

WAGO ETHERNET Accessories 852



852-303

Industrial Managed Switch

8 Port 100BASE-TX, 2 x 1000BASE-SX/LX

© 2019 WAGO Kontakttechnik GmbH & Co. KG
All rights reserved.

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	10
1.1	Validity of this Documentation.....	10
1.2	Copyright.....	10
1.3	Symbols	11
1.4	Number Notation	13
1.5	Font Conventions	13
2	Important Notes	14
2.1	Legal Bases.....	14
2.1.1	Subject to Changes.....	14
2.1.2	Personnel Qualification	14
2.1.3	Proper Use of the Industrial Switches	14
2.1.4	Technical Condition of Specified Devices.....	15
2.1.5	Standards and Regulations for Operating the Industrial Switches	15
2.2	Safety Advice (Precautions)	16
2.3	Special Use Conditions for ETHERNET Devices	19
3	General	20
3.1	Scope of Supply	20
3.2	Industrial ETHERNET Technology	20
3.3	Switching Technology.....	21
4	Device Description.....	23
4.1	View	24
4.1.1	Front View.....	24
4.1.2	Top View.....	26
4.2	Connectors	27
4.2.1	Power Supply (PWR/RPS).....	27
4.3	Network Connections	28
4.3.1	RJ-45 Port (RS-232 Port).....	29
4.3.2	SFP 1000BASE SX/LX / SFP 100BASE FX Ports.....	29
4.3.3	10/100BASE TX Ports.....	29
4.4	Display Elements.....	30
4.4.1	Device LEDs	30
4.4.2	Port LEDs	32
4.5	Operating Elements.....	33
4.5.1	DIP Switches	33
4.5.2	Reset Button	34
4.6	Label	35
4.6.1	Hardware and Software Version	35
4.7	Technical Data	36
4.7.1	Device Data	36
4.7.2	System Data	36
4.7.3	Power Supply.....	36
4.7.4	Communication	37
4.7.5	Environmental Conditions	37
4.8	Approvals	38
5	Mounting.....	39

5.1	Installation Site	39
5.2	Installation on a Carrier Rail	39
5.3	Removal from Carrier rail.....	39
6	Connect Devices	40
6.1	Power Supply	40
6.2	External Alarm Contact Port	41
6.3	Console Port Cable Connection.....	41
6.4	1000Base-SX/LX Port, 100BASE-FX Port, Fiber Optic.....	42
6.5	10/100BASE-TX Ports.....	43
7	Function Description	44
7.1	Default Settings	44
7.1.1	Jumbo Frame.....	44
7.1.2	SNTP	44
7.1.3	Management Host.....	45
7.1.4	MAC Management.....	45
7.1.4.1	Static MAC Settings.....	46
7.1.4.2	Refusal MAC Settings	46
7.1.5	Port Mirroring	47
7.1.6	Port Settings	47
7.2	Advanced Settings.....	51
7.2.1	Bandwidth Limitation	51
7.2.1.1	QoS.....	51
7.2.1.2	Rate Limitation	58
7.2.1.2.1	Storm Control.....	58
7.2.1.2.2	Rate Limitation.....	58
7.2.2	IGMP Snooping.....	59
7.2.2.1	MVR	62
7.2.2.2	Multicast Address	65
7.2.3	VLAN	68
7.2.3.1	Port Isolation	70
7.2.3.2	GARP/GVRP	71
7.2.3.3	Q-in-Q	73
7.2.3.3.1	Port-Based Q-in-Q	75
7.2.3.3.2	Selective Q-in-Q.....	76
7.2.4	DHCP Relay	77
7.2.5	DHCP Relay Option 82	79
7.2.6	Dual Ring	81
7.2.7	ERPS.....	82
7.2.8	Dual Homing	85
7.2.9	Link Aggregation	86
7.2.9.1	Static Trunk	86
7.2.9.2	LACP	86
7.2.10	LLDP.....	87
7.2.11	Loop Detection.....	88
7.2.12	Jet Ring.....	89
7.2.13	STP.....	90
7.2.14	Xpress Ring	95
7.3	Security	96
7.3.1	IP Source Guard	96

7.3.1.1	DHCP Snooping	97
7.3.1.1.1	Server Screening	99
7.3.1.2	Binding Table	99
7.3.1.3	ARP Inspection.....	100
7.3.1.3.1	Filter Table.....	101
7.3.2	Access Control List (ACL)	102
7.3.3	802.1x.....	103
7.3.4	Port Security	106
7.4	Monitor	107
7.4.1	Alarm Information.....	107
7.4.2	Monitor Information	107
7.4.3	RMON Statistics.....	107
7.4.4	SFP.....	107
7.4.4.1	DDM.....	108
7.4.5	Traffic Monitor	108
7.5	Management	109
7.5.1	SNMP	109
7.5.2	SNMP Trap	110
7.5.3	Auto Provision.....	110
7.5.4	Mail Alarm.....	112
8	Configuration	113
8.1	Overview of Configuration Options	113
8.2	Telnet Port.....	114
8.2.1	Console Port	115
9	Configuring in the Web-Based Management System	116
9.1	System Status	119
9.1.1	System Information	119
9.2	Basic Settings.....	121
9.2.1	General Settings	121
9.2.1.1	System	121
9.2.1.2	Jumbo Frame	123
9.2.1.3	SNTP.....	124
9.2.1.4	Management Host	127
9.2.2	MAC Management.....	128
9.2.2.1	Static MAC Settings.....	128
9.2.2.2	MAC Table	130
9.2.2.3	Age Time Setting.....	131
9.2.2.4	Blacklisting	132
9.2.3	Port Mirroring	133
9.2.4	Port Settings	135
9.2.4.1	General Settings.....	135
9.2.4.2	Information	137
9.3	Advanced Settings.....	138
9.3.1	Bandwidth Control.....	138
9.3.1.1	QoS.....	138
9.3.1.1.1	Port Priority	138
9.3.1.1.2	IP DiffServ (DSCP)	139
9.3.1.1.3	Priority/Queue Mapping	140
9.3.1.1.4	Schedule Mode	141

9.3.1.2	Rate Limitation	143
9.3.1.2.1	Storm Control.....	143
9.3.1.2.2	Bandwidth Limitation	145
9.3.2	IGMP Snooping.....	146
9.3.2.1	IGMP Snooping	146
9.3.2.1.1	General Settings	146
9.3.2.1.2	Port Settings	148
9.3.2.1.3	Querier Settings	150
9.3.2.2	IGMP Filtering	151
9.3.2.2.1	General Settings	151
9.3.2.2.2	Group Settings.....	152
9.3.2.2.3	Port Settings	153
9.3.2.3	MVR	154
9.3.2.3.1	MVR Settings.....	154
9.3.2.3.2	Group Settings.....	156
9.3.2.4	Multicast Address	157
9.3.2.5	Multicast IP Statistics.....	158
9.3.3	VLAN	159
9.3.3.1	Port Isolation	159
9.3.3.2	VLAN.....	161
9.3.3.2.1	VLAN Settings	161
9.3.3.2.2	Tag Settings.....	163
9.3.3.2.3	Port Settings	164
9.3.3.3	GARP/GVRP	166
9.3.3.3.1	GVRP	166
9.3.3.3.2	GARP Timer	168
9.3.3.4	IP-Subnet-VLAN.....	170
9.3.3.5	MAC VLAN.....	171
9.3.3.6	Protocol VLAN.....	172
9.3.3.6.1	Q-in-Q.....	173
9.3.3.6.2	VLAN Stacking.....	173
9.3.3.6.3	Port-based Q-in-Q.....	175
9.3.4	Selective Q-in-Q.....	176
9.3.5	DHCP Relay	178
9.3.5.1	DHCP Options.....	179
9.3.6	Option 82	179
9.3.7	Dual Homing	180
9.3.8	Dual Ring	182
9.3.8.1	ERPS	184
9.3.8.2	Ring Settings.....	184
9.3.9	Instance Settings	188
9.3.9.1	Link Aggregation	189
9.3.9.2	Static Trunk	189
9.3.9.3	LACP.....	191
9.3.10	LACP Info.	193
9.3.10.1	LLDP	195
9.3.10.2	Settings	195
9.3.11	Neighbor	197
9.3.12	Loop Detection.....	198
9.3.13	Jet Ring.....	200

9.3.14	MODBUS	201
9.3.14.1	STP	202
9.3.14.2	General Settings.....	202
9.3.14.3	Port Parameters	204
9.3.15	STP Status.....	207
9.3.16	Xpress Ring	208
9.4	Security	210
9.4.1	IP Source Guard	210
9.4.1.1	DHCP Snooping	210
9.4.1.1.1	DHCP Snooping	210
9.4.1.1.2	Port Settings	212
9.4.1.1.3	Server Screening	213
9.4.1.2	Binding Table	214
9.4.1.2.1	Static Entry	214
9.4.1.2.2	Binding Table.....	216
9.4.1.3	ARP Inspection.....	217
9.4.1.3.1	ARP Inspection	217
9.4.1.3.2	Filter Table.....	219
9.4.2	Access Control List	220
9.4.3	802.1x.....	224
9.4.3.1	Global Settings	224
9.4.3.2	Port Settings.....	227
9.4.4	Port Security	230
9.5	Monitor	232
9.5.1	Alarm Information.....	232
9.5.2	Monitor Information	233
9.5.3	Port Statistics.....	235
9.5.4	Port Utilization.....	236
9.5.5	RMON Statistics.....	237
9.5.6	SFP Information	240
9.5.7	Traffic Monitor	242
9.6	Management	244
9.6.1	SNMP	244
9.6.1.1	SNMP.....	244
9.6.1.1.1	SNMP Settings	244
9.6.1.1.2	Community Name	245
9.6.1.2	SNMP Trap	247
9.6.1.2.1	Trap Receiver Settings.....	247
9.6.2	Auto Provision.....	248
9.6.3	Mail Alarm.....	249
9.6.4	Maintenance	251
9.6.4.1	Configuration.....	251
9.6.4.2	Firmware	253
9.6.4.3	Reboot.....	254
9.6.4.4	Server.....	255
9.6.5	System Log.....	257
9.6.6	User Account	259
10	Appendix	261
10.1	Console Port (RJ-45 to DB9)	261

10.2	RJ-45 Cable	262
10.3	Configuring in the Command Line Interface (CLI).....	263
10.3.1	System Status.....	263
10.3.1.1	System Information.....	263
10.3.2	Default Settings.....	264
10.3.2.1	System	264
10.3.2.2	Jumbo Frame	264
10.3.2.3	SNTP.....	265
10.3.2.4	Management Host	266
10.3.2.5	MAC Management.....	266
10.3.2.6	Blackhole MAC.....	267
10.3.2.7	Port Mirroring.....	267
10.3.2.8	Port Settings.....	268
10.3.3	Advanced Settings	269
10.3.3.1	Bandwidth Control	269
10.3.3.2	QoS.....	269
10.3.3.3	Rate Limitation	269
10.3.3.4	Storm Control	270
10.3.3.5	IGMP Snooping	271
10.3.3.6	MVR	272
10.3.3.7	Multicast Address	272
10.3.3.8	VLAN.....	273
10.3.3.8.1	Port Isolation.....	273
10.3.3.8.2	VLAN Settings	274
10.3.3.9	GARP/GVRP	275
10.3.3.10	Q-in-Q	276
10.3.3.10.1	VLAN Stacking.....	276
10.3.3.11	DHCP Relay	277
10.3.3.12	Dual Homing.....	278
10.3.3.13	Link Aggregation	278
10.3.3.14	LACP.....	279
10.3.3.15	LLDP	280
10.3.3.16	Loop Detection	281
10.3.3.17	STP	282
10.3.3.18	Xpress Ring.....	283
10.3.4	Security.....	284
10.3.4.1	DHCP Snooping	284
10.3.4.2	Server Screening.....	285
10.3.4.3	Binding Table	285
10.3.4.4	ARP Inspection.....	286
10.3.4.5	Filter Table	286
10.3.4.6	Access Control List.....	287
10.3.4.7	802.1x	289
10.3.4.8	Port Security.....	290
10.3.5	Monitor.....	291
10.3.5.1	Alarm.....	291
10.3.5.2	Monitor Information.....	291
10.3.5.3	RMON Statistics	291
10.3.5.4	SFP Information	291
10.3.5.5	Traffic Monitor	292

10.3.6	Management	293
10.3.6.1	SNMP	293
10.3.6.2	Auto Provision	294
10.3.6.3	Mail Alarm	294
10.3.6.4	Maintenance	295
10.3.6.5	System Log	295
10.3.6.6	User Account	296
10.4	MODBUS/TCP Tables	297
10.4.1	Data Format and Function Code	297
10.4.2	MODBUS Registers	297
List of Figures		330
List of Tables		333

1 Notes about this Documentation



Note

Always retain this documentation!

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

1.1 Validity of this Documentation

This documentation is only applicable to WAGO ETHERNET accessory products “Industrial Managed Switch” (852-303).

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
<i>italic</i>	Names of paths and data files are marked in italic-type. e.g.: <i>C:\Program Files\WAGO Software</i>
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 managed switch with multipoint connector
- Protective covers for unused ports
- Data cable RS-232 for CLI

3.2 Industrial ETHERNET Technology

The range of WAGO Switches ensures scalability of your network infrastructure with outstanding electrical and mechanical characteristics. These rugged devices are designed for industrial use and are fully compliant with the IEEE 802.3, 802.3u, 802.3w, 802.3z, 802.3x, 802.3ab, 802.3ad, 802.1d, 802.1q, 802.1p und 802.1x standards.

They have power supply with a supply voltage range of 12 ... 60 V.

Characteristics such as auto-negotiation and auto MDI/MDIX (crossover) on all 10/100Base-TX ports are also realized.

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.

The Industrial Managed Switch was developed for easy installation in a manufacturing environment where vibration, shock, heat and radio frequency interference are common.

Due to its compact size, the Industrial Managed Switch makes mounting on the DIN rail particularly simple and installation possible in environments with limited space.

Two or more switches can be added in series to the Industrial Managed Switch. Since all ports support 100 Mbit/, this series connection is possible for the industrial managed switch from every port and with any number of switches.

The Industrial Managed Switch is also equipped with a variety of management functions that let you configure communication parameters as you desire to monitor network behavior in different ways. In addition, the Industrial Managed Switch is built with dual redundant power inputs for maximum reliability and network availability. Other integrated features of the switch such as Auto-negotiation, Rate limitation, Port isolation, etc. optimize your network performance and provide a secure network, offering a cost-effective solution in a small but powerful package.

The 1000BASE SX/LX ports are designed to connect Gigabit SFP modules that support network speeds of 100/1000 Mbit/s.

Other key features:

- Eight (8) 10/100Base-TX ports, two (2) 1000Base-SX/LX ports (fiber optice transceiver of the SFP type) and one (1) RS-232 port
- Web-based/SNMP Management
- Redundant DC power supply
- Large voltage range: 12 ... 60 V
- DIP switches to set alarm functions
- Full compliance with IEEE 802.3, 802.3u, 802.3z, 802.3x, 802.3ad, 802.3ab, 802.1d, 802.1q, 802.1p, 802.1w, 802.1x standards
- Implemented functions:
 - Dual ring
 - ERPS
 - Jet ring
 - Xpress Ring (redundant ring, recovery < 50 ms)
- Non-blocking, store-and-forward switching, rapid spanning tree protocol (RSTP)
- Auto-negotiation on all 10/100Base-TX ports
- Auto-MDI/MDIX (crossover) on all 10/100Base-TX ports
- VLAN (802.1q) VID
- IGMP snooping for multicast filtering
- Port configuration, status and statistics
- Port trunking
- SNMP v1/v2 and RMON
- Rugged IP30 metal housing
- Operable in vibration / shock

4 Device Description

The 852-0303 is an industrial ETHERNET switch with 8 10/100/1000Base-TX ports, autonegotiation and Auto-MDI-/MDI-X detection at every port. Using the Industrial Managed Switch's 8 ports, several segments can be set up for reducing network load and a dedicated bandwidth assigned to each user node.

In addition, the 852-0303 Industrial Managed Switch has 2 ports with SFP 100BASE-FX and SFP-1000BASE-SX/LX to connect multi-mode or single-mode fiber optic cables for wave lengths of 850 nm (SX), 1310 nm (LX) and 1550 nm (ZX).

The 852-0303 switch is a cost-effect solution to keep up with the constant demands of IP-based, industrial communication needs.

The Industrial Managed Switch is easy to configure and install and is best suited for small to medium-sized networks.

4.1 View

4.1.1 Front View

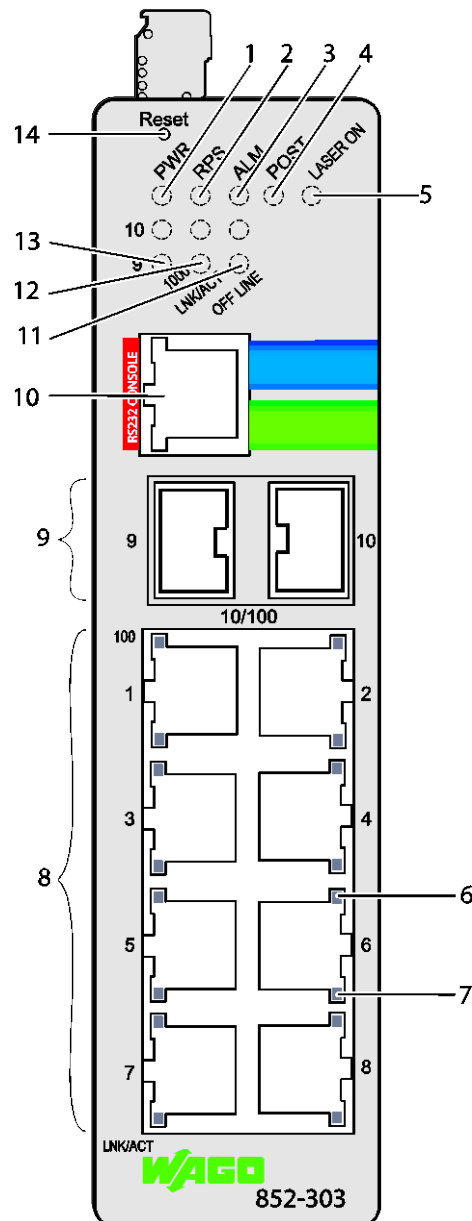


Figure 1: Front View of the Industrial Managed Switch

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

No.	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	POST	Status LED, POST	“Device Description” > “Display Elements”

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

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

4.1.2 Top View

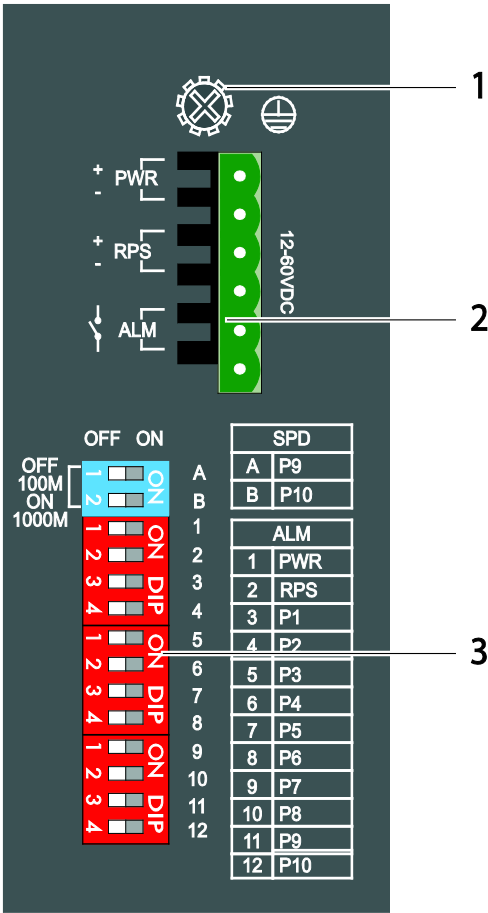


Figure 2: Top View of the Industrial Managed Switch (Example)

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

No.	Description	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"
3	-	DIP Switches	"Device Description" > "Operating Elements"

4.2 Connectors

4.2.1 Power Supply (PWR/RPS)

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

The male connector shows the following pin assignment:

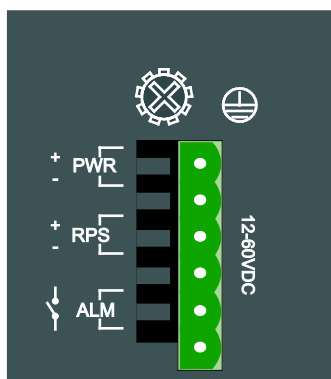


Figure 3: Power Supply (PWR/RPS)

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.

4.3 Network Connections

The industrial managed switch uses ports with fiber optic or copper connectors that can be used with ETHERNET and/or Fast ETHERNET protocols.

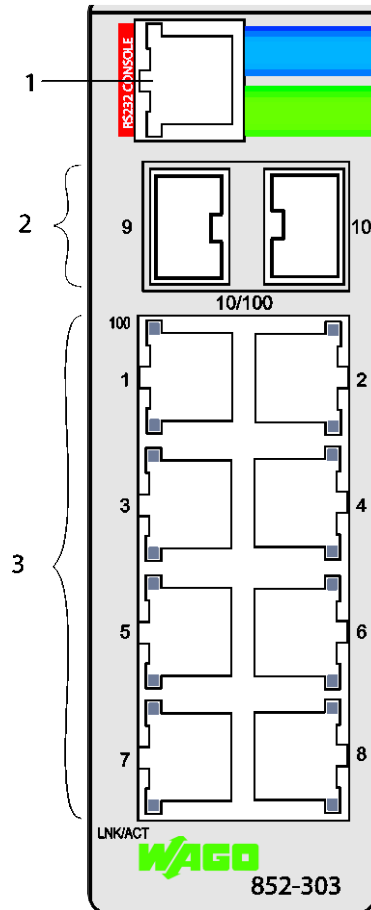


Figure 4: Network Connections

Table 6: Legend for Figure “Network Connections”

No.	Description	Meaning	For Details see Section
1	-	Connection 1 x RJ-45 (RS-232 port)	“Device Description” > ... > “RJ-45 Port (RS-232 Port)”
2	-	Connection 2 x SFP (SFP 100BASE-FX und SFP-1000BASE-SX/LX, fiber optic)	“Device Description” > ... > “1000BASE SX/LX Ports”
3	-	Connections 8 x RJ-45 (10/100BASE-TX ports)	“Device Description” > ... > “10/100BASE TX Ports”

4.3.1 RJ-45 Port (RS-232 Port)

This RJ-45 port is used to connect to a serial COM port via RS-232.

4.3.2 SFP 1000BASE SX/LX / SFP 100BASE FX Ports

The 1000BASE SX/LX ports are designed to connect Fast ETHERNET or gigabit SFP modules that support network speeds of 100/1000 Mbit/s.

4.3.3 10/100BASE TX Ports

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

The switch works in store-and-forward mode and for each port, supports transmission speeds 10/100 Mbit/s as well as the full and half-duplex transmission modes.

The RJ-45 socket is wired in accordance with 100Base TX requirements.

It is mandatory to use a Category 5e twisted-pair cable from the ETHERNET standard as a connecting cable. Cable types S-UTP (Screened Unshielded Twisted Pair) and STP (Shielded Twisted Pair) with a maximum segment length of 100 m can be used.

The connection point is designed for mounting into an 80 mm-high switchgear cabinet after connector attachment.

These ports also provide automatic crossover detection (Auto-MDI/MDI-X) with plug&play capabilities. Simply plug the network cables into the ports; they then adapt to the end node devices. We recommend the following cables for the RJ-45 ports.

- 10 m – Cat 3 or higher
- 100 m – Cat 5e or higher

4.4 Display Elements

The industrial managed switch is equipped with device LEDs and port LEDs. You can see the status of the switch at a quick glance of the device LEDs, while the port LEDs provide information about connection actions.

4.4.1 Device LEDs

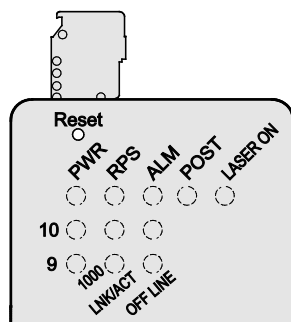


Figure 5: Device LEDs

Table 7: Legend for Figure "Device LEDs"

LED	Name	Status	Description
PWR	Primary Power LED	Green	The industrial managed switch uses the primary power supply.
		OFF	The primary power supply has been switched off or a fault has occurred.
RPS	Redundant Power System LED	Green	The industrial managed switch uses the redundant power supply.
		OFF	The redundant power supply has been switched off or a fault has occurred.
ALM	Alarm LED	Red	Lights up in the event of network, connection or ring errors (for Arbiter nodes).
		OFF	No alarm to report.
POST	Power On Self Test LED	Flashes	The Self Test is executed.
		Green	The Switch is operational.
		OFF	The Switch is not operational.
LASER ON	LASER ON LED	Yellow	Lights up if the SFP 1000BASE SX/LX or SFP 100BASE FX fiber optic port is used.
		OFF	No SFP 1000BASE SX/LX or SFP 100BASE FX fiber optic port is used.

Table 7: Legend for Figure "Device LEDs"

LED		Name	Status	Description
9/ 10	1000	Fiber 1000 Mbit/s LED	Green	Port in operation at 1000 Mbit/s.
			OFF	No proper link established at the port.
	LNK/ACT	Fiber port LNK/ACT LED	Green	Lights up when the ports are linked.
			Flashes	Data traffic being routed via the port.
			OFF	No proper link established at the port.
	OFF-LINE	Fiber port Offline LED	Red	Lights up when there is no SFP device.
			OFF	Both SFP devices are properly connected.

4.4.2 Port LEDs

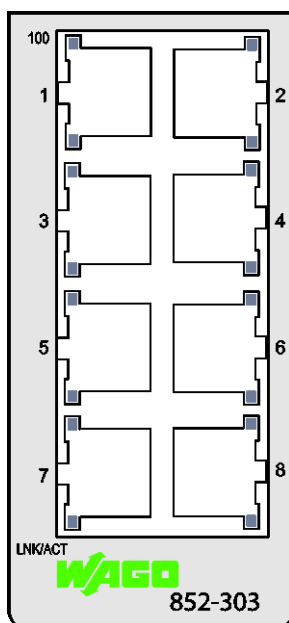


Figure 6: Port LEDs

Table 8: Legend for Figure "Port LEDs"

LED	Name	Status	Description
100	10/100Base-TX Ports LED (1 LED for each port)	Green	Port in operation at 100 Mbit/s.
		OFF	Connection in operation at less than 100 Mbit/s.
LNK/ACT	LNK/ACT LED (1 LED for each port)	Green	Lights up when the ports are linked.
		Flashes	Data traffic being routed via the port.
		OFF	No proper link established at the port.

4.5 Operating Elements

4.5.1 DIP Switches

On the top side of the industrial switch there are DIP switches to configure the alarm and speed configurations.

The meaning of the DIP switch settings are described below:

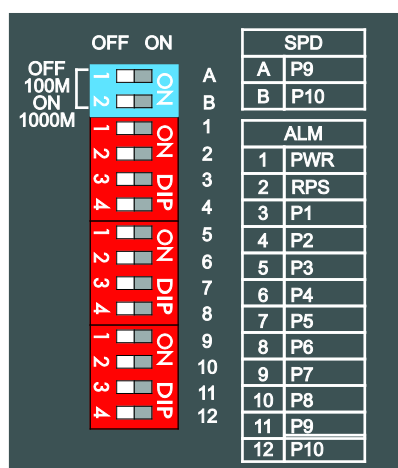


Figure 7: DIP Switches (Example)

Table 9: Legend for Figure “DIP Switches (Example)”

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

DIP switches let the user manually turn ON/OFF any port, the external alarm, or the redundant power supply.

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. Install the industrial managed switch in your network.
- 1 Select the port(s) to be monitored or the alarm to be activated.
- 2 Set the DIP switch of the corresponding port to “ON”.
- 3 Turn the industrial managed switch ON.

4.5.2 Reset Button



Figure 8: 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.



Note

Press the reset button

Use a suitable tool to press the reset button.

4.6 Label

4.6.1 Hardware and Software Version

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



Figure 9: Label (Example)

Table 11: Legend for Figure “Label”

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

4.7 Technical Data

4.7.1 Device Data

Table 12: Technical Data – Device Data

Width	Carrier rail mounting	50 mm
Height	Carrier rail mounting	120 mm (from the top edge of the carrier rail)
Depth	Carrier rail mounting	162 mm
Weight		910 g
Degree of protection		IP30

4.7.2 System Data

Table 13: Technical Data – System Data

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

4.7.3 Power Supply

Table 14: Technical Data – Power Supply

Supply voltage	12 ... 60 VDC
Power consumption, max.	12 W

4.7.4 Communication

Table 15: Technical Data – Communication

Ports	8 x 10/100BASE-TX (RJ-45) 2 x SFP 1000BASE-SX/LX, fiber optic 1 x RS-232 (RJ-45)
Standards	IEEE 802.3u 100BASE-TX/FX IEEE 802.3ad Link Aggregation IEEE 802.3 10BASE-T IEEE 802.1d Spanning Tree Protocol IEEE 802.3x Flow Control IEEE 802.1p CoS Prioritization IEEE 802.1q VLAN Tagging IEEE 802.3ab LLDP IEEE 802.3w RSTP IEEE 802.3z 1000BASE-SX/LX IEEE 802.1x Port Authentication
Topology	star, tree, line

4.7.5 Environmental Conditions

Table 16: Technical Data – Environmental Conditions

Surrounding air temperature (operation)	-40 ... +70 °C
Surrounding air temperature, operation, DNV GL (Temperature class D)	-25 ... +70 °C
Surrounding air temperature (storage)	-40 ... +80 °C
UL 61010 Use Pollution degree	Indoor 2
Relative humidity (without condensation)	5 ... 95 %
Vibration resistance	Acc. IEC 60068-2-6
Shock resistance	Acc. IEC 60068-2-27
EMC-1 immunity to interference	Acc. EN 61000-6-2
EMC-1 Emission of interference	Acc. EN 61000-6-4
Standard Compass Safe Distance 0.3 Degree deflection	750 mm
Steering, Standby, Emergency Compass Safe Distance 1.0 Degree deflection	450 mm

4.8 Approvals

The following approvals have been granted for the WAGO ETHERNET accessory product “Industrial Managed Switch” (852-303):

 Conformity Marking

 Ordinary Locations UL61010-2-201 (E175199)

Table 17: Assignment UL – Hardware Version

Approval	Hardware Version
UL	valid from version 04

The following ship approvals have been granted for the WAGO ETHERNET accessory product “Industrial Managed Switch” (852-303):



DNV GL
[Temperature: D, Humidity: B, Vibration: C, EMC: B,
Enclosure: A]



Note

Applicable from HW 03!

This ship approval is only applicable from HW 03. Switches with hardware version 2 do not have DNV GL approval!

5 Mounting

5.1 Installation Site

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

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

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

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

5.3 Removal from Carrier rail

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

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

6 Connect Devices

6.1 Power Supply

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

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

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

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

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

Note



Ground for the switch

The ground for the switch prevents electromagnetic interference from electromagnetic radiation.

Observe the corresponding standards for EMC-compatible installations as well.

2. Plug the female connector into the male connector of the switch if it has not already been plugged in. Check the tight fit of the multipoint connector by gently shaking it.
3. PWR +/-:
To connect or disconnect the conductors, actuate the spring directly in the female connector using a screwdriver or an operating tool and insert or remove the conductor.
4. Check whether the power LED "PWR" on the top of the device lights up when power is supplied to the device. If not, check to ensure that the power cable is plugged in correctly and fits securely.
5. RPS +/-:
To connect or disconnect the conductors, actuate the spring in the female connector directly using a screwdriver or an operating tool and insert or remove the conductor.
6. Check whether the power LED "RPS" on the top of the device lights up when power is supplied to the device. If not, check to ensure that the power cable is plugged in correctly and fits securely.

6.2 External Alarm Contact Port

The industrial 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 industrial 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 Link failure (e.g., cable disconnected, device breakdown, etc.)
- 2 PWR/RPS:
 - a Power failure (power cord is disconnected, power supply malfunction, etc.)
 - b Input power falls outside specification (12 ... 60 V)
- 3 Failure in jet ring or ERPS ring (Enhancement mode).

6.3 Console Port Cable Connection

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

1. Insert the RJ-45 side of the (8 pin RJ-45 to DB9) cable into the RJ-45 console port on the Industrial Managed Switch and the other end into the COM port of the computer.
2. Configure the Hyper Terminal settings as mentioned in chapter “Configuration” > ... > “Console Port”.

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

6.4 1000Base-SX/LX Port, 100BASE-FX Port, Fiber Optic

When connecting a fiber optic cable to a 1000Base-SX/LX port or to a 100BASE-FX port on the industrial managed switch, make sure to use the right connector type (LC) and SFP module.

There are various types of multi-mode, single mode or WDM SFP modules. Follow the steps below to connect the fiber optic cable properly:

Note



Rubber covers

Remove and safely store the rubber covers of the fiber optic port (LC).

If no fiber optic cable is connected, the rubber cover should be installed to protect the fiber optics.

- 1 Insert the respective SFP modules.
- 2 Ensure that the fiber optic ports are clean. You can clean the cable connectors by wiping them with a clean cloth or a cotton ball soaked with a little ethanol. Dirty fiber optic cables affect the quality of the light transmitted via the cable and leads to reduced performance at the port.
- 3 Connect one end of the fiber optic cable to the LC port of the industrial managed switch and the other end to the fiber optic port of the other device.

Note



Proper connection of the fiber optic cable to the SFP module

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

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

6.5 10/100BASE-TX Ports

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

- 1 Connect one end of the twisted pair cable of the type Category 3/4/5/5e to an available RJ-45 port on the industrial managed switch and the other end to the port of the selected network node.
- 2 Check the respective port LED on the industrial managed switch that the connection is established.
(see section “Display Elements” > ... > “Port LEDs”).

7 Function Description

7.1 Default Settings

7.1.1 Jumbo Frame

“Jumbo Frames” are ETHERNET frames with a size of more than 1500 bytes. Jumbo frames can increase data transmission efficiency in a network. The bigger the “Jumbo Frame”, the better the network performance.



Note

“Jumbo Frame” settings

The “Jumbo Frame” settings apply to all ports.

If the size of a packet exceeds the size of the “Jumbo Frame”, the packet is dropped.

7.1.2 SNTP

SNTP (“**S**imple **N**etwork **T**ime **P**rotocol”) is a protocol for synchronizing clocks in computer systems. It is a less complex implementation of an NTP (“**N**etwork **T**ime **P**rotocol”).

SNTP uses “**C**oordinated **U**niversal **T**ime” (French: “**T**emps **U**niversel **C**oordonné”). No information on time zones or daylight savings time is transmitted. This information falls outside the protocol range and must be obtained separately.

The SNTP port is 123.



Note

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.

7.1.3 Management Host

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

7.1.4 MAC Management

The MAC address (“**M**edia **A**ccess **C**ontrol”) is the unique hardware number in a network.

Dynamic Address

When receiving frames, the switch received the source MAC address, receiving port, VLAN and an “Age Time” in the address table. When the “Age Time” is expired, the address entry is deleted from the address table.

Static Address

A static address set by the user does not include the “age time” and is not deleted by the switch. The static address can only be deleted by a user. The switch supports an address table at up to 16 K.

Static and dynamic addresses share the same address table.

MAC Table

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

It also shows whether the MAC address is dynamic (assigned by the switch) or static (set manually).

MAC Address Table

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

1. The switch checks a received frame and detects the port from which the MAC source address originates.
2. The switch checks if the frame's destination MAC address matches a source MAC address already detected in the MAC address table.
 - If the switch already knows the port for this MAC address, the it forwards the frame to that port.

- If the switch does not already know the port for this MAC address, it forwards the frame to all ports. “Port Flooding” (forwarded too often to all ports) can lead to network congestion.
- If the switch already knows the port for this MAC address and the destination port is the same as the input port, the frame is filtered.

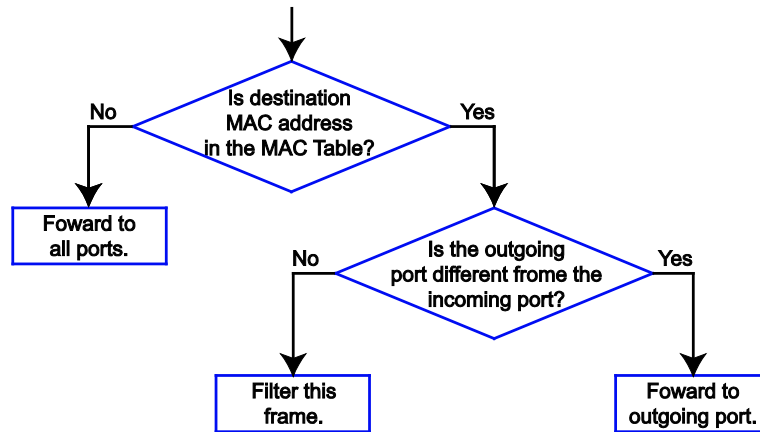


Figure 10: MAC Address Table Flowchart

7.1.4.1 Static MAC Settings

Static MAC Addresses

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

7.1.4.2 Refusal MAC Settings

This type of MAC address entries is configured manually. The switch ignores packets that have such MAC addresses as the source or destination contained in “Blackhole” MAC address entries. “Blackhole” entries are configured to filter frames with specific source or destination MAC addresses.

7.1.5 Port Mirroring

Port mirroring is used on switches to copy sent/received network packets from one or more areas of network monitoring or to send them to another switch port (monitor port).

Port mirroring is used in network systems that require monitoring of network traffic as in an IDS (“Intrusion **D**etection **S**ystem”).

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

Source Mode

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

Note



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

7.1.6 Port Settings

Duplex Mode

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

Half-Duplex

A half-duplex system provides for communication in both directions, but only one direction at a time (not simultaneously).

One device receives a signal and must wait for the other device to stop transmitting before replying.

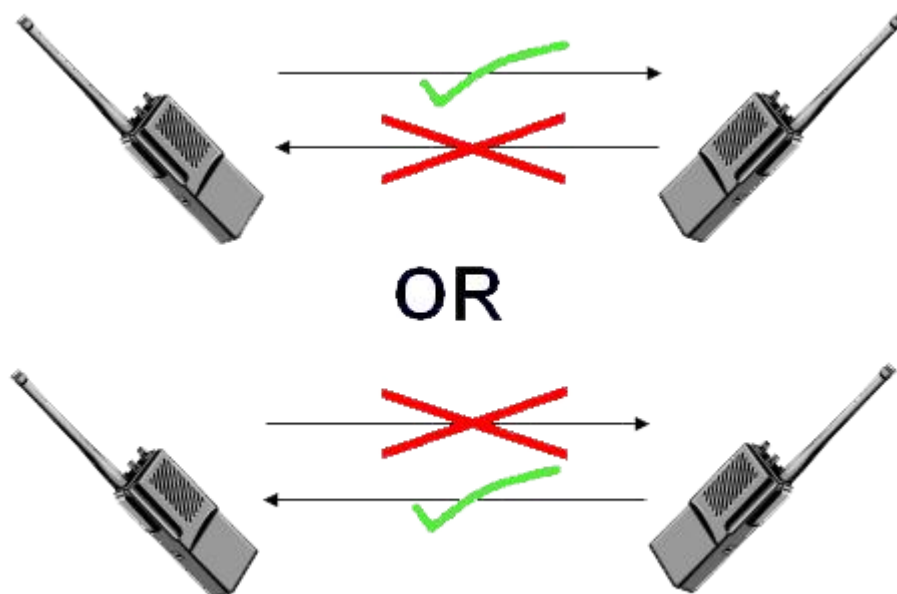


Figure 11: Half-Duplex Mode

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 12: Full-Duplex Mode

Loopback Test

In a “Loopback” test, a signal is sent from and then returned to a communication device (“looped back”).

The test checks the proper function of the device and looks for faulty nodes in the network.

For one type of “Loopback” test, a special plug (so-called “wrap plug”) is plugged into a communications device. The plug causes transmitted (output) data to be returned as received (input) data, simulating a closed communication circuit using a single computer.

Auto MDI/MDIX

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

Auto-MDIX (“**A**utomatic **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 of the interface and in the duplex settings must be set to “Auto”.

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) that independently negotiate and configure the maximum transmission speed and the duplex process.

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

If the port does not support auto-negotiation or the function is disabled, 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 IEEE802.3x, the switch uses “Flow Control” in full-duplex mode and “Backpressure Flow Control” in half-duplex mode.

For “Flow Control”, the switch sends a pause signal in full-duplex mode to the sending port, causing it to temporarily stop sending signals when the buffer memory of the receiving port is full.

For “Backpressure Flow Control”, the switch sends a collision signal to the sending port in half-duplex mode (mimicking a state of packet collision), 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”.

7.2 Advanced Settings

7.2.1 Bandwidth Limitation

7.2.1.1 QoS

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

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

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

Implementing QoS in a network improves network predictability and increases bandwidth utilization.

The industrial managed switch supports “802.1p Priority Queuing”.

The switch has eight “Priority Queues”. These priority queues are numbered, where Class 7 is the highest and Class 0 the lowest priority queue. The eight priority classes specified in IEEE 802.1p (p0 to p7) are mapped to the switches priority queues as follows:

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

The “Priority Scheduling” is implemented in “Priority Queues”. The switch operates the four “Hardware Priority Queues” sequentially, where it starts with the highest “Priority Queue” (3) and ends with the lowest (0). Each “Hardware Queue” transmits all packets in its buffer before the next lower priority is allowed to transmit its packets. If the lowest “Hardware Priority Queue” transmits all its packets, the highest starts to transmit its packets again that it received in the meantime.

QoS Enhancement

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

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

Note**Advanced QoS Methods**

Advanced QoS methods only affect the internal “Priority Queue” mapping for the switch. The switch does not modify the IEEE 802.1p value for the egress frames.

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

802.1p Priority

When using the 802.1p priority mechanism, the packet is examined for the presence of a valid “802.1p Priority Tag”. If it has a tag, the packet is designated to a configurable “Egress Queue” based on its priority value. The “Tag Priority” can be designated to any of the available “Queues”.

ETHERNET Packet

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

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

802.1Q Tag:

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

- **TPID (“Tag Protocol Identifier”)**
A 16-bit field is set to the value of 0x8100 to identify the frame as an “IEEE 802.1Q Tag Frame”.
- **TCI (“Tag Control Information”)**
 - **PCP (“Priority Code Point”)**
A 3-bit field that refers to the IEEE 802.1p priority. It indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc.).
 - **CFI (“Canonical Format Indicator”)**
A 1-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format. It is always set to 0 for ETHERNET switches. CFI is used for compatibility between ETHERNET and “Token Ring” networks. If a frame received at an ETHERNET port has a CFI of 1, the frame should not be output to an untagged port.
 - **VID (“VLAN Identifier”)**
A 12-bit field specifying the VLAN to which the frame belongs. A value of 0 means that the frame does not belong to any VLAN; in this case, the “802.1Q Tag” specifies only a priority and is referred to as a “Priority Tag”. A hexadecimal value of 0xFFF is reserved for implementation purposes. All other values may be used as “VLAN Identifiers”, allowing support for up to 4094 VLANs. On “Bridges”, VLAN 1 is often reserved for management.

Priority Levels

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

Table 18: Priority Levels

PCP	Network Priority	Traffic Characteristics
1	0 (lowest)	“Background”
0	1	“Best Effort”
2	2	“Excellent Effort”
3	3	“Critical Applications”
4	4	Video, < 100 ms latency
5	5	Video, < 10 ms latency
6	6	Internetwork Control
7	7 (highest)	Network Control

DiffServ (DSCP)

DiffServ (“**D**ifferentiated **S**ervices”) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism, managing network traffic and providing (“**Q**uality of **S**ervice”) guarantees in modern IP networks. DiffServ can, for example, be used to provide low-latency, guaranteed service (“**G**uaranteed **S**ervice”) to critical network traffic such as voice or video data while providing simple “Best Effort” traffic guarantees to non-critical services such as web traffic or file transfers.

DSCP (“**D**ifferentiated **S**ervices **C**ode **P**oint”) is a 6-bit field in the header of IP packets for packet classification purposes. DSCP replaces the outdated IP precedence, a 3-bit field in the “Type of Service” byte of the IP header originally used to classify and prioritize types of traffic.

When using the DiffServ priority mechanism, a packet is classified based on the DSCP field in the IP header. If the tag is present, the packet is assigned to a programmable “Egress Queue” based on the value of the “Tagged Priority”. The “Tagged Priority” can be designated to any available “Queue”.

Version	IHL	Type of Service	Total Length	
Marking			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				Padding

Example Internet Data Packet Header

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

The “Type of Service” field provides an indication of the abstract parameters of the “Quality of Service” desired. These parameters are to be used to guide the

manual selection of the actual service parameters when transmitting a data packet through a particular network. Several networks offer service precedence, which treats high precedence traffic as more important than other traffic (generally by accepting only traffic above certain precedence at time of high load). The most favorable choice is a compromise between low delay, high reliability and high throughput.

Bit 0 ... 2	Precedence.	
Bit 3	0 = Normal delay,	1 = Low delay.
Bit 4	0 = Normal throughput,	1 = High throughput.
Bit 5	0 = Normal reliability,	1 = High reliability.
Bit 6 ... 7	Reserve for future use.	



Precedence

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

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

The “Type of Service” is used to specify the type of processing of the data packet while it is transmitted through a network. Example mappings of the “Internet Type of Service” to the actual service provided in networks, such as AUTODIN II, ARPANET, SATNET and PRNET are specified in “Service Mappings”.

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

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

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

Example:

IP Header

DSCP=50 -> 45 C8 ...

Queuing Algorithms

“Queuing Algorithms” can be used to maintain separate “Queues” for packets that can be derived from any single source or any data flow, thus preventing a source from monopolizing the bandwidth.

SPQ

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

WRR

RR (“Round Robin”) is a scheduling service that queues packets on a rotating basis and is only activated when a port has more traffic than it can handle. A “Queue” is given an amount of bandwidth irrespective of the incoming traffic on that port. This “Queue” then moves to the back of the list. The next “Queue” is given an equal amount of bandwidth and then moves to the end of the list and so on until all “Queues” are processed. The entire process works in a looping fashion until a “Queue” is empty.

WRR (“Weighted Round Robin”) scheduling uses the same algorithm as “Round Robin” scheduling, but services “Queues” based on their priority and queue weight (the number you configure in the “Weight Value” field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. “Queues” with larger weights get more service than those with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different “Traffic Queues” and returns to queues that have not yet emptied.

Note



DiffServ Function

DiffServ is disabled on the industrial managed switch.

If the DiffServ is disabled, the “802.1p Tag Priority” is used.

7.2.1.2 Rate Limitation

7.2.1.2.1 Storm Control

A broadcast storm means that 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 those two types is not exceed.

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

The “Storm Control” unit is 625 pps (packets per second).

7.2.1.2.2 Rate Limitation

The “Rate Limitation” is used to control the rate of traffic sent or received on a network interface.

7.2.2 IGMP Snooping

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

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

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

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

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

Immediate Leave

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

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

Fast Leave

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

Last Member Query Interval

The “Last Member Query Interval” is the maximum response time in group-specific queries sent in response to “Leave Group” messages, and also shows the time between group-specific query messages.

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

IGMP Querier

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

Port IGMP Querier Mode

- Auto
 - The switch uses the port as an “IGMP Query Port” if the port receives “IGMP Query” packets.
- Fixed
 - The switch always uses the port(s) as “IGMP Query Port(s)”. This mode is used when connecting an IGMP multicast server to the port(s).
 - The switch always forwards the clients “Report/Leave” packets to the port. Normally, the port is connected to an IGMP server.
- Edge
 - The switch does not use the port as an “IGMP Query Port”.
 - The “IGMP Query” packets received on this port are dropped. Normally, the port is connected to an IGMP client.

Note



Forwarding “IGMP Join/Leave” packets

The industrial managed switch will forward the “IGMP Join/Leave” packets to the query port.

IGMP Proxy Snooping

The “IGMP Proxy Snooping” can reduce the number of “Reports” and “Leaves” sent through an IGMP router.

Configurations

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

Note



VLAN States

There is a global state and individual VLAN states.

If the global state is disabled, “IGMP Snooping” on the switch is disabled even if individual VLAN states have been enabled.

If the global state is enabled for “IGMP Snooping”, the function must be individually enabled by the user for specific VLANs.

7.2.2.1 MVR

MVR (“**M**ulticast **V**LAN **R**egistration”) through which a media server can transmit a multicast stream in an individual multicast VLAN and in which the clients receiving the VLAN stream can be located in different VLANs. Clients in different VLANs can join or leave the multicast group simply by sending an “IGMP Join Message” or “IGMP Leave Message” to a receiver port. The receiver port belonging to a multicast groups can receive the multicast stream from the media server. Without MVR support, the multicast stream from the media server and subscriber would have to be in the same VLAN.

- Source ports : The source ports of the stream.
- Receiver ports: The reports of the clients.
- Ports with tag: Configure ports with tags to designate them as source ports or receiver ports.

MVR Mode

- **Dynamic Mode**
If dynamic mode is enabled in the MVR settings, the “IGMP Report Message” is transmitted from the receiver port to the source ports of the multicast router. The multicast router can detect dynamically which multicast groups are on which interface.
- **Compatibility Mode**
If compatibility mode is enabled in the MVR settings, the “IGMP Report Message” send by the receiver port is not transmitted to the source ports of the multicast router. The multicast router must be statically configured.
- **Operating Mode**
Join Operation
A subscriber sends an “IGMP Report Message” to the switch to join a respective multicast. The next step depends on whether the “IGMP Report Message” matches the multicast MAC address configured on the switch. If it matches, the switch CPU modifies the hardware address table to include the receiver port and the VLAN as a forwarding destination for the MVLAN.
- **Leave Operation**
A subscriber sends an “IGMP Leave Message” to the switch to leave the multicast. The switch CPU sends a group-specific “IGMP Query” to the receiver port of the VLAN. If there is another subscriber in the VLAN, the subscriber must respond within the maximum response time. If there is no subscriber, the switch deletes the receiver port.

- **Immediate Leave Operation**

A subscriber sends an “IGMP Leave Message” to the switch to leave the multicast. The subscribers do not need to wait for the switch CPU to send a group-specific “IGMP Query” to the receiver port of the VLAN. The switch immediately deletes the receiver port.

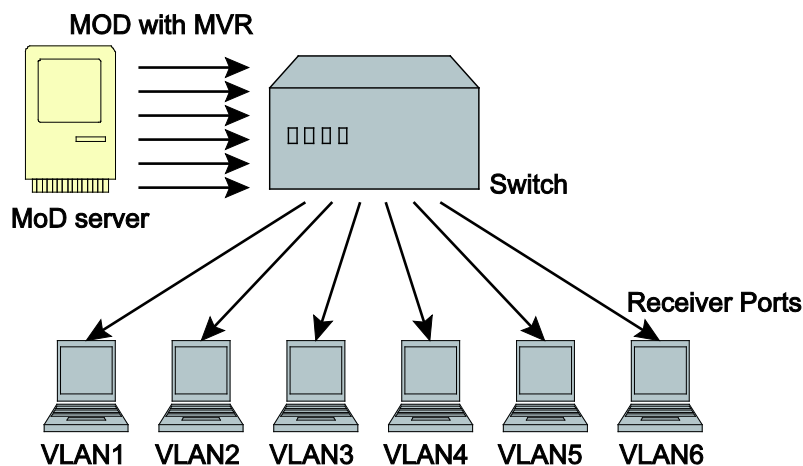


Figure 13: MOD without MVR

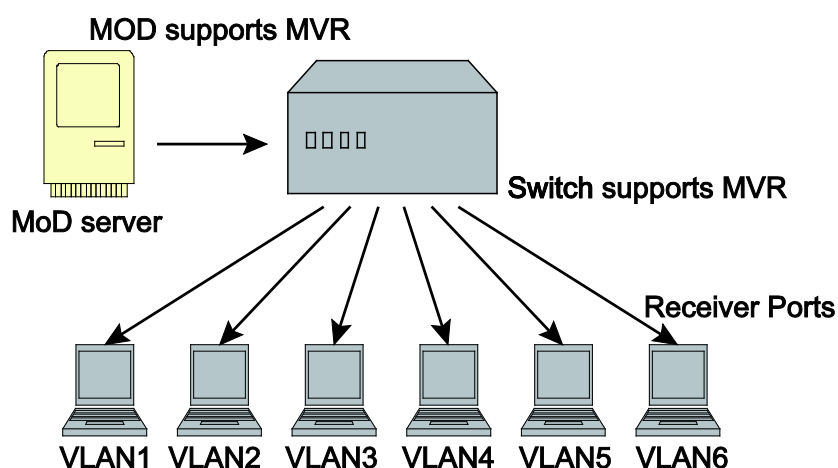


Figure 14: MOD supports MVR

Default configuration for a new MVR:

MVR VLAN information

VLAN ID:	2
Name:	MVR2
Active:	Enabled
Mode:	Dynamic
Source port(s):	None
Receiver port(s):	None
Port(s) with tag:	None

The switch allows the user to create up to 250 groups.
The switch allows the user to create up to 16 MVRs.

Note



- “IGMP Snooping” and MVR can be enabled independently.
 - “IGMP Snooping” and MVR use the same IGMP timer.
 - MVR can recognize IGMPv3 reports.
 - The switch as well as the following group record types do not treat group entries such as an IGMPv3 report as membership reports. The group record types are “MODE_IS_INCLUDE”, “CHANGE_TO_INCLUDE_MODE”, “ALLOW_NEW_SOURCES” and “BLOCK_OLD_SOURCES”.
 - Do not use group address X.0.0.1 for your multicast stream. The system detects and logs the address 224.0.0.1 for the dynamic “Querier Port”. The group address X.0.0.1 could cause a conflict with 224.0.0.1.
 - The lower 23 bits of the 28-bit multicast IP address are mapped to the 23 bits of the available ETHERNET address space.
When configuring the group address, the switch only compares the lower 23 bits.
 - The CLI command “group 1 start-address 224.1.1.1 6” creates 6 groups.
That is, one IP, one group.
 - The MVR name should be a combination of numbers and letters.
 - The group name should be a combination of numbers and letters.
-

7.2.2.2 Multicast Address

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

The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped to the 23 bits of the available ETHERNET address space. This means that there is ambiguity in delivering packets. If two hosts on the same subnet each subscribe to different multicast groups whose addresses differ only in the first 5 bits, ETHERNET packets for both multicast groups are sent to both hosts, requiring the network software in the hosts to discard the unnecessary packets.

Table 19: Multicast Classes and Address Ranges

Class	Address Range	Support
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use or research and development purposes.

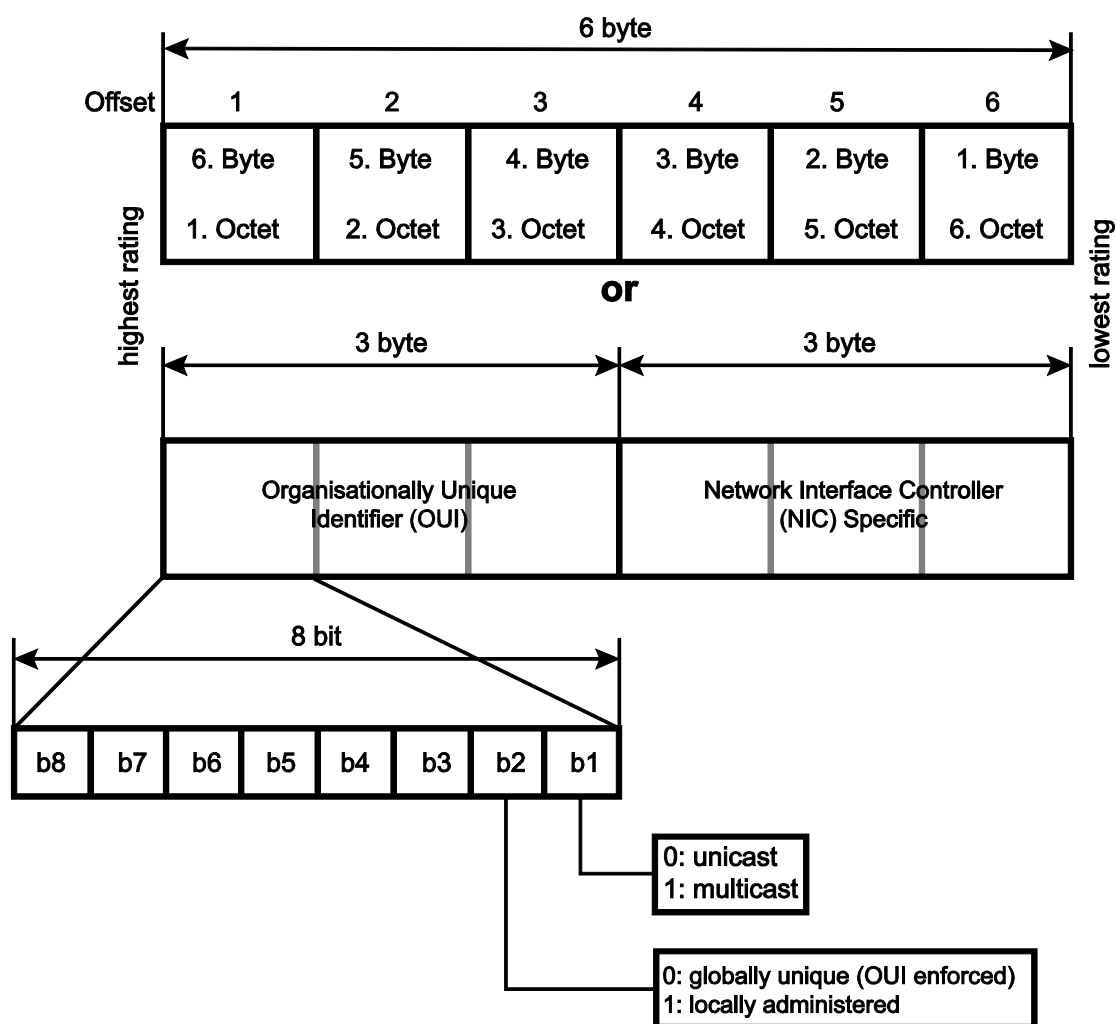


Figure 15: Multicast Address

Table 20: IP Multicast Addresses

IP multicast address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	“All Hosts Multicast” group that contains all systems on the same network segment.
224.0.0.2	“All Routers Multicast” group that contains all routers on the same network segment.
224.0.0.5	The “Open Shortest Path First” (OSPF protocol), the “AllSPFRouters” address. Used to send “Hello Packets” to all OSPF routers on a network segment
224.0.0.6	The “OSPF AllDRouters” address. Used to send OSPF routing information to “OSPF Designated Routers” on a network segment
224.0.0.9	The RIP (“Routing Information Protocol”) Version 2 of the group address. Used to send routing information to all RIPv2-compatible routers on a network segment.
224.0.0.10	The EIGRP group address. Used to send EIGRP routing information to all EIGRP routers on a network segment.
224.0.0.13	PIM Version 2 (“Protocol Independent Multicast”)

Table 20: IP Multicast Addresses

IP multicast address	Description
224.0.0.18	Virtual Router Redundancy Protocol
224.0.0.19 - 21	IS-IS over IP
224.0.0.22	IGMP Version 3 ("Internet Group Management Protocol")
224.0.0.102	Hot Standby Router Protocol Version 2
224.0.0.251	Multicast DNS address
224.0.0.252	"Link-local Multicast Name Resolution"-address
224.0.1.1	"Network Time Protocol" address
224.0.1.39	"Cisco Auto-RP-Announce" address
224.0.1.40	"Cisco Auto-RP-Discovery" address
224.0.1.41	"H.323 Gatekeeper Discovery" address

7.2.3 VLAN

A VLAN (“**Virtual 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 offset devices.

VID (“**VLAN-ID**”) is the identification of a VLAN that is generally used by the 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 VLAN configurations are 4094.

A “Tagged VLAN” uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across “Bridges” - they are not confined to the switch on which they were created. VLANs can be created statically (manually by users) or dynamically via the GVRP (“GARP VLAN Registration Protocol”). The VLAN ID associates a frame with a specific VLAN and provides the information that switches need 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”, 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 user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a “Priority Frame”, i.e., only the priority level is relevant 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 VLAN configurations are 4094.

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

- **Forwarded Tagged and Untagged Frames**

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

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

- **Port-Based 802.1Q VLAN**

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

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

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

This approach is quite simple, fast and easy to manage in that there are no complex lookup tables required for VLAN segmentation. If the "Port-to-VLAN" connection is designed with an application-specific integrated circuit (ASIC), performance is very good. An ASIC allows "Port-to-VLAN" mapping at the hardware level.

7.2.3.1 Port Isolation

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

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

If you want to allow communication between two subscriber ports, you must define the egress port for both ports. CPU refers to the switch 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.

7.2.3.2 GARP/GVRP

GARP (“**Generic Attribute Registration Protocol**”) and GVRP (“**GARP VLAN Registration Protocol**” or “**Generic VLAN Registration Protocol**”) are industry-standard protocols described in IEEE 802.1p. GVRP is a GARP application that provides 802.1Q-compliant “VLAN Pruning” and dynamic VLAN creation on “802.1Q Trunk Ports”.

With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches that are connected through “802.1Q Trunk Ports”.

GVRP makes use of GID (“**Group Identification**”) and GIP, which provide the common “State Machine Descriptions” and the common information propagation mechanisms defined for use in GARP-based applications. GVRP runs only on “802.1Q Trunk Links”. GVRP prunes “Trunk Links” so that only active VLANs are transmitted across trunk connections. GVRP expects to hear join messages from the switches before it will add a VLAN to the trunk. GVRP updates and hold timers can be altered. GVRP ports run in various modes to control how they will prune VLANs. GVRP can be configured to dynamically add and manage VLANs in the VLAN database for “Trunking” purposes.

In other words, GVRP allows the propagation of VLAN information from device to device. With GVRP, a single switch is manually configured for all VLANs required for the network and all other switches on the network learn detect the VLANs dynamically. End nodes can be plugged into any switch and connected to the required VLAN. For end nodes to make use of GVRP, they need GVRP-aware network interface cards (NICs). The GVRP-aware NIC is configured with the desired VLAN or VLANs, then connected to a GVRP-enabled switch. The NIC communicates with the switch once connectivity is established between the NIC and switch.

Registration Mode:

- **Normal**
The “normal” registration mode allows dynamic creation (if dynamic VLAN creation is enabled), registration and deregistration of VLANs on the trunk port. “Normal” mode is the default setting.
- **Forbidden**
The “forbidden” registration mode deregisters all VLANs (except VLAN 1) and prevents further creation or registration of VLANs on the trunk port.
- **Fixed**
The “fixed” registration mode allows manual creation and registration of VLANs, prevents VLAN deregistration and registers all known VLANs on other ports on the trunk port. (Same applies to the static VLAN)

GVRP Timer:

- **Join Timer**
The “Join Timer” specifies the maximum time in milliseconds that interface waits before sending VLAN messages.
- **Leave Timer**
The “Leave Timer” specifies the number maximum time in milliseconds an interface waits after receiving a “Leave Message” before the interface leaves the VLAN specified in the message.
- **Leaveall Timer**
The “Leaveall Timer” specifies the interval in milliseconds at which “Leaveall Messages” are sent on interfaces. “Leaveall Messages” help to maintain current GVRP VLAN subscriber information in the network.

7.2.3.3 Q-in-Q

“Q-in-Q Tunneling” is also known as “VLAN Stacking”. Both of them use 802.1Q double tagging technology. Q-in-Q is used by ISPs (Internet Service Providers) that need TLS (“**T**ransparent **L**AN **S**ervices”) and that have their own set of VLAN, independent of customer VLANs. Normally, each service provider VLAN interconnects a group of sites belonging to a customer. However, a service provider VLAN could also be shared by a set of customers sharing the same end points and QoS requirements of the VLAN. “Double Tagging” is considered to be a relatively simpler way of implementing a transparent LAN. This is accomplished by encapsulating “ETHERNET Frames”. A second or outer VLAN tag is inserted in “ETHERNET Frames” sent over the ingress PE (“**P**rovider **E**dge”). This VLAN tag corresponds to the VLAN of the service provider. If the frame reaches the destination PE, the service provider VLAN opens. The destination address of the encapsulated frame and VLAN ID are used for other L2 decisions, similar to an “ETHERNET Frame” that arrives from a physical ETHERNET port. The service provider VLAN tag determines the membership in the VPLS (“**V**irtual **P**riate **L**AN **S**ervice”). Double tagging aggregates multiple VLANs within another VLAN and allows a private dedicated ETHERNET connection between customers who want to reach their subnet transparently across multiple networks. Service providers can create their own VLANs without coming in contact with customer VLANs via “Double Tagging”. This allows customers to connect to ISPs and ASPs (“**A**pplication **S**ervice **P**roviders”).

The ports that are connected to the service provider VLANs are called “Tunnel Ports” and the ports that are connected to the customer VLANs are called “Access Ports”. If a port is configured as “Tunnel Port”, all outgoing packets on this port are transmitted with an SPVLAN tag (SPVID and 1p priority) tag. The incoming packet can have two tags (SPVLAN + CVLAN), one tag (SPVLAN or CVLAN), or no tag. In all cases, the packet is sent out with a SPVLAN tag. If a port is configured as an “Access Port”, the incoming traffic can have only a CVLAN tag (CVID and 1p priority) or no tag. Hence, all the packets that are being sent from “Access Ports” are untagged or single tagged (CVLAN). If a port is configured as a normal port, it ignores “Double Tagging Frames”.

Double Tagging Format

A VLAN tag (service provider “VLAN Stacking” or customer IEEE 802.1Q) consists of the following three fields:

TPID	Priority	VID

TPID

TPID (“Tag Protocol Identifier”) is a standard ETHERNET code identifying the frame and indicating whether the frame contains IEEE 802.1Q tag information. The value of this field is 0x8100 as described in IEEE 802.1Q. Other providers may use a different value, such as 0x9100.

“Tunnel TPID” is the “VLAN Stacking” tag type the switch adds to the outgoing frames sent through a “Tunnel Port” of the service provider's PE devices

Priority

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for. “0” is the lowest priority level and “7” is the highest.

VID

VID (“VLAN ID”). SP VID is the VID for the second or outer VLAN tag (of the service provider). CVID is the VID for the first or inner VLAN tag (of the customer).

The frame formats for an untagged “ETHERNET Frame” a single-tagged 802.1Q frame (customer) and a double-tagged 802.1Q frame (service provider) are shown as follows.

Untagged frame	DA		Len or Etype	Data	FCS						
Single-tagged frame	DA	SA	TPID	P	VID	Len or Etype	Data	FCS			
Double-tagged frame	DA	SA	Tunnel TPID	P	VID	TPID	P	VID	Len or Etype	Data	FCS
DA	Destination Address										
SA	Source Address										
Tunnel TPID	“Tag Protocol Identifier” added to a “Tunnel Port”										
VID	VLAN ID										
Len or Etype	Length or ETHERNET frame type										
Data	Frame data										
FCS	Frame Check Sequence										

VLAN Stacking Port Roles

For “VLAN Stacking”, each port can have one of three “roles”: Normal, “Access Port” or “Tunnel Port”.

- Select “normal” for normal (no “VLAN Stacking”) IEEE 802.1Q frame switching.
- Select “Access Port” for ingress ports on PE devices of the service provider. The incoming frame is treated as “untagged”, so a second VLAN tag (outer VLAN tag) can be added.
- Select “Tunnel Port” for egress ports in the PE range of the provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).



Note

Q-in-Q Configuration

For the double-tagged frames to switch correctly, users have to configure a service provider's VLAN (SPVLAN) on the Q-in-Q switch. Then, the double-tagged frames can be switched according to the SP VID. The SPVLAN should include all related “Tunnels” and “Access Ports”. In addition, the “Tunnel Ports” must be configured as tagged ports and the “Access Ports” as untagged ports.

7.2.3.3.1 Port-Based Q-in-Q

Q-in-Q encapsulation can be used to convert a single-tagged 802.1Q packet into a double-tagged Q-in-Q packet. The Q-in-Q encapsulation can be based on port or traffic. Port-based Q-in-Q can be used to encapsulate all incoming packets to a port with the same SPVID outer tag. This mode is less flexible.

In the following example figure, both X and Y are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 100 to distinguish customer X and tag 200 to distinguish customer Y at PE device A and then stripping those tags at PE device B as the data frames leave the network.

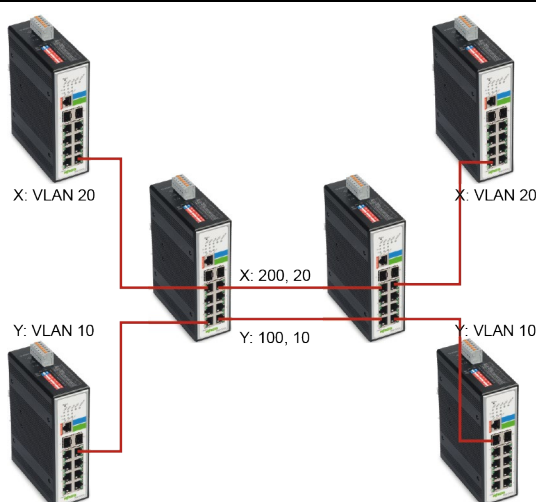


Figure 16: Port-Based Q-in-Q

This example shows how to configure switch A with port 1 on the switch to tag incoming frames with the service provider's VID of 200 (ports are connected to customer X network) and configure port 7 to the service provider's VID of 100 (ports are connected to customer Y network). This example also shows how to set the priority for port 1 to 3 and port 7 to 4.

7.2.3.3.2 Selective Q-in-Q

The traffic-based Q-in-Q is also called selective Q-in-Q. Selective Q-in-Q allows the switch to add different outer VLAN tags to the incoming frames received on one port according to their inner VLAN tags. In Selective Q-in-Q mode, the switch performs traffic classifies the incoming traffic on a port based on the VLAN ID. When a user uses different VLAN IDs for different services, traffic can be classified according to the VLAN ID. Example: VLAN ID 100 for surfing on the Internet on a PC, VLAN ID 200 for IPTV and VLAN ID 300 for VIP customers. After receiving user data, the switch labels the traffic for surfing on the Internet on a PC with 500 as a SPVID outer tag, IPTV with 600 and VIP customers with 700.

This following example shows how to configure port 3 on the switch to tag incoming frames with the different service provider's VID and priority.

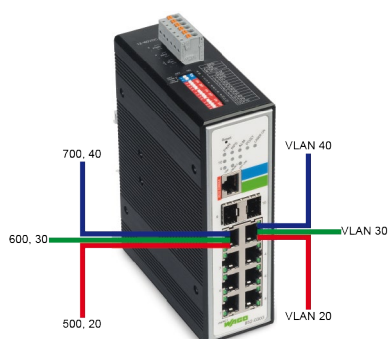


Figure 17: Configuration Example

7.2.4 DHCP Relay

Because the “DHCPDISCOVER” message is a broadcast message and broadcasts only cross other segments when they are explicitly routed, you might have to configure a “DHCP Relay Agent” on the router interface so that all “DHCPDISCOVER” messages can be forwarded to your DHCP server.

Alternatively, you can configure the router to forward DHCP messages and BOOTP message. In a routed network, you would need “DHCP Relay Agents” if you plan to implement only one DHCP server.

The “DHCP Relay” that is either a host or an IP router waits for DHCP client messages being broadcast on a subnet and then forwards those DHCP messages directly to a configured DHCP server. The DHCP server sends DHCP response messages directly back to the “DHCP Relay Agent”, which then forwards them to the DHCP client. The DHCP administrator uses “DHCP Relay Agents” to centralize DHCP servers, avoiding the need for a DHCP server on each subnet.

Most of the time in small networks, DHCP uses broadcasts, but there are some circumstances where unicast addresses are used. This can be the case when networks have a single DHCP server that provides IP addresses for multiple subnets. A router for such a subnet receives the DHCP broadcasts, converts them to unicast (with a MAC/IP destination address of the configured DHCP server, MAC/IP source address of the router itself). The GIADDR field on the main DHCP page contains the IP address of the interface on the router it received the DHCP request on. The DHCP server uses the GIADDR field to identify the subnet the device and selects an IP address from the correct pool. The DHCP server then sends the “DHCP OFFER” back to the router via unicast, which then converts it back to a broadcast and out to the correct subnet containing the device requesting an address.

Configurations

A user can enable/disable the “DHCP Relay” on the switch. It can also be enabled/disabled on a specific VLAN. If the “DHCP Relay” on the switch is disabled, it is disabled on all VLANs, even if enabled for individual VLANs.

Applications

- **Application 1 (via a router)**
DHCP client 1 and DHCP client 2 are in different IP segments. However, they receive IP address from the same DHCP server.

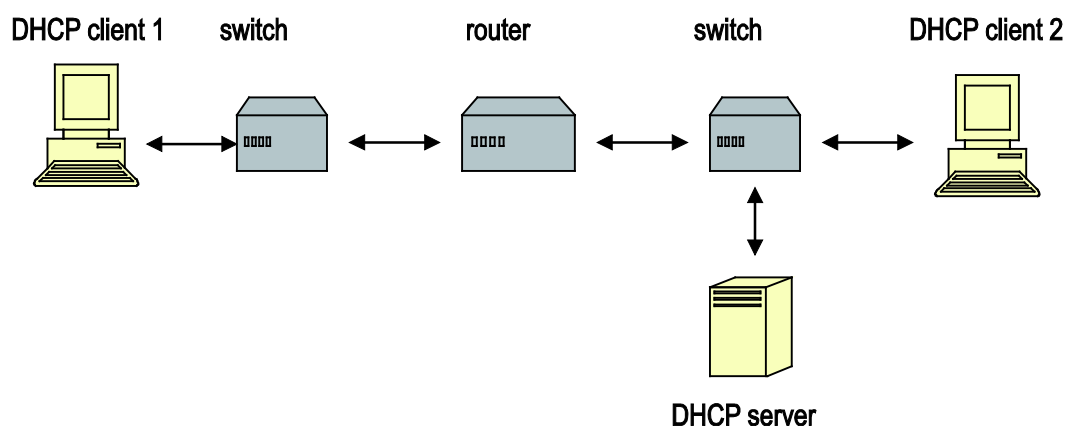


Figure 18: Application 1 (via a Router)

- **Application 2 (local in different VLANs)**
DHCP client 1 and DHCP client 2 are in different VLANs. However, they receive IP address from the same DHCP server.

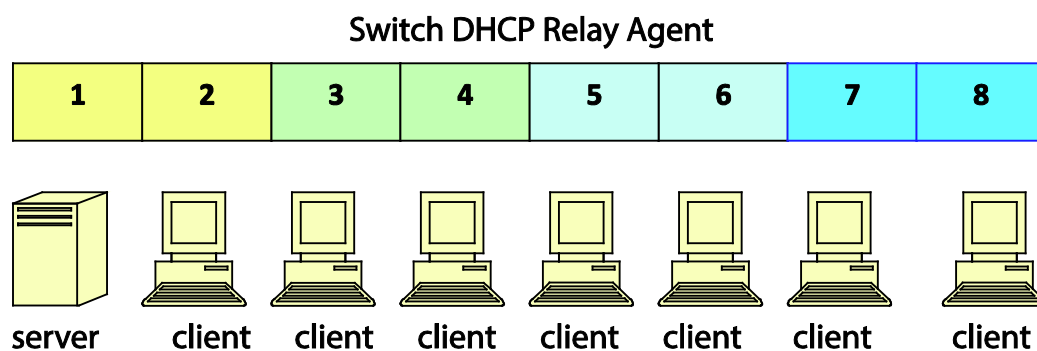


Figure 19: Application 2 (Local in Different VLANs)

VLAN 1: Port 1, 2 (Management VLAN)
 VLAN 2: Port 3, 4
 VLAN 3: Port 5, 6
 VLAN 4: Port 7, 8

DHCP Server -> Port 1.
 DHCP Client -> Port 2, 3, 4, 5, 6, 7, 8.

Result: Hosts connected to port 2, 3, 4, 5, 6, 7 and 8 receive an IP from the DHCP server.



Note

DHCP Server Connection

The DHCP server must be connected to the subscriber ports of the management VLAN.

The “DHCP Relay” in the management VLAN must be enabled.

7.2.5 DHCP Relay Option 82

“DHCP Option 82” (“**DHCP** Relay Agent Information **Option**”). Option 82 was designed to allow a “DHCP Relay Agent” to insert circuit-specific information into a request that is being forwarded to a DHCP server. Specifically, the option works by setting two sub-options: “Circuit ID” and “Remote ID”.

“DHCP Option 82” operates on the basis of “DHCP Snooping” or/and “DHCP Relay”.

The switch monitors the DHCP packets and append some information under “DHCPDISCOVER” and “DHCPREQUEST” packets. The switch deletes “DHCP Option 82” from the “DHCPOFFER” and “DHCPACK” packets. The DHCP server then assigns an IP domain to the client based on this information.

The maximum length of the information is 32 characters.

In residential, metropolitan ETHERNET-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. If the “DHCP Option 82” function is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the switch and are uniquely identified.

If you enable “DHCP Snooping Information Option 82” on the switch, the sequence of events is:

- The host (DHCP Client) generates a DHCP request and broadcasts it on the network.
- If the switch receives the DHCP request, it adds the “Option 82” information in the packet. The information contains the switch MAC address (the “Remote ID” sub-option), “Port Identifier” and “VLAN-Mod-PORT”, from which the packet is received (the “Circuit ID” sub-option).
- If the IP address of the “Relay Agent” has been configured, the switch adds the IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the Option 82 field to the DHCP server.
- The DHCP server receives the packet. If the server is Option 82 capable, it can use the “Remote ID”, “Circuit ID” or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single “Remote ID” or “Circuit ID”. The DHCP server then echoes the Option 82 field in the DHCP reply.
- The DHCP server forwards the reply to the switch as a unicast if the request was relayed to the server by the switch. If the client and server are on the same subnet, the server broadcasts the reply. The switch verifies the Option 82 data originally entered by checking the “Remote ID” and “Circuit ID” fields. The switch deletes the Option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

Option Frame Format

Table 21: Option Frame Format

Code	Len	Agent Information Field					
82	N	i1	i2	i3	i4	...	iN

The “Agent Information Field” consists of a sequence of SubOpt/Length/Value tuples for each sub-option, encoded in the following manner:

Table 22: Option Frame Format

Sub-Option	Len	Sub-Option Value					
1	N	s1	s2	s3	s4	...	sN

DHCP Agent Sub-Option Code	Sub-Option Description
-----	-----
1	“Agent Circuit ID” sub-option
2	“Agent Remote ID” sub-option

Table 23: Frame Format of the “Circuit ID” Sub-Option

Sub-Option Type	Length	“Circuit ID” Type	Length	VLAN	Module	Port
1	6	0	4	2	1	1

Table 24: Frame Format of the “Remote ID” Sub-Option

Sub-Option Type	Length	“Circuit ID” Type	Length	MAC address
2	8	0	6	6

Table 25: Format of the “Circuit ID” Sub-Option

Code	Len	Sub-Option Type	Length	Slot ID	Port ID	VLAN ID	Information
0x52	0x0c	0x01	0x0a	0x01	0x01	0x0002	justin

7.2.6 Dual Ring

The “Dual Ring” function can be used to connect 2 neighboring rings to each other on a switch without needing additional ports or cables. This configuration reduces the total number of required ports and wiring costs are saved because no additional wiring is required.

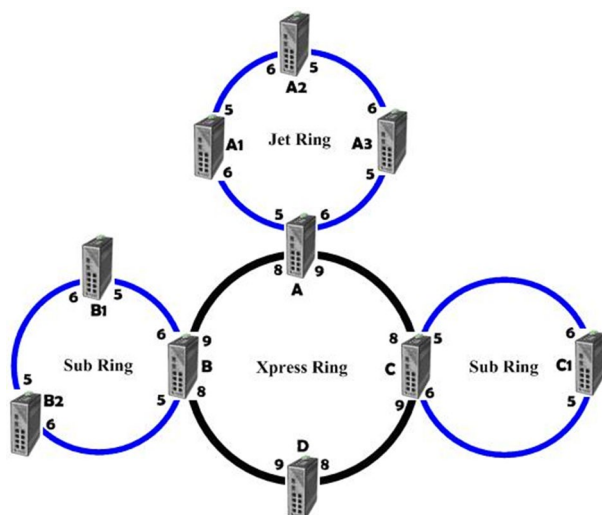


Figure 20: Dual Ring Switch ABC

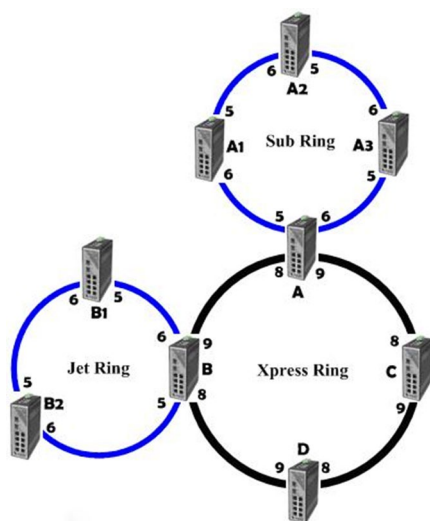


Figure 21: Dual Ring Switch AB

7.2.7 ERPS

The ERPS (**ETHERNET Ring Protection Switching**) function implements a protection switching mechanism for ETHERNET layer ring topologies according to ITU-T standard G.8032. The ERP (**ETHERNET Ring Protection**) protects ETHERNET traffic in a ring topology and ensures that no loops are within the ring in the ETHERNET later. 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 (**Ring Protection Link**). 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 conjoined ETHERNET rings by 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, each traffic channel and each R-APS channel is 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 sub-ring 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) 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.808.1]) for a failure on a ring link shall be less than 50 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 six rings.

Guard Timer

All ring subscribers use a “Guard Timer”. It prevents the possibility of forming a closed loop 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 (“**Switch Fail**”), MS (“**Manual Switch**”) or FS (“**Forced Switch**”) commands. When the timer expires, the ring subscriber begins executing actions it received from the R-APS. This timer cannot be manually stopped.

WTR Timer

The “WTR Timer” (“**Wait To Restore Timer**”) is used by the “RPL Owner”. The “WTR Timer” applies to the reset 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” (“**Wait To Block 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 be 5 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. Once 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 the control VLAN and its subscriber ports automatically. A subscriber port should have a right and left 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 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 or instance. If the control VLAN is configured for a ring and an instance should 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 then configure the instance.

7.2.8 Dual Homing

“Dual Homing” is a network topology in which a device is connected to the network by way of two independent access points (“Points of Attachment”). One access point establishes the primary connection, and the other is a reserve if the primary connection fails.

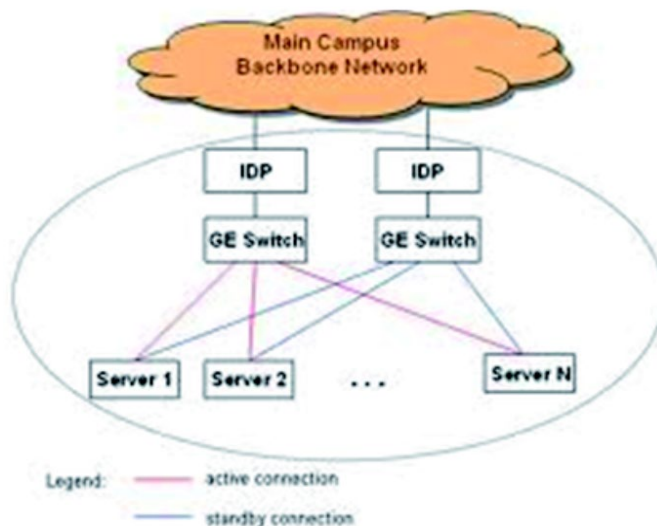


Figure 22: Dual Homing

Primary and secondary connections, for example, can be connected to the Internet in different ways. The primary connection could be connected to a physical network and the secondary to a wireless network. If the “Dual Homing” function is enabled, a device connects via the primary connection by default, while the secondary connection remains suspended. If the port or all ports of the primary connection fail, the device switches to the secondary connection. If the secondary connection also fails, the device remains inactive. The secondary connection only works if the primary connection is interrupted.

7.2.9 Link Aggregation

7.2.9.1 Static Trunk

“Link Aggregation” (also called “Trunking”), parallel link bundling) is the grouping of physical ports into one logical link with higher capacity. When bundling ports, it can be more cost effective to use multiple lower-speed links than to underutilize a high-speed, but expensive “Port Link”.

However, the more ports you aggregate, the fewer available ports you have. A “Trunk Group” is one logical link containing multiple ports. The switch supports both static and dynamic “Link Aggregation”.



Note

“Link Aggregation”

In a well-planned network, only static “Link Aggregation” is recommended. This ensures increased network stability and control over “Trunk Groups” on your switch.

7.2.9.2 LACP

The switch supports static and dynamic (LACP) “Port Trunking” according to IEEE 802.3ad. The IEEE 802.3ad standard describes LACP (“**L**ink **A**ggregation **C**ontrol **P**rotocol”) for dynamic creation and management of “Trunk Groups”.

When you enable “LACP Link Aggregation” on a port, the port can automatically negotiate with the ports at the remote end of a link to establish “Trunk Groups”. LACP also allows port redundancy, i.e., if an operational port fails, then one of the “standby” ports becomes operational without user intervention

The following should be noted:

- All ports must be connected peer-to-peer to the same ETHERNET switch and configured for “LACP Trunking”.
- LACP only works on full-duplex links.
- All ports in the same “Trunk Group” must have the same media type, speed, duplex mode and settings for “Flow Control”.
- Configure the “Trunk Groups” or LACPs before you connect to the ETHERNET switch to prevent looping in the network topology.

System Priority

LACP system priority is used to determine membership in an LAG (“Link Aggregation Group”) and identifies the device for other switches during LAG negotiations.

The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “Server”. The server controls the operation of the LACP settings. The smaller the number, the higher the priority level.

System ID

The “LACP System ID” is a combination of the LACP system priority value and the MAC address of the router.

Administrative Key

The “Administrative Key” defines the ability of a port to aggregate with other ports. This ability is determined by the following factors:

- The physical properties of the port, e.g., data rate, duplex capability and peer-to-peer or shared transmission medium.
- The configuration restrictions that you establish.

Port Priority

Port priority determines which ports should go into standby mode if there is a hardware limitation that prevents all compatible ports from bundling.

7.2.10 LLDP

The LLDP (“Link Layer Discovery Protocol”) described in this standard allows stations connected to a LAN acc. 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.

The information distributed via this protocol is stored by the recipients in a normal MIB (“Management Information Base”). That allows an NMS (“Network Management System”) to access the information using a management protocol such as SNMP (“Simple Network Management Protocol”).

7.2.11 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 Storm”.

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

Loop Recovery

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

7.2.12 Jet Ring

Setting up the Jet Ring function (redundant connection) in a network better protects critical connections against errors and network loops. In addition, network downtime is reduced to less than 300 ms.

The Jet Ring function can be used to set up a secondary path to the network. A data transmission safety route is then provided in case there is an abrupt interruption in a connection. This function is extremely important for industrial applications because connection errors without safeguards for network downtime can last several minutes and result in heavy losses.

The Jet Ring protocol is used to optimize secondary communication links and to ensure very short connection recovery time. The Jet Ring function is used to automatically identify a switch as the network “Master” and to automatically block connections. This prevents packets from being broadcast to all secondary loop segments of a network. If a ring segment is separated from the rest of the network due to a connection error, the Jet Ring protocol automatically adjust the ring again to restore the connection between the part of the network that was separated with the rest of the network.

Step 1

The Jet Ring function in the graphic below is applicable to connecting industrial managed switches.

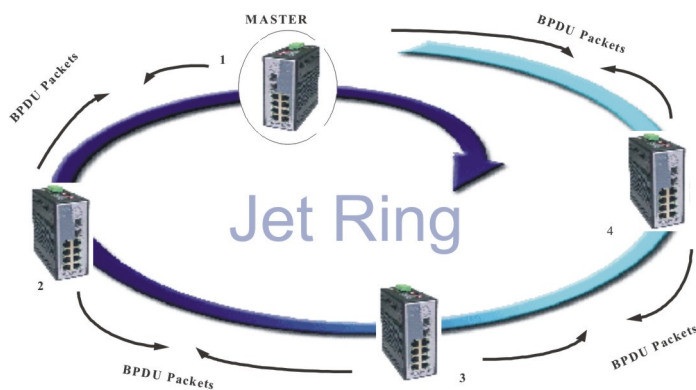


Figure 23: Jet Ring

Step 2

The Jet Ring function is used to automatically select the Arbiter switch. The network then ready for operation.

7.2.13 STP

The (R)STP (“(Rapid) Spanning Tree Protocol”) 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 that allows faster convergence of the “Spanning Tree” than STP (the switch is also backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, there are longer delays because the device that causes a topology change first notifies the “Root Bridge” and then the network. Both RSTP and STP remove unwanted learned addresses from the filtering database.

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

STP Switch Port States

- **“Blocking”**
If a port 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 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” 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 SSTP if a network loop is detected.

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

Table 26: STP Path Costs

Transmission Speed	Recommended Value	Recommended Range	Permissible Range
4 Mbps	250	100 ... 1000	1 ... 65535
10 Mbps	100	50 ... 600	1 ... 65535
16 Mbps	62	40 ... 400	1 ... 65535
100 Mbps	19	10 ... 60	1 ... 65535
1 Gbps	4	3 ... 10	1 ... 65535
10 Gbps	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 (BPDU “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 devices waits before changing states (e.g., from “Listening” to “Learning” to “Forwarding”). The valid range is from 4 to 30 seconds.

Transmission Limit

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

Bridge Priority

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

BPDU Guard

This setting is configured individual 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 manually enable the port.

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 of the “BPDU Filter” and “BPDU Guard” are enabled, the “BPDU Filter” has the higher priority.



Note

BPDU Filter and BPDU Guard

If both of the “BPDU Filter” and “BPDU Guard” are enabled, the “BPDU Filter” has the higher priority.

Root Guard

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

MSTP

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

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

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

The root bridge sends Bridge Protocol Data Units (BPDU) to all bridges and determines the network configuration from the configuration data contained in the BPDU data packets.

7.2.14 Xpress Ring

The Xpress Ring is a fast-acting, self-healing ring recovery technology that enables networks to recover from link failure within 50 ms.

Fast Link Recovery and Ring Redundancy are important functions for increasing the reliability of non-stop systems.

A well-planned network with an Arbiter switch and ring ports can recover from segment failure within a very short time.

A switch in the Xpress Ring has only two roles: either “Forwarder” or “Arbiter”. There can be only one Arbiter switch while all other switches are “Forwarders”.

One of the ring ports of an Arbiter switch is set to the blocking state. If one of the ring connections fails, the blocked port is set to the forwarding state.

7.3 Security

7.3.1 IP Source Guard

“IP Source Guard” is a security function that restricts IP traffic on untrusted Layer2 ports by filtering traffic based on a “DHCP Snooping” database connection or a manually configured IP source connection. This function helps prevent access such as “IP Snooping” (sending IP packets with a spoofed sender IP address) if a host attempts to spoof the IP address of another host. Any IP traffic coming into the interface with a source IP address other than that assigned (via DHCP or static configuration) is filtered out on untrusted Layer2 ports.

This function is used on untrusted Layer2 interfaces in combination with “DHCP Snooping”. An IP source binding table is manually configured (static IP source binding) or created from information from the “DHCP Snooping” function and used. Each entry in this table contains the IP address and associated MAC and VLAN addresses. The “IP Source Guard” only supports Layer2 ports, including “Access Ports” and “Trunk Ports”.

The “IP Source Guard” includes the following functions:

1. DHCP Snooping
2. DHCP Binding Table
3. ARP Inspection
4. Blacklist Filter (ARP inspection with MAC address filter table)

7.3.1.1 DHCP Snooping

“DHCP Snooping” is a DHCP security function that increases network security by filtering untrusted DHCP messages and creating and using a “DHCP Snooping” database connection (also called “DHCP Snooping” binding table).

“DHCP Snooping” acts like a firewall between untrusted hosts and DHCP servers. It can be used to differentiate between untrusted interfaces connected to end users and trusted interfaces connected to a DHCP server or another switch.

The “DHCP Snooping” binding table contains the MAC address, IP address, “Lease Time”, mount type, VLAN number and information on the local untrusted interfaces of a switch.

If a switch receives a packet from an untrusted interface and the interface belongs to a VLAN in which “DHCP Snooping” is enabled, the switch compares the MAC source address to the hardware address of the DHCP client. If the addresses match (as is normal), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of the following situations occur:

- A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from the untrusted port.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match any of the current bindings.

“DHCP Snooping” can be used to filter unauthorized DHCP packets on the network and to dynamically create a binding table. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

Trusted vs. Untrusted Ports

Every port is either a “Trusted Port” or an “Untrusted Port” for “DHCP Snooping”. This setting is independent of the “Trusted/Untrusted” setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (“trusted” or “untrusted”) can receive each second.

“Trusted Ports” are connected to DHCP servers or switches. The switch only drops DHCP packets from “Trusted Ports” if the transmission rate of the DHCP packets received is too high. The switch learns the dynamic bindings from the “Trusted Ports”.

Note



DHCP Requests

The switch drops all DHCP requests if “DHCP Snooping” is enabled, but there are no “Trusted Ports”.

“Untrusted Ports” are connected to subscribers. The switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (e.g., “OFFER”, “ACK” or “NACK”).
- The source MAC address and source IP address in a packet do not match any of the current bindings.
- The source MAC address and source port in a “RELEASE” or “DECLINE” packet do not match any of the current bindings.
- The transmission rate of the DHCP packets received are too high.

DHCP Snooping Database

The switch stores the binding table in volatile memory. If the switch restarts, it loads the static bindings from non-volatile memory, but loses the dynamic bindings, so that the devices in the network have to send DHCP requests again.

Configuring DHCP Snooping

Follow the steps below to configure “DHCP Snooping” on the switch:

1. Enable “DHCP Snooping” on the switch.
2. Enable “DHCP Snooping” for each VLAN.
3. Configure “Trusted Ports” and “Untrusted Ports”.
4. Configure the static bindings.

Note



DHCP Snooping

The switch drops all DHCP requests if “DHCP Snooping” is enabled, but there are no “Trusted Ports”.

If the port link fails, the entries from this port are deleted from the “DHCP Snooping” binding table.

You must first enable global “DHCP Snooping” and “DHCP Snooping” for VLANs.

The main purposes of the “DHCP Snooping” are:

- 1 To create and maintain a binding table for the ARP Inspection function.
- 2 To filter packets from DHCP servers that are connected to an “Untrusted Port”.

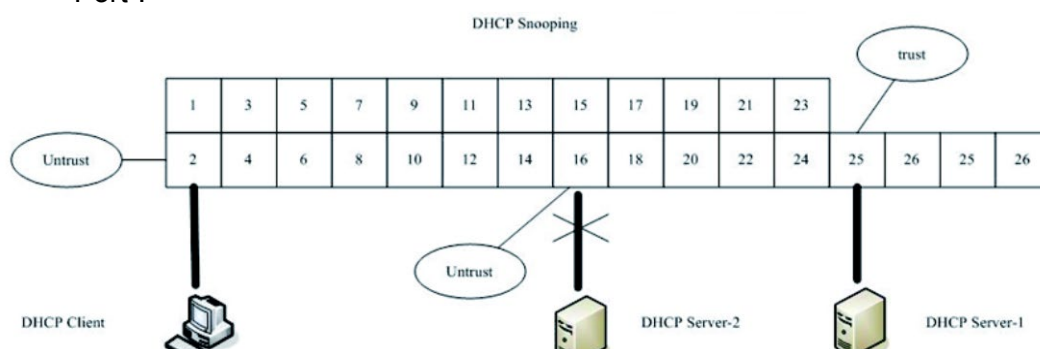


Figure 24: DHCP Snooping

The packets from DHCP servers connected to an “Untrusted Port” are filtered.

7.3.1.1.1 Server Screening

The switch supports “Server Screening”, a function that denies access to “Rogue DHCP Servers” (unauthorized, invalid DHCP servers). That is, when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients, the valid DHCP server’s packets are passed to the client.

If this function is enabled, the “DHCP Snooping” function must also be enabled beforehand. The switch allows users to configure up to three valid DHCP servers.

If no DHCP servers are configured, it means all DHCP server are valid.

7.3.1.2 Binding Table

The “DHCP Snooping” binding table records the host information learned from “DHCP Snooping” (dynamic) or set by user (static). The ARP inspection uses this table to decide if to forward or drop ARP packets. ARP packets sent from by invalid hosts are dropped. Once the “Lease Time” expires, the entry is deleted from the table.

Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you create a static binding with the MAC address and VLAN ID of an existing binding, the new static binding replaces the original on.

Bindings are used by “DHCP Snooping” and ARP inspection to distinguish between authorized and unauthorized packets in the network. The switch detects the dynamic bindings by “snooping” DHCP packets and from static information from the manual entries in the “Static Entry Settings” menu.

7.3.1.3 ARP Inspection

The dynamic “ARP Inspection” (“**A**ddress **R**esolution **P**rotocol **I**nspection”) is a security function in which ARP packets are inspected in a network. Dynamic ARP inspections validates the packet by performing IP-to-MAC address binding inspection stored in a trusted database (the “DHCP Snooping” database) before forwarding the packet. Dynamic ARP intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This function protects the network from certain “Man-in-the-Middle” attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed.

The switch executes the following processes:

- Interception of all ARP requests and responses on untrusted ports.
- Inspection of all intercepted packets for valid IP-to-MAC address binding before updating the local ARP cache or forwarding a packet to the respective destination.

Trusted Port and Untrusted Port

- This setting is independent of the “Trusted/Untrusted” setting for “DHCP Snooping”.
- The switch does not drop ARP packets from “Trusted Ports” for any reason.
- The switch drops ARP packets from “Untrusted Ports” if the information from the sender in the ARP packets does not match any current bindings.
- Normally, the “Trusted Ports” are the “Uplink Ports” and the “Untrusted Ports” are connected to subscribers.

Configurations

Users can enable/disable the ARP Inspection on the switch. It can also be enabled/disabled on a specific VLAN. If ARP Inspection is disabled on the switch, ARP Inspection is disabled on all VLANs, even if enabled for individual VLAN.



Note

Global State/VLAN State

There is a global state and individual VLAN states.

If the global state is disabled, ARP Inspection is disabled on the switch, even if individual VLAN states are enabled.

If the global state for ARP Inspection is enabled, this function must be enabled by the user for specific VLANs.

7.3.1.3.1 Filter Table

Dynamic ARP inspections validates the packet by performing IP-to-MAC address binding inspection stored in a trusted database (the “DHCP Snooping” database) before forwarding the packet. If the switch detects an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and the source VLAN ID of the packet. In addition, the switch regularly deletes entries whose “Age Time” has expired.

- If ARP Inspection is enabled and the system detects invalid hosts, the system creates a filtered entry in the MAC address table.
- If a port link fails and ARP Inspection is disabled, the switch deletes the MAC filter entries for this port.
- If a port link fails and ARP Inspection is enabled, the switch deletes the MAC filter entries for this port.
- The maximum number of entries in the MAC address filter table is 256.
- If the MAC address filter table for ARP inspection is full and the switch receives an unauthorized ARP packet, it automatically creates a “SYSLOG” and the ARP packet is dropped. The SYSLOG is created only once.

7.3.2 Access Control List (ACL)

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

The ACL function allows users to configure some rules to reject packets received from specific ingress ports or all ports. These rules check the source and destination MAC addresses of packets. If packets match these rules, the system does not deny the action, i.e., the packets are not rejected.

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

7.3.3 802.1x

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 to 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")

802.1X provides port-based authentication, which involves communications between a 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 an authentication server is generally a RADIUS ("**R**emote **A**uthentication **D**ial-In **U**ser **S**ervice") database.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity is authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as 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 at the network layer (Layer 3). The authenticator sends out the EAP identify request to the supplicant, the supplicant responds with the EAP response packet that 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-In **U**ser **S**ervice”) is a client-server-based security protocol for authentication and to control 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, access rights and account data, and consists of an accounting and authentication protocol.

In combination with DHCP and PPP, configuration of dial-in system can be automatic with RADIUS.

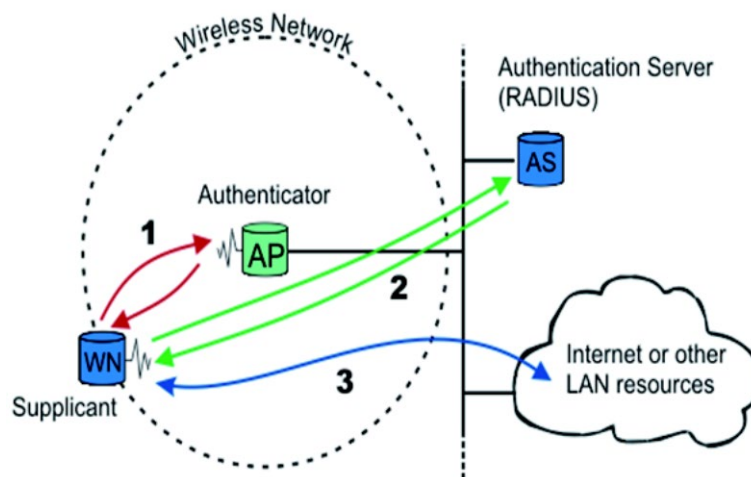


Figure 25: 802.1x

The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a 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 validates whether this client is allowed access to the port.

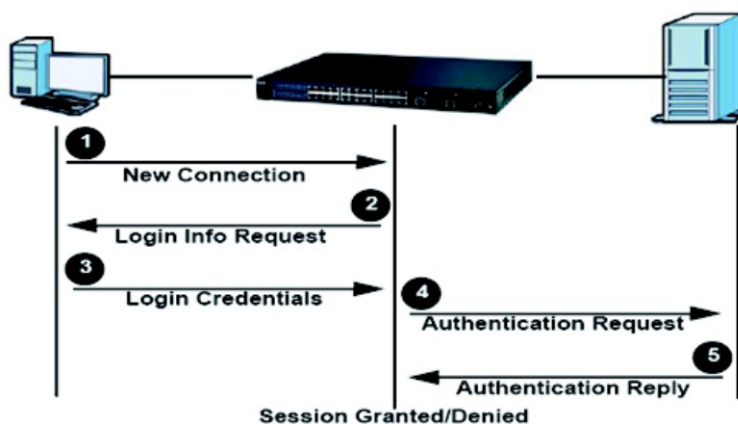


Figure 26: RADIUS Server

Local User Accounts

By storing user profiles locally on the switch, it can authenticate users without interacting with the network authentication server. However, there is a limit of 6 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 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 if 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 acceptable range for this field is 0 to 65535 seconds.
- **Port Control Mode**

"Auto"	Users can access the network after authenticating.
"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 acceptable 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 the server is down. The acceptable range for this field is 1 to 10 attempts.

7.3.4 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 the number is exceeded, incoming packets with new MAC addresses are dropped. A MAC address table can be used to check that number. The static MAC addresses are included for the 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.

7.4 Monitor

7.4.1 Alarm Information

This function alerts the network administrator to any abnormal network situations.



Note

Alarm DIP Switches

The alarm DIP switches allow users to configure if an alarm message should be sent when a corresponding event occurs.

Example

P1:	ON (AN)	– The switch sends an alarm message if the connection on Port 1 fails.
PWR:	ON	– The switch sends an alarm message if the primary power supply is interrupted.
RPS:	ON	– The switch sends an alarm message if the redundant power supply is interrupted.

7.4.2 Monitor Information

This function displays some hardware information to monitor the system and to guarantee proper network operation.

7.4.3 RMON Statistics

This function is used to monitor or delete RMON statistics.

Jabber

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

7.4.4 SFP

SFP (“**S**mall **F**orm-factor **P**luggable”) are small standardized modules for network connections.

SFP refers to a modular interface to support various transmission media and is used in network technology for interface flexibility.

7.4.4.1 DDM

DDM (“**D**ynamic **D**evice **M**apping”) is a technology for KVM switches with USB ports that are sometimes used as an alternative to standard USB keyboard and mouse emulation.

7.4.5 Traffic Monitor

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

7.5 Management

7.5.1 SNMP

The SNMP (“**S**imple **N**etwork **M**anagement **P**rotocol”) is used in network management systems to monitor the state of attached devices that require the attention of an administrator. SNMP is a component of the “Internet Protocol Suite” defined by the IETF (“**I**nternet **E**ngineering **T**ask **F**orce”). It consists of a set of standards for network management, including an application layer protocol, a database schema and a set of data objects.

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

Support for MIBs

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

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

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

Network ID of “Trusted Host”:

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

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

Note



Community String

It should allow users to configure the “Community String” and rights only.

A user configures the “Community String” and rights and the network ID of the “Trusted Host” = 0.0.0.0, subnet mask = 0.0.0.0, i.e., all hosts with this “Community String” can access the switch.

7.5.2 SNMP Trap

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

7.5.3 Auto Provision

The “Auto Provision” is a service that service providers can use to quickly, easily and automatically configure remote devices or update firmware from a remote location.

1. If the function is enabled, the switch first downloads an information file from the server of the service provider.

The file name is formed according to the following naming convention:

Model_Name_Autoprovision.txt

Example: MEN-5210_Autoprovision.txt

The contents of the file are:

```
AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version=5228-000-1.0.0.b1
Firmware_Image_File=5228-000-1.0.0.b1.fw
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File=5228-000-1.0.0.b1.save
Global_Configuration_Reboot=0
Specific_Configuration_State=0
Specific_Configuration_Reboot=0
```

2. If the “AUTO_PROVISION_VER” value is higher than the current version of the “Auto Provision”, continue to Step 3. If not, please wait 24 hours and start again with Step 1.
3. If “Firmware_Upgrade_State =1”, continue to Step 4. If not, continue to Step 6.
4. If the “Firmware_Version” differs from the current firmware version, please download the “Firmware_Image_File” and update the firmware.
5. If the firmware is updated successfully and “Firmware_Reboot=1”, “reboot_flag=1” is executed.
6. If “Global_Configuration_State =1”, please download the “Global_Configuration_File” and update the configuration. If not, continue to Step 8.
7. If the configuration is updated successfully and “Global_Configuration_Reboot =1”, “reboot_flag=1” is executed.

-
8. If "Global_Configuration_State =1", please download the specific configuration file and update the configuration. If not, continue to Step 10. The name is: "Model_Name _" with 12-bit MAC digits, e.g., "MEN-5210_00e04c8196b9.txt".
 9. If the configuration is updated successfully and "Specific_Configuration_Reboot =1", "reboot_flag=1" is executed.
 10. If "reboot_flag=1", save the executed configuration and reboot the switch. If not, please wait 24 hours and start again at Step 1.

7.5.4 Mail Alarm

The “Mail Alarm” function sends an e-mail trap to a previously defined administrator when certain events occur. The events are listed below:

System Reboot: start.	The system performs a warm or cold start.
Port Link Change:	A port connection is established or fails.
Configuration Change:	The system configurations in the NV-RAM have been updated.
Firmware Upgrade:	The system firmware has been updated.
User Login:	A user has logged into the system.
Port Blocked:	A port is blocked by “Loop Detection” or “BPDU Guard”.

8 Configuration

8.1 Overview of Configuration Options

The industrial managed switch provides two options for advanced management features:

Telnet/SSH Port

A menu-driven user interface can be called up from the WBM (“**Web Based Management**”) via the Telnet port.

Note



Additional Information

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

Console Port

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

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

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

Note



Additional Information

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

8.2 Telnet Port

1. Connect the computer to one of the ETHERNET ports.
2. Open a Telnet session to the switch's IP address. If this is your first login, use the default values.

Table 27: Default Settings for the Telnet Port

Setting	Default Value	
	FW Version 01	FW Version 02 or higher
IP Address	192.168.1.254	
Subnet Mask	255.255.255.0	
Default Gateway	0.0.0.0	
Management VLAN	1	
Default Username	admin	admin
Default Password	Wago1951	wago

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

8.2.1 Console Port

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

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

1. Connect the computer to the console port on the switch using the appropriate cable.
2. Use Telnet with the following settings:

Table 28: Default Settings for the Console Port

Setting	Default Value
Baud Rate	38400
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

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

Table 29: Login Screen

Setting	Default Value	
	FW Version 01	FW Version 02 or higher
Default Username	admin	admin
Default Password	Wago1951	wago



Note

Requirement to establish the connection

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

Please refer to the section “Appendix” > ... > “RJ-45 Cable” for details on the cable terminal assignment.

9 Configuring in the Web-Based Management System

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 System (WBM).

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 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., Microsoft Internet Explorer or Mozilla Firefox).
2. Enter the IP address of the fieldbus coupler/controller.
3. Click **[Enter]** to confirm.
4. Enter your user name and password in the query dialog:
Firmware version 01: User = "admin", password = "Wago1951"
Firmware version 02: User = "admin", password = "wago"
5. The start page of WBM loads.
6. Make the wanted settings.
7. Press **[Apply]** or **[Update]** or press **[Delete]** or **[Discard]** to discard your changes.
8. To apply the settings, press the **[Save configuration]** button to confirm your changes.

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

Table 30: Overview - Navigation Links and WBM Pages

Navigation Links and WBM Pages	
▶ [System Status]	
• System Information	
▶ [Basic Settings]	
• General Settings • MAC Management • Port Mirroring • Port Settings	
▶ [Advanced Settings]	
▶ [Bandwidth Control]	• QoS • Rate Limitation
▶ [IGMP Snooping] ▶	• IGMP Snooping • IGMP Filtering • MVR • Multicast Addr. • Multicast IP Statistics
▶ [VLAN] ▶	• Port Isolation • VLAN • GVRP • MAC VLAN • Protocol VLAN • Q-in-Q
	• DHCP Relay • DHCP Options • Dual Homing • Dual Ring • ERPS • Link Aggregation • LLDP • Loop Detection • Jet Ring • Modbus • STP • Xpress Ring

▶ [Security]
[IP Source Guard] ▶ • DHCP Snooping • Binding Table • ARP Inspection • Access Control List • 802.1x • Port Security
▶ [Monitor]
• Alarm • Monitor Information • Port Statistics • Port Utilization • RMON Statistics • SFP Information • Traffic Monitor
▶ [Management]
[SNMP] ▶ • SNMP • SNMP Trap • Auto Provision • Mail Alarm • Maintenance • System Log • User Account

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

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

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

9.1 System Status

9.1.1 System Information

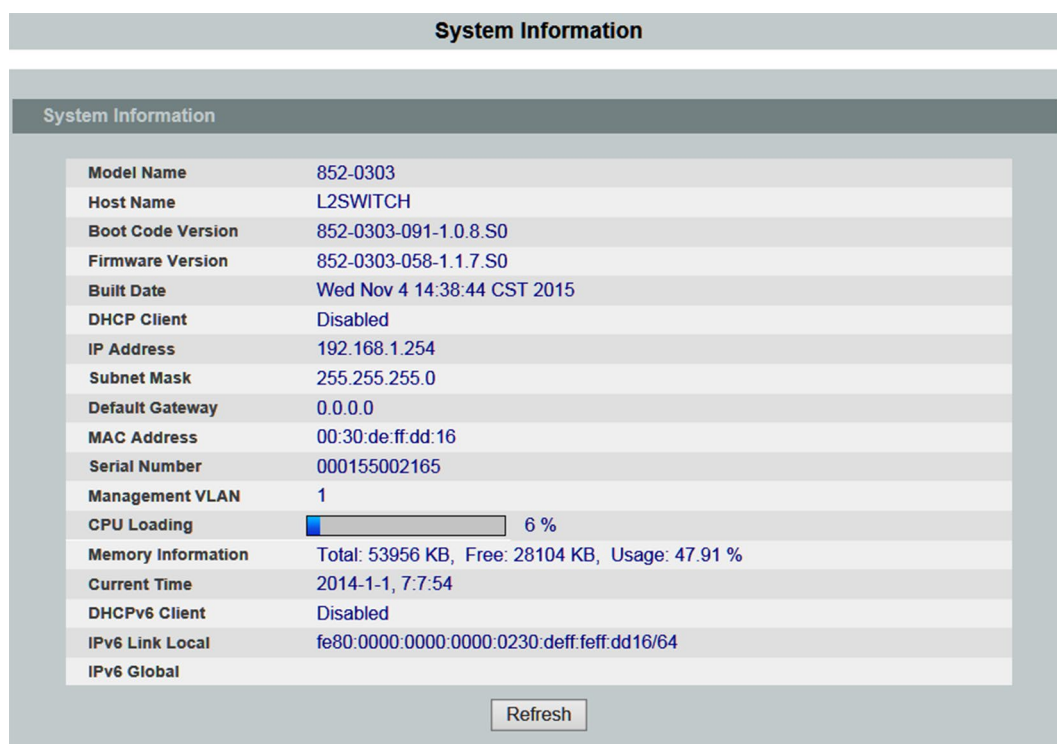


Figure 27: WBM "System Information" Page

Table 31: WBM "System Information" Page

Parameters	Description
Model Name	This display field shows the model name of the switch.
Host Name	This display field shows the host name of the switch.
Boot Code Version	This display field shows the boot code version.
Firmware Version	This display field shows the version number of the firmware currently installed.
Built Date	This display field shows the create date of the firmware currently installed.
DHCP Client	This display field shows if the DHCP client function is enabled.
IP Address	This display field shows the IP address of the switch.
Subnet mask	This display field shows the subnet mask of the switch.
Default Gateway	This display field shows the default gateway of the switch.
MAC Address	This display field shows the MAC (Media Access Control) address of the switch.
Serial Number	This display field shows the serial number.
Management VLAN	This display field shows the VLAN ID required for the switch management process.
CPU Loading	This display field shows the percentage system load of the switch.
Memory Informationen	This display field shows the switch's total (Total) memory, available memory ("Free") and used memory ("Usage").
Current Time	This display field shows the current date (yyyy-mm-dd) and current time (hh:mm:ss).
DHCPv6 Client	This display field shows if the DHCPv6 client is ON or OFF.
IPv6 Link Local	This display field shows the IPv6 Link-local address.
IPv6 Default Gateway	This display field shows if the global IPv6 Link address has also been entered.
IPv6 Global	This display field shows if the global IPv6 Link address.
Refresh	Click this button to update the information on this page.

9.2 Basic Settings

9.2.1 General Settings

9.2.1.1 System

The screenshot displays the 'General Settings' page in the WBM interface, specifically the 'System' tab. The page is organized into several sections:

- System Settings:** Contains fields for 'Hostname' (set to 'L2SWITCH') and 'Management VLAN' (set to '1').
- IPv4 Settings:** Includes a 'DHCP Client' dropdown set to 'Disable' with a 'Refresh' button, and text input fields for 'IP Address' (192.168.1.254), 'Subnet Mask' (255.255.255.0), and 'Default Gateway' (0.0.0.0).
- IPv6 Settings:** Includes a 'DHCPv6 Client' dropdown set to 'Disable' with a 'Refresh' button, an 'IPv6 Global Address' field, and a 'Default Gateway' dropdown set to 'Set' with an adjacent text input field.

At the bottom of the form, there are three buttons: 'Apply', 'Refresh', and 'Save Configurations'.

Figure 28: WBM Page, “General Settings” – “System” Tab

Table 32: WBM Page, "General Settings" – "System" Tab

Table 62: VDMN Page, General Settings, System Tab

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

9.2.1.2 Jumbo Frame



Note

Additional Information

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

General Settings

System
Jumbo Frame
SNTP
Management Host

Jumbo Frame Settings

Port	Frame Size
From: 1 To: 1	10240
Apply Refresh Save Configurations	

Port	Jumbo Frame	Port	Jumbo Frame
1	10240	2	10240
3	10240	4	10240
5	10240	6	10240
7	10240	8	10240
9	10240	10	10240
11	10240	12	10240

Figure 29: WBM Page, “General” – “Jumbo Frame” Tab

Table 33: WBM Page, “General” – “Jumbo Frame” Tab

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

9.2.1.3 SNTP

Note



Additional Information

Please refer to the section “Function Description” for more information on “SNTP” (Simple Network Time Protocol).

General Settings

System
Jumbo Frame
SNTP
Management Host

Current Time and Date

Current Time

10:43:02 (UTC)

Current Date

2019-05-13

Time and Date Settings

☒ **Manual**

New Time

2019

5

13

/

10

:

43

:

2

(yyyy.mm.dd / hh:mm:ss)

☐ **Enable Network Time Protocol**

NTP Server

☐ ntp0.fau.de - Europe
 ☒ IP

0.0.0.0

Time Zone

+0000

(+hh / -hh / +hhmm / -hhmm)

Daylight Saving Settings

State

Disable

Start Date

First

Sunday

of

January

at

0

o'clock

End Date

First

Sunday

of

January

at

0

o'clock

Apply

Refresh

Save Configurations

Figure 30: WBM Page, “General” – “SNTP” Tab

Table 34: WBM Page, “General” – “SNTP” Tab

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

Table 34: WBM Page, "General" – "SNTP" Tab

Daylight Saving Settings		
Parameters	Default	Description
State	Disable	Select "Disable" if you do not want to use daylight savings time.
	Enable	Select "Enable" if you want to use daylight savings time.
Start Date ¹⁾		Enter the date and time for the start of daylight savings if you have enabled this option. The time is displayed in 24-hour format.
End Date ²⁾		Enter the date and time for the end of daylight savings if you have enabled this option. The time is displayed in 24-hour format.
¹⁾	Daylight savings starts on the second Sunday of March in most places in the USA. Daylight savings starts at 2 A.M local time in each time zone in the USA. Correspondingly, you would select "Second, Sunday, March" and "2:00". In the EU, daylight savings starts on the last Sunday in March. It starts at the same time (1:00 A.M GMT or UTC) in all EU time zones. Correspondingly, you would select "Last, Sunday, March") and in the last field, enter the time based on your time zone. In Germany, for instance, you would select "2:00" because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).	
²⁾	In the USA, daylight savings ends on the last Sunday in October. It ends at 2:00 A.M. local time in each time zone in the USA. Correspondingly, you would select "First, Sunday, November" and "2:00". In the EU, daylight savings ends on the last Sunday in October. Daylight savings ends at the same time (1:00 AM GMT or UTC) in all EU times zones. Correspondingly, you would select "Last, Sunday, October") and in the last field, enter the time based on your time zone. In Germany, for instance, you would select "2:00" because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).	

9.2.1.4 Management Host



Note

Additional Information

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

Figure 31: WBM Page, “General” – “Management Host” Tab

Table 35: WBM Page, “General” – “Management Host” Tab

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

9.2.2 MAC Management

Note



Additional Information

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

9.2.2.1 Static MAC Settings

Note



Additional Information

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

MAC Management

Static MAC Settings
MAC Table
Age Time Setting
Blacklisting

Static MAC Settings

MAC Address	VLAN ID	Port
		1 ▾

Static MAC Table

MAC Address	VLAN ID	Port	Action
00:30:de:ff:f1:9b	1	CPU	

Total counts : 1

Figure 32: WBM Page, “MAC Management” – “Static MAC Settings” Tab

Table 36: WBM Page, “MAC Management” – “Static MAC Settings” Tab

Static MAC Settings		
Parameters	Default	Description
MAC Address		In this input field, enter the MAC address of a computer or device that you want to add to the MAC address table. The valid format is: hh:hh:hh:hh:hh:hh.
VLAN ID		In this input field, enter the VLAN ID to apply to the computer or device.
Port	1	In this selection box, select the port number to which the computer or device is connected.
Static MAC Table		
Parameters	Default	Description
MAC Address		This column displays the manually entered MAC address entries.
VLAN ID		This column displays the VLAN ID of the manually entered MAC address entries.
Port	1 ... 10 (12)	This column displays the port numbers of the manually entered MAC address entries. The MAC address “CPU” is the MAC address of the switch.
Action		Click [Delete] to delete the manually entered MAC address from the MAC address table. You cannot delete the MAC address of the switch from the static MAC address table.
Total counts		This display field displays the total number of entries in the static MAC address table.

9.2.2.2 MAC Table

MAC Management

Static MAC Settings **MAC Table** Age Time Setting Blacklisting

MAC Table

Show Type:

MAC Address	Type	VLAN ID	Port/Trunk ID
00:10:18:af:b7:d4	Dynamic	1	8
00:30:de:ff:f1:8c	Dynamic	1	11
00:30:de:ff:f1:9b	Static	1	CPU

Total counts : 3

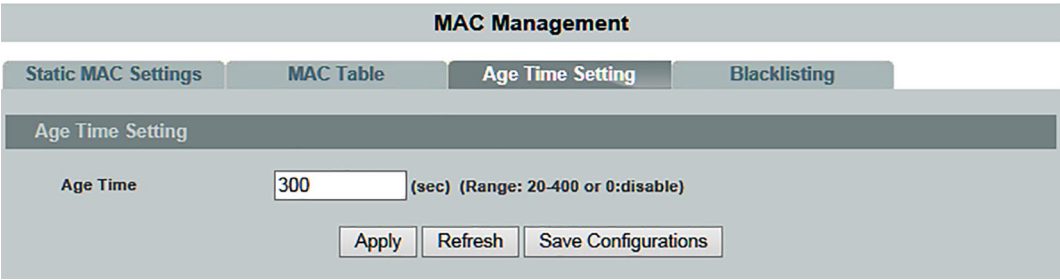
Page: 1/1 Page:

Figure 33: WBM Page, “MAC Management” – “MAC Table” Tab

Table 37: WBM Page, “MAC Management” – “MAC Table” Tab

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

9.2.2.3 Age Time Setting



The screenshot shows the 'MAC Management' section of the WBM page. Under the 'Age Time Setting' tab, there is a form with the following elements:

- Static MAC Settings** | **MAC Table** | **Age Time Setting** | **Blacklisting**
- Age Time Setting**
- Age Time: (sec) (Range: 20-400 or 0:disable)
- Buttons: **Apply**, **Refresh**, **Save Configurations**

Figure 34: WBM Page, “MAC Management” – “Age Time Setting” Tab

Table 38: WBM Page, “MAC Management” – “Age Time Setting” Tab

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

9.2.2.4 Blacklisting

Note



Additional Information

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

Note



Maximum number of MAC blacklist entries

Up to 20 entries can be configured.

Figure 35: WBM Page, “MAC Management” – “Refusal MAC Settings” Tab

Table 39: WBM Page, “MAC Management” – “Refusal MAC Settings” Tab

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

9.2.3 Port Mirroring

Note



Additional Information

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

Note



Monitor Port

The monitor port cannot be a member of any “Trunk Port” group.

The monitor port cannot be an ingress or egress port.

If a port has been configured as a source port and a user then configures it as a destination port, the port is automatically deleted from the source ports.

Port Mirroring

Port Mirroring Settings

State Disable ▾

Monitor to Port 1 ▾

All Ports : ▾

Source Port	Mirror Mode	Source Port	Mirror Mode
1	Disable ▾	2	Disable ▾
3	Disable ▾	4	Disable ▾
5	Disable ▾	6	Disable ▾
7	Disable ▾	8	Disable ▾
9	Disable ▾	10	Disable ▾
11	Disable ▾	12	Disable ▾

Apply
Refresh
Save Configurations

Figure 36: WBM “Port Mirroring” Page

Table 40: WBM "Port Mirroring" Page

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

9.2.4 Port Settings

9.2.4.1 General Settings

Port Settings

General Settings
Information

Port Settings

Port	State	Speed/Duplex	Flow Control
From: 1 To: 1	Enable	Auto	Off

Apply
Refresh
Save Configurations

Port Status

Port	State	Speed/Duplex	Flow Control	Link Status
1	Enabled	Auto	Off	Link Down
2	Enabled	Auto	Off	Link Down
3	Enabled	Auto	Off	Link Down
4	Enabled	Auto	Off	Link Down
5	Enabled	Auto	Off	Link Down
6	Enabled	Auto	Off	Link Down
7	Enabled	Auto	Off	Link Down
8	Enabled	Auto	Off	100M / Full / Off
9	Enabled	Auto	Off	Link Down
10	Enabled	Auto	Off	Link Down
11	Enabled	Auto	Off	1000M / Full / Off
12	Enabled	Auto	Off	Link Down

Figure 37: WBM Page, "Port Settings" – "General Settings" Tab

Table 41: WBM Page, "Port Settings" – "General Settings" Tab

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

9.2.4.2 Information

Port Settings

General Settings
Information

Port Settings

Port	Description
From: 1 To: 1	gigabitethernet1/0/1

Apply
Refresh
Save Configurations

Port Status

Port	Description	Status	Uptime	Medium Mode
1	gigabitethernet1/0/1	Normally	0 days 0:0:0	Copper
2	gigabitethernet1/0/2	Normally	0 days 0:0:0	Copper
3	gigabitethernet1/0/3	Normally	0 days 0:0:0	Copper
4	gigabitethernet1/0/4	Normally	0 days 0:0:0	Copper
5	gigabitethernet1/0/5	Normally	0 days 0:0:0	Copper
6	gigabitethernet1/0/6	Normally	0 days 0:0:0	Copper
7	gigabitethernet1/0/7	Normally	0 days 0:0:0	Copper
8	gigabitethernet1/0/8	Normally	5 days 4:5:11	Copper
9	gigabitethernet1/0/9	Normally	0 days 0:0:0	Fiber
10	gigabitethernet1/0/10	Normally	0 days 0:0:0	Fiber
11	gigabitethernet1/0/11	Normally	5 days 4:48:33	Fiber
12	gigabitethernet1/0/12	Normally	0 days 0:0:0	Fiber

Figure 38: WBM Page, “Port Settings” – “Information” Tab

Table 42: WBM Page, “Port Settings” – “Information” Tab

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

9.3 Advanced Settings

9.3.1 Bandwidth Control

9.3.1.1 QoS



Note

Additional Information

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

9.3.1.1.1 Port Priority

The screenshot displays the 'Port Priority' tab within the 'QoS' configuration page. It features a 'Port Priority Settings' section with a table for configuring IEEE802.1p priority for 12 ports. The table has two columns: 'Port' and 'IEEE802.1p priority'. The 'Port' column lists ports 1 through 12. The 'IEEE802.1p priority' column shows a dropdown menu for each port, all set to '0'. Above the table, there is a label 'All Ports IEEE802.1p priority : -' with a dropdown arrow. Below the table, there are three buttons: 'Apply', 'Refresh', and 'Save Configurations'.

Figure 39: WBM “QoS” Page – “Port Priority” Tab

Table 43: WBM “QoS” Page – “Port Priority” Tab

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

9.3.1.1.2 IP DiffServ (DSCP)

QoS

Port Priority
IP DiffServ (DSCP)
Priority/Queue Mapping
Schedule Mode

DSCP Settings

Mode Tag Over DSCP ▾

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
DSCP 0	0 ▾	DSCP 1	0 ▾	DSCP 2	0 ▾	DSCP 3	0 ▾
DSCP 4	0 ▾	DSCP 5	0 ▾	DSCP 6	0 ▾	DSCP 7	0 ▾
DSCP 8	0 ▾	DSCP 9	0 ▾	DSCP 10	0 ▾	DSCP 11	0 ▾
DSCP 12	0 ▾	DSCP 13	0 ▾	DSCP 14	0 ▾	DSCP 15	0 ▾
DSCP 16	0 ▾	DSCP 17	0 ▾	DSCP 18	0 ▾	DSCP 19	0 ▾
DSCP 20	0 ▾	DSCP 21	0 ▾	DSCP 22	0 ▾	DSCP 23	0 ▾
DSCP 24	0 ▾	DSCP 25	0 ▾	DSCP 26	0 ▾	DSCP 27	0 ▾
DSCP 28	0 ▾	DSCP 29	0 ▾	DSCP 30	0 ▾	DSCP 31	0 ▾
DSCP 32	0 ▾	DSCP 33	0 ▾	DSCP 34	0 ▾	DSCP 35	0 ▾
DSCP 36	0 ▾	DSCP 37	0 ▾	DSCP 38	0 ▾	DSCP 39	0 ▾
DSCP 40	0 ▾	DSCP 41	0 ▾	DSCP 42	0 ▾	DSCP 43	0 ▾
DSCP 44	0 ▾	DSCP 45	0 ▾	DSCP 46	0 ▾	DSCP 47	0 ▾
DSCP 48	0 ▾	DSCP 49	0 ▾	DSCP 50	0 ▾	DSCP 51	0 ▾
DSCP 52	0 ▾	DSCP 53	0 ▾	DSCP 54	0 ▾	DSCP 55	0 ▾
DSCP 56	0 ▾	DSCP 57	0 ▾	DSCP 58	0 ▾	DSCP 59	0 ▾
DSCP 60	0 ▾	DSCP 61	0 ▾	DSCP 62	0 ▾	DSCP 63	0 ▾

Apply
Refresh
Save Configurations

Figure 40: WBM “QoS” Page – “IP DiffServ (DSCP)” Tab

Table 44: WBM “QoS” Page – “IP DiffServ (DSCP)” Tab

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

9.3.1.1.3 Priority/Queue Mapping

The screenshot shows the 'Priority/Queue Mapping' tab in the WBM 'QoS' page. It features a table with two columns: 'Priority' and 'Queue ID'. The 'Priority' column lists values from 0 to 7. The 'Queue ID' column shows a selection box for each priority level, with values 1, 0, 2, 3, 4, 5, 6, and 7 respectively. A 'Reset to default' button is located above the table. At the bottom, there are three buttons: 'Apply', 'Refresh', and 'Save Configurations'.

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

Figure 41: WBM "QoS" Page – "Priority/Queue Mapping" Tab

Table 45: WBM "QoS" Page – "Priority/Queue Mapping" Tab

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

Table 46: Default Settings

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

9.3.1.1.4 Schedule Mode

QoS

Port Priority **IP DiffServ (DSCP)** **Priority/Queue Mapping** **Schedule Mode**

Schedule Mode Settings

Schedule Mode: High First(SPQ) ▾

Queue ID	Weight Value (Range:1~127)
0	
1	
2	
3	
4	
5	
6	
7	

Figure 42: WBM “QoS” Page – “Schedule Mode” Tab

Table 47: WBM “QoS” Page – “Schedule Mode” Tab

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

9.3.1.2 Rate Limitation

9.3.1.2.1 Storm Control

Note



Additional Information

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

Rate Limitation

Storm Control
Bandwidth Limitation

Storm Control Settings

Rate Limit Mode pps ▾

Port	Rate	Type
From: 1 ▾ To: 1 ▾	0 (units)	Mcast(Multicast) ▾

Disable:0. One unit is about 652 pps

Apply
Refresh
Save Configurations

Storm Control Status

Port	Rate(units)	Multicast	Broadcast	DLF	Port	Rate(units)	Multicast	Broadcast	DLF
1	1	Disable	Enable	Enable	2	1	Disable	Enable	Enable
3	1	Disable	Enable	Enable	4	1	Disable	Enable	Enable
5	1	Disable	Enable	Enable	6	1	Disable	Enable	Enable
7	1	Disable	Enable	Enable	8	1	Disable	Enable	Enable
9	1	Disable	Enable	Enable	10	1	Disable	Enable	Enable
11	1	Disable	Enable	Enable	12	1	Disable	Enable	Enable

Figure 43: WBM “Rate Limitation” Page – “Storm Control” Tab

Table 48: WBM “Rate Limitation” Page – “Storm Control” Tab

Storm Control Settings			
Parameters		Default	Description
Port	From:	1	Select a port or port range in the selection box to configure the “Storm Control” settings.
	to:	1	Select a port or port range in the selection box to configure the “Storm Control” settings.
Rate (units)		0	
Type	Bcast (Broadcast)		Choose “Bcast (Broadcast)” in the selection box to specify a limit for the number of broadcast packets received per second.
	Mcast (Multicast)		Choose “Mcast (Multicast)” in the selection box to specify a limit for the number of multicast packets received per second.
	DLF		Choose “DLF” in the selection box to specify a limit for the number of DLF packets received per second.
	Mcast+Bcast		Choose “Mcast+Bcast” in the selection box to specify a limit for the number of multicast and broadcast packets received per second.
	Mcast+DLF		Choose “Mcast+DLF” in the selection box to specify a limit for the number of multicast and DLF packets received per second.
	Bcast+DLF		Choose “Bcast+DLF” in the selection box to specify a limit for the number of broadcast and DLF packets received per second.
	Mcast+Bcast+DLF		Choose “Mcast+Bcast+DLF” in the selection box to specify a limit for the number of multicast, broadcast and DLF packets received per second.
Storm Control Status			
Parameters		Default	Description
Port		1 ... 10 (12)	This column displays the port numbers.
Rate (units)			This column displays the number of packets the switch can receive per second.
Multicast		Enable Disable	This column indicates if the rate setting applies to multicast.
Broadcast		Enable Disable	This column indicates if the rate setting applies to broadcast.
DLF		Enable Disable	This column indicates if the rate setting applies to DLF.

9.3.1.2.2 Bandwidth Limitation

Note



Additional Information

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

Rate Limitation

Storm Control
Bandwidth Limitation

Storm Control Settings

Rate Limit Mode pps

Port		Rate	Type
From:	1	To: 1	0 (units) Mcast(Multicast)

Disable:0. One unit is about 652 pps

Apply
Refresh
Save Configurations

Storm Control Status

Port	Rate(units)	Multicast	Broadcast	DLF	Port	Rate(units)	Multicast	Broadcast	DLF
1	1	Disable	Enable	Enable	2	1	Disable	Enable	Enable
3	1	Disable	Enable	Enable	4	1	Disable	Enable	Enable
5	1	Disable	Enable	Enable	6	1	Disable	Enable	Enable
7	1	Disable	Enable	Enable	8	1	Disable	Enable	Enable
9	1	Disable	Enable	Enable	10	1	Disable	Enable	Enable
11	1	Disable	Enable	Enable	12	1	Disable	Enable	Enable

Figure 44: WBM “Rate Limitation” Page – “Bandwidth Limitation” Tab

Table 49: WBM “Rate Limitation” Page – “Bandwidth Limitation” Tab

Bandwidth Limitation Settings			
Parameters		Default	Description
Port	From:	1	Select a port or port range in the selection box to configure the “Rate Limitation Settings”.
	to:	1	Select a port or port range in the selection box to configure the “Rate Limitation Settings”.
Ingress (Mbs)		0	Enter the “Rate Limitation” for incoming packets in the input field. Port 1 ... 8 0 ... 100 Port 9 ... 10 (12) 0 ... 1000
Egress (Mbs)		0	Enter the “Rate Limitation” for outgoing packets in the input field.
Bandwidth Limitation Status			
Parameters		Default	Description
Port		1 ... 10 (12)	This column displays the port numbers.
Ingress (Mbs)			This column displays the bandwidth set for “Ingress”.
Egress (Mbs)			This column displays the bandwidth set for “Egress”.

9.3.2 IGMP Snooping



Note

Additional Information

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

9.3.2.1 IGMP Snooping

9.3.2.1.1 General Settings

IGMP Snooping

General Settings
Port Settings
Querier Settings

IGMP Snooping Settings

IGMP Snooping State

Disable ▾

Report Suppression State

Disable ▾

IGMP Snooping VLAN State

Add ▾

Unknown Multicast Packets

Drop ▾

Apply
Refresh
Save Configurations

IGMP Snooping State

IGMP Snooping State	Disabled
Report Suppression State	Disabled
IGMP Snooping VLAN State	None
Unknown Multicast Packets	Drop

Figure 45: WBM “IGMP Snooping” Page – “General Settings” Tab

Table 50: WBM "IGMP Snooping" Page – "General Settings" Tab

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

9.3.2.1.2 Port Settings

IGMP Snooping

General Settings
Port Settings
Querier Settings

Port Settings

Port	Querier Mode	Immediate Leave
From: 1 ▼ To: 1 ▼	Auto ▼	Disable ▼

Apply
Refresh
Save Configurations

Port Status

Port	Querier Mode	Immediate Leave	Port	Querier Mode	Immediate Leave
1	Auto	Disable	2	Auto	Disable
3	Auto	Disable	4	Auto	Disable
5	Auto	Disable	6	Auto	Disable
7	Auto	Disable	8	Auto	Disable
9	Auto	Disable	10	Auto	Disable
11	Auto	Disable	12	Auto	Disable

Figure 46: WBM “IGMP Snooping” Page – “Port Settings” Tab

Table 51: WBM “IGMP Snooping” Page – “Port Settings” Tab

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

9.3.2.1.3 Querier Settings

The screenshot displays the 'IGMP Snooping' configuration page, specifically the 'Querier Settings' tab. It features two main sections: 'Querier Settings' and 'Querier Status'.

Querier Settings:

- Querier State:** A dropdown menu currently set to 'Disable'.
- Querier VLAN State:** A dropdown menu currently set to 'Add', followed by an empty text input field for the VLAN ID.
- Buttons:** 'Apply', 'Refresh', and 'Save Configurations'.

Querier Status:

Querier State	Disable
Querier VLAN State	None

Figure 47: WBM "IGMP Snooping" Page – "Querier Settings" Tab

Table 52: WBM "IGMP Snooping" Page – "Querier Settings" Tab

Querier Settings		
Parameters	Default	Description
Querier State	Disable	Select "Disable" in the selection box to disable this function.
	Enable	Select "Enable" in the selection box to enable this function.
Querier VLAN State	Add	Select "Add" in the selection box to enter the VLAN ID.
	Delete	Select "Delete" in the selection box to delete the VLAN ID.
Querier Status		
Parameters	Default	Description
Querier State	Querier State	This field displays the Querier State.
Querier VLAN State	None 0 ... 4094	This field displays the VLAN ID.

9.3.2.2 IGMP Filtering

9.3.2.2.1 General Settings

Figure 48: WBM "IGMP Filtering" Page – "General Settings" Tab

Table 53: WBM "IGMP Filtering" Page – "General Settings" Tab

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

9.3.2.2.2 Group Settings

Figure 49: WBM “IGMP Filtering” Page – “Group Settings” Tab

Table 54: WBM “IGMP Filtering” Page – “Group Settings” Tab

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

9.3.2.3 MVR

Note



Additional Information

Please refer to the section “Function Description” for more information on “MVR (Multicast VLAN Registration).”

9.3.2.3.1 MVR Settings

Multicast VLAN Registration

MVR Settings
Group Settings

MVR Settings

VLAN ID

State Enable ▾

Source Ports (ex. 1,3,5-8)

Receiver Ports (ex. 1,3,5-8)

Tagged Ports (ex. 1,3,5-8)

Name

Mode Dynamic ▾

Priority Override Disable ▾

IEEE802.1p Priority 0 ▾

Apply Refresh Save Configurations

MVR Status

VLAN ID	3	Name	Floor1	Priority override	Disable
State	Disable	Mode	Dynamic	IEEE802.1p Priority	0
Source Ports	None				
Receiver Ports	None				
Tagged Ports	None				

Delete

Figure 51: WBM “MVR” Page – “MVR Settings” Tab

Table 56: WBM “MVR” Page – “MVR Settings” Tab

MVR Settings		
Parameters	Default	Description
VLAN ID		Enter the VLAN ID in the input field.
Name		Enter the name for the MVR in the input field.
Priority Override	Disable	Select “Disable” in the selection box to disable this function.
	Enable	Select “Enable” in the selection box to enable this function.
State	Enable	Select “Enable” in the selection box to enable the MVR.
	Disable	Select “Disable” in the selection box to disable the MVR.
Mode	Dynamic	Select “Dynamic” in the selection box to configure the dynamic mode for the MVR.
	Compatible	Select “Compatible” in the selection box to configure the compatible mode for the MVR.
802.1p Priority	0 ... 7	In the selection box, select a priority for packets received on this port. Only packets without an “802.1p Tag Priority” are assigned the specified priority.
Source Ports	1 ... 8	Enter the source port or source port range for the MVR in the input field. Normally, the source ports are connected to the “Streaming Server”.
Receiver Ports	1 ... 8	Enter the receiver port or receiver port range for the MVR in the input field. Normally, the source ports are connected to the “Streaming Client”.
Tagged Ports	1 ... 8	Enter the tagged port or port range for the MVR in the input field. The same applies to VLAN tagged ports.
MVR Status		
Parameters	Default	Description
VLAN ID		This field displays the VLAN ID.
Name		This field displays the name you choose.
Priority Override	Disable Enable	This field displays the status.
State	Disable Enable	This field displays the status of the MVR.
Mode	Dynamic Compatible	This field displays the mode of the MVR.
802.1p Priority	0 ... 7	This field displays the packet priority you choose.
Source Ports	1 ... 8	This field displays the source port or source port range for the MVR.
Receiver Ports	1 ... 8	This field displays the receiver port or receiver port range for the MVR.
Tagged Ports	1 ... 8	This field displays the tagged port or port range for the MVR.

9.3.2.3.2 Group Settings

Figure 52: WBM “MVR” Page – “Group Settings” Tab

Table 57: WBM “MVR” Page – “Group Settings” Tab

Group Settings		
Parameters	Default	Description
MRV VLAN	1 ... 10 (12)	Select the number of MVR VLANs in the selection box.
Group Name		Enter the group name for the MVR in the input field.
Start Address		Enter the multicast start address in the input field.
Quantity		Enter the number of multicast addresses in the input field.
Group Status		
Parameters	Default	Description
MRV VLAN	1 ... 10 (12)	This field displays the number of MVR VLANs.
Group Name		This field displays the group name you choose.
Address range		This display fields shows the multicast start address.
Delete		Click [Delete] to delete this setting.
Delete All Group		Click [Delete All Group] to delete the settings for the entire group.

9.3.2.4 Multicast Address



Note

Additional Information

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

Static Multicast

Static Multicast Address Settings

VLAN ID	MAC Address	Port
1 ▾		

Multicast Address Table

VLAN ID	MAC Address	Status	Port	Action
1	01:00:5e:22:33:44	Static	1-12	Delete

Total counts : **1**

Figure 53: WBM “Multicast Address” Page

Table 58: WBM “Multicast Address” Page

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

9.3.2.5 Multicast IP Statistics

Multicast Statistics						
Multicast IP Table						
Index	Port	Multicast Group	VID	Timeout	Explicit Tracking	Host IP
1	1	0.0.0.0	1	260	Disabled	
2	2	0.0.0.0	1	260	Disabled	
3	3	0.0.0.0	1	260	Disabled	
4	4	0.0.0.0	1	260	Disabled	
5	5	0.0.0.0	1	260	Disabled	
6	6	0.0.0.0	1	260	Disabled	
7	7	0.0.0.0	1	260	Disabled	
8	8	0.0.0.0	1	260	Disabled	
9	9	0.0.0.0	1	260	Disabled	
10	10	0.0.0.0	1	260	Disabled	
11	11	0.0.0.0	1	260	Disabled	
12	12	0.0.0.0	1	260	Disabled	

Refresh

Figure 54: WBM “Multicast IP Statistics” Page

Table 59: WBM “Multicast IP Statistics” Page

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

9.3.3 VLAN

Note



Additional Information

Please refer to the section “Function Description” for more information on “VLAN” (Virtual Local Area Network).

9.3.3.1 Port Isolation

Note



Additional Information

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

Port Isolation

Port Isolation Settings

Port From: To:

Egress Port :

☐ Select All
 ☐ Deselect All

☒ 1

☒ 3

☒ 5

☒ 7

☒ 9

☒ 11

☒ 2

☒ 4

☒ 6

☒ 8

☒ 10

☒ 12

☒ 0 (CPU)

Port Isolation Status

	Egress Port												
Port	0	1	2	3	4	5	6	7	8	9	10	11	12
1	v	v	v	v	v	v	v	v	v	v	v	v	v
2	v	v	v	v	v	v	v	v	v	v	v	v	v
3	v	v	v	v	v	v	v	v	v	v	v	v	v
4	v	v	v	v	v	v	v	v	v	v	v	v	v
5	v	v	v	v	v	v	v	v	v	v	v	v	v
6	v	v	v	v	v	v	v	v	v	v	v	v	v
7	v	v	v	v	v	v	v	v	v	v	v	v	v
8	v	v	v	v	v	v	v	v	v	v	v	v	v
9	v	v	v	v	v	v	v	v	v	v	v	v	v
10	v	v	v	v	v	v	v	v	v	v	v	v	v
11	v	v	v	v	v	v	v	v	v	v	v	v	v
12	v	v	v	v	v	v	v	v	v	v	v	v	v

Figure 55: WBM “Port Isolation” Page

Table 60: WBM "Port Isolation" Page

Table 66: VDBW Port Isolation Page

Port Isolation Settings				
Parameters		Default	Description	
Port	From:	1	Select a port or port range in the selection box for which you want to configure the “Port Isolation” setting.	
	to:	1	Select a port or port range in the selection box for which you want to configure the “Port Isolation” setting.	
Egress Port			An egress port is an outgoing port through which a data packet is sent. The selection of a port as an egress port means that it can communicate with the port being configured.	
	Select All	☐	☐	No egress port is selected.
			☒	All egress ports are selected.
	Deselect All	☐	☐	No egress port is disabled.
			☒	All egress ports are disabled.
	☐ 0 (CPU) ...	☐	☐	The egress port is not enabled.
	☐ 10 (12)		☒	The egress port is enabled.
Port Isolation Status				
Parameters		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.

9.3.3.2 VLAN

9.3.3.2.1 VLAN Settings

The screenshot displays the 'VLAN' configuration page in the WBM system. It features three tabs: 'VLAN Settings', 'Tag Settings', and 'Port Settings'. The 'VLAN Settings' tab is active, showing a form to configure a new VLAN. The form includes fields for 'VLAN ID' (with 'From' and 'To' sub-fields), 'VLAN Name', and 'Member Port'. Below the form are buttons for 'Apply', 'Refresh', and 'Save Configurations'. Underneath the form is a 'VLAN List' table with the following data:

VLAN ID	VLAN Name	VLAN Status	Member Port	Action
1	VLAN1	Static	1-12	

Figure 56: WBM "VLAN" Page – "VLAN Settings" Tab

Table 61: WBM "VLAN" Page – "VLAN Settings" Tab

VLAN Settings			
Parameters		Default	Description
VLAN ID	From:		Enter the VLAN ID for this entry in the input field. Valid range: 1 ... 4094
	To:		Enter the VLAN ID for this entry in the input field. Valid range: 1 ... 4094
VLAN Name			Enter a descriptive name for the VLAN for identification purposes. The VLAN name should be a combination of numbers, letters, hyphens (-) or underscores (_).
Member Port			Enter the port numbers that the switch should assign to the VLAN as subscribers. You can specify multiple individual port numbers or ranges by using a comma (,) to separate individual ports or using a hyphen (-) for port ranges.

Table 61: WBM "VLAN" Page – "VLAN Settings" Tab

VLAN List		
Parameters	Default	Description
VLAN ID	1 ... 4094	This column displays the index number of the VLAN entry. Click the number to modify the VLAN entry.
VLAN Name		This field displays the name of the VLAN.
VLAN Status	Static Dynamic 802.1Q-VLAN	This field displays the status of the VLAN.
Member Port	1-10 (12)	This column displays which ports are assigned to the VLAN as subscribers.
Action		Click [Delete] to delete the VLAN.
		Note  Note Deleting VLAN1 VLAN1 cannot be deleted.

9.3.3.2.2 Tag Settings

VLAN

VLAN Settings **Tag Settings** Port Settings

Tag Settings

VLAN ID From: To:

Tag Port :

☐ Select All ☐ Deselect All

☐ 1 ☐ 3 ☐ 5 ☐ 7 ☐ 9 ☐ 11

☐ 2 ☐ 4 ☐ 6 ☐ 8 ☐ 10 ☐ 12

Tag State

VLAN ID	Tag Ports	Untagged Ports
1	1-7	8-12

Figure 57: WBM “VLAN” Page – “Tag Settings” Tab

Table 62: WBM “VLAN” Page – “TAG Settings” Tab

Tag Settings				
Parameters		Default	Description	
VLAN-ID	From:		Enter the VLAN ID for this entry in the input field. Valid range: 1 ... 4094	
	to:		Enter the VLAN ID for this entry in the input field. Valid range: 1 ... 4094	
Tag Port	Select All	☐	☐	No port is selected as a tagged port.
			☒	All ports are selected as tagged ports.
	Deselect All	☐	☐	No tagged port is disabled.
			☒	All tagged ports are disabled.
	☐ 1 ... ☐ 10 (12)	☐	☐	The port is not enabled.
			☒	The port is enabled.
Tag Status				
Parameters		Default	Description	
VLAN ID		1 ... 4094	This column displays the VLAN ID.	
Tag Ports		1 ... 7	This field displays the ports that have been assigned as tag ports.	
Un Tag Ports		1 ... 7	This field displays the ports that have been assigned as untagged ports.	

9.3.3.2.3 Port Settings

VLAN

VLAN Settings
Tag Settings
Port Settings

Port Settings

Port	PVID	Acceptable Frame
From: 1 ▼ To: 1 ▼	1 ▼	All ▼

Apply
Refresh
Save Configurations

Port State

Port	PVID	Acceptable Frame	Port	PVID	Acceptable Frame
1	1	untagged Frame	2	1	All
3	1	All	4	1	All
5	1	All	6	1	All
7	1	All	8	1	All
9	1	All	10	1	All
11	1	All	12	1	All

Figure 58: WBM "VLAN" Page – "Port Settings" Tab

Table 63: WBM "VLAN" Page – "Port Settings" Tab

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

9.3.3.3 GARP/GVRP

Note



Additional Information

Please refer to the section “Function Description” for more information on “GARP/GVRP” (**Generic Attribute Registration Protocol/GARP VLAN Registration Protocol or Generic VLAN Registration Protocol**).

9.3.3.3.1 GVRP

GARP VLAN Registration Protocol

GVRP
GARP Timer

GVRP Settings

GVRP State

Disable ▾

Port	State	Registration Mode
From: 1 ▾ To: 1 ▾	Enable ▾	Forbidden ▾

Apply
Refresh
Save Configurations

GVRP State

Port	State	Registration Mode	Port	State	Registration Mode
1	Enabled	Forbidden	2	Disabled	-
3	Disabled	-	4	Disabled	-
5	Disabled	-	6	Disabled	-
7	Disabled	-	8	Disabled	-
9	Disabled	-	10	Disabled	-
11	Disabled	-	12	Disabled	-

Figure 59: WBM “GARP VLAN Registration Protocol” Page – “GVRP” Tab

Table 64: WBM “GARP VLAN Registration Protocol” Page – “GVRP” Tab

GVRP Settings			
Parameters		Default	Description
GVRP State		Disable	Select “Disable” in the selection box to disable the GVRP function.
		Enable	Select “Enable” in the selection box to enable the GVRP function and to exchange the VLAN configuration information with other GVRP switches.
Port	From:	1	Select a port or port range in the selection box to configure the GVRP settings.
	To:	1	Select a port or port range in the selection box to configure the GVRP settings.
State		Disable	Select “Disable” in the selection box to disable the GVRP function for the port.
		Enable	Select “Enable” in the selection box to enable the GVRP function for the port.
Registration Mode		Normal	Select “Normal” in the selection box to allow dynamic creation (if dynamic VLAN creation is enabled), registration and deregistration of VLANs on the trunk port.
		Forbidden	Select “Forbidden” in the selection box to deregister all VLANs (except VLAN 1) and to prevent any further creation or deregistration of VLANs on the “Trunk Port”.
GVRP Status			
Parameters		Default	Description
Port		1 ... 10 (12)	This column displays the port numbers.
State		Disable Enable	This column displays the set status.
Registration Mode		Normal Forbidden	This column displays the selected registration mode.

9.3.3.3.2 GARP Timer

Note



Size of the “leave”, “join”, “leave” and “leaveall” values

The value for “leave” must be three times the value for “join” (leave $\geq$ join x 3).
The value for “leaveall” must be greater than the value for “leave” (leaveall > leave).

GARP VLAN Registration Protocol

GVRP
GARP Timer

GARP Timer Settings

Port	Join Time	Leave Time	Leave All Time
From: 1 To: 1	20	60	1000

2*Join Time < Leave Time < Leave All Time
Time unit:(centi-sec)

GARP Timer Status

Port	Join Time	Hold Time	Leave Time	Leave All Time
1	20	10	60	1000
2	20	10	60	1000
3	20	10	60	1000
4	20	10	60	1000
5	20	10	60	1000
6	20	10	60	1000
7	20	10	60	1000
8	20	10	60	1000
9	20	10	60	1000
10	20	10	60	1000
11	20	10	60	1000
12	20	10	60	1000

Figure 60: WBM “GARP VLAN Registration Protocol” Page – “GVRP Timer” Tab

Table 65: WBM “GARP VLAN Registration Protocol” Page – “GVRP Timer” Tab

GARP Timer Settings			
Parameters		Default	Description
Port	From:	1	Select a port or port range in the selection box to configure the GARP timer.
	To:	1	Select a port or port range in the selection box to configure the GARP timer.
Join Time		20	Enter the maximum time in milliseconds that the interface waits before sending VLAN messages.
Leave Time		60	Enter the maximum time in milliseconds that the interface waits after receiving a “Leave Message” before the interface leaves the VLAN specified in the message.
Leave All Time		1000	Enter the time interval in milliseconds after which the Leave All messages are sent to interfaces. Leave All messages can help to update information about current GVRP VLAN subscriber information in the network.
GARP Timer Status			
Parameters		Default	Description
Port		1 ... 10 (12)	This column displays the port numbers.
Join Time			This column displays the Join Time.
Hold Time		10	This column displays the Hold Time.
Leave Time			This column displays the Leave Time.
Leave All Time			This column displays the Leave All Time.

9.3.3.4 IP-Subnet-VLAN

Note



Additional information

Please refer to the section “Function Description” for more information on “IP Subnet VLAN.”

IP Subnet VLAN

IP Subnet VLAN Settings

IP Address	Subnet Mask	VLAN	Priority
			0 ▼

IP Subnet VLAN Table

Index	IP Address	Subnet Mask	VLAN	Priority	Action

Figure 61: WBM „IP-Subnet-VLAN“

Table 66: WBM “IP Subnet VLAN” Page

IP Subnet VLAN Settings		
Parameter	Default	Description
IP Address		Enter the IP address of the IP subnet VLAN in the input field.
Subnet Mask		Enter the subnet mask of the switch in the input field in decimal-point notation.
VLAN (1–4094)		Enter the value for the IP subnet VLAN for the instance in the input field. Valid range: 1 ... 4094 One or more data VLANs can be configured.
Priority	0 ... 7	Select the respective priority for the specific port in the selection box. 0 = Lowest priority 7 = Highest priority
IP Subnet VLAN Table		
Parameter	Default	Description
Index	1 ... 10 (12)	This column displays the number of entries.
IP Address		This column displays the IP address of the IP subnet VLAN.
Subnet Mask		This column shows the subnet mask of the switch.
VLAN		This column displays the IP subnet VLAN ID for the specific port.
Priority	0 ... 7	This column displays the priority for the specific port.
Action		Click [Delete] to delete the IP subnet VLAN addresses.
Number of Entries		This field displays the total number of entries in the IP subnet VLAN table.

Figure 62: WBM “MAC VLAN” Page

Table 67: WBM “MAC VLAN” Page



9.3.3.6 Protocol VLAN

Protocol VLAN

Protocol VLAN Settings

Frame Type	Ethernet Type	VLAN	Port List
EthernetII			
ApplyRefreshSave Configurations			

Protocol VLAN Table

Index	Frame Type	Ethernet Type	VLAN	Port List	Action

Figure 63: WBM “Protocol VLAN” Page

Table 68: WBM “Protocol VLAN” Page

Protocol VLAN Settings		
Parameters	Default	Description
Frame Type	EthernetII	Select "EthernetII" in the selection box if you want to configure this frame type.
	NonLLC-SNAP	Select "NonLLC-SNAP" in the selection box if you want to configure this frame type.
	LLC-SNAP	Select "LLC-SNAP" in the selection box if you want to configure this frame type.
Ethernet Type		Enter the ETHERNET type in the input field. (e.g., 0800)
VLAN (1~4094)	1 ... 4094	Enter the VLAN ID in the input field.
Port List	1 ... 10 (12)	Enter the port or port group (e.g., 1 – 3) for the protocol VLAN in the input field.

Protocol VLAN Table		
Parameters	Default	Description
Index		This column displays the number of entries.
Frame Type		This column displays the frame type.
Ethernet Type		This column displays the ETHERNET type.
VLAN		This column displays the VLAN ID.
Port List		This column displays the port list.
Action		Click [Delete] to delete the multicast addresses.

9.3.3.6.1 Q-in-Q



Note

Additional Information

Please refer to the section “Function Description” for more information on “Q-in-Q”.

9.3.3.6.2 VLAN Stacking

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

VLAN Stacking Setting

Action Disable ▼

Tunnel TPID Index	TPID
1 (Default) ▼	8100 (0000~ffff)

Port	Tunnel TPID Index
From: 1 ▼ To: 1 ▼	1 (Default) ▼

Apply
Refresh
Save Configurations

VLAN Stacking State

Tunnel TPID Index	TPID
1	8100
2	8100
3	8100
4	8100
5	8100
6	8100

Port	Tunnel TPID Index (TPID)	Port	Tunnel TPID Index (TPID)
1	1 (8100)	2	1 (8100)
3	1 (8100)	4	1 (8100)
5	1 (8100)	6	1 (8100)
7	1 (8100)	8	1 (8100)
9	1 (8100)	10	1 (8100)
11	1 (8100)	12	1 (8100)

Figure 64: WBM “Q-in-Q” Page – “VLAN Stacking” Tab

Table 69: WBM “Q-in-Q” Page – “VLAN Stacking” Tab

VLAN Stacking Setting			
Parameters		Default	Description
Action		Disable	Select “Disable” in the selection box to disable the VLAN Stacking function.
		Port-based	Select “Port-Based” in the selection box to execute the VLAN Stacking function port-based.
		Selective	Select “Selective” in the selection box to execute the VLAN Stacking function selectively.
Tunnel TPID Index		1 (Default) ... 6	Select a table index number in the selection box.
TPID (0000~ffff)			Enter a value for the TPID in the input field.
Port	From:	1	Select a port or port range in the selection box to configure the “VLAN Stacking”.
	To:	1	Select a port or port range in the selection box to configure the “VLAN Stacking”.
Tunnel TPID Index		1 (Default) ... 6	Select a “Tunnel TPID Index” in the selection box.
VLAN Stacking Status			
Parameters		Default	Description
Tunnel TPID Index		1 ... 6	This column displays the table index number.
TPID		0000 ... ffff	This column displays the TPID.
Port		1 ... 10 (12)	This column displays the port number.
Tunnel TPID Index (TPID)			This column displays the index number for the specific port.

9.3.3.6.3 Port-based Q-in-Q

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

Port-based Q-in-Q

Port	Role	SPVID	Priority
From: 1 To: 1	Normal	1 (1~4094)	0
Apply Refresh Save Configurations			

Port-based Q-in-Q Status

Port	Role	SPVID	Priority	Port	Role	SPVID	Priority
1	Normal	1	0	2	Normal	1	0
3	Normal	1	0	4	Normal	1	0
5	Normal	1	0	6	Normal	1	0
7	Normal	1	0	8	Normal	1	0
9	Normal	1	0	10	Normal	1	0
11	Normal	1	0	12	Normal	1	0

Figure 65: WBM “Q-in-Q” Page – “Port-based Q-in-Q” Tab

Table 70: WBM “Q-in-Q” Page – “Port-based Q-in-Q” Tab

Port-based Q-in-Q			
Parameters		Default	Description
Port	From:	1	Select a port or port range in the selection box to configure the “Q-in-Q”.
	To:	1	Select a port or port range in the selection box to configure the “Q-in-Q”.
Role		Normal	Select “Normal” in the selection box to select this role for the specific port.
		Access	Select “Access” in the selection box to select this role for the specific port.
		Tunnel	Select “Tunnel” in the selection box to select this role for the specific port.
SPVID (1~4094)		1	Enter the service provider VLAN “SPVID” in the input field.
Priority		0	Select the respective priority for the specific port in the selection box. 0 = Lowest priority 7 = Highest priority
Port-based Q-in-Q Status			
Parameters		Default	Description
Port		1 ... 10	This column displays the port number.
Role			This column displays the role of the specific port.
SPVID		1 ... 10	This column displays the SPVID.
Priority			This column displays the priority for the specific port.

9.3.4 Selective Q-in-Q

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

Selective Q-in-Q Setting

Name

Access Ports (ex. 1,3,5-6)

Tunnel Ports (ex. 1,3,5-6)

CVID (Range: 1~4094)

SPVID (Range: 1~4094)

Priority

Action

Selective Q-in-Q Status

No.	Name	Access Ports	Tunnel Ports	CVID	SPVID	Priority	Action	Disable
1	Floor1	2	3	1	1	0	Enable	Delete

Figure 66: WBM “Q-in-Q” Page – “Selective Q-in-Q” Tab

Table 71: WBM “Q-in-Q” Page – “Selective Q-in-Q” Tab

Selective Q-in-Q Setting		
Parameters	Default	Description
Name		Enter the name for the selective Q-in-Q profile in the input field.
Access Ports (ex. 1,3,5-6)		Enter the Access port or port range in the input field.
Tunnel Ports (ex. 1,3,5-6)		Enter the tunnel port or port range in the input field.
CVID (Range: 1~4094)		Enter a customer VLAN “CVID” in the input field.
SPVID (Range: 1~4094)		Enter a service provider VLAN “SPVID” in the input field.
Selective Q-in-Q Setting	0 ... 7	Select the respective priority level in the selection box. 0 = Lowest priority 7 = Highest priority
Priority	Disable	Select “Disable” in the selection box to disable this function.
	Enable	Select “Enable” in the selection box to enable this function.
Selective Q-in-Q Status		
Parameters	Default	Description
No.		This column displays the index No.
Name		This column displays the name of the selective Q-in-Q profile.
Access Ports		This column displays the Access port.
Tunnel Ports		This column displays the Tunnel port.
CVID		This column displays the customer VLAN “CVID”.
SPVID		This column displays the service provider VLAN “SPVID”.
Priority	0 ... 7	This column displays the respective priority level. 0 = Lowest priority 7 = Highest priority
Action	Disable Enable	This column displays the selected action.
Disable		Click [Delete] to delete the selective Q-in-Q settings.

9.3.5 DHCP Relay



Note

Additional Information

Please refer to the section “Function Description” for more information on “DHCP Relay” (**D**ynamic **H**ost **C**onfiguration **P**rotocol **R**elay).

Figure 67: WBM “DHCP Relay” Page

Table 72: WBM “DHCP Relay” Page

DHCP Relay Settings		
Parameters	Default	Description
State	Disable	Select “Disable” in the selection box to disable this function.
	Enable	Select “Enable” in the selection box to enable the “DHCP Relay”.
VLAN State	Add	Select “Add” in the selection box and enter the VLANs on which the switch should run “DHCP Relay”. Valid range of VLAN IDs: 1 ... 4094. Use a comma (,) or hyphen (-) to specify individual VLANs or VLAN ranges.
	Delete	Select “Delete” in the selection box and enter the VLANs on which the switch should not run “DHCP Relay”.
DHCP Server IP	0.0.0.0	Enter the IP address of the DHCP server in the input field.
DHCP Relay Status		
Parameters	Default	Description
DHCP Relay State	Disable Enable	This display field indicates if “DHCP Relay” is enabled or disabled.
Enabled on VLAN	None 0 ... 4094	This field displays if a VLAN is used.
DHCP Server IP		This field displays the IP address of the DHCP server.

9.3.5.1 DHCP Options

9.3.6 Option 82

DHCP Options

DHCP Option 82 Settings

Option 82 State:

Option 82 Frame:

Option 82 Shelf:

Option 82 Slot:

Circuit-ID Form:

Remote-ID Form:

Option 82 Command State

Port:

Option 82 State:

Circuit-ID String:

Remote-ID String:

Option 82 Command State

Port 1

Option 82 State:

Circuit-ID String:

Remote-ID String:

Port 2

Option 82 State:

Circuit-ID String:

Remote-ID String:

Figure 68: WBM "DHCP Options" Page – "Option 82" Tab

Table 73: WBM "DHCP Options" Page – "Option 82" Tab

DHCP Option 82 Settings		
Parameters	Default	Description
Option 82 State	Disable	Select "Disable" in the selection box to disable this function.
	Enable	Select "Enable" in the selection box to enable "DHCP Relay Option 82" on the switch.
Option 82 Frame	1	Enter the required frame number in the input field.
Option 82 Shelf	0	Enter the required shelf number in the input field to uniquely identify the switch.
Option 82 Slot	0	Enter the required slot number in the input field to uniquely identify the switch.
Circuit-ID Form	%HOSTNAME+%SPACE+eth/+%FRAME+/%SHELF+/%SLOT+:%PORT+_+%SVLAN+:%CVLAN	This input field gives you the option to adapt the appended string.
Remote-ID Form	%HOSTNAME+%SPACE+eth/+%FRAME+/%SHELF+/%SLOT+:%PORT+_+%SVLAN+:%CVLAN	This input field gives you the option to adapt the appended string.

9.3.7 Dual Homing



Note

Additional Information

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

Figure 69: WBM “Dual Homing” Page

Table 74: WBM “Dual Homing” Page

Dual Homing Settings		
Parameters	Default	Description
State	Disable	Select “Disable” in the selection box to disable this function.
	Enable	Select “Enable” in the selection box to enable “Dual Homing”.
Primary Channel	Port	This field configures the primary channel. Select only one individual port or a “Trunk Group” in the selection box.
Secondary Channel	Port	This field configures the secondary channel. Select only one individual port or a “Trunk Group” in the selection box.
Dual Homing Status		
Parameters	Default	Description
State	Disable Enable	This field displays what status “Dual Homing” has.
Primary Channel	None Port 1 ... 10 (12)	This field displays the selected primary channel.
Secondary Channel	None Port 1 ... 10 (12)	This field displays the selected secondary channel.

9.3.8 Dual Ring



Note

Additional Information

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

Dual Ring

Dual Ring Settings

State

Disable ▼

Xpress Ring Role

Forwarder ▼

Xpress Ring PORT-1

None ▼

Xpress Ring PORT-2

None ▼

Xpress Ring Destination MAC
(Last byte)

f0

Subring PORT-1

None ▼

Subring PORT-2

None ▼

Apply

Refresh

Save Configurations

Dual Ring Status

Xpress Ring PORT-1 State	No connection
Xpress Ring PORT-2 State	No connection
Subring PORT-1 State	No connection
Subring PORT-2 State	No connection
Subring Bridge Role	Disabled
Subring Master Bridge MAC	00:00:00:00:00:00

Figure 70: WBM “Dual Ring” Page

Table 75: WBM “Dual Ring” Page

Dual Ring Settings		
Parameters	Default	Description
State	Disable	Select “Disable” in the selection box to disable this function.
	Enable	Select “Enable” to enable “Dual ring”.
Xpress Ring Role	Forwarder	Select “Forwarder” in the selection box if the switch should operate in the Xpress Ring as a forwarder.
	Arbiter	Select “Arbiter” in the selection box if the switch should operate in the Xpress Ring as an Arbiter.
Xpress Ring PORT-1	None	Select “None” in the selection box if you do not want to select any port.
	1 ... 10 (12)	Select Port 1 in the Xpress Ring in the selection box.
Xpress Ring PORT-2	None	Select “None” in the selection box if you do not want to select any port.
	1 ... 10 (12)	Select Port 2 in the Xpress Ring in the selection box.
Xpress Ring Destination MAC (last byte)	f0	Enter the Xpress Ring ID in the input field.
Subring PORT-1	None	Select “None” in the selection box if you do not want to select any port.
	1 ... 10 (12)	Select Port 1 in the Jet Ring in the selection box.
Subring PORT-2	None	Select “None” if you do not want to select any port.
	1 ... 10 (12)	Select Port 2 in the Jet Ring.
Dual Ring Status		
Parameters	Default	Description
Xpress Ring PORT-1 State	Forwarding Blocking	This field displays what status Xpress Ring Port 1 has.
Xpress Ring PORT-2 State	Forwarding Blocking	This field displays what status Xpress Ring Port 2 has.
Subring PORT-1 State	Forwarding Blocking	This field displays what status Jet Ring Port 1 has.
Subring PORT-2 State	Forwarding Blocking	This field displays what status Jet Ring Port 2 has.
Subring Bridge Role	Forwarder Master	This field displays the role of the switch in the Xpress Ring.
Subring Master Bridge MAC		This field displays the MAD ID of the Jet Ring.

9.3.8.1 ERPS



Note

Additional Information

Please refer to the section “Function Description” for more information on “ERPS” (ETHERNET Ring Protection Switching).

9.3.8.2 Ring Settings

ERPS

Ring Settings
Instance Settings

ERPS Global Settings

Global State Disable ▾

ERPS Ring Settings

Ring ID (1~255)

Ring Name

Instance 0 (0:Disable, 0~30)

Control VLAN (1~4094)

Holdoff Timer (ms) 0 (0~10000)

MEL 7 (0~7)

Left Port None ▾ Normal ▾

Left Port Enhance Mode Disable ▾

Alarm Relay Diagnostic Disable ▾

State Disable ▾

Revertive Enable ▾

Ring Type Major-ring ▾

Version v2 ▾

WTR Timer (min) 300 (5~720)

Guard Timer (ms) 500 (10~2000)

Right Port None ▾ Normal ▾

Right Port Enhance Mode Disable ▾

Apply
Refresh
Save Configurations

ERPS Ring Status

Ring ID	249	State	Disable
Ring Name	Ring249	Revertive	Enable
Instance	None	Ring Type	Major-ring
Control VLAN	249	Version	v2
Holdoff Timer (ms)	0	WTR Timer (min)	300
MEL	7	Guard Timer (ms)	500
Left Port	None	Right Port	None
Left Port Type	Normal	Right Port Type	Normal
Left Port Enhance Mode	Disable	Right Port Enhance Mode	Disable
Left Port Status	N/A	Right Port Status	N/A
Ring Status	Initialization	Alarm Relay Diagnostic	Disable

delete

Figure 71: WBM “ERPS” Page – “Ring Settings” Tab

Table 76: WBM “ERPS” Page – “Ring Settings” Tab

ERPS Global Settings		
Parameters	Default	Description
Global State	Disable	Select “Disable” in the selection box to disable the ERPS function.
	Enable	Select “Enable” in the selection box to enable the ERPS function.
ERPS Ring Settings		
Parameters	Default	Description
Ring ID (1~255)		Enter the Ring ID in the input field.
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		Enter the name of the ring (max. 32 characters) in the input field. (e.g., Major-Ring ID255)
Revertive	Enable	Select “Enable” to enable revertive mode.
	Disable	Select “Disable” in the selection box to disable the revertive mode.
Instance (0:Disable, 0~30)		Enter the instance for the ring in the input field. Valid range: 0 ... 30. 0 (“Disable”) means that the ERPS is running in version 1. The control VLAN of the instance should be the same as the control VLAN below it.
Ring Type	Major-ring	Select “Major-Ring” in the selection box if the switch should operate in the Major-Ring.
	Sub-ring	Select “Sub-Ring” in the selection box if the switch should operate in the Sub-Ring.
Control VLAN (1~4084)	1 ... 4094	Enter the VLAN ID in the input field that should serve as the domain for the ERPS control packets.
Version	v2	Select “v2” in the selection box if you want to use ERPS Version v2.
	v1	Select “v1” in the selection box if you want to use ERPS Version v1.
Holdoff Timer (ms) (0~10000)	0 ... 10000	Enter the value for the “Hold-off Timer” for the ring in the input field. Valid range: 0 ... 10000 ms.
WTR Timer (min) (5~12)	5 ... 12	Enter the value for the “WTR Timer” for the ring in the input field.
MEL (0~7)	0 ... 7	Enter the value for the “Control MEL” (M aintenance E ntity Group L evel) for the ring in the input field. The MEL specifies the priority. 0 = Lowest priority 7 = Highest priority

Table 76: WBM “ERPS” Page – “Ring Settings” Tab

Guard Timer (ms) (10~2000)	500	Enter the value for the “Guard Timer” for the ring in this input field. Valid range: 10 ... 2000 ms.
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 any port.
	1 ... 10 (12)	Select the respective 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.
	Neighbour	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 the Owner function in the ERPS ring.
Right Port		The 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 any port.
	1 ... 10 (12)	Select the respective 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.
	Neighbour	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 the Owner function in the ERPS ring.
Left Port Enhance Mode	Disable	Select “Disable” in the selection box if a device that supports ERPS is connected to this port.
	Enable	Select “Enable” in the selection box if a device that does not support ERPS is connected to this port. Please note the Aging Time of the connected device.
Right Port Enhance Mode	Disable	Select “Disable” in the selection box if a device that supports ERPS is connected to this port.
	Enable	Select “Enable” in the selection box if a device that does not support ERPS is connected to this port. Please note the Aging Time of the connected device.
Alarm Relay	Disable	Select “Disable” in the selection box if you do not want the alarm relay to switch when the ERPS (Enhancement Mode) is open.
	Enable	Select “Enable” in the selection box if you want the alarm relay to switch when the ERPS (Enhancement Mode) is open.
ERPS Ring Status		
Parameters	Default	Description
Ring ID	1 ... 255	This field displays the Ring ID.
State	Disable Enable	This field displays the ring status.
Ring Name		This field displays the ring name.
Revertive	Enable Disable	This field displays the status of the revertive mode.
Instance		This field displays the instance for the ring.
Ring Type	Major-ring Sub-ring	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.

Table 76: WBM “ERPS” Page – “Ring Settings” Tab

Holdoff Timer (ms)	0 ... 10000	This field displays the time for the “Hold-off Timer”.
WTR Timer (min)	5 ... 12	This field displays the time for the “WTR Timer”.
MEL	0 ... 7	This field displays the value for the “Control MEL”.
Guard Timer (ms)	10 ...2000	This field displays the time for the “Guard Timer”.
Left Port	None 1 ... 10 (12)	This field displays the port number of the left port.
Right Port	None 1 ... 10 (12)	This field displays the port number of the right port.
Left Port Type	RPL Normal Neighbour Owner	This field displays the type of the left port.
Right Port Type	RPL Normal Neighbour Owner	This field displays the type of the right port.
Left Port Enhance Mode	Enable Disable	This field displays the status of the left port.
Right Port Enhance Mode	Enable Disable	This field displays the status 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.

9.3.9 Instance Settings

The screenshot displays the 'ERPS Instance' configuration page. At the top, there are two tabs: 'Ring Settings' and 'Instance Settings', with 'Instance Settings' being the active tab. Below the tabs, the 'Instance Settings' section contains three input fields: 'Instance' (with a range of 1~30), 'Control VLAN', and 'Data VLAN'. Below these fields are three buttons: 'Apply', 'Refresh', and 'Save Configurations'. Below the settings section is the 'Instance Status' section, which contains a table with the following data:

Instance	Control VLAN	Data VLAN
1	2	3

Below the table is a 'delete' button.

Figure 72: WBM “ERPS” Page – “Instance Settings” Tab

Table 77: WBM “ERPS” Page – “Instance Settings” Tab

Instance Settings		
Parameters	Default	Description
Instance (1~30)		Enter the instance ID in the input field. Valid range: 1 ... 31
Control VLAN		Enter the VLAN of the controller for the instance in the input field. Valid range: 1 ... 4094
Data VLAN		Enter the value for the data VLAN for the instance in the input field. Valid range: 1 ... 4094 One or more data VLANs can be configured.
Instance Status		
Parameters	Default	Description
Instance	1 ... 31	This field displays the instance ID.
Control VLAN	1 ... 4094	This field displays the controller VLAN of the instance.
Data VLAN	1 ... 4094	This field displays the data VLAN of the instance.
Delete		Click [Delete] to delete this setting.

9.3.9.1 Link Aggregation

9.3.9.2 Static Trunk

Note



Additional Information

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

Link Aggregation

Static Trunk
LACP
LACP info.

Static Trunk Settings

Group State Group 1 ▾ Disable ▾

Load Balance MAC ▾

Member Ports

☐ Select All
☐ Deselect All

☐ 1 ☐ 3 ☐ 5 ☐ 7

☐ 9 ☐ 11

☐ 2 ☐ 4 ☐ 6 ☐ 8

☐ 10 ☐ 12

Apply Refresh Save Configurations

Trunk Group Status

Group ID	State	Load Balance	Member Ports
1	Disable	MAC	
2	Disable	MAC	
3	Disable	MAC	
4	Disable	MAC	
5	Disable	MAC	
6	Disable	MAC	

Member Ports: T is Trunk member port but no link, A is Trunk member and link up.

Figure 73: WBM “Link Aggregation” Page – “Static Trunk” Tab

Table 78: WBM “Link Aggregation” Page – “Static Trunk” Tab

Static Trunk Settings				
Parameters		Default	Description	
Group State		Group 1 ... Group 6	Select a group ID for the “Trunk Group” (a logical link containing multiple ports) in the selection box.	
		Disable	Select “Disable” in the selection box to disable a static “Trunk Group”.	
		Enable	Select “Enable” in the selection box to use a static “Trunk Group”.	
Load Balance		MAC	Select “MAC” in the selection box to configure the algorithm for load balancing of a specific “Trunk Group”.	
		IP	Select “IP” in the selection box to configure the algorithm for load balancing of a specific “Trunk Group”.	
Member Ports	Select All	☐	☐	No port is selected to be added to the static “Trunk Port”.
			☒	All ports are selected to be added to the status “Trunk Group”.
	Deselect All	☐	☐	No port is disabled.
			☒	All ports are disabled.
	☐ 1 ... ☐ 10 (12)	☐	☐	The port is not enabled.
			☒	The port is enabled.
Trunk Group Status				
Parameters		Default	Description	
Group ID		1 ... 6	This column displays the group ID for a “Trunk Group” (a logical link containing multiple ports).	
State		Disable Enable	This column displays if a “Trunk Group” is enabled or disabled.	
Load Balance		1 ... 6	This column displays the policy for load balancing of the “Trunk Group”.	
Member Ports			This column displays the ports assigned to the “Trunk Group”.	

9.3.9.3 LACP

Note



Additional Information

Please refer to the section “Function Description” for more information on “LACP” (Link Aggregation Control Protocol).

Link Aggregation

StaticTrunk
LACP
LACP info.

LACP Settings

State Enable ▾

System Priority 32768

Group LACP Group 1 ▾ Disable ▾

Port Priority From: - ▾ - ▾ :

Apply
Refresh
Save Configurations

LACP Group Status

Group ID	LACP State
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable

LACP Port Priority Status

Port	Priority	Port	Priority
1	32768	2	32768
3	32768	4	32768
5	32768	6	32768
7	32768	8	32768
9	32768	10	32768
11	32768	12	32768

Figure 74: WBM “Link Aggregation” Page – “LACP” Tab

Table 79: WBM “Link Aggregation” Page – “LACP” Tab

LACP Settings			
Parameters		Default	Description
State		Disable	Select “Disable” in the selection box if you do not want to use LACP.
		Enable	Select “Enable” in the selection box to enable the “Link Aggregation Control Protocol” (LACP).
System Priority		1 ... 65535	Select the LACP system priority in the selection box. Enter a number to set the priority of an active port with “Link Aggregation Control Protocol” (LACP). The smaller the number, the higher the priority level.
Group LACP		Group 1 ... Group 6	Select a “Trunk Group ID” in the selection box.
		Disable	Select “Disable” in the selection box to disable LACP for this “Trunk Group”.
		Enable	Select “Enable” in the selection box to enable LACP for this “Trunk Group”.
Port Priority	From:	-	Select a port or port range in the selection box for which you want to configure the LACP priority.
	To:	-	Select a port or port range in the selection box for which you want to configure the LACP priority.
		32768	The default System Priority is 32768.
LACP Group Status			
Parameters		Default	Description
Group ID		1 ... 6	This column displays the LACP group ID.
LACP State		Enable Disable	This column displays if LACP is enabled or disabled for a group.
LACP Port Priority Status			
Parameters		Default	Description
Port		1 ... 10 (12)	This column displays the port ID.
Priority		1 ... 65535	This column displays the LACP priority of the port.

9.3.10 LACP Info.

Link Aggregation

StaticTrunk
LACP
LACP info.

LACP Information

Group ID

Group ID	1						
Neighbor Information							
Port	System Priority	System ID	Port	Age	Port State	Port Priority	Oper Key
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-
Internal Information							
Port	Port Priority	Admin Key	Oper Key	Port State			
5	32768	5	5	0x45			
6	32768	6	6	0x45			

Neighbor Information: '-' means the port is link down.

Figure 75: WBM “Link Aggregation” Page – “LACP Info.” Tab

Table 80: WBM “Link Aggregation” Page – “LACP Info.” Tab

LACP Information		
Parameters	Default	Description
Group ID	-	Select an LACP group that you want to view.
Neighbor Informationen		
Parameters	Default	Description
Port	1 ... 10 (12)	This column displays the LACP ID of the subscriber port.
System Priority	0 ... 65535	This column displays the LACP system priority.
System ID		This column displays the system ID of the neighboring switch.
Port	1 ... 10 (12)	This column displays the ID of the directly connected port of the neighboring switch.
Age		This column displays the available time period for the LACP information of the neighboring switch.
Port State		This column displays the status of the port connected directly to the neighboring switch.
Port Priority		This column displays the priority of the port connected directly to the neighboring switch.
Oper Key		This column displays the “Oper Key” of the neighboring switch.
Internal Information		
Parameters	Default	Description
Port		This column displays the LACP ID of the subscriber port.
Port Priority		This column displays the port priority of the LACP subscriber port.
Admin Key		This column displays the “Admin Key” of the LACP subscriber port.
Oper Key		This column displays the “Oper Key” of the LACP subscriber port.
Port State		This column displays the port status of the LACP subscriber port.

9.3.10.1 LLDP



Note

Additional Information

Please refer to the section “Function Description” for more information on “LLDP” (Link Layer Discovery Protocol).

9.3.10.2 Settings

LLDP

LLDP Settings
Neighbor

LLDP Settings

State Disable ▾

Tx Interval 30 seconds (Range: 1-3600)

Tx Hold 4 times (Range: 2-100)

Time To Live 120 seconds

Port	State
From: 1 ▾ To: 1 ▾	Enabled ▾

Apply
Refresh
Save Configurations

LLDP State

Port	Status	Port	Status
1	Enabled	2	Enabled
3	Enabled	4	Enabled
5	Enabled	6	Enabled
7	Enabled	8	Enabled
9	Enabled	10	Enabled
11	Enabled	12	Enabled

Figure 76: WBM “LLDP” Page – “Settings” Tab

Table 81: WBM “LLDP” Page – “Settings” Tab

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

9.3.11 Neighbor

LLDP

Settings
Neighbor

LLDP Neighbor Information

Port

Local Port 1	
Remote Port ID	GigabitEthernet1/0/8
Chassis ID	00-30-de-ff-f1-8c
System Name	L2SWITCH
System Description	WAGO/852-1305/000-001/V1.0.2.S0/Mon Mar 11 16:31:08 CST 2019
System Capabilities	Bridge/Switch (enabled)
Management IP	192.168.1.253
Time To Live	120 seconds

Figure 77: WBM “LLDP” Page – “Neighbor” Tab

Table 82: WBM “LLDP” Page – “Neighbor” Tab

LLDP Neighbor Information		
Parameters	Default	Description
Port	All	Select “All” in the selection box if you want to display information from all neighboring ports.
	1 ... 10 (12)	Select a port in the selection box for which you want to display the information for its neighboring port.
Local Port	1 ... 10 (12)	This field displays the port number.
Remote Port ID		This field displays the ID of the connected port.
Chassis ID		This field displays the chassis ID of the neighboring port.
System Name		This field displays the system name of the neighboring port.
System Description		This field displays the system description of the neighboring port.
System Capabilities		This field displays the system capabilities of the neighboring port.
Management Address		This field displays the management address of the neighboring port.
Time To Live		This field displays the validity period of the information of the neighboring port.

9.3.12 Loop Detection

Note



Additional Information

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

Loop Detection

Loop Detection Settings

State Disable ▾

MAC Address 00:0b:04:aa:aa:ab

Port	State	Manual Recovery	Recovery State	Recovery Time (min)
From: 1 ▾ To: 1 ▾	Disable ▾	None ▾	Enable ▾	1 (Range: 1-60)

Apply
Refresh
Save Configurations

Loop Detection Status

Port	State	Status	Recovery State	Recovery Time (min)
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
9	Disabled	Normal	Enabled	1
10	Disabled	Normal	Enabled	1
11	Disabled	Normal	Enabled	1
12	Disabled	Normal	Enabled	1

Figure 78: WBM “Loop Detection” Page

Table 83: WBM “Loop Detection” Page

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

9.3.13 Jet Ring

Jet Ring

Jet Ring Setting

State

Enable ▼

Master Bridge MAC

00:30:DE:FF:DD:16

Jet Ring Total Nodes

1

Bridge Role

Learning...

Jet Ring Status

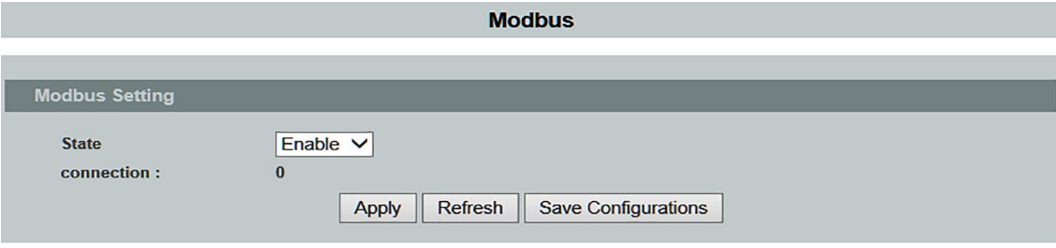
Port	Port Status	Ring Port
1	Forwarding	
2	No connection	
3	No connection	
4	No connection	
5	No connection	
6	No connection	
7	Forwarding	
8	No connection	
9	No connection	
10	No connection	

Figure 79: WBM “Jet Ring” Page

Table 84: WBM “Jet Ring” Page

Jet Ring Setting		
Parameters	Default	Description
State	Disable	In this selection box, select “Disable” to disable the “Jet Ring” function on individual ports.
	Enable	In this selection box, select “Enable” to enable the “Jet Ring” function on individual ports.
Master Bridge MAC		This field displays the IP address of the Jet Ring Master.
Jet Ring Total Nodes		This field displays the number of switches in the Jet Ring.
Bridge Role		This field displays the function of the switch in the Jet Ring.
Jet Ring Status		
Parameters	Default	Description
Port	1 ... 10 (12)	This column displays the port numbers.
Port Status	No connection Forwarding Blocking	This column displays the port status.
Ring Port	Yes	This column displays if the port operates in a ring.

9.3.14 MODBUS



Modbus

Modbus Setting

State Enable ▾

connection : 0

Apply Refresh Save Configurations

Figure 80: WBM “MODBUS” Page

Table 85: WBM “MODBUS” Page

MODBUS Settings		
Parameters	Default	Description
State	Disable	Select “Disable” in the selection box to disable the “MODBUS” function on individual ports.
	Enable	Select “Enable” in the selection box to enable the “MODBUS” function on individual ports.

9.3.14.1 STP



Note

Additional Information
Please refer to the section “Function Description” for more information on “STP” (Spanning Tree Protocol).

9.3.14.2 General Settings

Spanning Tree Protocol

General Settings Port Parameters STP Status

Spanning Tree Protocol Settings

State

Disable ▾

Mode

RSTP ▾

Bridge Parameters

Forward Delay

15

(Range:4-30)

Max Age

20

(Range:6-40)

Hello Time

2

(Range:1-10)

Priority

32768

(Range:0-61440)

Pathcost Method

Short ▾

Relationships:
2*(Forward Delay-1) >= Max Age
Max Age >= 2*(Hello Time+1)

Apply

Refresh

Save Configurations

Figure 81: WBM “STP” Page – “General Settings” Tab

Table 86: WBM “STP” Page – “General Settings” Tab

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

9.3.14.3 Port Parameters

Spanning Tree Protocol

General Settings
Port Parameters
STP Status

Port Parameters Settings

Port	Active	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
From: 1 ▼ To: 1 ▼	Enable ▼	4	128	Disable ▼	Disable ▼	Disable ▼	Disable ▼

Apply
Refresh
Save Configurations

Port Status

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

Figure 82: WBM “STP” Page – “Port Parameters” Tab

Table 87: WBM “STP” Page – “Port Parameters” Tab

Port Parameters Settings			
Parameters		Default	Description
Port	From:	1	Select a port or port range in the selection box to configure the “STP Function”.
	To:	1	Select a port or port range in the selection box to configure the “STP Function”.
Active		Enable	Select “Enable” in the selection box if you want to enable the STP function for the specific port.
		Disable	Select “Disable” in the selection box if you want to disable the STP function for the specific port.
Path Cost		250	Enter the value for the path costs for the specific port in the input field.
Priority		128	Enter the value for the priority for the specific port in the input field.
Edge Port		Disable	Select “Disable” in the selection box to disable the “Edge Port” 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			
Parameters		Default	Description
Port		1 ... 10 (12)	This column displays the port numbers.
Active		Enable Disable	This column displays the status of the STP function.
Role		Alternated Designated Root Backup None	This column displays the role of the port.
Status		Discarding Blocking Listening Learning Forwarding Disabled	This column displays the port status.
Path Cost		0 ... 65535	This column displays the path cost of the port.
Priority		0 ... 61440	This column displays the port priority.
Edge Port		Disable Enable	This column displays the status of the “Edge Port” function.
BPDU Filter		Disable Enable	This column displays the status of the BPDU filter function.
BPDU Guard		Disable Enable	This column displays the status of the “BPDU Guard” function.

Table 87: WBM “STP” Page – “Port Parameters” Tab

ROOT Guard	Disable Enable	This column displays the status of the “Root Guard” function.

9.3.15 STP Status

Spanning Tree Protocol

General Settings

Port Parameters

STP Status

Current Root Status

MAC Address	Priority	Max Age	Hello Time	Forward Delay
00:30:de:ff:f1:8c	32768	20	2	15

Current Bridge Status

MAC Address	Priority	Max Age	Hello Time	Forward Delay	Path Cost	Root Port
00:30:de:ff:f1:9b	32768	20	2	15	4	1

Refresh

Figure 83: WBM “STP” Page – “STP Status” Tab

Table 88: WBM “STP” Page – “STP Status” Tab

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

9.3.16 Xpress Ring

Note



Additional Information

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

Xpress Ring

Xpress Ring Settings

Global State : Disabled ▾

	Ring1	Ring2
State	Disabled ▾	Disabled ▾
Destination MAC (Last byte)	f0	f1
Role	Forwarder ▾	Forwarder ▾
Primary Port	None ▾	None ▾
Secondary Port	None ▾	None ▾

Apply Refresh Save Configurations

Xpress Ring Status

	Ring1	Ring2
State	Disabled	Disabled
Destination MAC	01:80:c2:ff:ff:f0	01:80:c2:ff:ff:f1
Role	Forwarder	Forwarder
Primary Port	N/A (No connection)	N/A (No connection)
Secondary Port	N/A (No connection)	N/A (No connection)

Figure 84: WBM “Xpress Ring” Page

Table 89: WBM “Xpress Ring” Page

Xpress Ring Settings		
Parameters	Default	Description
Global State	Disabled	Select “Disable” in the selection box to disable the “Xpress Ring” function.
	Enabled	Select “Enable” in the selection box to enable the “Xpress Ring” function.
Ring 1		This column can be used to configure Ring 1.
Ring 2		This column can be used to configure Ring 2.
Status	Disabled	Select “Disable” in the selection box to disable the “Xpress Ring” function for the respective ring.
	Enabled	Select “Enable” in the selection box to enable the “Xpress Ring” function for the respective ring.
Destination MAC (Last byte)		Enter the MAC address of the respective ring in the input field.
Role	Forwarder	Select the “Forwarder” role for the switch in the selection box.
	Arbiter	Select the “Arbiter” role for the switch in the selection box.
Primary Port	None	Select “None” in the selection box if you do not want to enable a primary port in the ring.
	1 ... 10 (12)	Select the respective primary port in the selection box.
Secondary Port	None	Select “None” in the selection box if you do not want to enable a secondary port in the ring.
	1 ... 10 (12)	Select the respective secondary port in the selection box.
Xpress Ring Status		
Parameters	Default	Description
Status	Disabled Enabled	This field displays the current status of the Xpress Ring.
Ring 1		This column displays the configurations for Ring 1.
Ring 2		This column displays the configurations for Ring 2.
Destination MAC (Last byte)		This field displays the last byte of the respective MAC address of the Xpress Ring.
Role	Forwarder Arbiter	This field displays the role of switch.
Primary Port	N/A (No connection) 0 ... 10 (12) (Forwarding, Blocking)	This field displays the status of the primary port.
Secondary Port	N/A (No connection) 0 ... 10 (12) (Forwarding, Blocking)	This field displays the status of the secondary port.

9.4 Security

9.4.1 IP Source Guard



Note

Additional Information

Please refer to the section “Function Description” for more information on “IP Source Guard”.

9.4.1.1 DHCP Snooping



Note

Additional Information

Please refer to the section “Function Description” for more information on “DHCP Snooping” (**D**ynamic **H**ost **C**onfiguration **P**rotocol).

9.4.1.1.1 DHCP Snooping

DHCP Snooping	
DHCP Snooping	Port Settings Server Screening
DHCP Snooping Settings	
State	Disable ▼
VLAN State	Add ▼
Apply Refresh Save Configurations	
DHCP Snooping State	
DHCP Snooping State	Disable
Enabled on VLAN	None

Figure 85: WBM “DHCP Snooping” Page – “DHCP Snooping” Tab

Table 90: WBM “DHCP Snooping” Page – “DHCP Snooping” Tab

DHCP Snooping Settings		
Parameters	Default	Description
State	Disable	Select “Disable” in the selection box if you do not want to use this function.
	Enable	Select “Enable” in the selection box to enable the “DHCP Snooping”. You must then enable this function for specific VLANs and configure “Trusted Ports”.
	Note 	Note Configuring DHCP requests The switch drops all DHCP requests when “DHCP Snooping” is enabled and there are no “Trusted Ports”. Select “Disable” if you do not want to use this function.
VLAN State	Add	Select “Add” in the selection box and enter the VLANs for which “DHCP Snooping” should be enabled. Valid range of VLAN IDs: 1 ... 4094. Use a comma (,) or hyphen (-) to specify individual VLANs or VLAN ranges.
	Delete	Select “Delete” in the selection box and enter the VLANs for which “DHCP Snooping” should be disabled.
DHCP Snooping Status		
Parameters	Default	Description
DHCP Snooping Status	Disable Enable	This field displays if “DHCP Snooping” is enabled or disabled.
Enabled on VLAN	None 1 ... 4094	This field displays the VLANs in which the “DHCP Snooping” function is enabled. “None” is displayed if no VLANs have been specified.

9.4.1.1.2 Port Settings

DHCP Snooping

DHCP Snooping
Port Settings
Server Screening

Port Settings

Port

From: To:

Trust

Maximum Host Count

(Range: 1-32)

Port Status

Port	Trust	Maximum Host Count	Port	Trust	Maximum Host Count
1	No	32	2	No	32
3	No	32	4	No	32
5	No	32	6	No	32
7	No	32	8	No	32
9	No	32	10	No	32
11	No	32	12	No	32

Figure 86: WBM “DHCP Snooping” Page – “Port Settings” Tab

Table 91: WBM “DHCP Snooping” Page – “Port Settings” Tab

Port Settings			
Parameters		Default	Description
Port	From:	1	Select a port or port range in the selection box for which you want to specify the maximum number of hosts.
	To:	1	Select a port or port range in the selection box for which you want to specify the maximum number of hosts.
Trust		No	Select “No” in the selection box if the specific port should not be a “Trusted Port”.
		Yes	Select “Yes” in the selection box if the specific port should be a “Trusted Port”.
Maximum Host Count (Range: 1~32)		32	Enter the maximum number of hosts in the input field that can be connected to a port at the same time. Valid range: 1 ... 32
Port Status			
Parameters		Default	Description
Port		1 ... 10	This column displays the port numbers.
Trust		No Yes	This column displays the status of the “Trusted Ports”.
Maximum Host Count			This column displays the maximum number of hosts that can be connected to a port at the same time.

9.4.1.1.3 Server Screening

Note



Additional Information

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

DHCP Snooping		
DHCP Snooping	Port Settings	Server Screening
Server Screening Setting		
IP Address		
Apply Refresh Save Configurations		
Server Screening List		
No.	IP Address	Action
1	225.225.225.225	Delete

Figure 87: WBM “DHCP Snooping” Page – “Server Screening” Tab

Table 92: WBM “DHCP Snooping” Page – “Server Screening” Tab

Server Screening Setting		
Parameters	Default	Description
IP Address		Enter the IP address of a valid DHCP server in this input field.
Server Screening List		
Parameters	Default	Description
No.		This column displays the index number of the DHCP server entry. Click the number to modify the entry.
IP Address		This column displays the IP address of the DHCP server.
Action		Click [Delete] to delete a specific entry.

9.4.1.2 Binding Table



Note

Additional Information

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

9.4.1.2.1 Static Entry

DHCP Snooping Binding Table

Static Entry Settings
Binding Table

Static Entry Settings

MAC Address

IP Address

VLAN ID

Port

1
▼

Static Binding Table

No.	MAC Address	IP Address	Lease(hour)	VLAN	Port	Type	Action

Figure 88: WBM “Binding Table” Page – “Static Entry” Tab

Table 93: WBM “Binding Table” Page – “Static Entry” Tab

Static Entry Settings		
Parameters	Default	Description
MAC Address		Enter the source MAC address for the binding in this input field.
IP Address		Enter the IP address assigned to the source MAC address for the binding.
VLAN ID		Enter the source VLAN ID for the binding in this input field.
Port	1 ... 10	Select the physical port of the binding in the selection box.
Static Binding Table		
Parameters	Default	Description
No.	1 ... 10	This column displays the sequential numbers for each binding. Click to update the existing entries.
MAC Address		This column displays the MAC address for the binding.
IP Address		This column displays the IP address assigned to the source MAC address for the binding.
Lease (hour)		This column displays how long the binding is valid.
VLAN		This column displays the source VLAN ID for the binding.
Port	1 ... 10	This column displays the port number for the binding.
Type	Static Dynamic	This column displays how the binding was communicated to the switch. “Static”: This binding was manually entered by an administrator. “Dynamic”: This binding was entered by information from “DHCP Snooping”.
Action		Click [Delete] to delete a specific entry.

9.4.1.2.2 Binding Table

DHCP Snooping Binding Table

Static Entry Settings
Binding Table

DHCP Snooping Binding Table

Show Type

All ▼

Show

*You can select the dynamic entry and convert it to static status.

*All ☐	MAC Address	IP Address	Lease(hour)	VLAN	Port	Type

Apply

Refresh

Save Configurations

Figure 89: WBM “Binding Table” Page – “Binding Table” Tab

Table 94: WBM “Binding Table” Page – “Binding Table” Tab

DHCP Snooping Binding Table		
Parameters	Default	Description
Show Type	All	Select “All” in the selection box if you want to display all binding table entries.
	Dynamic	Select “Dynamic” in the selection box if you want to display the dynamic binding table entries.
	Static	Select “Static” in the selection box if you want to display the static binding table entries.
Parameters	Default	Description
All	1 ... 10	This column displays the sequential numbers for each binding. Click to update the existing entries.
MAC Address		This column displays the MAC address for the binding.
IP Address		This column displays the IP address assigned to the source MAC address for the binding.
Lease (hour)		This column displays how long the binding is valid.
VLAN		This column displays the source VLAN ID for the binding.
Port		This column displays the port number for the binding. If this field is empty, the binding applied to all ports.
Type	Static Dynamic	This column displays how the binding is communicated to the switch. “Static”: This binding was manually entered by an administrator. “Dynamic”: This binding was entered by information from “DHCP Snooping”.

9.4.1.3 ARP Inspection



Note

Additional Information

Please refer to the section “Function Description” for more information on “ARP Inspection” (“**Address Resolution Protocol Inspection**”).

9.4.1.3.1 ARP Inspection

ARP Inspection

ARP Inspection **Filter Table**

ARP Inspection Settings

State

Disable ▾

VLAN State

Add ▾

Trusted Ports

☐ Select All

☐ Deselect All

☐ 1 ☐ 3 ☐ 5 ☐ 7 ☐ 9 ☐ 11

☐ 2 ☐ 4 ☐ 6 ☐ 8 ☐ 10 ☐ 12

Apply

Refresh

Save Configurations

ARP Inspection State

ARP Inspection State	Disable
Enabled on VLAN	None
Trusted Ports	None

Figure 90: WBM “ARP Inspection” Page – “ARP Inspection” Tab

Table 95: WBM “ARP Inspection” Page – “ARP Inspection” Tab

ARP Inspection Settings				
Parameters		Default	Description	
State		Disable	Select “Disable” in the selection box if you want to disable ARP inspection on the switch.	
		Enable	Select “Enable” in the selection box if you want to enable ARP inspection on the switch.	
VLAN State		Add	Select “Add” in the selection box and enter the VLANs for which “ARP Inspection” should be enabled on the switch. Valid range of VLAN IDs: 1 ... 4094. Use a comma (,) or hyphen (-) to specify individual VLANs or VLAN ranges.	
		Delete	Select “Delete” in the selection box and enter the VLANs on which the switch should not run “ARP Inspection”.	
Trusted Ports			Select the ports that you want to select or deselect as “Trusted Ports”. The switch does not drop ARP packets from “Trusted Ports” for any reason. The switch discards DHCP packets from “Untrusted Ports” in the following situations: - The sender information in an ARP packet does not match any current bindings. - The transmission rate of the DHCP packets received are too high. You can specify the maximum rate for receiving packets on “Untrusted Ports”.	
	Select All	☐	☐	No port is selected as “Trusted”.
			☒	All ports are selected as “Trusted”.
	Deselect All	☐	☐	No port is disabled as “Trusted”.
			☒	All ports are disabled as “Trusted”.
	☐ 1 ... ☐ 10	☐	☐	The port is not enabled.
			☒	The port is enabled.
ARP Inspection Status				
Parameters		Default	Description	
ARP Inspection State		Disable Enable	This field displays the current status of the ARP inspection.	
Enabled on VLAN		None 1 ... 10	This field displays the VLAN IDs for which ARP Inspection is enabled.	
Trusted Ports		Nonr 1 ... 10	This field displays the ports specified as “Trusted Ports”.	

9.4.1.3.2 Filter Table



Note

Additional Information

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

Figure 91: WBM “ARP Inspection” Page – “Filter Table” Tab

Table 96: WBM “ARP Inspection” Page – “Filter Table” Tab

Filter Age Time Settings		
Parameters	Default	Description
Filter Age Time min (Range: 1~10080)	5	Enter a time (1 to 10,080 minutes) in the input field for how long a MAC address filter entry should remain in the switch after the switch has received an unauthorized ARP packet. Once the time has elapsed, the switch deletes the entry automatically. This setting has no effect on existing MAC address filters.
Filter Table		
Parameters	Default	Description
No.		This column displays the sequential number of each MAC address filter entry.
MAC Address		This column displays the source MAC address in the MAC address filter.
VLAN		This column displays the source VLAN IDs in the MAC address filter.
Port		This column displays the source ports of the dropped ARP packets.
Expiry (min)		This column displays how long (in minutes) a MAC address filter entry remains in the switch.
Action		Click [Delete] to delete a specific entry.
Total		This field displays the total number of current MAC address filter entries that the switch created due to identified unauthorized ARP packets.

9.4.2 Access Control List

Note



Additional Information

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

Access Control List

Access Control List Settings

IP Type IPv4 ▾

Profile Name

Ethernet Type Any ▾

Source MAC Address Any ▾

Destination MAC Address Any ▾

DSCP Any ▾ 0 ▾

Source IP Any ▾

Destination IP Address Any ▾

IP Protocol Any ▾

Source Application Any ▾

Destination Application Any ▾

Source Interface Any ▾ -- ▾

Action Disable ▾

VLAN Any ▾

Mask of Source MAC Address

Mask of Destination MAC Address

Mask of Source IP Address

Mask of Destination IP Address

Apply Refresh Save Configurations

Access Control List Status

IP Type	IPv4	Action	Disable
Profile Name	521582	VLAN	Any
Ethernet Type	Any		
IP Protocol	Any		
Source MAC Address	Any	Mask of Source MAC Address	None
Destination MAC Address	Any	Mask of Destination MAC Address	None
DSCP	Any		
IP Protocol	Any		
Source IP	Any	Mask of Source IP Address	None
Destination IP Address	Any	Mask of Destination IP Address	None
Source Application	10	Destination Application	Any
Source Application	Any		

Delete

Figure 92: WBM “Access Control List” Page

Table 97: WBM "Access Control List" Page

Access Control List Settings			
Parameters	Default	Description	
Profile Name		Enter the name of the profile in the input field.	
Action	Disable	Select "Disable" in the selection box to disable access control.	
	Permit	Select "Permission" in the selection box to forward data packet that match the information.	
	Drop	Select "Drop" in the selection box to drop data packet that match the information.	
	DSCP	Select "DSCP" to give data packet a new priority that match the information (only IPv4).	
ETHERNET Type (only IPv4)	Any	Select "any" in the selection box, so every ETHERNET type is valid.	
	Other	Select "Other" in the selection box to specify an ETHERNET type for which access control is valid.	
VLAN	Any	Select "any" in the selection box, so every VLAN ID is valid.	
	Other	Select "Other" in the selection box to enter a specific VLAN ID in the access control list.	
Source MAC (only IPv4)	Any	Select "any" in the selection box, so every MAC address is valid.	
	Other	Select "Other" in the selection box to enter the MAC address for the source in the access control list.	
Mask of Source MAC (only IPv4)		In the input field, enter the source MAC ID of the bitmap mask for source MAC addresses of packets to be filtered. If you selected "any" in the "Source MAC Address" selection box, the field remains empty. The profile then only filters the MAC address entered in the source MAC address field.	
Destination MAC (only IPv4)	Any	Select "any" in the selection box, so every MAC address is valid.	
	Other	Select "Other" in the selection box to enter the destination MAC address in the access control list.	
Mask of Destination MAC (only IPv4)		In the input field, enter the destination MAC address of the bitmap mask for designation MAC addresses of packets to be filtered. If you selected "Destination MAC Address" in the selection box, the field remains empty. The profile then only filters the MAC address entered in the designation MAC address field.	
DSCP (only IPv4)	Any	Select "any" in the selection box, so every DSCP priority for the access control list is valid.	
	Other	0 ... 63	Select the DSCP priority in the selection box.
Source IP	Any	Select "any" in the selection box, so every IP address is valid.	
	Other	Select "Other" in the selection box to enter the source IP address in the access control list.	
Mask of Source IP		In the input field, enter the source IP address of the bitmap mask for source IP addresses of packets to be filtered. If you selected "Source IP" in the selection box, the field remains empty. The profile then only filters the IP address entered in the source IP address field.	

Table 97: WBM "Access Control List" Page

Destination IP	Any	Select "any" in the selection box, so every IP address is valid.	
	Other	Select "Other" in the selection box to enter the destination IP address in the access control list.	
Mask of Destination IP		In the input field, enter the destination IP address of the bitmap mask for designation IP addresses of packets to be filtered. If you selected "Destination IP Address" in the selection box, the field remains empty. The profile then only filters the IP address entered in the destination IP address field.	
IP Protocol	Any	Select "any" in the selection box, so every IP protocol for the access control list is valid.	
	Other	Enter "Other" in the selection box to enter the protocol.	
Source Application	Any	Select "any" in the selection box, so every application is valid.	
	Other	Select "Other" in the selection box to enter the source port (e.g., 2234).	
Destination Application	Any	Select "any" in the selection box, so every target application is valid.	
	Other	Select "Other" in the selection box to enter the destination port (e.g., 502) in the access control list.	
Source Interface	Any	Select "any" in the selection box, if every physical port is valid.	
	Other	1 ... 10	Enter the physical port in the input field for which this entry is valid in the access control list.
Access Control List Status			
Parameters	Default	Description	
IP-Type	IPv4 IPv6	This field displays the selected IP Type.	
Profile Name		This field displays the selected name of the profile.	
Action	Disable Permit Drop DSCP	This field displays the status of the access control. (DSCP only at IPv4).	
ETHERNET Type (only IPv4)	Any Other	This field displays the ETHERNET type.	
VLAN	Any Other	This field displays the VLAN ID.	
IP Protocol	Any Other	This field displays the IP protocol.	
Source MAC (only IPv4)	Any Other	This field displays the source MAC address.	
Mask of Source MAC (only IPv4)		This field displays the source MAC ID of the bitmap mask.	
Destination MAC (only IPv4)	Any Other	This field displays the destination MAC address.	
Mask of Destination MAC (only IPv4)		This field displays the destination MAC ID of the bitmap mask.	
DSCP (only IPv4)	Any Other	This field displays the DSCP priority.	
IP Protocol	Any Other	This field displays the IP protocol.	

Table 97: WBM "Access Control List" Page

Source IP	Any Other	This field displays the source IP.
Mask of Source IP		This field displays the source MAC ID of the bitmap mask.
Destination IP	Any Other	This field displays the destination IP address.
Mask of Destination IP		This field display the destination IP ID of the bitmap mask.
Source Application	Any Other	This field display the source application.
Destination Application	Any Other	This field displays the target application.
Source Application	1 ... 10	This field display the source application.

9.4.3 802.1x



Note

Additional Information

Please refer to the section “Function Description” for more information on the “IEEE 802.1x” standard.

9.4.3.1 Global Settings

IEEE802.1X

Global Settings
Port Settings

Global Settings

State	Disable ▾		
Authentication Method	Local ▾		
Guest VLAN	0		
Primary Radius Server	IP :	UDP Port :	Shared Key :
Secondary Radius Server	IP :	UDP Port :	Shared Key :
Local Authentic User	None ▾		
	User Name :		
	Password :		

Apply

Refresh

Save Configurations

Global Status

State	Disable		
Authentication Method	Local		
Guest VLAN	0		
Primary Radius Server	IP : -	UDP Port : -	Shared Key : -
Secondary Radius Server	IP : -	UDP Port : -	Shared Key : -
Local Authentic User	admin,		

Figure 93: WBM “802.1x” Page – “Global Settings” Tab

Table 98: WBM “802.1x” Page – “Global Settings” Tab

Global Settings			
Parameters		Default	Description
State	Disable		Select “Disable” in the selection box to disable 802.1x authentication on the switch.
	Enable		Select “Enable” in the selection box to enable 802.1x authentication on the switch.
	Note 		Note 802.1x Authentication You must first enable 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 node 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.
Guest VLAN			This field is used to configure the VLAN ID.
Primary Radius Server			If you select “Radius” for the authentication method, the primary RADIUS server is used for all authentication requests.
	IP:		In the input field, enter the IP address of the external RADIUS server in decimal-point notation.
	UDP Port:		Enter the UDP port in the input field.
	Shared Key:		Enter a password (up to 32 alphanumeric characters) in the input field to use as the common key for the connection between the external RADIUS server and the switch. This key may not be sent over the network. The key must be identical on the external RADIUS server and the switch.

Table 98: WBM “802.1x” Page – “Global Settings” Tab

Secondary Radius Server			This is the back-up server that is only used if the primary RADIUS server fails.	
	IP:		In the input field, enter the IP address of the external RADIUS server in decimal-point notation.	
	UDP Port:	0 ... 65535	Enter the port number of the RADIUS server in the input field.	
	Shared Key:		Enter a password (up to 32 alphanumeric characters) in the input field to use as the common key for the connection between the external RADIUS server and the switch. This key may not be sent over the network. The key must be identical on the external RADIUS server and the switch.	
Authentication Method			The user name and password are displayed, added or deleted in these input fields.	
		None	If you selected “None” in the selection box, you then cannot change the user name and password.	
		Delete	User Name:	If you selected “Delete” in the selection box, you can change the user name.
		Add	Password:	If you selected “Add” in the selection box, you can change the user name and password.
Global Status				
Parameters		Default	Description	
State		Disable Enable	This field indicates if 802.1x authentication is enabled or disabled.	
Authentication Method		Local Radius	This field displays the authentication method.	
Guest VLAN			This field displays the guest VLAN.	
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 executed.	
	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 executed.	
	UDP Port:			
	Shared Key:			
Local Authentic User		admin,	This field displays the list of users logged in.	

9.4.3.2 Port Settings

IEEE802.1X

Global Settings
Port Settings

Port Settings

Port From: 1 To: 1
IEEE802.1X State Disable

Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times
Both	Disable	Auto	Disable	2

Reauth-period	Quiet-period	Supp-timeout	Server-timeout	Reset to Default
3600	20	30	16	☐

Note : Please don't set "enable" on all ports at the same time.

Apply
Refresh
Save Configurations

Port Status

Port	IEEE802.1X State	Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times	Reauth-period	Quiet-period	Supp-timeout	Server-timeout
1	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
2	Enable	Both	Disable	Auto	Disable	2	3600	20	30	16
3	Enable	Both	Disable	Auto	Disable	2	3600	20	30	16
4	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
5	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
6	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
7	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
8	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
9	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
10	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
11	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16
12	Disable	Both	Disable	Auto	Disable	2	3600	20	30	16

Figure 94: WBM "802.1x" Page – "Port Settings" Tab

Table 99: WBM “802.1x” Page – “Port Settings” Tab

Port Settings			
Parameters		Default	Description
Port	From:	1	Select a port or port range in the selection box to configure the “Port Settings”.
	To:	1	Select a port or port range in the selection box to configure the “Port Settings”.
802.1x State		Disable	Select “Disable” in the selection box to disable this function.
		Enable	Select “Enable” in the selection box to enable 802.1x authentication for the port. You must first enable 802.1x authentication on the switch before you can configure this function for individual ports.
Admin Control Direction		Both	Select “Both” in the selection box if both incoming and outgoing packets should be dropped if 802.1x port authentication of a user fails.
		In	Select “Input” in the selection box if only incoming packets should be dropped if 802.1x port authentication of a user fails.
Reauthentication		Disable	Select “Disable” in the selection box if a subscriber does not regularly enter the user name and password to remain connected to the port.
		Enable	Select “Enable” in the selection box if a subscriber regularly enters 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.
Guest VLAN		Ausschalten	Select “Disable” in the selection box to disable the guest VLAN on the port.
		Einschalten	Select “Enable” in the selection box to enable the guest VLAN on the port.
Max-req Times		2	Enter a value for the maximum required time in the input field that the switch should attempt to connect to the authentication server before it sees the server as not connected.
Reauth-period		3600	Enter a value for the time in the input field during which a subscriber has to enter the user name and password to remain connected to the port.
Quiet-period		60	Enter a value for the time in the input field that the client must wait before it can request authentication again. This prevents the switch from becoming overloaded with continuous authentication attempts from the client.
Supp-timeout		30	Enter a value for the time in the input field that the switch must wait before it can communicate with the server.
Server-timeout		30	Enter a value for the time in the input field that the switch should wait for a response from the authentication server.

Table 99: WBM “802.1x” Page – “Port Settings” Tab

Reset to Default	☐	☐	No custom settings for 802.1x port authentication are reset to the default values.
		☒	The custom settings for 802.1x port authentication are reset to the default values.
Port Status			
Parameters	Default	Description	
Port	1 ... 10	This column displays the port numbers.	
802.1x State	Disable Enable	This column displays if 802.1x authentication for a port is enabled or disabled.	
Admin Control Direction	Both In	This column displays the “Admin Control Direction”.	
Reauthentication	Disable Enable	This column displays if the subscriber has to enter the user name and password regularly to remain connected to the port.	
Port Control Mode	Auto, Force Authorized, Force Unauthorized	This column displays the port control mode.	
Guest VLAN	Disable Enable	This column displays the guest VLAN setting for hosts where authentication failed.	
Max-req Times	1 ... 10	This column displays how often the switch attempts to connect to the authentication server before it sees the server as not connected.	
Reauth-period	0 ... 65535	This column displays at what interval a subscriber must enter the user name and password to remain connected to the port.	
Quiet-period	0 ... 65535	This column displays the time that a client must wait before it can request authentication again.	
Supp-timeout	0 ... 65535	This column displays how long the switch should wait before communicating with the switch.	
Server-timeout	0 ... 65535	This column displays how long the switch should wait before communicating with the client.	

9.4.4 Port Security



Note

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

Port Security

Sticky MAC Settings

Port Security Settings

Port Security

Disable

Port	State	Sticky State	Maximum MAC
From: 1 To: 1	Disable	Disable	5 (1~1000)

Apply

Refresh

Save Configurations

Port Security Status

Port	State	Sticky State	Maximum MAC	Port	State	Sticky State	Maximum MAC
1	Disable	Disable	5	2	Disable	Disable	5
3	Disable	Disable	5	4	Disable	Disable	5
5	Disable	Disable	5	6	Disable	Disable	5
7	Disable	Disable	5	8	Disable	Disable	5
9	Disable	Disable	5	10	Disable	Disable	5
11	Disable	Disable	5	12	Disable	Disable	5

Figure 95: WBM “Port Security” Page

Table 100: WBM "Port Security" Page

Port Security Settings			
Parameters		Default	Description
Port Security		Disable	Select "Disable" in the selection box to disable port security on the switch.
		Enable	Select "Enable" in the selection box to enable port security on the switch.
Port	From:	1	Select a port or port range in the selection box to configure the "Port Security".
	To:	1	Select a port or port range in the selection box to configure the "Port Security".
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 (1~30)		5	Enter the maximum number of MAC addresses per interface in the input field.
Port Security Status			
Parameters		Default	Description
Port		1 ... 10	This column displays the port numbers.
State		Enable Disable	This column displays if port security is enabled or disabled.
Maximum MAC		0 ... 30	This column displays the maximum number of MAC addresses.

9.5 Monitor

9.5.1 Alarm Information



Note

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

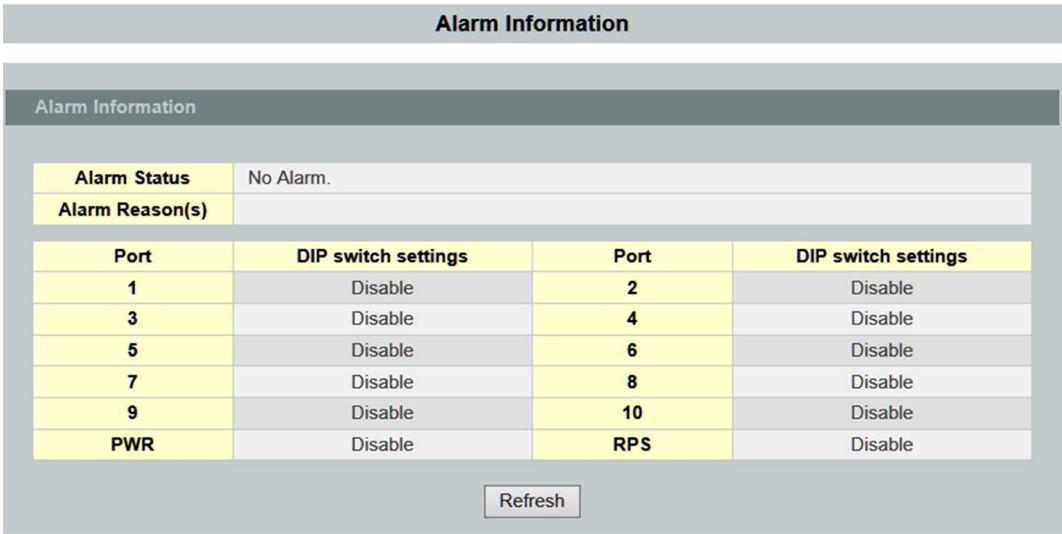


Figure 96: WBM “Alarm Information” Page

Table 101: WBM “Alarm Information” Page

Alarm Information		
Parameters	Default	Description
Alarm Status		This display field shows if there are any alarm events.
Alarm Reason(s)		This display field shows details about the alarm events.
Port	0 ... 10 PWR RPS	This column displays the DIP switch name.
DIP switch settings	Enable Disable	This column displays the current status of the DIP switch.

9.5.2 Monitor Information

Note



Additional Information

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

Monitor Information

Temperature unit: Celsius(C)

Hardware-Monitor Alarm: Enable

Hardware Information:

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

Apply
Refresh
Save Configurations

Figure 97: WBM “Monitor Information” Page

Table 102: WBM "Monitor Information" Page

Hardware Information		
Parameters	Default	Description
Temperature unit	Celsius (C)	Select "Celsius (C)" in the selection box if you want to display the temperature in Celsius.
	Fahrenheit (F)	Select "Fahrenheit (F)" in the selection box if you want to display the temperature in Fahrenheit.
Hardware Working Information		
Parameters	Default	Description
Temperature (C)		
Current		This column displays the current temperature of the "BOARD", "CPU" and "PHY" MAC chip.
MAX		This column displays the maximum temperature of the "BOARD", "CPU" and "PHY" MAC chip.
MIN		This column displays the minimum temperature of the "BOARD", "CPU" and "PHY" MAC chip.
Threshold		This column displays the threshold set.
Status		This column displays the status.
Voltage (V)		
Current		This column displays the current voltage of the "1.0 V IN", "2.5 V IN" and "3.3 V IN" inputs.
MAX		This column displays the maximum voltage of the "1.0 V IN", "2.5 V IN" and "3.3 V IN" inputs.
MIN		This column displays the minimum voltage of the "1.0 V IN", "2.5 V IN" and "3.3 V IN" inputs.
Threshold		This column displays the threshold set.
Status		This column displays the status.

9.5.3 Port Statistics

Note



Additional Information

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

Port Statistics								
Port Statistics								
Port	Receive Drops	Transmit Drops	Receive Errors	Transmit Errors	Receive Packets	Transmit Packets	Receive Bytes	Transmit Bytes
1	0	0	0	0	162814	219841	23349083	38610264
8	0	0	0	0	821080	871944	135804810	121615480
11	0	0	0	0	52356	922	3870714	118703
Refresh Clear								

Figure 98: WBM “Port Statistics” Page

Table 103: WBM “Port Statistics” Page

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

9.5.4 Port Utilization



Note

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

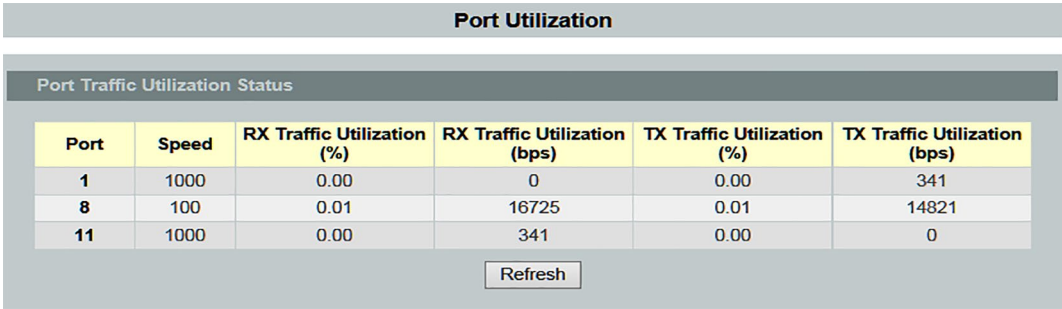


Figure 99: WBM “Port Utilization” Page

Table 104: WBM “Port Utilization” Page

Port Traffic Utilization Status		
Parameters	Default	Description
Port		This column displays the port numbers.
Speed		This column displays the transfer rate.
Traffic Utilization (%)		This column displays the percentage utilization of the bandwidth.

9.5.5 RMON Statistics



Note

Additional Information

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

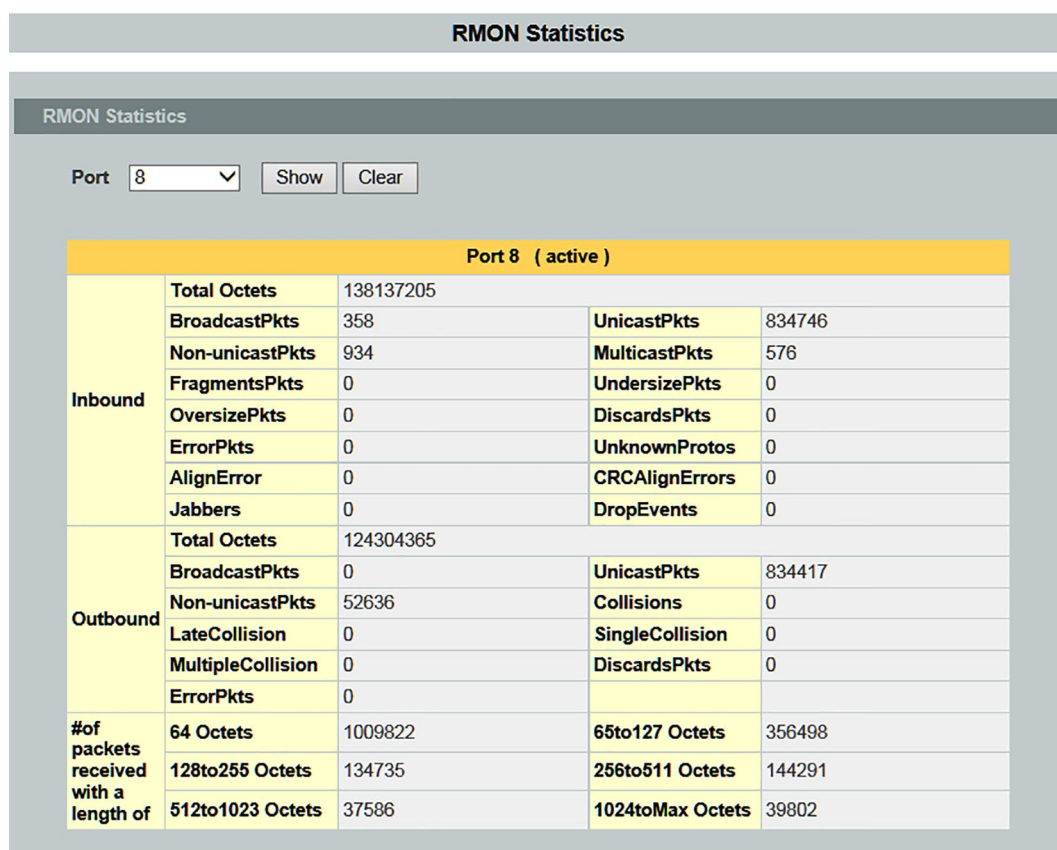


Figure 100: WBM “RMON Statistics” Page

Table 105: WBM "RMON Statistics" Page

RMON Statistics			
Parameters		Default	Description
Port		-	Select "-" in the selection box, if you do not want to view any statistics.
		1 ... 10 All	In the selection box, select a port or all ports to display their RMON statistics.
Select Port (s) (active)			
Parameters		Default	Description
Inbound	Total Octets		This display field shows the number of data packets received on the port.
	Broadcast Pkts		This display field shows the number of broadcast packets received on the port.
	Unicast Pkts		This display field shows the number of unicast packets received on the port.
	Non-unicast Pkts		This display field shows the total number of broadcast and multicast packets received on the port.
	Multicast Pkts		This display field shows the number of multicast packets received on the port.
	Fragments Pkts		This display field shows the number of fragmented data packets received on the port.
	Undersize Pkts		This display field shows the number of data packets received on the port that are too small.
	Oversize Pkts		This display field shows the number of data packets received on the port that are too large.
	Discards Pkts		This display field shows the number of data packets received on the port that were dropped.
	Error Pkts		This display field shows the number of data packets received on the port that were faulty.
	Unknown Protos		This display field shows the number of packets received by this port that contain an unknown or unsupported protocol as the target.
	Align Error		This display field shows the number of data packets received where the total number of bits of a received frame is not divisible by eight.
	CRC Align Errors		This display field shows the number of data packets received with a checksum error.
	Jabbers		This display field shows the number of jabbers received by this port.
	Drop Events		This display field shows the number of discarded data packets.

Table 105: WBM "RMON Statistics" Page

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

9.5.6 SFP Information

SFP Information

SFP Information

Port 11 Apply

SFP Information	
Fiber Cable	Link Up
Connector	LC
Wavelength	850
Transfer Distance	550m(50um, OM2), Multi mode
DDM Supported	YES (Internally Calibrated)
Vendor Name	WAGO
Vendor PN	852-1200
Vendor rev	V2.0
Vendor SN	AX15470009620
Date code	151120

DDMI Information					
	Current	High-Alarm	Low-Alarm	High-Warn	Low-Warn
Temperature(C)	50.199	90.000	-45.000	85.000	-40.000
Voltage(V)	3.264	3.600	3.000	3.500	3.100
Tx Bias(mA)	6.088	25.000	1.000	20.000	2.000
Tx Power(mW)	0.197	0.501	0.089	0.398	0.112
Tx Power(dBm)	-7.065	-3.000	-10.505	-4.001	-9.506
Rx Power(mW)	0.242	0.631	0.016	0.501	0.020
Rx Power(dBm)	-6.160	-2.004	-18.016	-3.000	-17.012

Refresh

Figure 101: WBM "SFP Information" Page

Table 106: WBM “SFP Information” Page

SFP Information		
Parameters	Default	Description
Port	-, 9, 10	Select a port number to configure.
SFP Information		
Parameters	Default	Description
Fiber Cable		This display field shows if the fiber optic cable is connected.
Connector		This display field shows the code for the optical connector type.
Wavelength (nm)		This display field shows the wave length.
Transfer Distance (nm)		This display field shows the wave length.
DDM Supported (nm)		This display field shows if the SFP module supports DDM (“Dynamic Device Mapping”).
Vendor Name (nm)		This display field shows the name of the SFP provider.
Vendor PN (nm)		This display field shows the part number.
Vendor rev (nm)		This display shows the revision status of the part number.
Vendor SN (nm)		This display field shows the serial number (ASCII).
Date code (nm)		This display field shows the date code of the manufacturer.
DDMI Information (nm)		
Parameters	Default	Description
Current (nm)		This column displays the “Current” values of temperature, voltage, Tx Bias, Tx Power and Rx Power.
High Alarm (nm)		This column displays the "High Alarm" values of temperature, voltage, Tx Bias, Tx Power and Rx Power.
Low Alarm (nm)		This column displays the "Low Alarm" values of temperature, voltage, Tx Bias, Tx Power and Rx Power.
High Warn (nm)		This column displays the "High Warning" values of temperature, voltage, Tx Bias, Tx Power and Rx Power.
Low Warn (nm)		This column displays the "Low Warning" values of temperature, voltage, Tx Bias, Tx Power and Rx Power.

9.5.7 Traffic Monitor

Note



Additional Information

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

Traffic Monitor

Traffic Monitor Settings

State Disable ▾

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

Apply
Refresh
Save Configurations

Traffic Monitor Status

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

Figure 102: WBM “Traffic Monitor” Page

Table 107: WBM "Traffic Monitor" Page

Traffic Monitor Settings		
Parameters		Default
		Description
Status		Disable
		Select "Switch OFF" in the selection box to disable the "Traffic Monitor" function globally.
		Enable
		Select "Switch ON" in the selection box to enable the "Traffic Monitor" function globally.
Port	From:	1
	To:	1
		Select a port or port range in the selection box that you want to configure.
		Select a port or port range in the selection box that you want to configure.
State		Disable
		Select "Switch OFF" in the selection box if you want to disable the "Traffic Monitor" function for the port or port range.
		Enable
		Select "Switch ON" in the selection box if you want to enable the "Traffic Monitor" function for the port or port range.
Action		None
		Select "None" in the selection box if you do not want to cancel port blocking.
		Unblock
		Select "Unblock" in the selection box if you want to cancel port blocking.
Packet Type		Broadcast
		Select "Broadcast" in the selection box, if you want to monitor this as the packet type.
		Multicast
		Select "Multicast" in the selection box, if you want to monitor this as the packet type.
		Bcast+Mcast
		Select "Bcast+Mcast" in the selection box, if you want to monitor both as the packet types.
Packet Rate (pps)		
		In the input field, enter the packet rate that you want to monitor.
Recovery State		Enable
		Select "Switch ON" in the selection box if you want to enable the "Recover" function in the "Traffic Monitor" for the port or port range.
		Disable
		Select "Switch OFF" in the selection box if you want to disable the "Recovery" function in the "Traffic Monitor" for the port or port range.
Recovery Time (min)		1 ... 60
		Enter a value in the input field for the "Recovery Time" for the "Traffic Monitor" function.
Traffic Monitor Status		
Parameters		Default
		Description
Port		1 ... 10
		This column displays the port numbers.
State		Disable Enable
		This column displays the status of the specific port.
Status		Normal
		This column displays the status of the operational state.
Packet Type		Broadcast Multicast Bcast+Mcast
		This column displays the type of data packet.
Packet Rate (pps)		
		This column displays the selected packet rate.
Recovery State		Enable Disable
		This column displays the status of the selection Recover function.
Recovery Time (min)		1 ... 60
		This column displays the selected Recovery time.

9.6 Management

9.6.1 SNMP

9.6.1.1 SNMP

9.6.1.1.1 SNMP Settings



Note

Additional Information

Please refer to the section “Function Description” for more information on “SNMP” (Simple Network Management Protocol).

The screenshot shows the 'SNMP Settings' tab in the WBM interface. The 'SNMP State' is set to 'Disable'. The 'System Name' is 'L2SWITCH'. The 'System Location' and 'System Contact' fields are empty. There are buttons for 'Apply', 'Refresh', and 'Save Configurations'.

Figure 103: WBM Page, “SNMP” – “SNMP Settings” Tab

Table 108: WBM Page, “SNMP” – “SNMP Settings” Tab

SNMP Setting		
Parameters	Default	Description
SNMP State	Disable	Select “Disable” in the selection box to disable SNMP on the switch.
	Enable	Select “Enable” in the selection box to enable SNMP on the switch.
System Name	L2SWITCH	Enter the system name for the switch in the input field. (System name and host name are identical.)
System Location	192.168.0.254	Enter the IP address (location information) of the switch in decimal-point notation.
System Contact	255.255.255.0	Enter the IP subnet mask of the switch in decimal-point notation.

9.6.1.1.2 Community Name

SNMP

SNMP Settings
Community Name

Community Name Settings

Community String	Rights	IP version	Network ID of Trusted Host	Number of Mask Bit
	Read-Only ▼	IPv4 ▼		

Community Name List

No.	Community String	Rights	IP version	Network ID of Trusted Host	Number of Mask Bit	Action

Figure 104: WBM Page, “SNMP” – “Community Name” Tab

Table 109: WBM Page, “SNMP” – “Community Name” Tab

Community Name Settings		
Parameters	Default	Description
Community String		Enter the “Community String” to act as a password for requests from the management station.
Rights	Read-Only	Select “Read Only” in the selection box so that the SNMP manager can use this string to receive information from the switch.
	Read/Write	Select “Read/Write” in the selection box so that the SNMP manager can use this string to configure settings on the switch.
IP Version	IPv4	Select “IPv4” in the selection box if you want to choose this version of the internet protocol.
	IPv6	Select “IPv6” in the selection box if you want to choose this version of the internet protocol.
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).
Mask		Enter the IP address of the subnet mask for the remote SNMP management station in decimal-point notation (e.g., 255.255.255.0).

Table 109: WBM Page, “SNMP” – “Community Name” Tab

Community Name List		
Parameters	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		This column displays the rights for the “SNMP Community String”.
IP Version	IPv4 IPv6	This column displays the selected IP Version.
Network ID of Trusted Host		This column displays the IP address of the remote SNMP management station after it has been modified by the subnet mask.
Mask		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”.

9.6.1.2 SNMP Trap

9.6.1.2.1 Trap Receiver Settings

The screenshot displays the 'SNMP Trap' configuration page. At the top, there are three tabs: 'Trap Receiver Settings' (selected), 'Trap Event State', and 'Port Trap Settings'. Below the tabs, the 'Trap Receiver Settings' section contains four input fields: 'IP Version' (set to IPv4), 'IP Address' (empty), 'Version' (set to v1), and 'Community String' (empty). Below these fields are three buttons: 'Apply', 'Refresh', and 'Save Configurations'. At the bottom, there is a 'Trap Receiver List' table with columns: No., IP Version, IP Address, Version, Community String, and Action.

Figure 105: WBM Page, “SNMP Trap” – “Trap Receiver Settings” Tab

Table 110: WBM Page, “SNMP Trap” – “Trap Receiver Settings” Tab

Trap Receiver Settings		
Parameters	Default	Description
IP Version	IPv4	Select “IPv4” in the selection box if you want to choose this version of the internet protocol.
	IPv6	Select “IPv6” in the selection box if you want to choose this version of the internet protocol.
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		
Parameters	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 Version	IPv4 IPv6	This column displays the selected IP Version.
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.

9.6.2 Auto Provision



Note

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

Auto Provision

Auto-Provison-Einstellungen

Status

Ausschalten ▾

Status

Ausschalten

Version

0

Protokoll

TFTP ▾

Protokoll

IPv4 ▾

Server-IP-Adresse

0.0.0.0

User Name

Password

Verzeichnis

Anwenden

Aktualisieren

Konfiguration speichern

Figure 106: WBM “Auto Provision” Page

Table 111: WBM “Auto Provision” Page

Auto Provision Settings		
Parameters	Default	Description
State	Disable	Select “Disable” in the selection box to disable “Auto Provision” function on the switch.
	Enable	Select “Enable” in the selection box to enable the “Auto Provision” function on the switch.
Status	Disable	This field displays the “Auto Provision” status.
Version	0	This field displays the version.
Protocol	FTP	Select “FTP” (“File Transfer Protocol”) in the selection box if you want to select this type as the Auto Provision server.
	TFTP	Select “TFTP” (“Trivial File Transfer Protocol”) in the selection box if you want to select this type as the Auto Provision server.
	HTTP	Select “HTTP” (“Hypertext Transfer Protocol”) in the selection box if you want to select this type as the Auto Provision server.
Server IP		Enter the ID for the IP subnet mask of the server in decimal-point notation.
User Name		Enter the name for the FTP server in the input field.
Password		Enter the password for the FTP server in the input field.
Folder Path		Select the folder structure of the FTP server in this input field.

9.6.3 Mail Alarm

Note



Additional Information

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

Mail Alarm

Mail Alarm Settings

State

Disable

Server IP

IP

0.0.0.0

Server Port

25

(Default:25)

Account Name

Account Password

Mail From

Mail To

UTF-8 encoding

Enable

Trap State :

☐ Select All

☐ Deselect All

☐ System Reboot

☐ Port Link Change

☐ Configuration Change

☐ Firmware Upgrade

☐ User Login

☐ Port Blocked

☐ Alarm

Apply

Refresh

Save Configurations

Figure 107: WBM “Mail Alarm” Page

Table 112: WBM "Mail Alarm" Page

Table 112: VDM Mail Alarm Page

Mail Alarm Settings				
Parameters		Default	Description	
State		Disable	Select "Disable" in the selection box to disable the "Mail Alarm" function.	
		Enable	Select "Enable" in the selection box to enable the "Mail Alarm" function.	
Server IP		IP	Select "IP" in the selection box if you want to use the server IP of the mail server.	
		IPv6	Select "IPv6" in the selection box if you want to use the server IP of the IPv6 server.	
		Domain	Select "Domain" in the selection box if you want to use the domain address of the mail server.	
		0.0.0.0	Enter the IP address in the input field.	
Server Port (Default:25)		25	Enter the TCP port for SMTP in the input field.	
Account Name			Enter the name of the e-mail account in the input field.	
Account Password			Enter the password for the e-mail account in the input field.	
Mail From			Enter the name of the e-mail sender in the input field.	
Mail To			Enter the name of the e-mail recipient in the input field.	
Trap State	Select All	☐	☐	No port has been selected for sending event traps.
			☒	All ports are selected for sending event traps.
	Deselect All	☐	☐	No port has been disabled for sending event traps.
			☒	All ports are disabled for sending event traps.
	System Reboot	☐	☐	The port is not enabled.
			☒	The port is enabled.
	Port Link Change	☐	☐	The "Port Link Change" state is disabled.
			☒	The "Port Link Change" state is enabled.
	Configuration Change	☐	☐	The "Configuration Change" state is disabled.
			☒	The "Configuration Change" state is enabled.
	Firmware Upgrade	☐	☐	The "Firmware Upgrade" state is disabled.
			☒	The "Firmware Upgrade" state is enabled.
	User Login	☐	☐	The "User Login" state is disabled.
			☒	The "User Login" state is enabled.
	Port Blocked	☐	☐	The "Port Blocked" state is disabled.
			☒	The "Port Blocked" state is enabled.
	Alarm	☐	☐	The "Alert" state is disabled.
			☒	The "Alert" state is enabled.

9.6.4 Maintenance

9.6.4.1 Configuration

The screenshot displays the 'Maintenance' section of the WBM page, specifically the 'Configuration' tab. It features four sub-sections: 'Save Configurations', 'Upload and Download Configurations', 'Reset Configurations', and 'The configurations status'. The 'Save Configurations' section has a 'Save Configurations' button. The 'Upload and Download Configurations' section has two radio buttons: 'Upload configuration file to your Switch.' (selected) and 'Press "Download" to save configuration file to your PC.'. The 'Upload' section includes a 'File path' field, a 'Choose File' button, and an 'Upload' button. The 'Download' section includes a 'Download' button. The 'Reset Configurations' section has a 'Reset' button. The 'The configurations status' section shows a timestamp and message: '1999-11-14 05:50:42.000: Configurations are changed by UI.'

Figure 108: WBM Page, "Maintenance" – "Configuration" Tab

Save Configuration

- Click the **[Save]** button to save the current settings in NV-RAM (Flash).

Upload and Download the Configuration

Execute the following steps to save the configuration file to your PC.

1. Select "Press Download to save the configuration file to your PC".
2. Click the **[Download]** button to start the download.

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

1. Select "Upload the configuration file to the switch".
2. Click the **[Select file]** button.
Select the configuration file by specifying the full path.
3. Click the **[Upload]** button to begin uploading the file.

Reset Configuration

- Click the **[Reset]** button to reset the switch configuration to the factory default.

Configuration Status

“The configurations have been changed” indicates that changes have been made to the configurations.

“The user configuration file is the default. The configurations are default values.” indicates that no changes have been made to the configurations.

9.6.4.2 Firmware

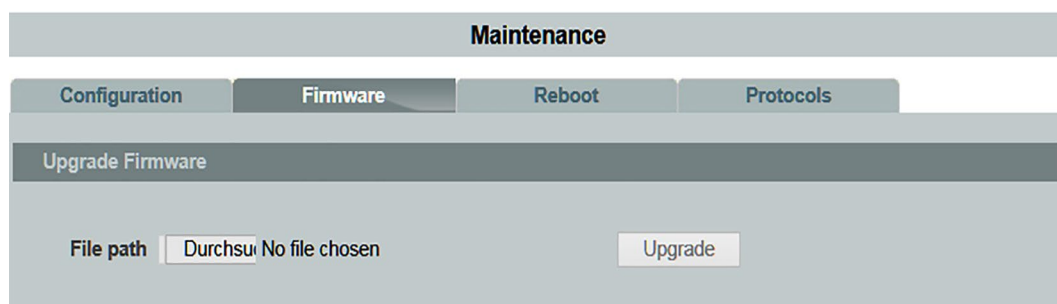


Figure 109: WBM Page, "Maintenance" – "Firmware" Tab

Firmware Update

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

1. Click the **[Select file]** button.
The file selection dialog opens. Select the respective firmware file.
2. Click the **[Update]** button to load the new firmware.

9.6.4.3 Reboot

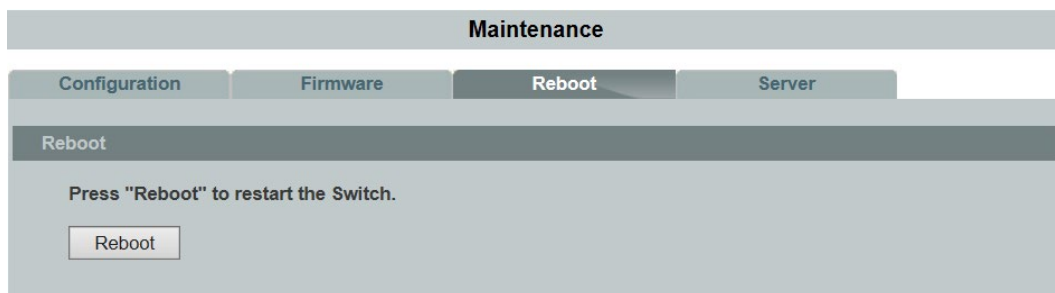


Figure 110: WBM Page, "Maintenance" – "Reboot" Tab

Reboot

The "Reboot" function allows you to restart the switch without physically turning the power off.

Follow the steps below to reboot the switch.

1. Click the **[Reboot]** button in the "Reboot" menu. The following windows open:

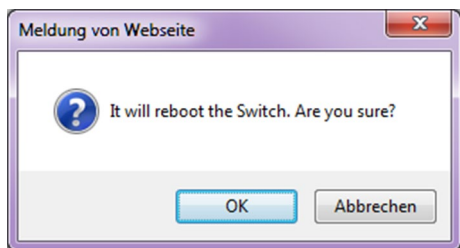


Figure 111: WBM Page, "Maintenance" – "Reboot" Tab – Message

2. Click **[OK]** and wait for the switch to restart. The process can take up to two minutes. The process does not change the switch configuration.

9.6.4.4 Server

Maintenance

Configuration
Firmware
Reboot
Protocols

Server Settings

HTTP Server State	Enable ▼	HTTP Server TCP Port	80 (80,1025~9999)
HTTPS Server State	Enable ▼		
SNMP v1/v2c Server State	Enable ▼		
SNMP v3 Server State	Enable ▼		
SSH Server State	Enable ▼		
TELNET Server State	Enable ▼	TELNET Server TCP Port	23 (23,1025~9999)

Apply
Refresh
Save Configurations

Server State

HTTP Server State	Enable	HTTP Server TCP Port	80
HTTPS Server State	Enable		
SNMP v1/v2c Server State	Enable		
SNMP v3 Server State	Enable		
SSH Server State	Enable		
TELNET Server State	Enable	TELNET Server TCP Port	23

Figure 112: WBM "Maintenance" Page – "Server" Tab

Table 113: WBM “Maintenance” Page – “Protocols” Tab

Server Settings		
Parameter	Default	Description
HTTP Server Status	Enable	Select “Enable” to enable the HTTP server.
	Disable	Select “Disable” to disable the HTTP server.
HTTP Server TCP Port (80, 1025–9999)	80 1025 ... 9999	Enter the “HTTP Server TCP Port” in the input field.
HTTP Server Status	Enable	Select “Enable” to enable the HTTPS server.
	Disable	Select “Disable” to disable the HTTPS server.
SNMP v1/v2c Server Status	Enable	Select “Enable” to enable the SNMP v1/v2c server.
	Disable	Select “Disable” to disable the SNMP v1/v2c server.
SNMP v3 Server Status	Enable	Select “Enable” to enable the SNMP v3 server.
	Disable	Select “Disable” to disable the SNMP v3 server.
SSH Server Status	Enable	Select “Enable” to enable the SSH server.
	Disable	Select “Disable” to disable the SSH server.
Telnet Server Status	Enable	Select “Enable” to enable the Telnet server.
	Disable	Select “Disable” to disable the Telnet server.
Telnet Server TCP Port (23, 1025–9999)	23 1025 ... 9999	Enter the “Telnet Server TCP Port” in the input field.
Server Status		
Parameter	Default	Description
HTTP Server Status	Enable Disable	This field displays the status of the HTTP server.
HTTP Server TCP Port	80 1025 ... 9999	This field displays the status of the HTTP server TCP port.
HTTP Server Status	Enable Disable	This field displays the status of the HTTPS server.
SNMP v1/v2c Server Status	Enable Disable	This field displays the status of the SNMP v1/v2c server.
SNMP v3 Server Status	Enable Disable	This field displays the status of the SNMP v3 server.
SSH Server Status	Enable Disable	This field displays the status of the SSH server.
Telnet Server Status	Enable Disable	This field displays the status of the Telnet server.
Telnet Server TCP Port	23 1025 ... 9999	This field displays the status of the Telnet server TCP port.

9.6.5 System Log

The “syslog” function records various system information for “Debugging”. Each log entry records one of the following levels:

- Alert
- Critical
- Error
- Warning
- Notice
- Information

The Syslog function can be enabled or disabled. The default setting is “disabled”. The log message is recorded in the switch file system. If the IP address of the Syslog server has been configured, the switch sends a copy to it.

Note



Size of the Log Message File

The size of the log message file is limited to 4 KB. If the file is full, the oldest message is replaced.

System Log

Syslog Server Setting

Server IP: IPv4 [] Disable []

Facility: (5) Messages generated internally by syslog []

[Apply] [Save Configurations]

System Log

Log Level: All [] [Show] [Refresh] [Clear] [Save]

```
<6> 2019 Mar 20 16:02:33 60003:System Cold Start!
<4> 2019 Mar 20 16:02:34 40005:Port 11 Link Up.
<4> 2019 Mar 20 16:02:43 40005:Port 1 Link Up.
<4> 2019 Mar 20 16:45:41 40004:Port 1 Link Down.
<4> 2019 Mar 20 16:45:56 40005:Port 8 Link Up.
<6> 2019 Mar 20 16:50:07 60001:User(admin) Login Succeeded!
<6> 2019 Mar 20 16:51:40 60005:Save configurations to file!
<6> 2019 Mar 20 21:14:18 60001:User(admin) Login Succeeded!
<6> 2019 Mar 21 20:52:14 60001:User(admin) Login Succeeded!
<6> 2019 Mar 22 15:32:02 60001:User(admin) Login Succeeded!
<6> 2019 Mar 22 16:25:14 60005:Save configurations to file!
<6> 2019 Mar 22 16:26:27 60005:Save configurations to file!
<6> 2019 Mar 22 16:26:51 60005:Save configurations to file!
<6> 2019 Mar 22 16:26:56 60005:Save configurations to file!
<6> 2019 May 10 09:18:26 60005:Save configurations to file!
<6> 2019 May 10 13:48:22 60001:User(admin) Login Succeeded!
<6> 2019 May 13 07:46:04 60001:User(admin) Login Succeeded!
<6> 2019 May 13 10:05:11 60001:User(admin) Login Succeeded!
```

Figure 113: WBM “System Log” Page

Table 114: WBM "System Log" Page

Syslog Server Settings		
Parameters	Default	Description
Server IP	IPv4	In the "IPv4" selection box, choose if you want to select this version of the Internet protocol.
	IPv6	In the "IPv6" selection box, choose if you want to select this version of the Internet protocol.
		Enter the IP address in decimal-point notation. (e.g., 192.168.1.1).
	Disable	Select "Disable" in the selection box to prevent the switch from sending all new log messages to the Syslog server.
	Enable	Select "Enable" in the selection box to allow the switch to send all new log messages to the Syslog server.
Facility	(1) User-level messages	Select "(1) User-level messages" in the selection box if you want to display user-specific messages.
	(5) Messages generated internally by syslogd	Select "(5) Messages generated internally by syslogd" in the selection box if you want to display messages generated by syslog internally.
	(14) Log alert	
	(16) Local use 0	
	(17) Local use 1	
	(18) Local use 2	
	(19) Local use 3	
	(20) Local use 4	
	(21) Local use 5	
	(22) Local use 6	
	(23) Local use 7	
System Log		
Parameters	Default	Description
Log Level	All	Select "All" in the selection box if you want to display all log messages.
	1:Alert	Select "Log alert" 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:Informational	Select "Informational" in the selection box if you want to display all information.

9.6.6 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:

Firmware version 01: User Name = „admin“
User Password = „Wago1951“
Firmware version 02: User Name = „admin“
User Password = „wago“

1. Admin account Read/Write permissions
2. Normal user account Read permission only
 - Cannot enter privileged mode in the CLI.
 - Configurations cannot be changed in the Web-Based Management.

The switch also supports a “Backdoor” user account. If a user has forgotten his user name or password, the switch can create a “backdoor” account with the MAC address of the system. A user can then log into the switch and create a new account.

User Account

User Account Settings

User Name

User Password

User Authority

Normal
▼

No.	Name	Authority	Action
1	admin	Admin	

Figure 114: WBM “User Account” Page

Table 115: WBM "User Account" Page

User Account Settings		
Parameters	Default	Description
User Name		Enter a new or modify the existing user name in the input field.
User Password		Enter a new or modify an existing password in the input field. You can enter up to 32 alphanumeric characters.
User Authority		In this box, select the type of user account.
	Normal	Select "Normal" 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.
No.		
Parameters	Default	Description
No.		This column displays the index number of an entry.
Name		This column displays the name of the user account.
Authority		This column displays the type of user account.
Action		Click the [Delete] button to delete the user account.
		Note  Note Deleting an administrator account The last admin account cannot be deleted.

10 Appendix

10.1 Console Port (RJ-45 to DB9)

Use the included console cable to connect the console port of the industrial managed switch to the COM port. The connector pin assignment is:

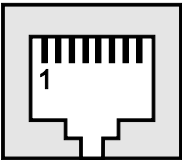


Figure 115: RJ-45 Connector Pin Assignment

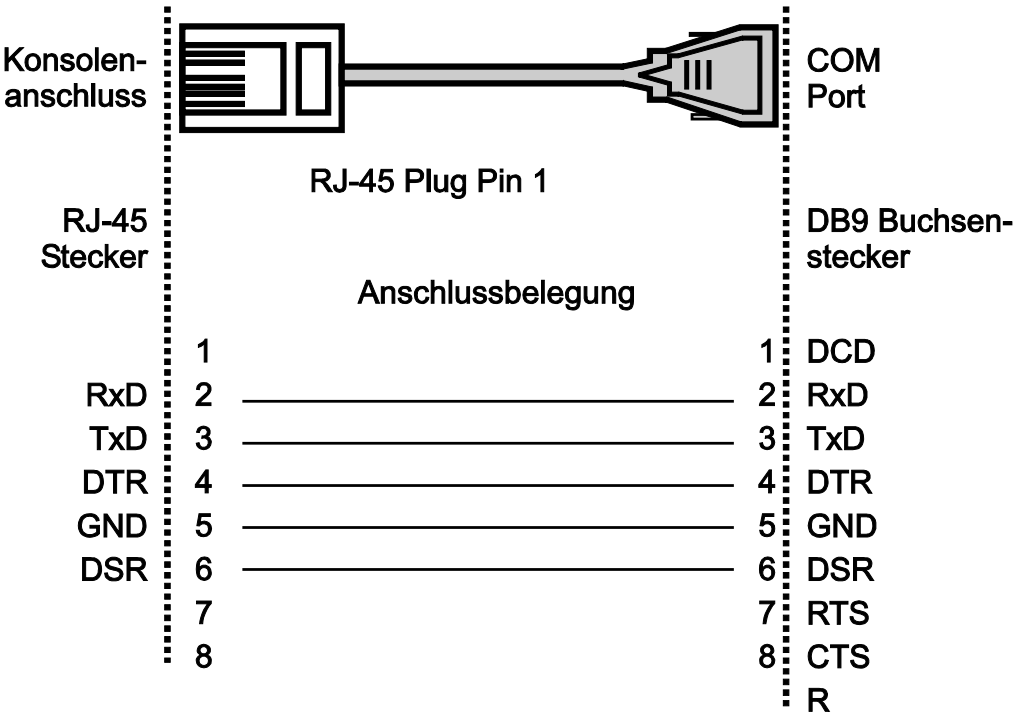


Figure 116: Connector Pin Assignment RJ-45 to DB9

10.2 RJ-45 Cable

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

Table 116: RJ-45 Cable

Contact	Description		Pair	Color (acc. EIA/TIA 568B)
	4-wire	8-wire		
1	TD	D1+	2	White/Orange
2	TD-	D1-	2	Orange
3	RX+	D2+	3	White/Green
4	Not assigned	D3+	1	Blue
5	Not assigned	D3-	1	White/Blue
6	RX-	D2-	3	Green
7	Not assigned	D4+	4	White/Brown
8	Not assigned	D4-	4	Brown

Note



Functions on the RJ45 connector

The industrial managed switch offers the functions autocrossing und autonegotiation to the RJ-45 connection.

10.3 Configuring in the Command Line Interface (CLI)

10.3.1 System Status

10.3.1.1 System Information

Table 117: CLI "System Information" Configuration

Node	Command	Description
enable	show hostname	This command displays the system's network name.
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 up time.

10.3.2 Default Settings

10.3.2.1 System

Table 118: CLI "System" Configuration

Node	Command	Description
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.
eth0	ip address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
eth0	ip address default-gateway A.B.C.D	This command configures the system 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.

10.3.2.2 Jumbo Frame

Table 119: 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 of frame size.

10.3.2.3 SNTP

Table 120: CLI "SNTP" Configuration

Node	Command	Description
enable	show time	This command displays the current time and date configurations.
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 configure daylight savings time after you configure the date and time, the switch uses daylight savings 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 the daylight saving time.
configure	time daylight-saving-time start-date <month> <day> <hour>	This command sets the start date of daylight savings time.
configure	time daylight-saving-time end-date <month> <day> <hour>	This command sets the end date of daylight saving time.
configure	no time daylight-saving-time	This command disables daylight saving time on the switch.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of the time server.
configure	no time ntp-server	This command disables the NTP server settings.
configure	time timezone operator (+/-) hour (VALUE 0~14) min (VALUE 00 or 30)	This command sets the time difference between UTC (formerly GMT) and the time zone.

Example

L2SWITCH(config)#*time ntp-server 192.5.41.41*

L2SWITCH(config)#*time timezone operator + hour 8 min 0*

10.3.2.4 Management Host

Table 121: CLI “Management Host” Configuration

Node	Command	Description
enable	show interface eth0	The command displays the all eth0 interface configurations.
eth0	show	The command displays the 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
```

10.3.2.5 MAC Management

Table 122: 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 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.

Example

```
L2SWITCH(config)#mac-address-table static 00:11:22:33:44:55 vlan 1 port 1
```

10.3.2.6 Blackhole MAC

Table 123: CLI "Blackhole MAC" Configuration

Node	Command	Description
enable	show mac-address-table refusal	This command displays the current rejected MAC address only.
configure	mac-address-table refusal MACADDR vlan VLANID	This command configures the rejection of a MAC address in a specific VLAN.
configure	mac-address-table refusal MACADDR	This command configures the rejection of a MAC address.

10.3.2.7 Port Mirroring

Table 124: 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 the "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 3-10 mode both*

10.3.2.8 Port Settings

Table 125: CLI “Port Settings” Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
interface	show	This command displays the current port configurations.
interface	loopback (none phy)	This command specifies the “Loopback” mode for a specific port.
interface	flowcontrol (off on)	This command disables / enables the “Flow Control” for a port.
interface	speed (auto 10-full 10-half 100-full 100-half)	This command configures the speed and duplex mode for a port.
interface	shutdown	This command disables a specific port.
interface	no shutdown	This command enables a specific port.
interface	loopback (none mac)	This command tests the transmission or data transport infrastructure.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#interface fa1/0/1
```

```
L2SWITCH(config-if)#speed auto
```

```
L2SWITCH#show interface fastethernet1/0/1
```


10.3.3 Advanced Settings

10.3.3.1 Bandwidth Control

10.3.3.2 QoS

Table 126: CLI “QoS” Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the “Service Queue”.
enable	show qos mode	This command displays the current IEEE 802.1p QoS mode.
configure	queue cos-map PRIORITY QUEUE_ID	This command configures the 802.1p priority mapping of the “Service Queue”.
configure	no queue cos-map	This command configures the default settings for the 802.1p priority mapping of the “Service Queue”.
configure	qos mode high-first	This command configures the QoS mode to “high_first”, so that “Hardware Queue” transmits all packets in its buffer before permitting the next lower priority to transmit its packets.
configure	qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE	This command configures the QoS mode to “Weighted Round Robin”.
interface	default-priority	This command allows the user to specify which priority is assigned by default to the packets received by the switch without any tag. The priority value entered with this command is used to determine which of the “Hardware Priority Queues” the packet is forwarded to. Default: 0.
interface	no default-priority	This command configures the default priority for the specific port to 0.

10.3.3.3 Rate Limitation

Table 127: CLI “Rate Limitation” Configuration

Node	Command	Description
enable	show bandwidth-limit	This command displays the current “Rate Limitation” configurations.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for outgoing packets and sets the limit.
configure	no bandwidth-limit egress ports PORTLISTS	This command disables the bandwidth limit for outgoing packets.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for incoming packets and set the limit.
configure	no bandwidth-limit ingress ports PORTLISTS	This command disables the bandwidth limit for incoming packets.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#bandwidth-limit egress 1 ports 1-8
```

```
L2SWITCH(config)#bandwidth-limit ingress 1 ports 1-8
```

10.3.3.4 Storm Control

Table 128: 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 the bandwidth limit for broadcast, multicast or DLF packets and sets the bandwidth limit of 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 the bandwidth limit 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
```

10.3.3.5 IGMP Snooping

Table 129: CLI “IGMP Snooping” Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current “IGMP Snooping” configurations.
configure	igmp-snooping (disable enable)	This command disables / enables “IGMP Snooping” on the switch.
configure	igmp-snooping vlan VLAN_ID	This command enables “IGMP Snooping” on a VLAN or VLAN range.
configure	no igmp-snooping vlan VLAN_ID	This command disables “IGMP Snooping” on a VLAN or VLAN range.
configure	igmp-snooping querier (disable enable)	This command disables / enables “IGMP Snooping Querier” on the switch.
configure	igmp-snooping querier vlan VLAN_ID	This command enables the “IGMP Snooping Querier” function on a VLAN or VLAN range.
configure	no igmp-snooping querier vlan VLAN_ID	This command disables the “IGMP Snooping Querier” function on a VLAN or VLAN range.
configure	igmp-snooping unknown-multicast (drop flooding)	This command configures the process for unknown multicast packets when the “IGMP Snooping” function is enabled. drop: All unknown multicast packets are dropped.
configure	igmp-snooping report-suppression (disable enable)	This command disables / enables the “IGMP Snooping Report Suppression” function on the switch.
interface	igmp-querier-mode (auto fixed edge)	This command specifies if and under what conditions the port(s) are “IGMP Query Ports”. The switch forwards the “IGMP Join/Leave” packets to an “IGMP Query Port”, treating the port as if it were connected to an IGMP multicast router (or server). “IGMP Snooping” must also be enabled (default: “Auto”).
interface	igmp-immediate-leave	The command enables the “Immediate Leave” function for “IGMP Snooping” for a specific interface.
interface	no igmp-immediate-leave	The command disables the “Immediate Leave” function for “IGMP Snooping” for a specific interface.

Example

L2SWITCH(config)#igmp-snooping enable

L2SWITCH(config)#igmp-snooping vlan 1

L2SWITCH(config)#igmp-snooping querier enable

L2SWITCH(config)#igmp-snooping querier vlan 1

L2SWITCH(config)#interface 1/0/1

L2SWITCH(config-if)#igmp-immediate-leave

L2SWITCH(config-if)# igmp-querier-mode fixed

10.3.3.6 MVR

Table 130: CLI "MVR" Configuration

Node	Command	Description
enable	show mvr	This command displays the current MVR configurations.
enable	show mvr vlan VLANID	This command displays the current MVR configurations of the specific VLAN.
enable	show igmp-snooping	This command displays the current "IGMP Snooping" configurations.
configure	mvr VLANID	This command creates the MVR configurations for the specific VLAN.
configure	no mvr VLANID	This command disables the MVR configurations for the specific VLAN.
MVR	group NAME	This command creates a group configuration for the MVR.
MVR	no group NAME	This command deletes the group configurations from the MVR.
MVR	inactive	This command disables the MVR settings.
MVR	no inactive	This command enables the MVR settings.
MVR	mode (dynamic compatible)	This command configures the mode for the MVR. - Dynamic: Sends "IGMP Reports" to all MVR source ports in the multicast VLAN. - Compatibility: The switch does not send any "IGMP Reports".
MVR	name STRING	This command configures the name for the MVR.
MVR	no name	This command configures the default name for the MVR.
MVR	receiver-port PORTLIST	This command assigns a receiver port or receiver port range. Normally, the source ports are connected to the "Streaming Client".
MVR	no receiver-port PORTLIST	This command deletes a port or port range from the list of receiver ports.
MVR	source-port PORTLIST	This command assigns a source port or source port range. Normally, the source ports are connected to the "Streaming Server".
MVR	no source-port PORTLIST	This command deletes a port or port range from the list of source ports.
MVR	tagged PORTLIST	This command assigns a tagged port or port range. The same applies to VLAN tagged ports.
MVR	no tagged PORTLIST	

10.3.3.7 Multicast Address

Table 131: CLI "Multicast Address" Configuration

Node	Command	Description
enable	show mac-address-table multicast	This command displays the current static/dynamic multicast address entries.
configure	mac-address-table multicast MACADDR vlan VLAN_ID ports PORTLIST	This command configures a static multicast entry.
configure	no mac-address-table multicast MACADDR	This command deletes a static multicast entry from the address table.

10.3.3.8 VLAN

10.3.3.8.1 Port Isolation

Table 132: CLI "Port Isolation" Configuration

Node	Command	Description
enable	show port-isolation	This command displays the current "Port Isolation" configurations. "V" indicates that the port's packets can be sent to that port. "-" indicates that the port's packets cannot be sent to that 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
```

10.3.3.8.2 VLAN Settings

Table 133: CLI "VLAN Settings" Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1~4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1~4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	name STRING	This command assigns a name for the specific VLAN. The VLAN name should be a combination of numbers, letters, hyphens (-) or 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 is comprised as follows: "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 member 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 acceptable frame type.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#vlan 2
```

```
L2SWITCH(config-vlan)#fixed 1-6
```

```
L2SWITCH(config-vlan)#untagged 1-3
```

10.3.3.9 GARP/GVRP

Table 134: CLI “GARP/GVRP” Configuration

Node	Command	Description
enable	show gvrp configuration	This command displays the GVRP configurations.
enable	show gvrp statistics	This command displays the GVRP configurations for one port or all ports.
enable	show garp timer	This command displays the timers for GARP.
configure	gvrp (disable enable)	This command disables / enables GVRP on the switch.
configure	no gvrp configuration	This command resets the GVRP configuration to the default setting.
interface	gvrp (disable enable)	This command disables / enables GVRP on a specific port.
interface	gvrp registration (normal forbidden)	This command configures the registration mode for GVRP on a specific port.
interface	no gvrp configuration	This command resets the GVRP configuration for a specific port to the default setting.
interface	garp join-time VALUE leave-time VALUE leaveall-time VALUE	This command configures the “Join Time”, “Leave Time” and “Leaveall Time” for GVRP on a specific port.
interface	no garp time	This command resets the Join, Leave and Leaveall times for GVRP on a specific port to the default settings.

10.3.3.10 Q-in-Q**10.3.3.10.1 VLAN Stacking**

Table 135: CLI "VLAN Stacking" Configuration

Node	Command	Description
enable	show vlan-stacking	This command displays the current "VLAN Stacking" type.
enable	show vlan-stacking selective-qinq	This command displays the selective Q-in-Q configurations.
enable	show vlan-stacking portbased-qinq	This command displays the port-based q-in-Q configurations.
enable	show vlan-stacking tpid-inform	This command displays the TPID configurations.
config	vlan-stacking (disable port-based selective)	This command disables "VLAN Stacking" or enables port-based or selective "VLAN Stacking" on the switch.
config	vlan-stacking selective-qinq STRINGS	This command creates a selective Q-in-Q profile with name.
config	no vlan-stacking selective-qinq STRINGS	This command deletes a selective Q-in-Q profile with name.
config	vlan-stacking tpid-table index <2-6> value STRINGS	This command configures the TPID table.
interface	vlan-stacking port-based priority <0~7>	This command sets the priority in the port based Q-in-Q.
interface	vlan-stacking port-based role (tunnel access normal)	This command sets the "VLAN Stacking" port role.
interface	vlan-stacking port-based spvid <1~4096>	This command sets the service provider VID of the specified port.
interface	vlan-stacking tunnel-tpid index <1-6>	This command sets the TPID for a "Q-in-Q Tunnel Port".
qinq	active	This command enables the selective Q-in-Q profile.
qinq	inactive	This command disables the selective Q-in-Q profile.
qinq	cvid VLANID	This command specifies the service provider's VLAN range for incoming packets.
qinq	spvid VLANID	This command specifies the service provider's VLAN range for outgoing packets in the selective Q-in-Q.
qinq	priority <0-7>	This command sets the priority in the selective Q-in-Q.
qinq	access-ports PORTLISTS	This command specifies the "Access Ports" to apply the rules.
qinq	tunnel-ports PORTLISTS	This command specifies the "Tunnel Ports" to apply the rules.
qinq	end	The command exits the "CLI Q-in-Q" node and enables the "CLI enable" node.
qinq	exit	The command exits the "CLI Q-in-Q" node and enables the "CLI configure" node.
qinq	show	The command displays the current configurations of the Q-in-Q profile.

10.3.3.11 DHCP Relay

Table 136: CLI “DHCP Relay” Configuration

Node	Command	Description
enable	show dhcp relay	This command displays the current configurations for the “DHCP Relay”.
configure	dhcp relay (disable enable)	This command disables / enables the “DHCP Relay” on the switch.
configure	dhcp relay vlan VLAN_RANGE	This command enables the “DHCP Relay” function for a VLAN or a VLAN range.
configure	no dhcp relay vlan VLAN_RANGE	This command disables the “DHCP Relay” function for a VLAN or a VLAN range.
configure	dhcp helper-address IP_ADDRESS	This command configures IP address of the DHCP server.
configure	no dhcp helper-address	This command deletes the IP address of the DHCP server.
configure	dhcp option82 (disable enable)	This command disables / enables the “DHCP Relay Option 82” function on the switch.
configure	dhcp option82 information STRING	This command configures the information for the “DHCP Relay Option 82” function.
configure	no dhcp option82 information	This command deletes the information for the “DHCP Relay Option 82” function.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)# interface eth0
```

```
L2SWITCH(config-if)# ip address 172.20.1.101/24
```

```
L2SWITCH(config-if)# ip address default-gateway 172.20.1.1
```

```
L2SWITCH(config)#dhcp relay enable
```

```
L2SWITCH(config)# dhcp relay vlan 1
```

```
L2SWITCH(config)# dhcp helper-address 172.20.1.1
```

```
L2SWITCH(config)#dhcp option82 enable
```

```
L2SWITCH(config)#dhcp option82 information Justin
```

10.3.3.12 Dual Homing

Table 137: CLI “Dual Homing” Configuration

Node	Command	Description
enable	show dual-homing	This command displays the “Dual Homing” information.
configure	dual-homing (disable enable)	This command disables / enables the “Dual Homing” function in the system.
configure	no dual-homing primary-channel	This command deletes the primary channel for “Dual Homing” from the system.
configure	no dual-homing primary-channel	This command deletes the primary channel for “Dual Homing” from the system.
configure	dual-homing secondary-channel (port trunk) VALUE	This command configures the secondary channel for “Dual Homing” in the system. The channel can be a single port or a “Trunk Group”.
configure	no dual-homing secondary-channel	This command deletes the secondary channel for “Dual Homing” from the system.

Example

```
L2SWITCH(config)# link-aggregation 1 ports 5-6
```

```
L2SWITCH(config)# link-aggregation 1 enable
```

```
L2SWITCH(config)# dual-homing primary-channel port 2
```

```
L2SWITCH(config)# dual-homing secondary -channel trunk 1
```

```
L2SWITCH(config)# dual-homing enable
```

10.3.3.13 Link Aggregation

Table 138: CLI “Link Aggregation” Configuration

Node	Command	Description
enable	show link-aggregation	The command displays the current configuration for “Trunking”.
configure	link-aggregation [GROUP_ID] (disable enable)	The command disables / enables “Trunking” for the specific “Trunk Group”.
configure	link-aggregation [GROUP_ID] interface PORTLISTS	The command adds ports to a specific “Trunk Group”.
configure	no link-aggregation [GROUP_ID] interface PORTLISTS	The command deletes ports from a specific “Trunk Group”.

10.3.3.14 LACP

Table 139: CLI “LACP” Configuration

Node	Command	Description
enable	show trunk	The command displays the current configuration for “Trunking”.
enable	show lacp counters [GROUP_ID]	This command displays the LACP counters for the specific group or all groups.
enable	show lacp internal [GROUP_ID]	This command displays internal LACP information for the specific group or all groups.
enable	show lacp neighbor [GROUP_ID]	This command displays the LACP neighbor information for the specific group or all groups.
enable	show lacp port_priority	This command displays the port priority for LACP.
enable	show lacp sys_id	This command displays the system ID for the “LACP Actor” and “LACP Partner”.
configure	Lacp (disable enable)	This command disables / enables LACP on the switch.
configure	Lacp GROUP_ID (disable enable)	This command disables / enables LACP for a specific “Trunk Group”.
configure	clear lacp counters [PORT_ID]	This command clears the LACP statistics for a specific port or all ports.
configure	lacp system-priority <1-65535>	This command configures the system priority for LACP. Note: The default value is 32768.
configure	no lacp system-priority	This command configures the default setting for system priority for LACP.
interface	lacp port_priority <1-65535>	This command configures the priority for the specific port.
interface	no lacp port_priority	Note: The default value is 32768.

10.3.3.15 LLDP

Table 140: CLI “LLDP” Configuration

Node	Command	Description
enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all information of port neighbors.
configure	lldp (disable enable)	This command globally enables / disables the LLDP function on the switch.
configure	lldp tx-interval	This command configures the transmission interval for LLDP packets.
configure	lldp tx-hold	This command configures the “tx-Hold Time” that determines the TTL of the switch message. (TTL = tx-hold * tx-interval)
interface	lldp-agent (disable enable rx-only tx-only)	This command configures the Agent function for LLDP. “disable”: LLDP is enabled for a specific port. “enable”: The LLDP packet is transmitted on a specific port and received. “tx-only”: The LLDP packet is only transmitted on a specific port. “rx-only”: The LLDP packet is only received on a specific port.

10.3.3.16 Loop Detection

Table 141: 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 target MAC address for special “Loop Detection” packets.
configure	no loop-detection address	This command resets the target 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. It 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
```

10.3.3.17 STP

Table 142: 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”, “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 pathcost 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 142: 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 of 1 to 65,535, 32-bit-based value range of 1 to 200,000,000.
interface	no spanning-tree cost	This command configures 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 configures the priority to of the specific port to the default value.

10.3.3.18 Xpress Ring

Table 143: CLI "Xpress Ring" Configuration

Node	Command	Description
enable	show xpress-ring	This command displays the current status of the Xpress ring.
config	xpress-ring (disable enable)	This command enables / disables the Xpress ring function on the switch.
config	xpress-ring role (forwarder arbiter)	This command configures the role ("Forwarder" or "Arbiter") on the switch.
config	xpress-ring ring-port1	This command configures one port of the ring.
config	xpress-ring ring-port2	This command configures the other port of the ring.

10.3.4 Security

10.3.4.1 DHCP Snooping

Table 144: CLI "DHCP Snooping" Configuration

Node	Command	Description
enable	show dhcp-snooping	This command displays the current "DHCP Snooping" configurations.
configure	dhcp-snooping (disable enable)	This command disables / enables the "DHCP Snooping" on the switch.
configure	dhcp-snooping vlan VLANID	This command enables the "DHCP Snooping" function on a VLAN or VLAN range.
configure	no dhcp-snooping vlan VLANID	This command disables the "DHCP Snooping" function on a VLAN or VLAN range.
configure	dhcp option82 (disable enable)	This command disables / enables the "DHCP Relay Option 82" function.
configure	dhcp option82 information STRING	This command configures the information for the "DHCP Relay Option 82" function.
configure	no dhcp option82 information	This command deletes the information for the "DHCP Relay Option 82" function.
interface	dhcp-snooping host	This command configures the maximum host count for the specific port.
interface	no dhcp-snooping host	This command configures the maximum host count for the specific port to the default value.
interface	dhcp-snooping trust	This command configures the "Trusted Port" for the specific port.
interface	no dhcp-snooping trust	This command configures the "Untrusted Port" for the specific port.

Example

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#dhcp-snooping enable
```

```
L2SWITCH(config)#dhcp-snooping vlan 1
```

```
L2SWITCH(config)#interface 1/0/1
```

```
L2SWITCH(config-if)#dhcp-snooping trust
```

```
L2SWITCH(config)#dhcp option82 enable
```

```
L2SWITCH(config)#dhcp option82 information Test01
```


10.3.4.2 Server Screening

Table 145: CLI "Server Screening" Configuration

Node	Command	Description
enable	show dhcp-snooping server	This command displays the IP address of the valid DHCP server.
configure	dhcp-snooping server IPADDR	This command configures the IP address of a valid DHCP server.
configure	no dhcp-snooping server IPADDR	This command deletes the IP address of a valid DHCP server.

10.3.4.3 Binding Table

Table 146: CLI "Binding Table" Configuration

Node	Command	Description
enable	show dhcp-snooping binding	This command displays the current "DHCP Snooping" binding table.
configure	dhcp-snooping binding mac MAC_ADDR ip IP_ADDR vlan VLANID port PORT_NO	This command configures a static host into the "DHCP Snooping" binding table.
configure	no dhcp-snooping binding mac MACADDR	This command deletes a static host from the "DHCP Snooping" binding table.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*dhcp-snooping binding mac 00:11:22:33:44:55 ip 1.1.1.1 vlan 1 port 2*

L2SWITCH(config)#*no dhcp-snooping binding mac 00:11:22:33:44:55*

L2SWITCH#*show dhcp-snooping binding*

10.3.4.4 ARP Inspection

Table 147: CLI “ARP Inspection” Configuration

Node	Command	Description
enable	show arp-inspection	This command displays the current configurations for the ARP Inspection.
configure	arp-inspection (disable enable)	This command disables / enables the ARP Inspection function on the switch.
configure	arp-inspection vlan VLANID	This command enables the ARP Inspection function on a VLAN or VLAN range.
configure	no arp-inspection vlan VLANID	This command disables the ARP Inspection function on a VLAN or VLAN range.
interface	arp-inspection trust	This command configures the “Trusted Port” for the specific port.
interface	no arp-inspection trust	This command configures the “Untrusted Port” for the specific port.

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*arp-inspection enable*

L2SWITCH(config)#*arp-inspection vlan 1*

L2SWITCH(config)#*interface 1/0/1*

L2SWITCH(config-if)#*arp-inspection trust*

10.3.4.5 Filter Table

Table 148: CLI “Filter Table” Configuration

Node	Command	Description
enable	show arp-inspection mac-filter	This command displays the current MAC address filter for the ARP Inspection.
configure	arp-inspection mac-filter age VALUE	This command configures the “Age Time” for the MAP address filter entries of the ARP Inspection.
configure	no arp-inspection mac-filter mac MACADDR	This command deletes a MAC address filter entry from the MAC filter table of the ARP Inspection.

10.3.4.6 Access Control List

Table 149: 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 activates this profile. "disable": The profile is disabled. "drop": If packets match the profile, the packets are dropped. "permit": If packets match the profile, the packets are forwarded.
acl	destination mac host 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.
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 mask for the profile.
acl	source mac MACADDR MACADDR	This command configures the source MAC address and mask for the profile.
acl	no source mac	This command deletes the source MAC and 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 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 mask for the profile.
acl	no destination ip	This command deletes the destination IP address from the profile.
acl	I4-source-port IPADDR	This command configures the UDP/TCP source port for the profile.
acl	no I4-source-port IPADDR	This command deletes the UDP/TCP source port from the profile.
acl	L4-destination-port PORT	This command configures the UDP/TCP destination port for the profile.

Table 149: CLI "Access Control List" Configuration

Node	Command	Description
acl	no l4-destination-port	This command deletes the UDP/TCP destination port from the profile.
acl	vlan VLANID	This command configures the VLAN for the profile.
acl	no vlan	This command deletes the VLAN limit from the profile.
acl	source interface PORT_ID	This command configures the source interface for the profile.
acl	no source interface PORT_ID	This command deletes the source interface from the profile.

10.3.4.7 802.1x

Table 150: CLI “802.1x” Configuration

Node	Command	Description
enable	show dot1x	This command displays the current 802.1x configurations.
enable	show dot1x username	This command displays the current user accounts for local authentication.
enable	show dot1x accounting-record	This command displays the local accounting records.
configure	dot1x authentication (disable enable)	This command enables / disables 802.1x authentication on the switch.
configure	dot1x authentic-method (local radius)	This command configures the 802.1x authentication method.
configure	no dot1x authentic-method	This command sets the 802.1x authentication method to the default setting.
configure	dot1x radius primary-server-ip <IP> port PORTID	This command configures the primary radius server.
configure	dot1x radius primary-server-ip <IP> port PORTID key KEY	This command configures the primary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID	This command configures the secondary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID key KEY	This command configures the secondary radius server.
configure	no dot1x radius secondary-server-ip	This command deletes the secondary radius server.
configure	dot1x username <STRING> passwd <STRING>	This command configures the user account for local authentication.
configure	no dot1x username <STRING>	This command deletes the user account for local authentication.
configure	dot1x accounting (disable enable)	This command enables / disables the local .1x accounting records.
configure	dot1x guest-vlan VLANID	This command configures the guest VLAN.
configure	no dot1x guest-vlan	This command deletes the guest VLAN.
interface	dot1x admin-control-direction (both in)	This command configures the control direction for blocking packets.
interface	dot1x default	This command resets the port configuration to the default settings.
interface	dot1x max-req <1-10>	This command sets the “Max-req Times” of a port. (1 to 10).
interface	dot1x port-control (auto force-authorized force-unauthorized)	This command configures the port control mode on the port.
interface	dot1x authentication (disable enable)	This command enables / disables 802.1x authentication on the port.
interface	dot1x reauthentication (disable enable)	This command enables / disables the authentication interval on the port.
interface	dot1x timeout quiet-period	This command configures the “Quiet Period” value on the port.
interface	dot1x timeout server-timeout	This command configures the server timeout value on the port.

Table 150: CLI "802.1x" Configuration

Node	Command	Description
interface	dot1x timeout reauth-period	This command configures the authentication interval value on the port.
interface	dot1x timeout supp-timeout	This command configures the supp-timeout value on the port.
interface	dot1x guest-vlan (disable enable)	This command configures the 802.1x state on the port.

10.3.4.8 Port Security

Table 151: CLI "Port Security" Configuration

Node	Command	Description
enable	show port-security	This command displays the current configurations for port security.
config	port-security (disable enable)	This command enables / disables the Port Security function globally.
interface	port-security (disable enable)	This command enables / disables the Port Security function for the specific port.
interface	port-security limit VALUE	This command configures the maximum number of MAC address entries for the specific port.

10.3.5 Monitor

10.3.5.1 Alarm

Table 152: CLI "Alarm" Configuration

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

10.3.5.2 Monitor Information

Table 153: CLI "Monitor Information" Configuration

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

10.3.5.3 RMON Statistics

Table 154: CLI "RMON Statistics" Configuration

Node	Command	Description
enable	show rmon statistics	This command displays the RMON statistics.
configure	clear rmon statistics [IFNAME]	This command clears the RMON statistics for one or all ports.

10.3.5.4 SFP Information

Table 155: 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.

10.3.5.5 Traffic Monitor

Table 156: CLI "Traffic Monitor" Configuration

Node	Command	Description
enable	show traffic-monitor	This command displays the "Traffic Monitor" configurations and current status.
configure	traffic-monitor (disable enable)	This command enables / disables the "Traffic Monitor" on the switch.
interface	traffic-monitor rate RATE_LIMIT type (bcast mcast bcast+mcast)	This command configures the packet rate and type for the "Traffic Monitor" on a specific port. mcast: broadcast packet mcast: multicast packet The rate should be greater than 50 pps.
interface	traffic-monitor (disable enable)	This command enables / disables the "Traffic Monitor" on a specific port.
interface	traffic-monitor recovery (disable enable)	This command enables / disables the "Recover" function for the "Traffic Monitor" on a specific port.
interface	traffic-monitor recovery time VALUE	This command configures the "Recovery Time" for the "Traffic Monitor" on a specific port.

10.3.6 Management

10.3.6.1 SNMP

Table 157: 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 configures 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*

10.3.6.2 Auto Provision

Table 158: CLI “Auto Provision” Configuration

Node	Command	Description
auto-provision	show	This command displays the current configurations for the “Auto Provision”.
auto-provision	active (enable disable)	This command enables / disables the “Auto Provision” function.
auto-provision	server-address IPADDR	This command sets the IP address of the server for the “Auto Provision”.
auto-provision	protocol (tftp http ftp)	The command configures the update protocol.
auto-provision	FTP-user username STRING password STRING	The command configures the username and password for the FTP server.
auto-provision	folder STRING	The command sets the folder for the “Auto Provision” server.
auto-provision	version <0-65535>	The command configures the version for “Auto Provision” on the switch.
auto-provision	no folder	The command resets the folder to the default setting.
auto-provision	no FTP-user	The command resets the username and password to default setting.

10.3.6.3 Mail Alarm

Table 159: CLI “Mail Alarm” Configuration

Node	Command	Description
enable	show mail-alarm	This command displays the “Mail Alarm” configurations.
configure	mail-alarm (disable enable)	This command disables / enables the “Mail Alarm” function.
configure	mail-alarm mail-from	This command configures the e-mail sender.
configure	mail-alarm mail-to	This command configures the e-mail receiver.
configure	mail-alarm server-ip IPADDR server-port VALUE	This command configures IP address and TCP port for the mail server.
configure	mail-alarm server-ip IPADDR server-port Default	This command configures the IP address of the mail server and sets its TCP port to 25.
configure	mail-alarm trap-event (reboot link-change config. firmware login port-blocked) (disable enable)	This command disables / enables mail trap events.

10.3.6.4 Maintenance

Table 160: 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 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 / FTP / HTTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

Example

L2SWITCH#*configure terminal*

L2SWITCH(config)#*interface eth0*

L2SWITCH(config-if)#*ip address 172.20.1.101/24*

L2SWITCH(config-if)#*ip address default-gateway 172.20.1.1*

L2SWITCH(config-if)#*management vlan 1*

10.3.6.5 System Log

Table 161: CLI "System Log" Configuration

Node	Command	Description
enable	show syslog	The command displays all log messages recorded in the switch.
enable	show syslog level LEVEL	This command displays the log messages with the "LEVEL" recorded in the switch.
enable	show syslog server	The command displays the syslog server configurations.
configure	syslog (disable enable)	The command disables / enables the System Log function.
configure	syslog ip IPADDR	The command configures the IP address of the syslog server.

Example

```
L2SWITCH#configure terminal
```

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

```
L2SWITCH(config)#syslog-server enable
```

10.3.6.6 User Account

Table 162: 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 q admin
```

```
L2SWITCH(config)#add user 1 1 normal
```

10.4 MODBUS/TCP Tables

10.4.1 Data Format and Function Code

MODBUS/TCP supports different types of data formats for reading. The most important 4 types are:

Table 163: 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	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.

10.4.2 MODBUS Registers

The MODBUS base address of the industrial managed switch is 1001 (decimal) for function code 4.

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
1001	3E9	1	HEX	Vendor ID = 0x30DE
1002	3EA	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	16	ASCII	Product Name = "852-0303"
				Word 0 Hi byte = '8'
				Word 0 Lo byte = '5'
				Word 1 Hi byte = '2'
				Word 1 Lo byte = '-'
				Word 2 Hi byte = '0'
				Word 2 Lo byte = '3'
				Word 3 Hi byte = '0'
				Word 3 Lo byte = '3'
				Word 4 Hi byte = '\0'
				Word 4 Lo byte = '\3'
1065	429	7	ASCII	Product Serial Number
				Ex: Serial No=A0000000000001

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
1081	439	12	ASCII	Firmware Version=" V1.2.1.S0"
				Word 0 Hi byte = 'V'
				Word 0 Lo byte = '1'
				Word 1 Hi byte = '.'
				Word 1 Lo byte = '2'
				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	16	ASCII	Firmware Release Date=" Mon Sep 30 18:51:45 2013"
1113	459	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	1	HEX	Power 1 (PWR) Alarm, DIP switch 1 need ON
				0x0000: no alarm
				0x0001: input voltage < 11.7V
				0x0002: input voltage > 57V
				0x0003: No PWR input
1130	46A	1	HEX	Power 2(RPS) Alarm, DIP switch 1 need ON
				0x0000: no alarm
				0x0001: input voltage < 11.7V
				0x0002: input voltage > 57V
				0x0003: No RPS input
1145	479	1	HEX	Fault LED Status
				0x0000: No
				0x0001: Yes

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
Port Information				
		1	HEX	Port 1 to 10 Link Status
				0x0000: Link down
1257	4E9			0x0001: 10M-Full-FC_ON (FC: Flow Control)
1258	4EA			0x0002: 10M-Full-FC_OFF
1259	4EB			0x0003: 10M-Half-FC_ON
1260	4EC			0x0004: 10M-Half-FC_OFF
1261	4ED			0x0005: 100M-Full-FC_ON
1262	4EE			0x0006: 100M-Full-FC_OFF
1263	4EF			0x0007: 100M-Half-FC_ON
1264	4F0			0x0008: 100M-Half-FC_OFF
1265	4F1			0x0009: 1000M-Full-FC_ON
1266	4F2			0x000A: 1000M-Full-FC_OFF
				0xFFFF: No port
		32	ASCII	Port 1 to 10 Medium
1513	5E9			Port Description = "100TX, RJ45." Or "1000TX, SFP."
1545	609			Word 0 Hi byte = '1'
1577	629			Word 0 Lo byte = '0'
1609	649			Word 1 Hi byte = '0'
1641	669			Word 1 Lo byte = 'T'
1673	689			...
1705	6A9			Word 4 Hi byte = '4'
1737	6C9			Word 4 Lo byte = '5'
1769	6E9			Word 5 Hi byte = '.'
1801	709			Word 5 Lo byte = '\0'
		2	HEX	Port 1 to 10 Tx Packets
2025	7E9			Ex: port 1 Tx Packet Amount = 0x87654321
2027	7EB			Word 0 = 8765
2029	7ED			Word 1 = 4321
2031	7EF			
2033	7F1			
2035	7F3			
2037	7F5			
2039	7F7			
2041	7F9			
2043	7FB			
		2	HEX	Port 1 to 10 Rx Packets
2089	829			Ex: port 1 Rx Packet Amount = 0x123456
2091	82B			Word 0 = 0012
2093	82D			Word 1 = 3456
2095	82F			
2097	831			
2099	833			
2101	835			
2103	837			
2105	839			
2107	83B			

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
		2	HEX	Port 1 to 10 Tx Error Packets
2153	869			Ex: port 1 Tx Error Packet Amount = 0x87654321
2155	86B			Word 0 =8765
2157	86D			Word 1 = 4321
2159	86F			
2161	871			
2163	873			
2165	875			
2167	877			
2169	879			
2171	87B			
		2	HEX	Port 1 to 10 Rx Error Packets
2217	8A9			Ex: port 1 Rx Error Packet Amount = 0x123456
2219	8AB			Word 0 = 0012
2221	8AD			Word 1 = 3456
2223	8AF			
2225	8B1			
2227	8B3			
2229	8B5			
2231	8B7			
2233	8B9			
2235	8BB			
Redundancy & Ring Information				
2281	8E9	1	HEX	Spanning Tree Status
				0x0000 : none
				0x0001 : STP
				0x0002 : RSTP
				0x0003 : MSTP
2282	8EA	1	HEX	Xpress-ring Status
				0x0000 : Disabled
				0x0001 : Enabled
2283	8EB	1	HEX	Jet-ring Status
				0x0000 : Disabled
				0x0001 : Enabled
2284	8EC	1	HEX	Dual-ring Status
				0x0000 : Disabled
				0x0001 : Enabled
2285	8ED	1	HEX	ERPS Status
				0x0000 : Disabled
				0x0001 : Enabled
2297	8F9	1	HEX	Xpress-ring Status Ring 1
				0x0000 : Disabled
				0x0001 : Enabled
2298	8FA	1	HEX	Xpress-ring Status Ring 2
				0x0000 : Disabled
				0x0001 : Enabled

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
2299	8FB	3	HEX	Xpress-ring MAC Ring 1
				Ex:
				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
2302	8FE	3	HEX	Xpress-ring MAC Ring 2
				Ex:
				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
2305	901	1	HEX	Primary Port of Xpress_Ring 1
				Ex:
				Port 5 = 0x0005
2306	902	1	HEX	Secondary Port of Xpress_Ring 1
				Ex:
				Port 6 = 0x0006
2307	903	1	HEX	Primary Port of Xpress_Ring 2
				Ex:
				Port 5 = 0x0005
2308	904	1	HEX	Secondary Port of Xpress_Ring 2
				Ex:
				Port 6 = 0x0006
2309	905	1	HEX	Xpress-ring Role Ring 1
				0x0000 : Forwarder
				0x0001 : Arbiter
2310	906	1	HEX	Xpress-ring Role Ring 2
				0x0000 : Forwarder
				0x0001 : Arbiter
2311	907	1	HEX	Xpress-ring Current status for Ring 1
				Primary Port
				0x0000 : No connection
				0x0001 : Forwarding
				0x0002 : Blocking
2312	908	1	HEX	Xpress-ring Current status for Ring 1
				Secondary Port
				0x0000 : No connection
				0x0001 : Forwarding
				0x0002 : Blocking

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
2313	909	1	HEX	Xpress-ring Current status for Ring 2
				Primary Port
				0x0000 : No connection
				0x0001 : Forwarding
0x0002 : Blocking				
2314	90A	1	HEX	Xpress-ring Current status for Ring 2
				Secondary Port
				0x0000 : No connection
				0x0001 : Forwarding
0x0002 : Blocking				
Jet-Ring Information				
2537	9E9	1	HEX	Jet Ring State
				0x0000: Disabled.
				0x0001: Enabled.
2538	9EA	3	HEX	Master Bridge MAC:
				Ex: MAC=00:01:02:03:04:05
				Word 0, high byte=0x00.
				Word 0, low byte=0x01.
				Word 1, high byte=0x02.
				Word 1, low byte=0x03.
				Word 2, high byte=0x04.
Word 2, low byte=0x05.				
2541	9ED	1	HEX	Jet Ring Total Nodes:
				Ex: When total nodes is 255(0xff).
				Word 0, high byte=0x00.
Word 0, low byte=0xff.				
2542	9EE	1	HEX	Bridge Role:
				0x0000: Learning.
				0x0001: Master.
				0x0002: Arbiter.
				0x0003: Forwarder.
0x0004: Pre-Forwarder.				
		1	HEX	Port Role (Port 1 to Port 10)
2553	9F9			0x0000: Disabled.
2554	9FA			0x0001: Listening.
2555	9FB			0x0002: Learning.
2556	9FC			0x0003: Forwarding.
2557	9FD			0x0004: Blocking.
2558	9FE			0x0005: No connection.
2559	9FF			
2560	A00			
2561	A01			
2562	A02			

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
		1	HEX	Ring Role (Port 1 to Port 10)
2585	A19			0x0000: No
2586	A1A			0x0001: Yes
2587	A1B			
2588	A1C			
2589	A1D			
2590	A1E			
2591	A1F			
2592	A20			
2593	A21			
2594	A22			
Dual-Ring Information				
2793	AE9	1	HEX	Dual-Ring State:
				0x0000: Disabled.
				0x0001: Enabled.
2794	AEA	3	HEX	Xpress-ring MAC for Dual-Ring:
				Ex: MAC=00:01:02:03:04:05
				Word 0, high byte=0x00.
				Word 0, low byte=0x01.
				Word 1, high byte=0x02.
				Word 1, low byte=0x03.
				Word 2, high byte=0x04.
				Word 2, low byte=0x05.
2797	AED	1	HEX	Xpress-ring Role for Dual-Ring:
				0x0000 : Forwarder
				0x0001 : Arbiter
2798	AEE	1	HEX	Xpress-ring Current status for Dual-Ring
				Port-1 – (Primary Port)
				High byte – Port No.
				0x01~ 0x0a: Port 1~Port 10
				Low byte – Port Status
				0x00 : No connection
				0x01 : Forwarding
				0x02 : Blocking
				Ex: 0x0501– Port 5 Forwarding
				0x0b02 – Port 10 Blocking
2799	AEF	1	HEX	Xpress-ring Current status for Dual-Ring
				Port-2 – (Secondary Port)
				High byte – Port No.
				0x01~ 0x0a: Port 1~Port 10
				Low byte – Port Status
				0x00 : No connection
				0x01 : Forwarding
				0x02 : Blocking
				Ex: 0x0501– Port 5 Forwarding
				0x0b02 – Port 10 Blocking

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
2800	AF0	3	HEX	Sub-Ring Master Bridge MAC :
				Ex: MAC=00:01:02:03:04:05
				Word 0, high byte=0x00.
				Word 0, low byte=0x01.
				Word 1, high byte=0x02.
				Word 1, low byte=0x03.
				Word 2, high byte=0x04.
				Word 2, low byte=0x05.
2803	AF3	1	HEX	Jet Ring Total Nodes for Sub-Ring.
				Ex: When total nodes is 255(0xff).
				Word 0, high byte=0x00.
2804	AF4	1	HEX	Bridge Role for Sub-Ring:
				0x0000: Learning.
				0x0001: Master.
2805	AF5	1	HEX	0x0002: Arbiter.
				0x0003: Forwarder.
				0x0004: Pre-Forwarder.
				Sub-ring Current status for Dual-Ring
				Support-1 – (Primary Port)
2806	AF6	1	HEX	High byte – Port No.
				0x01~ 0x0a: Port 1~Port 10
				Low byte – Port Status
				0x00 : No connection
				0x01 : Forwarding
				0x02 : Blocking
				Ex: 0x0501– Port 5 Forwarding
				0x0b02 – Port 10 Blocking
				Support-2 – (Secondary Port)
				High byte – Port No.
0x01~ 0x0a: Port 1~Port 10				
Low byte – Port Status				
0x00 : No connection				
0x01 : Forwarding				
0x02 : Blocking				
Ex: 0x0501– Port 5 Forwarding				
0x0b02 – Port 10 Blocking				
ERPS Information(Active Ring Only)				
3049	BE9	1	HEX	Ring ID for ERPSn (n=1)
				Ex: 0x001 Ring ID=1
3050	BEA	1	HEX	State for ring of ERPS
				0x0000: Disabled.
				0x0001: Enabled.

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3051	BEB	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	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	1	HEX	Instance of Ring
				Ex: 0x0001 Instance ID=1
3086	C0E	1	HEX	Control VLAN of Ring
				E:0x000b Control VLAN=11
3087	C0F	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	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	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

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3090	C12	1	HEX	Ring ID for ERPSn (n=2)
3091	C13	1		State of ERPS Ring
3092	C14	33	ASCII	Name of Ring
3125	C35	1	HEX	Version & Ring Type
3126	C36	1		Instance of Ring
3127	C37	1		Control VLAN of Ring
3128	C38	1		Right Port of Ring
3129	C39	1		Left Port of Ring
3130	C3A	1		Ring port state
3131	C3B	1	HEX	Ring ID for ERPSn (n=3)
3132	C3C	1		State of ERPS Ring
3133	C3D	33	ASCII	Name of Ring
3166	C5E	1	HEX	Version & Ring Type
3167	C5F	1		Instance of Ring
3168	C60	1		Control VLAN of Ring
3169	C61	1		Right Port of Ring
3170	C62	1		Left Port of Ring
3171	C63	1		Ring port state
3172	C64	1	HEX	Ring ID for ERPSn (n=4)
3173	C65	1		State of ERPS Ring
3174	C66	33	ASCII	Name of Ring
3207	C87	1	HEX	Version & Ring Type
3208	C88	1		Instance of Ring
3209	C89	1		Control VLAN of Ring
3210	C8A	1		Right Port of Ring
3211	C8B	1		Left Port of Ring
3212	C8C	1		Ring port state
3213	C8D	1	HEX	Ring ID for ERPSn (n=5)
3214	C8E	1		State of ERPS Ring
3215	C8F	33		Name of Ring
3248	CB0	1		Version & Ring Type
3249	CB1	1		Instance of Ring
3250	CB2	1		Control VLAN of Ring
3251	CB3	1		Right Port of Ring
3252	CB4	1		Left Port of Ring
3253	CB5	1		Ring port state

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3254	CB6	1	HEX	Ring ID for ERPSn (n=6)
3255	CB7	1		State of ERPS Ring
3256	CB8	33	ASCII	Name of Ring
3289	CD9	1	HEX	Version & Ring Type
3290	CDA	1		Instance of Ring
3291	CDB	1		Control VLAN of Ring
3292	CDC	1		Right Port of Ring
3293	CDD	1		Left Port of Ring
3294	CDE	1		Ring port state
MSTP Information				
3305	CE9	1	HEX	Instance ID (Fixed 0x00, 0)
				High byte –Instance ID.
				Low byte –Used State.
				0x01: used
				0x00: non used
3306	CEA	3	HEX	Root bridge MAC
				Ex: MAC=00:01:02:03:04:05
				Word 0, high byte=0x00.
				Word 0, low byte=0x01.
				Word 1, high byte=0x02.
				Word 1, low byte=0x03.
				Word 2, high byte=0x04.
				Word 2, low byte=0x05.
3309	CED	1	HEX	Port 1 status
				High byte –Port No.
				Low byte –Port Status.
				b'0:1 Type
				00: Bound(STP)
				01: Bound(RSTP)
				10: Bound(MSTP)
				11: Internal(MSTP)
				b'2 P2P
				0: non P2P
				1: P2P
				b'3:4 State
				00: Blocking
				01: Learning
				10: Forwarding
				b'5:7 Role
				000: Master
				001:Alternate
				010: Root
				011: Designated
				100: Backup
				101: Disabled
				110: Boundary
				111: Unknown

Table 164: MODBUS Register

Table 10-1: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3309	CED	1	HEX	Port 1 status
3310	CEE			Port 2 status
3311	CEF			Port 3 status
3312	CF0			Port 4 status
3313	CF1			Port 5 status
3314	CF2			Port 6 status
3315	CF3			Port 7 status
3316	CF4			Port 8 status
3317	CF5			Port 9 status
3318	CF6			Port 10 status
3337	D09	1	HEX	Instance ID (Fixed 0x00, 1)
3338	D0A	3		Root bridge MAC
3341	D0D	1		Port 1 status
3342	D0E	1		Port 2 status
3343	D0F	1		Port 3 status
3344	D10	1		Port 4 status
3345	D11	1		Port 5 status
3346	D12	1		Port 6 status
3347	D13	1		Port 7 status
3348	D14	1		Port 8 status
3349	D15	1		Port 9 status
3350	D16	1		Port 10 status
3369	D29	1	HEX	Instance ID (Fixed 0x00, 2)
3370	D2A	3		Root bridge MAC
3373	D2D	1		Port 1 status
3374	D2E	1		Port 2 status
3375	D2F	1		Port 3 status
3376	D30	1		Port 4 status
3377	D31	1		Port 5 status
3378	D32	1		Port 6 status
3379	D33	1		Port 7 status
3380	D34	1		Port 8 status
3381	D35	1		Port 9 status
3382	D36	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description	
Dec	Hex				
System Information					
3401	D49	1	HEX	Instance ID (Fixed 0x00, 3)	
3402	D4A	3		Root bridge MAC	
3405	D4D	1		Port 1 status	
3406	D4E	1		Port 2 status	
3407	D4F	1		Port 3 status	
3408	D50	1		Port 4 status	
3409	D51	1		Port 5 status	
3410	D52	1		Port 6 status	
3411	D53	1		Port 7 status	
3412	D54	1		Port 8 status	
3413	D55	1		Port 9 status	
3414	D56	1		Port 10 status	
3433	D69	1		HEX	Instance ID (Fixed 0x00, 4)
3434	D6A	3	Root bridge MAC		
3437	D6D	1	Port 1 status		
3438	D6E	1	Port 2 status		
3439	D6F	1	Port 3 status		
3440	D70	1	Port 4 status		
3441	D71	1	Port 5 status		
3442	D72	1	Port 6 status		
3443	D73	1	Port 7 status		
3444	D74	1	Port 8 status		
3445	D75	1	Port 9 status		
3446	D76	1	Port 10 status		
3465	D89	1	HEX	Instance ID (Fixed 0x00, 5)	
3466	D8A	3		Root bridge MAC	
3469	D8D	1		Port 1 status	
3470	D8E	1		Port 2 status	
3471	D8F	1		Port 3 status	
3472	D90	1		Port 4 status	
3473	D91	1		Port 5 status	
3474	D92	1		Port 6 status	
3475	D93	1		Port 7 status	
3476	D94	1		Port 8 status	
3477	D95	1		Port 9 status	
3478	D96	1		Port 10 status	

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3497	DA9	1	HEX	Instance ID (Fixed 0x00, 6)
3498	DAA	3		Root bridge MAC
3501	DAD	1		Port 1 status
3502	DAE	1		Port 2 status
3503	DAF	1		Port 3 status
3504	DB0	1		Port 4 status
3505	DB1	1		Port 5 status
3506	DB2	1		Port 6 status
3507	DB3	1		Port 7 status
3508	DB4	1		Port 8 status
3509	DB5	1		Port 9 status
3510	DB6	1		Port 10 status
3529	DC9	1	HEX	Instance ID (Fixed 0x00, 7)
3530	DCA	3		Root bridge MAC
3533	DCD	1		Port 1 status
3534	DCE	1		Port 2 status
3535	DCF	1		Port 3 status
3536	DD0	1		Port 4 status
3537	DD1	1		Port 5 status
3538	DD2	1		Port 6 status
3539	DD3	1		Port 7 status
3540	DD4	1		Port 8 status
3541	DD5	1		Port 9 status
3542	DD6	1		Port 10 status
3561	DE9	1	HEX	Instance ID (Fixed 0x00, 8)
3562	DEA	3		Root bridge MAC
3565	DED	1		Port 1 status
3566	DEE	1		Port 2 status
3567	DEF	1		Port 3 status
3568	DF0	1		Port 4 status
3569	DF1	1		Port 5 status
3570	DF2	1		Port 6 status
3571	DF3	1		Port 7 status
3572	DF4	1		Port 8 status
3573	DF5	1		Port 9 status
3574	DF6	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3593	E09	1	HEX	Instance ID (Fixed 0x00, 9)
3594	E0A	3		Root bridge MAC
3597	E0D	1		Port 1 status
3598	E0E	1		Port 2 status
3599	E0F	1		Port 3 status
3600	E10	1		Port 4 status
3601	E11	1		Port 5 status
3602	E12	1		Port 6 status
3603	E13	1		Port 7 status
3604	E14	1		Port 8 status
3605	E15	1		Port 9 status
3606	E16	1		Port 10 status
3625	E29	1	HEX	Instance ID (Fixed 0x00, 10)
3626	E2A	3		Root bridge MAC
3629	E2D	1		Port 1 status
3630	E2E	1		Port 2 status
3631	E2F	1		Port 3 status
3632	E30	1		Port 4 status
3633	E31	1		Port 5 status
3634	E32	1		Port 6 status
3635	E33	1		Port 7 status
3636	E34	1		Port 8 status
3637	E35	1		Port 9 status
3638	E36	1		Port 10 status
3657	E49	1	HEX	Instance ID (Fixed 0x00, 11)
3658	E4A	3		Root bridge MAC
3661	E4D	1		Port 1 status
3662	E4E	1		Port 2 status
3663	E4F	1		Port 3 status
3664	E50	1		Port 4 status
3665	E51	1		Port 5 status
3666	E52	1		Port 6 status
3667	E53	1		Port 7 status
3668	E54	1		Port 8 status
3669	E55	1		Port 9 status
3670	E56	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3689	E69	1	HEX	Instance ID (Fixed 0x00, 12)
3690	E6A	3		Root bridge MAC
3693	E6D	1		Port 1 status
3694	E6E	1		Port 2 status
3695	E6F	1		Port 3 status
3696	E70	1		Port 4 status
3697	E71	1		Port 5 status
3698	E72	1		Port 6 status
3699	E73	1		Port 7 status
3700	E74	1		Port 8 status
3701	E75	1		Port 9 status
3702	E76	1		Port 10 status
3721	E89	1	HEX	Instance ID (Fixed 0x00, 13)
3722	E8A	3		Root bridge MAC
3725	E8D	1		Port 1 status
3726	E8E	1		Port 2 status
3727	E8F	1		Port 3 status
3728	E90	1		Port 4 status
3729	E91	1		Port 5 status
3730	E92	1		Port 6 status
3731	E93	1		Port 7 status
3732	E94	1		Port 8 status
3733	E95	1		Port 9 status
3734	E96	1		Port 10 status
3753	EA9	1	HEX	Instance ID (Fixed 0x00, 14)
3754	EAA	3		Root bridge MAC
3757	EAD	1		Port 1 status
3758	EAE	1		Port 2 status
3759	EAF	1		Port 3 status
3760	EB0	1		Port 4 status
3761	EB1	1		Port 5 status
3762	EB2	1		Port 6 status
3763	EB3	1		Port 7 status
3764	EB4	1		Port 8 status
3765	EB5	1		Port 9 status
3766	EB6	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3785	EC9	1	HEX	Instance ID (Fixed 0x00, 15)
3786	ECA	3		Root bridge MAC
3789	ECD	1		Port 1 status
3790	ECE	1		Port 2 status
3791	ECF	1		Port 3 status
3792	ED0	1		Port 4 status
3793	ED1	1		Port 5 status
3794	ED2	1		Port 6 status
3795	ED3	1		Port 7 status
3796	ED4	1		Port 8 status
3797	ED5	1		Port 9 status
3798	ED6	1		Port 10 status
3817	EE9	1	HEX	Instance ID (Fixed 0x00, 16)
3818	EEA	3		Root bridge MAC
3821	EED	1		Port 1 status
3822	EEE	1		Port 2 status
3823	EEF	1		Port 3 status
3824	EF0	1		Port 4 status
3825	EF1	1		Port 5 status
3826	EF2	1		Port 6 status
3827	EF3	1		Port 7 status
3828	EF4	1		Port 8 status
3829	EF5	1		Port 9 status
3830	EF6	1		Port 10 status
3849	F09	1	HEX	Instance ID (Fixed 0x00, 17)
3850	F0A	3		Root bridge MAC
3853	F0D	1		Port 1 status
3854	F0E	1		Port 2 status
3855	F0F	1		Port 3 status
3856	F10	1		Port 4 status
3857	F11	1		Port 5 status
3858	F12	1		Port 6 status
3859	F13	1		Port 7 status
3860	F14	1		Port 8 status
3861	F15	1		Port 9 status
3862	F16	1		Port 10 status

Table 164: MODBUS Register

Table 10-1: M02B00 Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3881	F29	1	HEX	Instance ID (Fixed 0x00, 18)
3882	F2A	3		Root bridge MAC
3885	F2D	1		Port 1 status
3886	F2E	1		Port 2 status
3887	F2F	1		Port 3 status
3888	F30	1		Port 4 status
3889	F31	1		Port 5 status
3890	F32	1		Port 6 status
3891	F33	1		Port 7 status
3892	F34	1		Port 8 status
3893	F35	1		Port 9 status
3894	F36	1		Port 10 status
3913	F49	1	HEX	Instance ID (Fixed 0x00, 19)
3914	F4A	3		Root bridge MAC
3917	F4D	1		Port 1 status
3918	F4E	1		Port 2 status
3919	F4F	1		Port 3 status
3920	F50	1		Port 4 status
3921	F51	1		Port 5 status
3922	F52	1		Port 6 status
3923	F53	1		Port 7 status
3924	F54	1		Port 8 status
3925	F55	1		Port 9 status
3926	F56	1		Port 10 status
3945	F69	1	HEX	Instance ID (Fixed 0x00, 20)
3946	F6A	3		Root bridge MAC
3949	F6D	1		Port 1 status
3950	F6E	1		Port 2 status
3951	F6F	1		Port 3 status
3952	F70	1		Port 4 status
3953	F71	1		Port 5 status
3954	F72	1		Port 6 status
3955	F73	1		Port 7 status
3956	F74	1		Port 8 status
3957	F75	1		Port 9 status
3958	F76	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
3977	F89	1	HEX	Instance ID (Fixed 0x00, 21)
3978	F8A	3		Root bridge MAC
3981	F8D	1		Port 1 status
3982	F8E	1		Port 2 status
3983	F8F	1		Port 3 status
3984	F90	1		Port 4 status
3985	F91	1		Port 5 status
3986	F92	1		Port 6 status
3987	F93	1		Port 7 status
3988	F94	1		Port 8 status
3989	F95	1		Port 9 status
3990	F96	1		Port 10 status
4009	FA9	1	HEX	Instance ID (Fixed 0x00, 22)
4010	FAA	3		Root bridge MAC
4013	FAD	1		Port 1 status
4014	FAE	1		Port 2 status
4015	FAF	1		Port 3 status
4016	FB0	1		Port 4 status
4017	FB1	1		Port 5 status
4018	FB2	1		Port 6 status
4019	FB3	1		Port 7 status
4020	FB4	1		Port 8 status
4021	FB5	1		Port 9 status
4022	FB6	1		Port 10 status
4041	FC9	1	HEX	Instance ID (Fixed 0x00, 23)
4042	FCA	3		Root bridge MAC
4045	FCD	1		Port 1 status
4046	FCE	1		Port 2 status
4047	FCF	1		Port 3 status
4048	FD0	1		Port 4 status
4049	FD1	1		Port 5 status
4050	FD2	1		Port 6 status
4051	FD3	1		Port 7 status
4052	FD4	1		Port 8 status
4053	FD5	1		Port 9 status
4054	FD6	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
4073	FE9	1	HEX	Instance ID (Fixed 0x00, 24)
4074	FEA	3		Root bridge MAC
4077	FED	1		Port 1 status
4078	FEE	1		Port 2 status
4079	FEF	1		Port 3 status
4080	FF0	1		Port 4 status
4081	FF1	1		Port 5 status
4082	FF2	1		Port 6 status
4083	FF3	1		Port 7 status
4084	FF4	1		Port 8 status
4085	FF5	1		Port 9 status
4086	FF6	1		Port 10 status
4105	1009	1	HEX	Instance ID (Fixed 0x00, 25)
4106	100A	3		Root bridge MAC
4109	100D	1		Port 1 status
4110	100E	1		Port 2 status
4111	100F	1		Port 3 status
4112	1010	1		Port 4 status
4113	1011	1		Port 5 status
4114	1012	1		Port 6 status
4115	1013	1		Port 7 status
4116	1014	1		Port 8 status
4117	1015	1		Port 9 status
4118	1016	1		Port 10 status
4137	1029	1	HEX	Instance ID (Fixed 0x00, 26)
4138	102A	3		Root bridge MAC
4141	102D	1		Port 1 status
4142	102E	1		Port 2 status
4143	102F	1		Port 3 status
4144	1030	1		Port 4 status
4145	1031	1		Port 5 status
4146	1032	1		Port 6 status
4147	1033	1		Port 7 status
4148	1034	1		Port 8 status
4149	1035	1		Port 9 status
4150	1036	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
4169	1049	1	HEX	Instance ID (Fixed 0x00, 27)
4170	104A	3		Root bridge MAC
4173	104D	1		Port 1 status
4174	104E	1		Port 2 status
4175	104F	1		Port 3 status
4176	1050	1		Port 4 status
4177	1051	1		Port 5 status
4178	1052	1		Port 6 status
4179	1053	1		Port 7 status
4180	1054	1		Port 8 status
4181	1055	1		Port 9 status
4182	1056	1		Port 10 status
4201	1069	1	HEX	Instance ID (Fixed 0x00, 28)
4202	106A	3		Root bridge MAC
4205	106D	1		Port 1 status
4206	106E	1		Port 2 status
4207	106F	1		Port 3 status
4208	1070	1		Port 4 status
4209	1071	1		Port 5 status
4210	1072	1		Port 6 status
4211	1073	1		Port 7 status
4212	1074	1		Port 8 status
4213	1075	1		Port 9 status
4214	1076	1		Port 10 status
4233	1089	1	HEX	Instance ID (Fixed 0x00, 29)
4234	108A	3		Root bridge MAC
4237	108D	1		Port 1 status
4238	108E	1		Port 2 status
4239	108F	1		Port 3 status
4240	1090	1		Port 4 status
4241	1091	1		Port 5 status
4242	1092	1		Port 6 status
4243	1093	1		Port 7 status
4244	1094	1		Port 8 status
4245	1095	1		Port 9 status
4246	1096	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
4265	10A9	1	HEX	Instance ID (Fixed 0x00, 30)
4266	10AA	3		Root bridge MAC
4269	10AD	1		Port 1 status
4270	10AE	1		Port 2 status
4271	10AF	1		Port 3 status
4272	10B0	1		Port 4 status
4273	10B1	1		Port 5 status
4274	10B2	1		Port 6 status
4275	10B3	1		Port 7 status
4276	10B4	1		Port 8 status
4277	10B5	1		Port 9 status
4278	10B6	1		Port 10 status
4297	10C9	1	HEX	Instance ID (Fixed 0x00, 31)
4298	10CA	3		Root bridge MAC
4301	10CD	1		Port 1 status
4302	10CE	1		Port 2 status
4303	10CF	1		Port 3 status
4304	10D0	1		Port 4 status
4305	10D1	1		Port 5 status
4306	10D2	1		Port 6 status
4307	10D3	1		Port 7 status
4308	10D4	1		Port 8 status
4309	10D5	1		Port 9 status
4310	10D6	1		Port 10 status
4329	10E9	1	HEX	Instance ID (Fixed 0x00, 32)
4330	10EA	3		Root bridge MAC
4333	10ED	1		Port 1 status
4334	10EE	1		Port 2 status
4335	10EF	1		Port 3 status
4336	10F0	1		Port 4 status
4337	10F1	1		Port 5 status
4338	10F2	1		Port 6 status
4339	10F3	1		Port 7 status
4340	10F4	1		Port 8 status
4341	10F5	1		Port 9 status
4342	10F6	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
4361	1109	1	HEX	Instance ID (Fixed 0x00, 33)
4362	110A	3		Root bridge MAC
4365	110D	1		Port 1 status
4366	110E	1		Port 2 status
4367	110F	1		Port 3 status
4368	1110	1		Port 4 status
4369	1111	1		Port 5 status
4370	1112	1		Port 6 status
4371	1113	1		Port 7 status
4372	1114	1		Port 8 status
4373	1115	1		Port 9 status
4374	1116	1		Port 10 status
4393	1129	1	HEX	Instance ID (Fixed 0x00, 34)
4394	112A	3		Root bridge MAC
4397	112D	1		Port 1 status
4398	112E	1		Port 2 status
4399	112F	1		Port 3 status
4400	1130	1		Port 4 status
4401	1131	1		Port 5 status
4402	1132	1		Port 6 status
4403	1133	1		Port 7 status
4404	1134	1		Port 8 status
4405	1135	1		Port 9 status
4406	1136	1		Port 10 status
4425	1149	1	HEX	Instance ID (Fixed 0x00, 35)
4426	114A	3		Root bridge MAC
4429	114D	1		Port 1 status
4430	114E	1		Port 2 status
4431	114F	1		Port 3 status
4432	1150	1		Port 4 status
4433	1151	1		Port 5 status
4434	1152	1		Port 6 status
4435	1153	1		Port 7 status
4436	1154	1		Port 8 status
4437	1155	1		Port 9 status
4438	1156	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
4457	1169	1	HEX	Instance ID (Fixed 0x00, 36)
4458	116A	3		Root bridge MAC
4461	116D	1		Port 1 status
4462	116E	1		Port 2 status
4463	116F	1		Port 3 status
4464	1170	1		Port 4 status
4465	1171	1		Port 5 status
4466	1172	1		Port 6 status
4467	1173	1		Port 7 status
4468	1174	1		Port 8 status
4469	1175	1		Port 9 status
4470	1176	1		Port 10 status
4489	1189	1	HEX	Instance ID (Fixed 0x00, 37)
4490	118A	3		Root bridge MAC
4493	118D	1		Port 1 status
4494	118E	1		Port 2 status
4495	118F	1		Port 3 status
4496	1190	1		Port 4 status
4497	1191	1		Port 5 status
4498	1192	1		Port 6 status
4499	1193	1		Port 7 status
4500	1194	1		Port 8 status
4501	1195	1		Port 9 status
4502	1196	1		Port 10 status
4521	11A9	1	HEX	Instance ID (Fixed 0x00, 38)
4522	11AA	3		Root bridge MAC
4525	11AD	1		Port 1 status
4526	11AE	1		Port 2 status
4527	11AF	1		Port 3 status
4528	11B0	1		Port 4 status
4529	11B1	1		Port 5 status
4530	11B2	1		Port 6 status
4531	11B3	1		Port 7 status
4532	11B4	1		Port 8 status
4533	11B5	1		Port 9 status
4534	11B6	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
4553	11C9	1	HEX	Instance ID (Fixed 0x00, 39)
4554	11CA	3		Root bridge MAC
4557	11CD	1		Port 1 status
4558	11CE	1		Port 2 status
4559	11CF	1		Port 3 status
4560	11D0	1		Port 4 status
4561	11D1	1		Port 5 status
4562	11D2	1		Port 6 status
4563	11D3	1		Port 7 status
4564	11D4	1		Port 8 status
4565	11D5	1		Port 9 status
4566	11D6	1		Port 10 status
4585	11E9	1	HEX	Instance ID (Fixed 0x00, 40)
4586	11EA	3		Root bridge MAC
4589	11ED	1		Port 1 status
4590	11EE	1		Port 2 status
4591	11EF	1		Port 3 status
4592	11F0	1		Port 4 status
4593	11F1	1		Port 5 status
4594	11F2	1		Port 6 status
4595	11F3	1		Port 7 status
4596	11F4	1		Port 8 status
4597	11F5	1		Port 9 status
4598	11F6	1		Port 10 status
4617	1209	1	HEX	Instance ID (Fixed 0x00, 41)
4618	120A	3		Root bridge MAC
4621	120D	1		Port 1 status
4622	120E	1		Port 2 status
4623	120F	1		Port 3 status
4624	1210	1		Port 4 status
4625	1211	1		Port 5 status
4626	1212	1		Port 6 status
4627	1213	1		Port 7 status
4628	1214	1		Port 8 status
4629	1215	1		Port 9 status
4630	1216	1		Port 10 status

Table 164: MODBUS Register

Table 10-7. M0B500 Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
4649	1229	1	HEX	Instance ID (Fixed 0x00, 42)
4650	122A	3		Root bridge MAC
4653	122D	1		Port 1 status
4654	122E	1		Port 2 status
4655	122F	1		Port 3 status
4656	1230	1		Port 4 status
4657	1231	1		Port 5 status
4658	1232	1		Port 6 status
4659	1233	1		Port 7 status
4660	1234	1		Port 8 status
4661	1235	1		Port 9 status
4662	1236	1		Port 10 status
4681	1249	1	HEX	Instance ID (Fixed 0x00, 43)
4682	124A	3		Root bridge MAC
4685	124D	1		Port 1 status
4686	124E	1		Port 2 status
4687	124F	1		Port 3 status
4688	1250	1		Port 4 status
4689	1251	1		Port 5 status
4690	1252	1		Port 6 status
4691	1253	1		Port 7 status
4692	1254	1		Port 8 status
4693	1255	1		Port 9 status
4694	1256	1		Port 10 status
4713	1269	1	HEX	Instance ID (Fixed 0x00, 44)
4714	126A	3		Root bridge MAC
4717	126D	1		Port 1 status
4718	126E	1		Port 2 status
4719	126F	1		Port 3 status
4720	1270	1		Port 4 status
4721	1271	1		Port 5 status
4722	1272	1		Port 6 status
4723	1273	1		Port 7 status
4724	1274	1		Port 8 status
4725	1275	1		Port 9 status
4726	1276	1		Port 10 status

Table 164: MODBUS Register

Table 10-1: M0B500 Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
4841	12E9	1	HEX	Instance ID (Fixed 0x00, 48)
4842	12EA	3		Root bridge MAC
4845	12ED	1		Port 1 status
4846	12EE	1		Port 2 status
4847	12EF	1		Port 3 status
4848	12F0	1		Port 4 status
4849	12F1	1		Port 5 status
4850	12F2	1		Port 6 status
4851	12F3	1		Port 7 status
4852	12F4	1		Port 8 status
4853	12F5	1		Port 9 status
4854	12F6	1		Port 10 status
4873	1309	1	HEX	Instance ID (Fixed 0x00, 49)
4874	130A	3		Root bridge MAC
4877	130D	1		Port 1 status
4878	130E	1		Port 2 status
4879	130F	1		Port 3 status
4880	1310	1		Port 4 status
4881	1311	1		Port 5 status
4882	1312	1		Port 6 status
4883	1313	1		Port 7 status
4884	1314	1		Port 8 status
4885	1315	1		Port 9 status
4886	1316	1		Port 10 status
4905	1329	1	HEX	Instance ID (Fixed 0x00, 50)
4906	132A	3		Root bridge MAC
4909	132D	1		Port 1 status
4910	132E	1		Port 2 status
4911	132F	1		Port 3 status
4912	1330	1		Port 4 status
4913	1331	1		Port 5 status
4914	1332	1		Port 6 status
4915	1333	1		Port 7 status
4916	1334	1		Port 8 status
4917	1335	1		Port 9 status
4918	1336	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
4937	1349	1	HEX	Instance ID (Fixed 0x00, 51)
4938	134A	3		Root bridge MAC
4941	134D	1		Port 1 status
4942	134E	1		Port 2 status
4943	134F	1		Port 3 status
4944	1350	1		Port 4 status
4945	1351	1		Port 5 status
4946	1352	1		Port 6 status
4947	1353	1		Port 7 status
4948	1354	1		Port 8 status
4949	1355	1		Port 9 status
4950	1356	1		Port 10 status
4969	1369	1	HEX	Instance ID (Fixed 0x00, 52)
4970	136A	3		Root bridge MAC
4973	136D	1		Port 1 status
4974	136E	1		Port 2 status
4975	136F	1		Port 3 status
4976	1370	1		Port 4 status
4977	1371	1		Port 5 status
4978	1372	1		Port 6 status
4979	1373	1		Port 7 status
4980	1374	1		Port 8 status
4981	1375	1		Port 9 status
4982	1376	1		Port 10 status
5001	1389	1	HEX	Instance ID (Fixed 0x00, 53)
5002	138A	3		Root bridge MAC
5005	138D	1		Port 1 status
5006	138E	1		Port 2 status
5007	138F	1		Port 3 status
5008	1390	1		Port 4 status
5009	1391	1		Port 5 status
5010	1392	1		Port 6 status
5011	1393	1		Port 7 status
5012	1394	1		Port 8 status
5013	1395	1		Port 9 status
5014	1396	1		Port 10 status

Table 164: MODBUS Register

Table 10-1: M05B00 Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
5033	13A9	1	HEX	Instance ID (Fixed 0x00, 54)
5034	13AA	3		Root bridge MAC
5037	13AD	1		Port 1 status
5038	13AE	1		Port 2 status
5039	13AF	1		Port 3 status
5040	13B0	1		Port 4 status
5041	13B1	1		Port 5 status
5042	13B2	1		Port 6 status
5043	13B3	1		Port 7 status
5044	13B4	1		Port 8 status
5045	13B5	1		Port 9 status
5046	13B6	1		Port 10 status
5065	13C9	1	HEX	Instance ID (Fixed 0x00, 55)
5066	13CA	3		Root bridge MAC
5069	13CD	1		Port 1 status
5070	13CE	1		Port 2 status
5071	13CF	1		Port 3 status
5072	13D0	1		Port 4 status
5073	13D1	1		Port 5 status
5074	13D2	1		Port 6 status
5075	13D3	1		Port 7 status
5076	13D4	1		Port 8 status
5077	13D5	1		Port 9 status
5078	13D6	1		Port 10 status
5097	13E9	1	HEX	Instance ID (Fixed 0x00, 56)
5098	13EA	3		Root bridge MAC
5101	13ED	1		Port 1 status
5102	13EE	1		Port 2 status
5103	13EF	1		Port 3 status
5104	13F0	1		Port 4 status
5105	13F1	1		Port 5 status
5106	13F2	1		Port 6 status
5107	13F3	1		Port 7 status
5108	13F4	1		Port 8 status
5109	13F5	1		Port 9 status
5110	13F6	1		Port 10 status

Table 164: MODBUS Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
5129	1409	1	HEX	Instance ID (Fixed 0x00, 57)
5130	140A	3		Root bridge MAC
5133	140D	1		Port 1 status
5134	140E	1		Port 2 status
5135	140F	1		Port 3 status
5136	1410	1		Port 4 status
5137	1411	1		Port 5 status
5138	1412	1		Port 6 status
5139	1413	1		Port 7 status
5140	1414	1		Port 8 status
5141	1415	1		Port 9 status
5142	1416	1		Port 10 status
5161	1429	1	HEX	Instance ID (Fixed 0x00, 58)
5162	142A	3		Root bridge MAC
5165	142D	1		Port 1 status
5166	142E	1		Port 2 status
5167	142F	1		Port 3 status
5168	1430	1		Port 4 status
5169	1431	1		Port 5 status
5170	1432	1		Port 6 status
5171	1433	1		Port 7 status
5172	1434	1		Port 8 status
5173	1435	1		Port 9 status
5174	1436	1		Port 10 status
5193	1449	1	HEX	Instance ID (Fixed 0x00, 59)
5194	144A	3		Root bridge MAC
5197	144D	1		Port 1 status
5198	144E	1		Port 2 status
5199	144F	1		Port 3 status
5200	1450	1		Port 4 status
5201	1451	1		Port 5 status
5202	1452	1		Port 6 status
5203	1453	1		Port 7 status
5204	1454	1		Port 8 status
5205	1455	1		Port 9 status
5206	1456	1		Port 10 status

Table 164: MODBUS Register

Table 10-1: M0B500 Register

Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
5225	1469	1	HEX	Instance ID (Fixed 0x00, 60)
5226	146A	3		Root bridge MAC
5229	146D	1		Port 1 status
5230	146E	1		Port 2 status
5231	146F	1		Port 3 status
5232	1470	1		Port 4 status
5233	1471	1		Port 5 status
5234	1472	1		Port 6 status
5235	1473	1		Port 7 status
5236	1474	1		Port 8 status
5237	1475	1		Port 9 status
5238	1476	1		Port 10 status
5257	1489	1	HEX	Instance ID (Fixed 0x00, 61)
5258	148A	3		Root bridge MAC
5261	148D	1		Port 1 status
5262	148E	1		Port 2 status
5263	148F	1		Port 3 status
5264	1490	1		Port 4 status
5265	1491	1		Port 5 status
5266	1492	1		Port 6 status
5267	1493	1		Port 7 status
5268	1494	1		Port 8 status
5269	1495	1		Port 9 status
5270	1496	1		Port 10 status
5289	14A9	1	HEX	Instance ID (Fixed 0x00, 62)
5290	14AA	3		Root bridge MAC
5293	14AD	1		Port 1 status
5294	14AE	1		Port 2 status
5295	14AF	1		Port 3 status
5296	14B0	1		Port 4 status
5297	14B1	1		Port 5 status
5298	14B2	1		Port 6 status
5299	14B3	1		Port 7 status
5300	14B4	1		Port 8 status
5301	14B5	1		Port 9 status
5302	14B6	1		Port 10 status

Table 164: MODBUS Register

Table 10-1: MDDB00 Register				
Register Address		Data Length/ Word	Format	Description
Dec	Hex			
System Information				
5321	14C9	1	HEX	Instance ID (Fixed 0x00, 63)
5322	14CA	3		Root bridge MAC
5325	14CD	1		Port 1 status
5326	14CE	1		Port 2 status
5327	14CF	1		Port 3 status
5328	14D0	1		Port 4 status
5329	14D1	1		Port 5 status
5330	14D2	1		Port 6 status
5331	14D3	1		Port 7 status
5332	14D4	1		Port 8 status
5333	14D5	1		Port 9 status
5334	14D6	1		Port 10 status

List of Figures

Figure 1: Front View of the Industrial Managed Switch.....	24
Figure 2: Top View of the Industrial Managed Switch (Example).....	26
Figure 3: Power Supply (PWR/RPS)	27
Figure 4: Network Connections	28
Figure 5: Device LEDs	30
Figure 6: Port LEDs.....	32
Figure 7: DIP Switches (Example).....	33
Figure 8: Reset Button	34
Figure 9: Label (Example)	35
Figure 10: MAC Address Table Flowchart.....	46
Figure 11: Half-Duplex Mode.....	48
Figure 12: Full-Duplex Mode	48
Figure 13: MOD without MVR.....	63
Figure 14: MOD supports MVR	63
Figure 15: Multicast Address	66
Figure 16: Port-Based Q-in-Q.....	76
Figure 17: Configuration Example	76
Figure 18: Application 1 (via a Router)	78
Figure 19: Application 2 (Local in Different VLANs).....	78
Figure 20: Dual Ring Switch ABC.....	81
Figure 21: Dual Ring Switch AB	81
Figure 22: Dual Homing	85
Figure 23: Jet Ring.....	89
Figure 24: DHCP Snooping	99
Figure 25: 802.1x	104
Figure 26: RADIUS Server	104
Figure 27: WBM “System Information” Page	119
Figure 28: WBM Page, “General Settings” – “System” Tab	121
Figure 29: WBM Page, “General” – “Jumbo Frame” Tab	123
Figure 30: WBM Page, “General” – “SNTP” Tab	124
Figure 31: WBM Page, “General” – “Management Host” Tab	127
Figure 32: WBM Page, “MAC Management” – “Static MAC Settings” Tab.....	128
Figure 33: WBM Page, “MAC Management” – “MAC Table” Tab	130
Figure 34: WBM Page, “MAC Management” – “Age Time Setting” Tab	131
Figure 35: WBM Page, “MAC Management” – “Refusal MAC Settings” Tab ...	132
Figure 36: WBM “Port Mirroring” Page	133
Figure 37: WBM Page, “Port Settings” – “General Settings” Tab	135
Figure 38: WBM Page, “Port Settings” – “Information” Tab	137
Figure 39: WBM “QoS” Page – “Port Priority” Tab.....	138
Figure 40: WBM “QoS” Page – “IP DiffServ (DSCP)” Tab	139
Figure 41: WBM “QoS” Page – “Priority/Queue Mapping” Tab	140
Figure 42: WBM “QoS” Page – “Schedule Mode” Tab.....	141
Figure 43: WBM “Rate Limitation” Page – “Storm Control” Tab	143
Figure 44: WBM “Rate Limitation” Page – “Bandwidth Limitation” Tab	145
Figure 45: WBM “IGMP Snooping” Page – “General Settings” Tab	146
Figure 46: WBM “IGMP Snooping” Page – “Port Settings” Tab	148
Figure 47: WBM “IGMP Snooping” Page – “Querier Settings” Tab.....	150

Figure 48: WBM "IGMP Filtering" Page – "General Settings" Tab.....	151
Figure 49: WBM "IGMP Filtering" Page – "Group Settings" Tab	152
Figure 50: WBM "IGMP Filtering" Page – "Port Settings" Tab.....	153
Figure 51: WBM "MVR" Page – "MVR Settings" Tab	154
Figure 52: WBM "MVR" Page – "Group Settings" Tab	156
Figure 53: WBM "Multicast Address" Page.....	157
Figure 54: WBM "Multicast IP Statistics" Page	158
Figure 55: WBM "Port Isolation" Page	159
Figure 56: WBM "VLAN" Page – "VLAN Settings" Tab	161
Figure 57: WBM "VLAN" Page – "Tag Settings" Tab	163
Figure 58: WBM "VLAN" Page – "Port Settings" Tab	164
Figure 59: WBM "GARP VLAN Registration Protocol" Page – "GVRP" Tab	166
Figure 60: WBM "GARP VLAN Registration Protocol" Page – "GVRP Timer" Tab	168
Figure 61: WBM "IP-Subnet-VLAN"	170
Figure 62: WBM "MAC VLAN" Page.....	171
Figure 63: WBM "Protocol VLAN" Page.....	172
Figure 64: WBM "Q-in-Q" Page – "VLAN Stacking" Tab	173
Figure 65: WBM "Q-in-Q" Page – "Port-based Q-in-Q" Tab	175
Figure 66: WBM "Q-in-Q" Page – "Selective Q-in-Q" Tab	176
Figure 67: WBM "DHCP Relay" Page.....	178
Figure 68: WBM "DHCP Options" Page – "Option 82" Tab	179
Figure 69: WBM "Dual Homing" Page	180
Figure 70: WBM "Dual Ring" Page	182
Figure 71: WBM "ERPS" Page – "Ring Settings" Tab.....	184
Figure 72: WBM "ERPS" Page – "Instance Settings" Tab.....	188
Figure 73: WBM "Link Aggregation" Page – "Static Trunk" Tab	189
Figure 74: WBM "Link Aggregation" Page – "LACP" Tab.....	191
Figure 75: WBM "Link Aggregation" Page – "LACP Info." Tab	193
Figure 76: WBM "LLDP" Page – "Settings" Tab.....	195
Figure 77: WBM "LLDP" Page – "Neighbor" Tab	197
Figure 78: WBM "Loop Detection" Page	198
Figure 79: WBM "Jet Ring" Page.....	200
Figure 80: WBM "MODBUS" Page	201
Figure 81: WBM "STP" Page – "General Settings" Tab	202
Figure 82: WBM "STP" Page – "Port Parameters" Tab.....	204
Figure 83: WBM "STP" Page – "STP Status" Tab.....	207
Figure 84: WBM "Xpress Ring" Page	208
Figure 85: WBM "DHCP Snooping" Page – "DHCP Snooping" Tab.....	210
Figure 86: WBM "DHCP Snooping" Page – "Port Settings" Tab	212
Figure 87: WBM "DHCP Snooping" Page – "Server Screening" Tab	213
Figure 88: WBM "Binding Table" Page – "Static Entry" Tab.....	214
Figure 89: WBM "Binding Table" Page – "Binding Table" Tab	216
Figure 90: WBM "ARP Inspection" Page – "ARP Inspection" Tab.....	217
Figure 91: WBM "ARP Inspection" Page – "Filter Table" Tab	219
Figure 92: WBM "Access Control List" Page	220
Figure 93: WBM "802.1x" Page – "Global Settings" Tab.....	224
Figure 94: WBM "802.1x" Page – "Port Settings" Tab.....	227
Figure 95: WBM "Port Security" Page	230
Figure 96: WBM "Alarm Information" Page.....	232

Figure 97: WBM “Monitor Information” Page	233
Figure 98: WBM “Port Statistics” Page	235
Figure 99: WBM “Port Utilization” Page	236
Figure 100: WBM “RMON Statistics” Page	237
Figure 101: WBM “SFP Information” Page	240
Figure 102: WBM “Traffic Monitor” Page	242
Figure 103: WBM Page, “SNMP” – “SNMP Settings” Tab	244
Figure 104: WBM Page, “SNMP” – “Community Name” Tab	245
Figure 105: WBM Page, “SNMP Trap” – “Trap Receiver Settings” Tab	247
Figure 106: WBM “Auto Provision” Page	248
Figure 107: WBM “Mail Alarm” Page	249
Figure 108: WBM Page, “Maintenance” – “Configuration” Tab	251
Figure 109: WBM Page, “Maintenance” – “Firmware” Tab	253
Figure 110: WBM Page, “Maintenance” – “Reboot” Tab	254
Figure 111: WBM Page, “Maintenance” – “Reboot” Tab – Message	254
Figure 112: WBM “Maintenance” Page – “Server” Tab	255
Figure 113: WBM “System Log” Page	257
Figure 114: WBM “User Account” Page	259
Figure 115: RJ-45 Connector Pin Assignment	261
Figure 116: Connector Pin Assignment RJ-45 to DB9	261

List of Tables

Table 1: Number Notation	13
Table 2: Font Conventions	13
Table 3: Legend for the Figure “Front View of the Industrial Managed Switch” ...	24
Table 4: Legend for the Figure “Front View of the Industrial Managed Switch” ...	26
Table 5: Legend for Figure “Power Supply (PWR/RPS)”	27
Table 6: Legend for Figure “Network Connections”	28
Table 7: Legend for Figure “Device LEDs”	30
Table 8: Legend for Figure “Port LEDs”	32
Table 9: Legend for Figure “DIP Switches (Example)”	33
Table 10: Legend for Figure “Reset Button”	34
Table 11: Legend for Figure “Label”	35
Table 12: Technical Data – Device Data	36
Table 13: Technical Data – System Data	36
Table 14: Technical Data – Power Supply	36
Table 15: Technical Data – Communication	37
Table 16: Technical Data – Environmental Conditions	37
Table 17: Assignment UL – Hardware Version	38
Table 18: Priority Levels	54
Table 19: Multicast Classes and Address Ranges	65
Table 20: IP Multicast Addresses	66
Table 21: Option Frame Format	80
Table 22: Option Frame Format	80
Table 23: Frame Format of the “Circuit ID” Sub-Option	80
Table 24: Frame Format of the “Remote ID” Sub-Option	80
Table 25: Format of the “Circuit ID” Sub-Option	80
Table 26: STP Path Costs	92
Table 27: Default Settings for the Telnet Port	114
Table 28: Default Settings for the Console Port	115
Table 29: Login Screen	115
Table 30: Overview - Navigation Links and WBM Pages	117
Table 31: WBM “System Information” Page	120
Table 32: WBM Page, “General Settings” – “System” Tab	122
Table 33: WBM Page, “General” – “Jumbo Frame” Tab	123
Table 34: WBM Page, “General” – “SNTP” Tab	125
Table 35: WBM Page, “General” – “Management Host” Tab	127
Table 36: WBM Page, “MAC Management” – “Static MAC Settings” Tab	129
Table 37: WBM Page, “MAC Management” – “MAC Table” Tab	130
Table 38: WBM Page, “MAC Management” – “Age Time Setting” Tab	131
Table 39: WBM Page, “MAC Management” – “Refusal MAC Settings” Tab	132
Table 40: WBM “Port Mirroring” Page	134
Table 41: WBM Page, “Port Settings” – “General Settings” Tab	136
Table 42: WBM Page, “Port Settings” – “Information” Tab	137
Table 43: WBM “QoS” Page – “Port Priority” Tab	138
Table 44: WBM “QoS” Page – “IP DiffServ (DSCP)” Tab	139
Table 45: WBM “QoS” Page – “Priority/Queue Mapping” Tab	140
Table 46: Default Settings	140
Table 47: WBM “QoS” Page – “Schedule Mode” Tab	142

Table 48: WBM "Rate Limitation" Page – "Storm Control" Tab	144
Table 49: WBM "Rate Limitation" Page – "Bandwidth Limitation" Tab	145
Table 50: WBM "IGMP Snooping" Page – "General Settings" Tab	147
Table 51: WBM "IGMP Snooping" Page – "Port Settings" Tab	149
Table 52: WBM "IGMP Snooping" Page – "Querier Settings" Tab	150
Table 53: WBM "IGMP Filtering" Page – "General Settings" Tab	151
Table 54: WBM "IGMP Filtering" Page – "Group Settings" Tab	152
Table 55: WBM "IGMP Filtering" Page – "Port Settings" Tab	153
Table 56: WBM "MVR" Page – "MVR Settings" Tab	155
Table 57: WBM "MVR" Page – "Group Settings" Tab	156
Table 58: WBM "Multicast Address" Page	157
Table 59: WBM "Multicast IP Statistics" Page	158
Table 60: WBM "Port Isolation" Page	160
Table 61: WBM "VLAN" Page – "VLAN Settings" Tab	161
Table 62: WBM "VLAN" Page – "TAG Settings" Tab	163
Table 63: WBM "VLAN" Page – "Port Settings" Tab	165
Table 64: WBM "GARP VLAN Registration Protocol" Page – "GVRP" Tab	167
Table 65: WBM "GARP VLAN Registration Protocol" Page – "GVRP Timer" Tab	169
Table 66: WBM "IP Subnet VLAN" Page	170
Table 67: WBM "MAC VLAN" Page	171
Table 68: WBM "Protocol VLAN" Page	172
Table 69: WBM "Q-in-Q" Page – "VLAN Stacking" Tab	174
Table 70: WBM "Q-in-Q" Page – "Port-based Q-in-Q" Tab	175
Table 71: WBM "Q-in-Q" Page – "Selective Q-in-Q" Tab	177
Table 72: WBM "DHCP Relay" Page	178
Table 73: WBM "DHCP Options" Page – "Option 82" Tab	179
Table 74: WBM "Dual Homing" Page	180
Table 75: WBM "Dual Ring" Page	183
Table 76: WBM "ERPS" Page – "Ring Settings" Tab	185
Table 77: WBM "ERPS" Page – "Instance Settings" Tab	188
Table 78: WBM "Link Aggregation" Page – "Static Trunk" Tab	190
Table 79: WBM "Link Aggregation" Page – "LACP" Tab	192
Table 80: WBM "Link Aggregation" Page – "LACP Info." Tab	194
Table 81: WBM "LLDP" Page – "Settings" Tab	196
Table 82: WBM "LLDP" Page – "Neighbor" Tab	197
Table 83: WBM "Loop Detection" Page	199
Table 84: WBM "Jet Ring" Page	200
Table 85: WBM "MODBUS" Page	201
Table 86: WBM "STP" Page – "General Settings" Tab	203
Table 87: WBM "STP" Page – "Port Parameters" Tab	205
Table 88: WBM "STP" Page – "STP Status" Tab	207
Table 89: WBM "Xpress Ring" Page	209
Table 90: WBM "DHCP Snooping" Page – "DHCP Snooping" Tab	211
Table 91: WBM "DHCP Snooping" Page – "Port Settings" Tab	212
Table 92: WBM "DHCP Snooping" Page – "Server Screening" Tab	213
Table 93: WBM "Binding Table" Page – "Static Entry" Tab	215
Table 94: WBM "Binding Table" Page – "Binding Table" Tab	216
Table 95: WBM "ARP Inspection" Page – "ARP Inspection" Tab	218
Table 96: WBM "ARP Inspection" Page – "Filter Table" Tab	219

Table 97: WBM "Access Control List" Page.....	221
Table 98: WBM "802.1x" Page – "Global Settings" Tab	225
Table 99: WBM "802.1x" Page – "Port Settings" Tab	228
Table 100: WBM "Port Security" Page.....	231
Table 101: WBM "Alarm Information" Page	232
Table 102: WBM "Monitor Information" Page	234
Table 103: WBM "Port Statistics" Page	235
Table 104: WBM "Port Utilization" Page	236
Table 105: WBM "RMON Statistics" Page	238
Table 106: WBM "SFP Information" Page	241
Table 107: WBM "Traffic Monitor" Page	243
Table 108: WBM Page, "SNMP" – "SNMP Settings" Tab	244
Table 109: WBM Page, "SNMP" – "Community Name" Tab	245
Table 110: WBM Page, "SNMP Trap" – "Trap Receiver Settings" Tab	247
Table 111: WBM "Auto Provision" Page	248
Table 112: WBM "Mail Alarm" Page	250
Table 113: WBM "Maintenance" Page – "Protocols" Tab.....	256
Table 114: WBM "System Log" Page	258
Table 115: WBM "User Account" Page.....	260
Table 116: RJ-45 Cable	262
Table 117: CLI "System Information" Configuration	263
Table 118: CLI "System" Configuration	264
Table 119: CLI "Jumbo Frame" Configuration	264
Table 120: CLI "SNTP" Configuration	265
Table 121: CLI "Management Host" Configuration	266
Table 122: CLI "MAC Management" Configuration.....	266
Table 123: CLI "Blackhole MAC" Configuration	267
Table 124: CLI "Port Mirroring" Configuration.....	267
Table 125: CLI "Port Settings" Configuration	268
Table 126: CLI "QoS" Configuration	269
Table 127: CLI "Rate Limitation" Configuration.....	269
Table 128: CLI "Storm Control" Configuration	270
Table 129: CLI "IGMP Snooping" Configuration	271
Table 130: CLI "MVR" Configuration	272
Table 131: CLI "Multicast Address" Configuration	272
Table 132: CLI "Port Isolation" Configuration.....	273
Table 133: CLI "VLAN Settings" Configuration	274
Table 134: CLI "GARP/GVRP" Configuration	275
Table 135: CLI "VLAN Stacking" Configuration.....	276
Table 136: CLI "DHCP Relay" Configuration	277
Table 137: CLI "Dual Homing" Configuration.....	278
Table 138: CLI "Link Aggregation" Configuration.....	278
Table 139: CLI "LACP" Configuration	279
Table 140: CLI "LLDP" Configuration	280
Table 141: CLI "Loop Detection" Configuration.....	281
Table 142: CLI "STP" Configuration	282
Table 143: CLI "Xpress Ring" Configuration	283
Table 144: CLI "DHCP Snooping" Configuration	284
Table 145: CLI "Server Screening" Configuration	285
Table 146: CLI "Binding Table" Configuration.....	285

Table 147: CLI “ARP Inspection” Configuration	286
Table 148: CLI “Filter Table” Configuration	286
Table 149: CLI “Access Control List” Configuration	287
Table 150: CLI “802.1x” Configuration	289
Table 151: CLI “Port Security” Configuration	290
Table 152: CLI “Alarm” Configuration	291
Table 153: CLI “Monitor Information” Configuration	291
Table 154: CLI “RMON Statistics” Configuration	291
Table 155: CLI “SFP Information” Configuration	291
Table 156: CLI “Traffic Monitor” Configuration	292
Table 157: CLI “SNMP” Configuration	293
Table 158: CLI “Auto Provision” Configuration	294
Table 159: CLI “Mail Alarm” Configuration	294
Table 160: CLI “Maintenance” Configuration	295
Table 161: CLI “System Log” Configuration	295
Table 162: CLI “System Log” Configuration	296
Table 163: Data Format and Function Code	297
Table 164: MODBUS Register	297



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