎

Figure 75: Tab “Diagnostic” – Menu “Port Utilization” (Example)

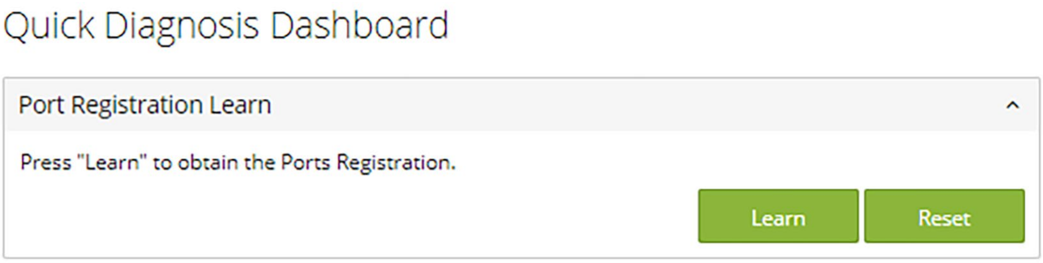
Table 64: Tab “Diagnostic” – Menu “Port Utilization” (Example)

Port Utilization Settings		
Parameter	**Default**	**Description**
Global State	□	□ Global State is disable.
		☑ Global State is enable.
Port Range	**1** … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Port Utilization” settings.
	1 … 8 (16)	Select a port or port range in the selection box for which you want to configure the “Port Utilization” settings.
Port State	**Disable**	Select “Disable” in the selection box to disable the “Port Utilization” function for the switch.
	Enable	Select “Enable” in the selection box to enable the “Port Utilization” function for the switch.
Rx Packet Rate (%) (10-100)	**100**	User can configure allowable packets per second and the configurable range is 10 to 100 %.
Port Utilization Status		
Parameter	**Default**	**Description**
Port	1 … 8 (16)	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.
Rx Packet Rate (%)		This column displays the selected packet rate.
Edit		Preselection for editing.

9.5.2 Dashboard Configuration

9.5.2.1 Quick Diagnosis Dashboard

9.5.2.1.1 Port Registration Learn



Quick Diagnosis Dashboard

Port Registration Learn

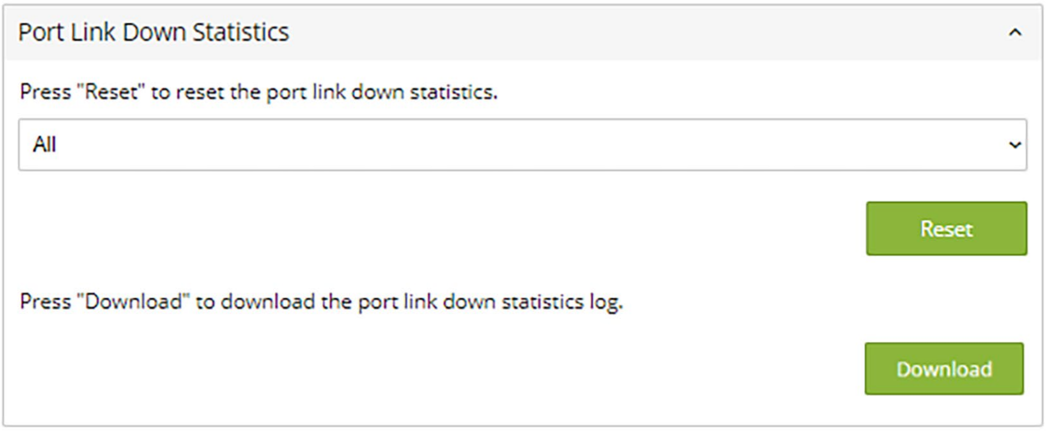
Press "Learn" to obtain the Ports Registration.

Figure 76: Tab “Diagnostic” – Menu “Dashboard Configuration” – “Port Registration Learn”

In this dashboard click the **[Learn]** button to save configuration of the port settings.
If the network is correctly connected, the current state of the connections in the switch can be saved as a reference. Future deviations from this will be displayed as errors.

In this dashboard click the **[Reset]** button to reset to default configuration (learned register ports are forget).

9.5.2.1.2 Port Link Down Statistics



Port Link Down Statistics

Press "Reset" to reset the port link down statistics.

All

Press "Download" to download the port link down statistics log.

Figure 77: Tab “Diagnostic” – Menu “Dashboard Configuration” – “Port Link Down Statistics”

In this dashboard user can select particular interface or all statistics, user can reset, download, and print.

Click the **[Reset]** button to reset the port link down statistics.

Click the **[Download]** button to download the port link down statistics log.
In addition, by click the [Download] button, the Port Link Down Statistic can be downloaded individually per port or completely.

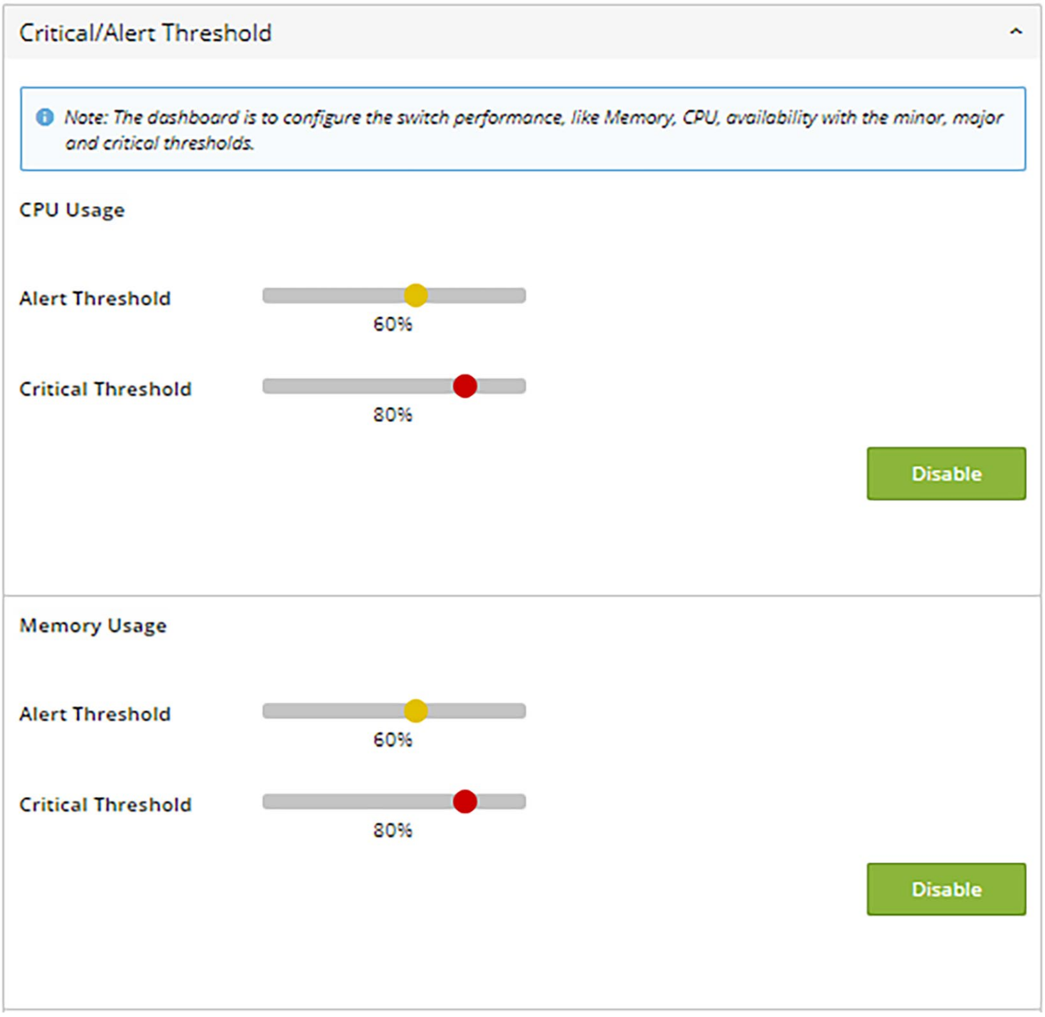
9.5.2.1.3 Critical/Alert Threshold

Here you can set the thresholds at which the tiles "CPU Usage", "Memory Usage", "Transmitting Port Usage" and "Receiving Port Usage" change colors in the dashboard (see Section "Diagnostics").

Note

Functions of the threshold values

The Alert Threshold controls at which value the tiles turns yellow and the Critical Threshold controls at which value the tiles turns red. These thresholds can be set individually for CPU, memory and port send (Tx) / receive (Rx) utilization.


Critical/Alert Threshold

Note: The dashboard is to configure the switch performance, like Memory, CPU, availability with the minor, major and critical thresholds.

CPU Usage

Alert Threshold 60%

Critical Threshold 80%

Memory Usage

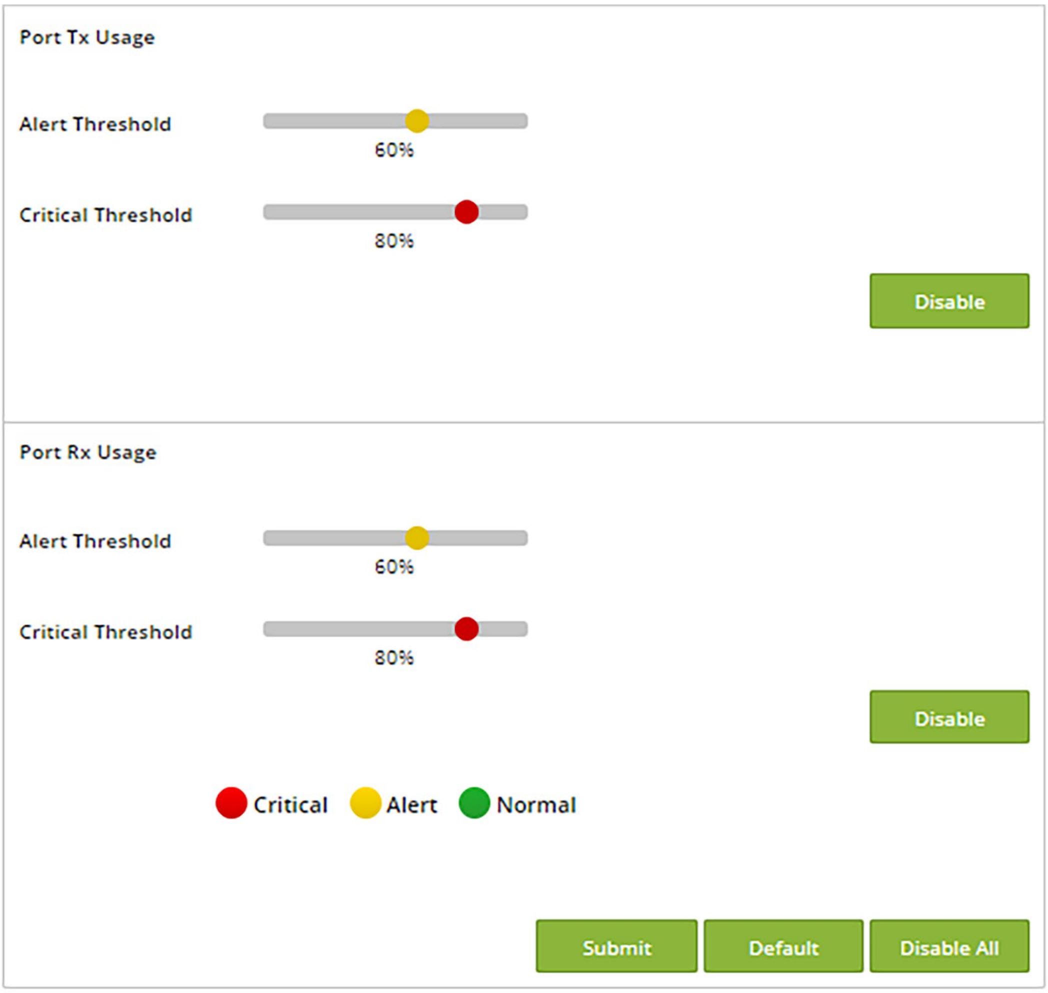
Alert Threshold 60%

Critical Threshold 80%

Figure 78: Tab “Diagnostic” – Menu “Dashboard Configuration” – “Critical/Alert Threshold 01”

In this dashboard click the **[Disable/Enable]** button to disable/enable the

- CPU Usage Visualization
- Memory Usage Visualization



Port Tx Usage

Alert Threshold 60%

Critical Threshold 80%

Port Rx Usage

Alert Threshold 60%

Critical Threshold 80%

Figure 79: Tab “Diagnostic” – Menu “Dashboard Configuration” – “Critical/Alert Threshold 02”

In this dashboard click the **[Disable/Enable]** button to disable/enable the

- Port Tx Usage Visualization
- Port Rx Usage Visualization

9.5.3 Modbus

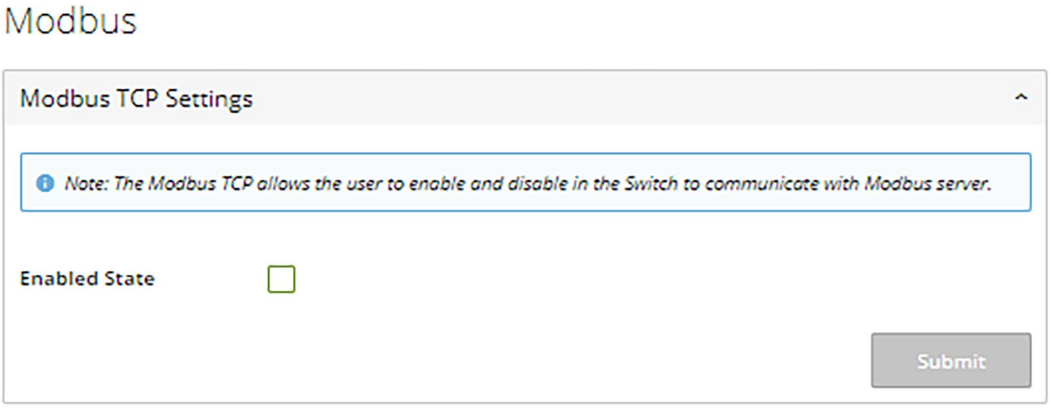
9.5.3.1 Data Format and Function Code

MODBUS TCP supports different types of data formats for reading. The four most important types are:

Table 65: Data Format and Function Code

Data Access Type		Function Code	Function Name	Note
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs	Not supported.
	Internal Bits or Physical Coils	1	Read Coils	Not supported.
Word access (16-bit access)	Physical Input Registers	4	Read Input Registers	
	Physical Output	3	Read Holding Registers	Not supported.

9.5.3.2 MODBUS Register


Modbus

Modbus TCP Settings

Note: The Modbus TCP allows the user to enable and disable in the Switch to communicate with Modbus server.

Enabled State □

Figure 80: Tab “Diagnostic” – Menu “Modbus”

Table 66: Modbus

Modbus TCP Settings			
Parameter	**Default**	**Description**	
Enabled State	□	□	Function „Modbus“ is disable.
		☑	Function „Modbus“ is enable.

Note

Modbus/TCP Tables

The table „Modbus/TCP Tables“ can be found in section “Appendix” > “Modbus/TCP Tables”.

9.5.4 SNMP

Note

Change to the "Configuration" menu
If you click the “SNMP” menu in the “Diagnostic” tab, you can access the “Configuration” tab in the “SNMP” menu.
Refer to the “Configuration” > “SNMP” section for a detailed description.

9.5.5 System Log

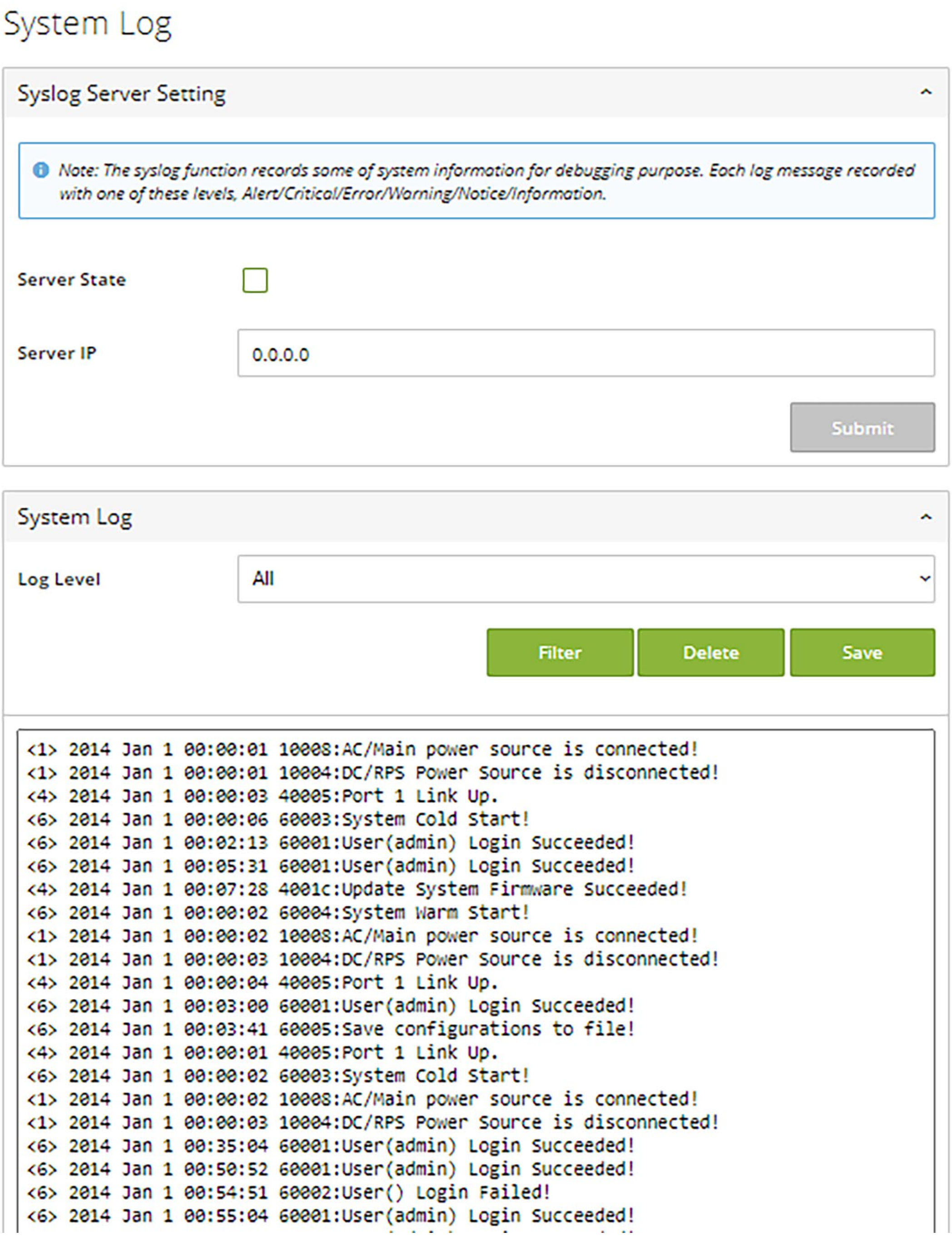
9.5.5.1 Syslog Server Setting

The syslog function can be enabled or disabled. The default setting is disabled. The log message is recorded in the Switch file system. If the syslog server's IP address has been configured, the Switch will send a copy to the syslog server.

The log message file is limited in 4 kB size. If the file is full, the oldest one will be replaced.

Note

Syslog function
The syslog function records some of system information for debugging purpose. Each log message recorded with one of these levels, Alert/Critical/Error/Warning/Notice/Information.



System Log

Syslog Server Setting

Note: The syslog function records some of system information for debugging purpose. Each log message recorded with one of these levels, Alert/Critical/Error/Warning/Notice/Information.

Server State □

Server IP 0.0.0.0

System Log

Log Level All

```
<1> 2014 Jan 1 00:00:01 10008:AC/Main power source is connected!
<1> 2014 Jan 1 00:00:01 10004:DC/RPS Power Source is disconnected!
<4> 2014 Jan 1 00:00:03 40005:Port 1 Link Up.
<6> 2014 Jan 1 00:00:06 60003:System Cold Start!
<6> 2014 Jan 1 00:02:13 60001:User(admin) Login Succeeded!
<6> 2014 Jan 1 00:05:31 60001:User(admin) Login Succeeded!
<4> 2014 Jan 1 00:07:28 4001c:Update System Firmware Succeeded!
<6> 2014 Jan 1 00:00:02 60004:System Warm Start!
<1> 2014 Jan 1 00:00:02 10008:AC/Main power source is connected!
<1> 2014 Jan 1 00:00:03 10004:DC/RPS Power Source is disconnected!
<4> 2014 Jan 1 00:00:04 40005:Port 1 Link Up.
<6> 2014 Jan 1 00:03:00 60001:User(admin) Login Succeeded!
<6> 2014 Jan 1 00:03:41 60005:Save configurations to file!
<4> 2014 Jan 1 00:00:01 40005:Port 1 Link Up.
<6> 2014 Jan 1 00:00:02 60003:System Cold Start!
<1> 2014 Jan 1 00:00:02 10008:AC/Main power source is connected!
<1> 2014 Jan 1 00:00:03 10004:DC/RPS Power Source is disconnected!
<6> 2014 Jan 1 00:35:04 60001:User(admin) Login Succeeded!
<6> 2014 Jan 1 00:50:52 60001:User(admin) Login Succeeded!
<6> 2014 Jan 1 00:54:51 60002:User() Login Failed!
<6> 2014 Jan 1 00:55:04 60001:User(admin) Login Succeeded!
```

Figure 81: Tab “Diagnostic” – Menu “System Log”

Table 67: Tab “Diagnostic” – Menu “System Log”

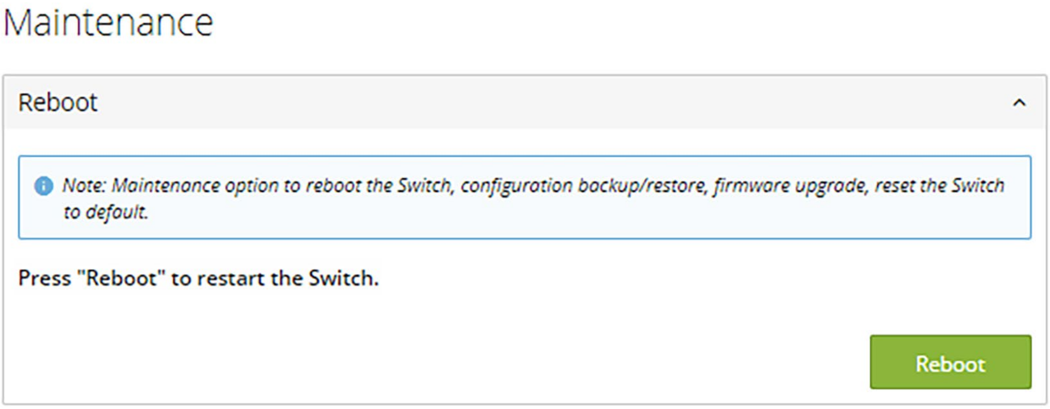
Syslog Server Settings			
Parameter	**Default**	**Description**	
Global State	□	□	Global State is disable.
		☑	Global State is enable.
Server IP	**0.0.0.0**	Enter the IP address in decimal-point notation (e.g., 192.168.1.1).	
System Log			
Parameter	**Default**	**Description**	
Log Level	**All**	Select “All” in the selection box if you want to display all log messages.	
	1:Alarm	Select “Alarm” in the selection box if you want to display the log messages.	
	2:Critical	Select “Critical” in the selection box if you want to display critical log messages.	
	3:Error	Select “Error” in the selection box if you want to display the errors.	
	4:Warning	Select “Warning” in the selection box if you want to display the warnings.	
	5:Notice	Select “Notice” in the selection box if you want to display the notices.	
	6:Information	Select “Information” in the selection box if you want to display all information.	

9.6 Maintenance

9.6.1 Reboot

Note

Function of Maintenance
Maintenance option to reboot, configuration backup/restore, firmware upgrade, reset the switch to default.


Maintenance

Reboot

Note: Maintenance option to reboot the Switch, configuration backup/restore, firmware upgrade, reset the Switch to default.

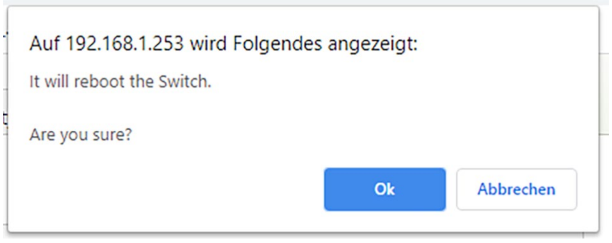
Press "Reboot" to restart the Switch.

Figure 82: Tab “Maintenance” – Menu “Maintenance” – “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 windows open:


Auf 192.168.1.253 wird Folgendes angezeigt:

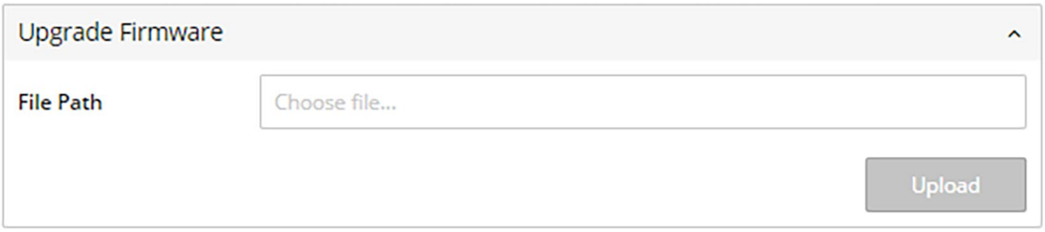
It will reboot the Switch.

Are you sure?

Figure 83: Tab “Maintenance” – “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.

9.6.2 Upgrade Firmware


Upgrade Firmware

File Path

Figure 84: Tab “Maintenance” – Menu “Maintenance” – “Upgrade Firmware”

Execute the following steps to update the switch’s firmware.

1. Click the **[Choose file]** button.
   The file selection dialog opens. Select the respective firmware file.

2. Click the **[Upgrade]** button to load the new firmware.

9.6.3 Upload Configuration

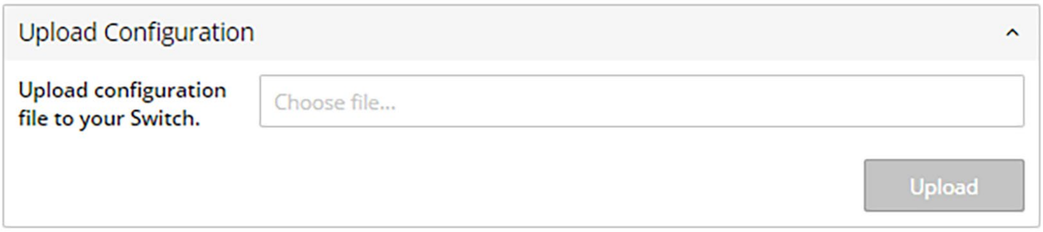


Figure 85: Tab “Maintenance” – Menu “Maintenance” – “Upload Configuration”

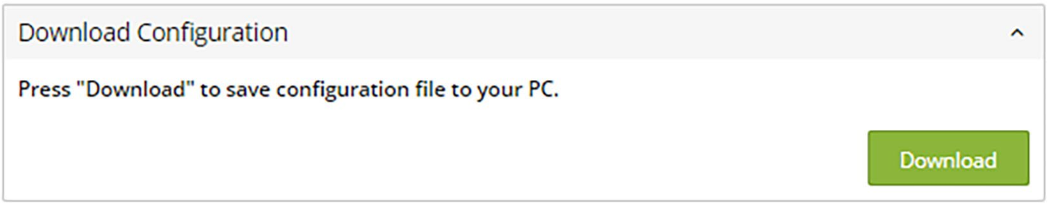
Execute the following steps to upload the configuration file from your PC to the switch.

1. Select “Upload configuration file to your Switch.”

2. Click the **[Choose file]** button.
   Select the configuration file by specifying the full path.

3. Click the **[Upload]** button to begin uploading the file.

9.6.4 Download Configuration


Download Configuration

Press "Download" to save configuration file to your PC.

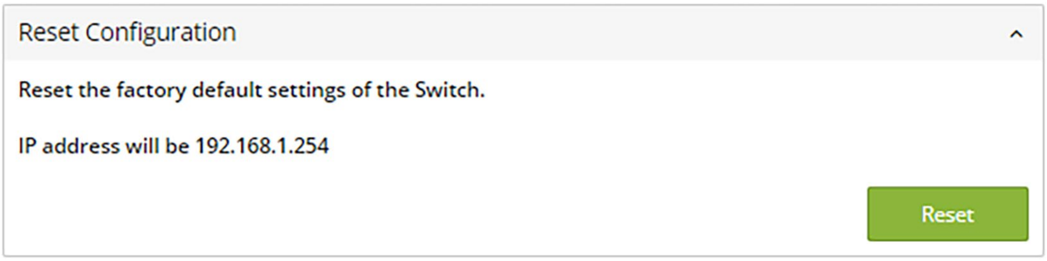
Figure 86: Tab “Maintenance” – Menu “Maintenance” – “Download Configuration”

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.

9.6.5 Reset Configuration



Reset Configuration

Reset the factory default settings of the Switch.

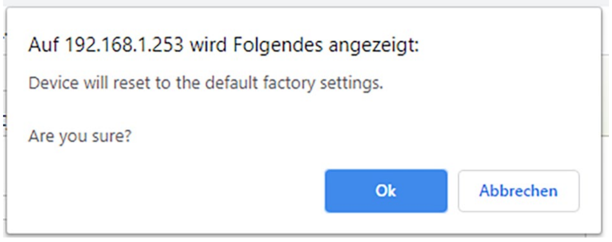
IP address will be 192.168.1.254

Figure 87: Tab “Maintenance” – Menu “Maintenance” – “Reset Configuration”

The “Reset” function allows you to restart the switch without physically turning the power off.

Follow the steps below to restart the switch.

1. Click the **[Reset]** button in the “Reset” menu. The following windows open:



Auf 192.168.1.253 wird Folgendes angezeigt:

Device will reset to the default factory settings.

Are you sure?

Figure 88: Tab “Maintenance” – “Reset” Tab – Message

2. Click **[OK]** and wait for the switch to restart. The process can take up to two minutes. This system configuration reset to default values.

10 Appendix

10.1 RJ-45 Cable

Always use category 5e cables to connect your network devices. The pin assignment is given below:

Table 68: 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 Lean Managed Switch offers the functions autocrossing und autonegotiation to the RJ-45 connection.

10.2 Configuring in the Command Line Interface (CLI)

This chapter lists a selection of available Command Line Interface commands.

10.2.1 System Status

10.2.1.1 System Information

Table 69: 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.

10.2.2 Default Settings

10.2.2.1 System

Table 70: CLI “System” Configuration

Node	Command	Description
enable	ping IPADDR [–c COUNT]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4.
enable	ping IPADDR [–s SIZE]	This command sends an echo request to the destination host. The –s parameter allow user to specific the packet size. Valid range: 0 … 1047 bytes
enable	ping IPADDR [–c COUNT –s SIZE]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 … 1047 bytes
enable	ping IPADDR [-s SIZE –c COUNT]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 … 1047 bytes
configure	Reboot	This command reboots the system.
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	This command enter the configuration mode.
configure	interface eth0	This command enter the configuration mode of the interface.
eth0	Show	This command show information about eth0.
eth0	ip address A.B.C.D/M	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 … 1047 bytes
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.

10.2.2.1.1 Jumbo Frame

Table 71: 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.

10.2.2.1.2 SNTP

Table 72: 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*

10.2.2.1.3 Management Host

Table 73: 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*

10.2.2.2 MAC Management

Table 74: 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*

10.2.2.3 Port Mirroring

Table 75: 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*

10.2.2.4 Port Settings

Table 76: 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	flowcontrol (off | on)	This command disables/enables "Flow Control" for a port.
interface	speed (auto|10-full | 10-full-n | 10-half | 10-half-n | 100-full | 100-full -n | 100-half | 100-half-n | 1000-full | 1000-full-n)	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.
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-full-n | 10-half | 10-half-n | 100-full | 100-full -n | 100-half | 100-half-n | 1000-full | 1000-full-n)	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*

10.2.3 Advanced Settings

10.2.3.1 Storm Control

Table 77: 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*

10.2.3.1.1 VLAN

10.2.3.1.2 Port Isolation

Table 78: 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*

10.2.3.1.2.1 VLAN Settings

Table 79: 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
```

10.2.3.2 LLDP

Table 80: 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-hold <2-100>	This command configures the “tx-Hold Time” that determines the TTL of the switch message (TTL = tx-hold * tx-interval).
interface	lldp tx-interval <1-3600>	This command configures the interval to transmit the LLDP packets.

10.2.3.2.1 Loop Detection

Table 81: 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
```

10.2.3.2.2 STP

Table 82: 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 82: 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.

10.2.3.3 Security

10.2.3.4 Access Control List

Table 83: 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.

10.2.3.4.1 Monitor

10.2.3.4.2 Alarm

Table 84: CLI “Alarm” Configuration

Node	Command	Description
enable	show alarm-info	This command displays alarm information.

10.2.3.4.3 Monitor Information

Table 85: CLI “Monitor Information” Configuration

Node	Command	Description
enable	show hardware-monitor (C|F)	This command displays hardware operation information.

10.2.3.5 SFP Information

Table 86: 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.

10.2.3.6 Management

10.2.3.7 SNMP

Table 87: 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
```

10.2.3.8 Maintenance

Table 88: 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

10.2.4 System Log

Table 89: CLI “System Log” Configuration

Node	Command	Description
enable	show syslog	The command displays all log messages recorded in the switch.
enable	show syslog level <1-6>	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	clear syslog	The command clears the syslog message.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*syslog-server ip 192.168.200.106*

L2SWITCH(config)#*syslog-server enable*

10.2.4.1 User Account

Table 90: 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*

10.3 Modbus/TCP Tables

10.3.1 Data Format and Function Code

Modbus/TCP supports different types of data formats for reading. The four most important types are:

Table 91: Data Format and Function Code

Data Access Type		Function Code	Function Name	Note
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs	Not supported.
	Internal Bits or Physical Coils	1	Read Coils	Not supported.
Word access (16-bit access)	Physical Input Registers	4	Read Input Registers	
	Physical Output	3	Read Holding Registers	Not supported.

10.4 Modbus Register

The Modbus address space of the Lean Managed Switches starts at 1000 (decimal) for function code 4.

Note

Modbus address space

The Modbus address space is also displayed in Web based management.

Table 92: Modbus Registers

Read Input Registers (Function Code 04) Register Number 30001~39999						
Register Offset		**Data Address**		**Date Length/ Word**	**For-mat**	**Description**
Dec	**Hex**	**Dec**	**Hex**			
System Information						
1001	3E9	1000	3E8	1	HEX	Vendor ID = 0x30DE
1002	3EA	1001	3E9	16	ASCII	Vendor Name = “WAGO” Word 0 Hi byte = ‘W’ Word 0 Lo byte = ‘A’ Word 1 Hi byte = ‘G’ Word 1 Lo byte = ‘O’ Word 2 Hi byte = ‘\0’

1033	409	1032	408	16	ASCII	**Product Name = “852-1812”**
						Word 0 Hi byte = ‘8’ Word 0 Lo byte = ‘5’ Word 1 Hi byte = ‘2’ Word 1 Lo byte = ‘-’ Word 2 Hi byte = ‘1’ Word 2 Lo byte = ‘8’ Word 3 Hi byte = ‘1’ Word 3 Lo byte = ‘2’ Word 4 Hi byte = ‘\0’ Word 4 Lo byte = ‘\0
1065	429	1064	428	7	ASCII	**Product Serial Number**
						Ex: Serial No=A000000000001
1081	439	1080	438	12	ASCII	**Firmware Version=” V1.0.1.S0”**
						Word 0 Hi byte = ‘V’ Word 0 Lo byte = ‘1’ Word 1 Hi byte = ‘.’ Word 1 Lo byte = ‘0’ Word 2 Hi byte = ‘.’ Word 2 Lo byte = ‘1’ Word 3 Hi byte = ‘.’ Word 3 Lo byte = ‘S’ Word 4 Hi byte = ‘0’ Word 4 Lo byte = ‘\0’ Word 5 Hi byte = ‘\0’ Word 5 Lo byte = ‘\0’ Word 6 Hi byte = ‘\0’ Word 6 Lo byte = ‘\0’ Word 7 Hi byte = ‘\0’ Word 7 Lo byte = ‘\0’ Word 8 Hi byte = ‘\0’ Word 8 Lo byte = ‘\0’
1097	449	1096	448	16	ASCII	Firmware Release Date="Mon Sep 30 18:51:45 2013"
1113	459	1112	458	3	HEX	**ETHERNET MAC Address**
						Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 04 Word 2 Lo byte = 0 x 05

1129	469	1128	468	1	HEX	**Power 1 (PWR) Alarm**
						0x0000: no alarm 0x0003: No PWR input
1130	46A	1129	469	1	HEX	**Power 2(RPS) Alarm**
						0x0000: no alarm 0x0003: No RPS input
1145	479	1144	478	1	HEX	**Fault LED Status**
						0x0000: No 0x0001: Yes
Port Information						
				1	HEX	**1256 (Port 1) ... 1263 (Port 8)** **Port 1 to 8 Link Status**
1257	4E9	1256	4E8			0x0000: Link down
1258	4EA	1257	4E9			0x0001: 10M-Full-FC_ON (FC: Flow Control)
1259	4EB	1258	4EA			0x0002: 10M-Full-FC_OFF
1260	4EC	1259	4EB			0x0003: 10M-Half-FC_ON
1261	4ED	1260	4EC			0x0004: 10M-Half-FC_OFF
1262	4EE	1261	4ED			0x0005: 100M-Full-FC_ON
1263	4EF	1262	4EE			0x0006: 100M-Full-FC_OFF
1264	4F0	1263	4EF			0x0007: 100M-Half-FC_ON
						0x0008: 100M-Half-FC_OFF 0x0009: 1000M-Full-FC_ON 0x000A: 1000M-Full-FC_OFF 0x000B: 1000M-Half-FC_ON ON0x000C: 1000M-Half-FC_OFF 0xFFFF: No port
				32	ASCII	**Port 1 to 12 Medium**
1513	5E9	1512	5E8			Port Description = “1000TX, RJ45.” Or “1000TX.”
1545	609	1544	608			Word 0 Hi byte = ‘1’
1577	629	1576	628			Word 0 Lo byte = ‘0’
1609	649	1608	648			Word 1 Hi byte = ‘0’
1641	669	1640	668			Word 1 Lo byte = ‘T’
1673	689	1672	688			…
1705	6A9	1704	6A8			Word 4 Hi byte = ‘4’
1737	6C9	1736	6C8			Word 4 Lo byte = ‘5’
						Word 5 Hi byte = ‘.’
						Word 5 Lo byte = ‘\0’

				2	HEX	**Port 1 to 12 Tx Packets**
2025	7E9	2024	7E8			Ex: port 1 Tx Packet Amount = 0x87654321
2027	7EB	2026	7EA			Word 0 = 8765
2029	7ED	2028	7EB			Word 1 = 4321
2031	7EF	2030	7EE			
2033	7F1	2032	7F0			
2035	7F3	2034	7F2			
2037	7F5	2036	7F4			
2039	7F7	2038	7F6			
				2	HEX	**Port 1 to 12 Rx Packets**
2089	829	2088	828			Ex: port 1 Rx Packet Amount = 0x123456
2091	82B	2090	82A			Word 0 = 0012
2093	82D	2092	82C			Word 1 = 3456
2095	82F	2094	82E			
2097	831	2096	830			
2099	833	2098	832			
2101	835	2100	834			
2103	837	2102	836			
				2	HEX	**Port 1 to 10 Tx Error Packets**
2153	869	2152	868			Ex: port 1 Tx Error Packet Amount = 0x87654321
2155	86B	2154	86A			Word 0 =8765
2157	86D	2156	86C			Word 1 = 4321
2159	86F	2158	86E			
2161	871	2160	870			
2163	873	2162	872			
2165	875	2164	874			
2167	877	2166	876			

				2	HEX	**Port 1 to 10 Rx Error Packets**
2217	8A9	2216	8A8			Ex: port 1 Rx Error Packet Amount = 0x123456
2219	8AB	2218	8AA			Word 0 = 0012
2221	8AD	2220	8AC			Word 1 = 3456
2223	8AF	2222	8AE			
2225	8B1	2224	8B0			
2227	8B3	2226	8B2			
2229	8B5	2228	8B4			
2231	8B7	2230	8B6			
Redundancy & Ring Information						
2281	8E9	2280	8E8	1	HEX	**Spanning Tree Status**
						0x0000 : STP is disabled
						0x0001 : STP
						0x0002 : RSTP
2285	8ED	2284	8EC	1	HEX	**ERPS Status**
						0x0000 : Disabled
						0x0001 : Enabled
ERPS Information						
3049	BE9	3048	BE8	1	HEX	**Ring ID for ERPSn (n=1)**
						Ex: 0x001 Ring ID=1
3050	BEB	3049	BE9	1	HEX	**State for ring of ERPS**
						0x0000: Disabled.
						0x0001: Enabled.
3051	C0B	3050	BEA	33	ASCII	**Name of Ring**
						Ring Name = “Ring1”
						Word 1 Lo byte = ‘R’
						Word 2 Lo byte = ‘i’
						Word 3 Lo byte = ‘n’
						Word 4 Lo byte = ‘g’
						Word 5 Lo byte = ‘1’
						Word 6 Lo byte = ‘\0’
3084	C0C	3083	C0B	1	HEX	**Version & Ring Type**
						High byte – Version.
						Low byte – Ring Type.
						0x01:Major-ring
						0x02:Sub-ring
						Ex: 0x0201– Version2, Type: Major-ring
3085	C0D	3084	C0C	1	HEX	**Instance of Ring**
						Ex: 0x0001 Instance ID=1
3086	C0E	3085	C0D	1	HEX	**Control VLAN of Ring**
						E:0x000b Control VLAN=11

3087	C0F	3086	C0E	1	HEX	**Right Port of Ring**
						High byte –Port No. Low byte – Port Type. 0x01:Normal 0x02:RPL Owner 0x03:RPL Neighbour Ex: 0x0502– Port 5, RPL Owner
3088	C10	3087	C0F	1	HEX	**Left Port of Ring**
						High byte –Port No. Low byte – Port Type. 0x01:Normal 0x02:RPL Owner 0x03:RPL Neighbour Ex: 0x0303– Port 3, RPL Neighbour
3089	C11	3088	C10	1	HEX	**Ring port state**
						High byte –Left port state. Low byte – Right port state. 0x00: No connection 0x01: Forwarding 0x02: Blocking Ex: 0x0001– Left Port No connection Right Port Forwarding
3090	C12	3089	C11	1	HEX	**Ring ID for ERPSn (n=2)**
3091	C13	3090	C12	1		State of ERPS Ring
3124	C34	3091	C13	33	ASCII	Name of Ring
3125	C35	3124	C34	1	HEX	Version & Ring Type
3126	C36	3125	C35	1		Instance of Ring
3127	C37	3126	C36	1		Control VLAN of Ring
3128	C38	3127	C37	1		Right Port of Ring
3129	C39	3128	C38	1		Left Port of Ring
3130	C3A	3129	C39	1		Ring port state

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