


MANUAL

RocketLinx

ICRL-M-16RJ45/4CP-G-DIN
ICRL-M-8RJ45/4SFP-G-DIN





With regard to the supply of products, the current issue of the following document is applicable: The General Terms of Delivery for Products and Services of the Electrical Industry, published by the Central Association of the Electrical Industry (Zentralverband Elektrotechnik und Elektroindustrie (ZVEI) e.V.) in its most recent version as well as the supplementary clause: "Expanded reservation of proprietorship".

Table of Contents

1. Introduction	7
1.1. ICRL-M-8RJ45/4SFP-G-DIN Overview	7
1.2. ICRL-M-16RJ45/4CP-G-DIN Overview	7
2. Hardware Installation	9
2.1. ICRL-M-8RJ45/4SFP-G-DIN Procedures	9
2.1.1. Connect the Power and Ground (ICRL-M-8RJ45/4SFP-G-DIN)	10
2.1.2. Connect the Relay Output (ICRL-M-8RJ45/4SFP-G-DIN)	11
2.1.3. Connect the Digital Input (ICRL-M-8RJ45/4SFP-G-DIN)	12
2.2. ICRL-M-16RJ45/4CP-G-DIN Procedures	13
2.2.1. Connect the Power and Ground (ICRL-M-16RJ45/4CP-G-DIN)	13
2.2.2. Connect the Relay Output Contacts (ICRL-M-16RJ45/4CP-G-DIN)	14
2.3. Mount the ICRL-M	15
2.4. Connect the Ethernet Ports	16
2.5. Connect SFP Transceivers	17
2.6. LED Descriptions	17
2.7. Reset Button	18
3. Using PortVision DX	19
3.1. PortVision DX Overview	19
3.2. PortVision DX Requirements	20
3.3. Installing PortVision DX	20
3.4. Configuring the Network Settings	23
3.5. Checking the Firmware Version	26
3.6. Uploading the Latest Firmware or Bootloader	27
3.7. Uploading Firmware to Multiple ICRL-M Switches	28
3.8. Adding a New Device in PortVision DX	29
3.9. Using Configuration Files	30
3.9.1. Saving a Configuration File	30
3.9.2. Loading a Configuration File	30
3.10. Using the LED Tracker	31
3.11. Customizing PortVision DX	32
4. Configuration - Web User Interface	33
4.1. Configuration Overview	33
4.2. Web User Interface	34
4.3. Basic Settings	35
4.3.1. Switch Setting	36
4.3.2. Admin Password	37
4.3.3. IP Configuration	39
4.3.4. Time Setting	41
4.3.4.1. Time Setting Page	41
4.3.5. IEEE 1588 PTPv2	44
4.3.6. Jumbo Frame	45
4.3.7. DHCP Server Configuration	47

4.3.8. DHCP Leased Entries	50
4.3.9. Option82 Information Page.....	51
4.3.10. Backup and Restore.....	53
4.3.11. Firmware Upgrade.....	55
4.3.12. Load Default.....	57
4.4. Port Configuration	59
4.4.1. Port Control	59
4.4.2. Port Status.....	61
4.4.3. Rate Control	63
4.4.4. Storm Control	64
4.4.5. Port Trunking.....	65
4.4.5.1. Aggregation Configuration.....	66
4.4.5.2. Aggregation Information	67
4.5. Network Redundancy	69
4.5.1. STP Configuration	70
4.5.2. STP Port Configuration.....	72
4.5.3. STP Information.....	73
4.5.4. MSTP Configuration	75
4.5.5. MSTP Port Configuration.....	78
4.5.6. MSTP Information	79
4.5.7. Redundant Ring Configuration	81
4.5.8. Redundant Ring Information.....	83
4.5.9. ERPS Configuration	84
4.5.10. ERPS Information	87
4.6. VLAN.....	88
4.6.1. VLAN Configuration.....	89
4.6.2. VLAN Port Configuration	92
4.6.3. VLAN Information	94
4.7. Private VLAN.....	95
4.7.1. PVLAN Configuration	96
4.7.2. PVLAN Port Configuration	97
4.7.3. PVLAN Information.....	98
4.7.4. GVRP Configuration	99
4.7. Traffic Prioritization	101
4.7.1. QoS Setting	102
4.7.2. CoS-Queue Mapping	104
4.7.3. DSCP-Queue Mapping.....	105
4.8. Multicast Filtering	106
4.8.1. IGMP Query	107
4.8.2. IGMP Snooping & Filtering	108
4.8.3. GMRP Configuration	110
4.9. SNMP	111
4.9.1. SNMP Configuration.....	111
4.9.2. SNMP V3 Profile.....	112
4.9.3. SNMP Traps.....	113
4.10. Security	114
4.10.1. Filter Set (Access Control List)	115
4.10.1.1. IP Filter	116
4.10.1.2. MAC Filter (Port Security).....	118
4.10.1.3. ARP Filter	120
4.10.1.4. Filter Attach	122
4.10.2. Port Security.....	123
4.10.3. 802.1X Configuration.....	125

4.10.4. 802.1X Port Configuration	127
4.10.5. 802.1X Port Information	129
4.10.6. DHCP Snooping	130
4.10.7. DHCP Binding Configuration	132
4.10.8. IP Source Guard	134
4.10.9. Dynamic ARP Inspection	136
4.10.10. Dynamic ARP Inspection Status	138
4.11. Warning	140
4.11.1. Fault Relay	140
4.11.2. Event Selection	142
4.11.3. SysLog Configuration	144
4.11.4. SMTP Configuration	145
4.12. Monitor and Diag	146
4.12.1. LLDP Configuration	146
4.12.2. MAC Address Table	148
4.12.3. Port Statistics	150
4.12.4. Port Mirroring	151
4.12.5. Event Logs	152
4.12.6. Ping	153
4.13. Device Front Panel	154
4.14. Save (to Flash)	156
4.15. Logout	157
4.16. Reboot	158
5. Configuration - Command Line Interface (CLI)	159
5.1. Overview	159
5.1.1. Using the Serial Console	160
5.1.2. Using a Telnet/SSH Console	163
5.2. Command Line Interface Introduction	165
5.3. Accessing the Options for a Command	165
5.3.1. User EXEC Mode	168
5.3.2. Privileged EXEC Mode	169
5.3.3. Global Configuration Mode	169
5.3.4. (Port) Interface Configuration	171
5.3.5. (VLAN) Interface Configuration	172
5.4. Command Mode Summary	172
5.5. Basic Settings (CLI)	174
5.6. Port Configuration (CLI)	180
5.7. Network Redundancy (CLI)	184
5.8. VLAN (CLI)	191
5.9. Private VLAN (CLI)	195
5.10. Traffic Prioritization (CLI)	199
5.11. Multicast Filtering (CLI)	202
5.12. SNMP (CLI)	206
5.13. Security (CLI)	207
5.14. Warnings (CLI)	211
5.15. Monitor and Diag (CLI)	214
5.16. Saving to Flash (CLI)	217
5.17. Logging Out (CLI)	217
5.18. Service (CLI)	217



6. Complete CLI List.....	218
6.1. User EXEC Mode	218
6.2. Privileged EXEC Mode	219
6.3. Global Configuration Mode	226
6.4. Port Interface Configuration Mode.....	234
6.5. VLAN Interface Configuration Mode	237
7. Technical Support.....	238
7.1. Pepperl+Fuchs SFP Modules.....	238
7.2. Pepperl+Fuchs Private MIB.....	238

1. Introduction

This manual discusses the following switches.

- RocketLinx ICRL-M-8RJ45/4SFP-G-DIN
- RocketLinx ICRL-M-16RJ45/4CP-G-DIN

Note: The ICRL-M-16RJ45/4CP-G-DIN and ICRL-M-8RJ45/4SFP-G-DIN are simply referred to as ICRL-M in the remainder of this manual unless there are differences between the models.

1.1. ICRL-M-8RJ45/4SFP-G-DIN Overview

The RocketLinx ICRL-M-8RJ45/4SFP-G-DIN is a 12-port fully managed industrial layer 2 Gigabit Ethernet switch combining eight 10/100/1000 BASE-T copper Ethernet ports with four 100/1000 BASE-T SFP optical fiber ports that provide flexibility to add fiber connectivity in distances to meet the unique requirements of each project. Featuring a rugged metal enclosure, wide operating temperature, and advanced security and network performance, the ICRL-M-8RJ45/4SFP-G-DIN is an ideal solution for mission critical industrial networking applications.

The ICRL-M-8RJ45/4SFP-G-DIN provides:

- Eight RJ45 Gigabit ports
- Four 100/1000 SFP slots for optical fiber connection
- Redundant power input with an input power range of 10 to 36VDC
- IP31 with an extreme operating temperature range of -40 to 75°C
- Meets the Rolling Stock Track Side EN50121-4 standard

1.2. ICRL-M-16RJ45/4CP-G-DIN Overview

The RocketLinx ICRL-M-16RJ45/4CP-G-DIN is a 20-port fully managed industrial layer 2 Gigabit Ethernet switch combining 16 10/100/1000 BASE-T copper Ethernet ports with four 100/1000 BASE-T copper or SFP optical fiber combo ports. Featuring a rugged metal enclosure, wide operating temperature, and advanced security and network performance, the ICRL-M-16RJ45/4CP-G-DIN is an ideal solution for mission critical industrial networking applications.

The ICRL-M-16RJ45/4CP-G-DIN provides:

- 16 RJ45 Gigabit ports
- 4 combination RJ45/SFP ports
- Redundant power input with a input power range of 10 to 60VDC
- IP31 with an extreme operating temperature range of -40 to 75°C
- Meets the Rolling Stock Track Side EN50121-4 standard



4/21/20

2. Hardware Installation

You can use the following subsections to install the RocketLinX ICRL-M.

- *ICRL-M-8RJ45/4SFP-G-DIN Procedures* on Page 9
- *ICRL-M-16RJ45/4CP-G-DIN Procedures* on Page 13
- *Mount the ICRL-M* on Page 15
- *Connect the Ethernet Ports* on Page 16
- *Connect SFP Transceivers* on Page 17
- *LED Descriptions* on Page 17
- *Reset Button* on Page 18

Note: *The ICRL-M-16RJ45/4CP-G-DIN and ICRL-M-8RJ45/4SFP-G-DIN are simply referred to as ICRL-M in the remainder of this chapter unless there is model-specific information.*

2.1. ICRL-M-8RJ45/4SFP-G-DIN Procedures

Use the following subsections to begin installation on the ICRL-M-8RJ45/4SFP-G-DIN.

- *Connect the Power and Ground (ICRL-M-8RJ45/4SFP-G-DIN)* on Page 10
- *Connect the Relay Output (ICRL-M-8RJ45/4SFP-G-DIN)* on Page 11
- *Connect the Digital Input (ICRL-M-8RJ45/4SFP-G-DIN)* on Page 12

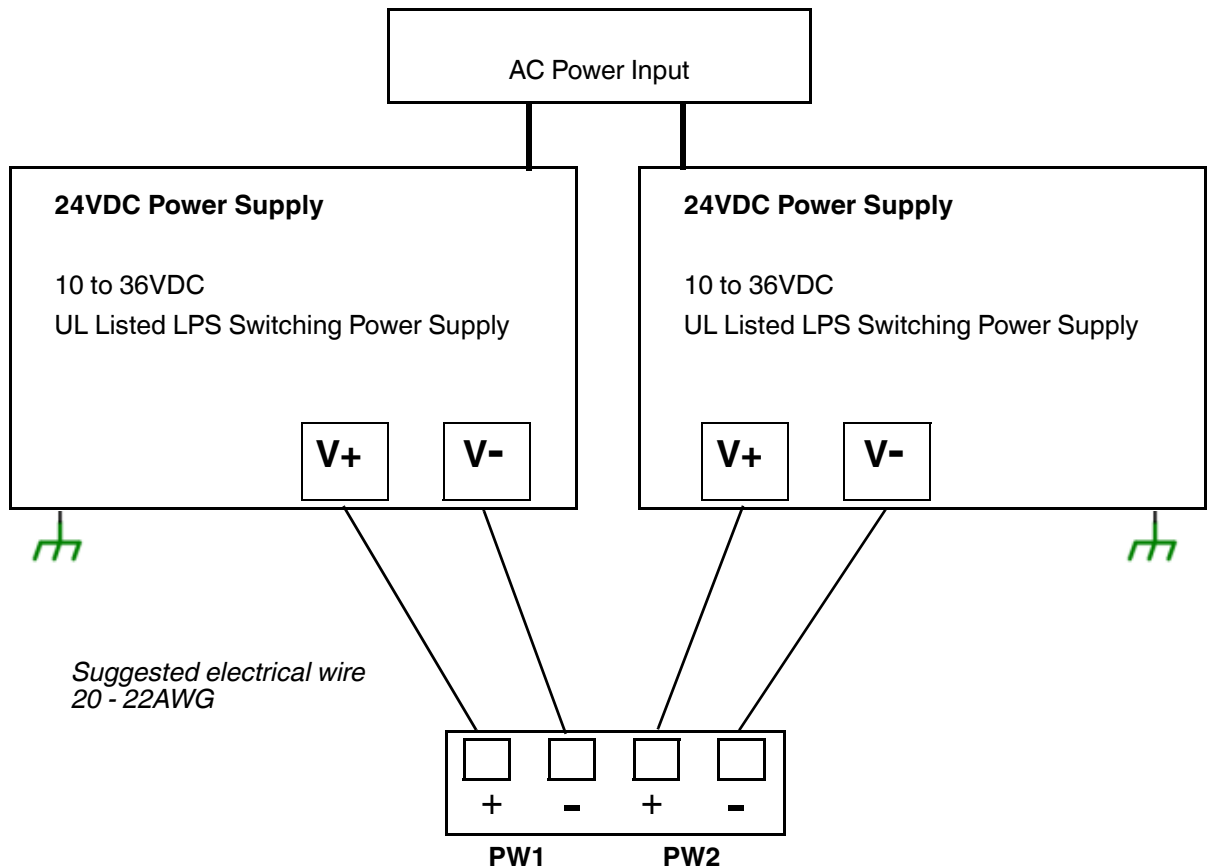
To complete installation, use the common procedures below:

- *Connect the Ethernet Ports* on Page 16
- *Connect SFP Transceivers* on Page 17
- *LED Descriptions* on Page 17
- *Reset Button* on Page 18

2.1.1. Connect the Power and Ground (ICRL-M-8RJ45/4SFP-G-DIN)

Use the following procedure to connect the ICRL-M-8RJ45/4SFP-G-DIN power and ground.

1. Connect the DC power inputs by inserting the positive and negative wires (20 - 22AWG) into the PW+ and PW- contacts.
 - PW1 and PW2 support power redundancy and reverse polarity protection.
 - Accepts a positive or negative power source but PW1 and PW2 must apply to the same mode.
 - If both power inputs are connected, the ICRL-M-8RJ45/4SFP-G-DIN is powered from the highest connected voltage.
 - The ICRL-M-8RJ45/4SFP-G-DIN can emit an alarm if PW1 or PW2 are no longer receiving power. See the *Warning* discussion on Page 140 to configure an alarm.



Note: Power should be disconnected from the power supply before connecting it to the switch. Otherwise, your screw driver blade can inadvertently short your terminal connections to the grounded enclosure. Tighten the wire-clamp screws to prevent the wires from coming loose.

2. Connect a ground wire between the chassis and earth ground using 12-24AWG wire to ensure that the ICRL-M-8RJ45/4SFP-G-DIN is not damaged by noise or electrical shock.
 - a. Loosen the ground screw on the back of the ICRL-M-8RJ45/4SFP-G-DIN.
 - b. Insert the ground wire.
 - c. Tighten the ground screw after the ground wire is connected.

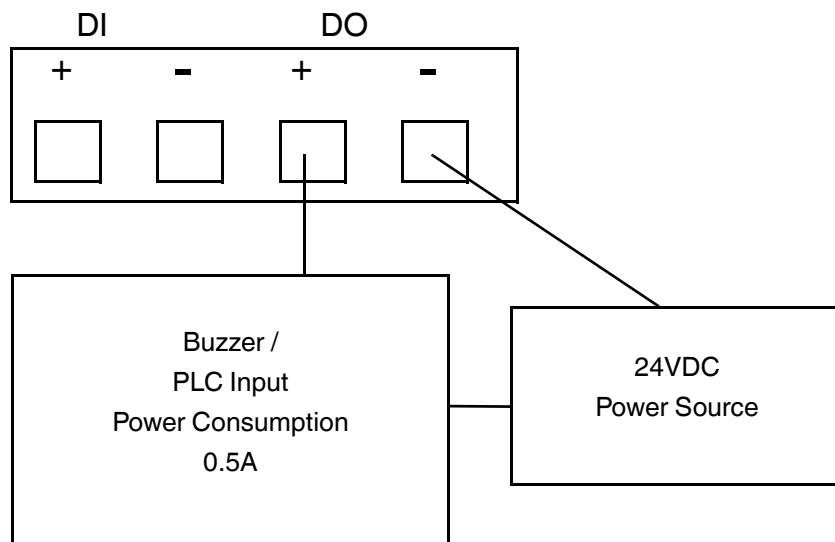
2.1.2. Connect the Relay Output (ICRL-M-8RJ45/4SFP-G-DIN)

If desired, connect the Relay Output (digital output) located on the bottom of the ICRL-M-8RJ45/4SFP-G-DIN. The relay output is controlled by the predefined operating rules. To activate relay output functions, refer to *Fault Relay* on Page 140.

Relay contacts are energized (open) for normal operation and close for fault conditions. The fault conditions include:

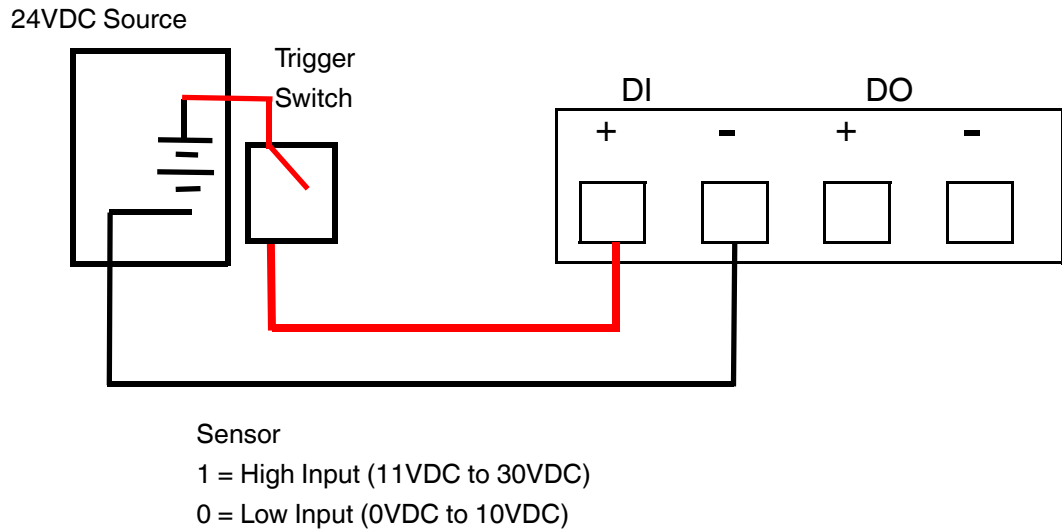
- Power failure
- Link failure
- Ring
- Ping failure
- Ping reset
- Dry output
- DI state

Note: The relay contact (DO) supports 0.5A at 24VDC. Do not apply voltage and current that exceeds these specifications.



2.1.3. Connect the Digital Input (ICRL-M-8RJ45/4SFP-G-DIN)

The Digital Input contacts are located on the bottom of the ICRL-M-8RJ45/4SFP-G-DIN. It accepts one external DC type signal input and can be configured to send alert message through Ethernet when the signal is changed. The signal may trigger and be generated by an external power change, like an open door trigger switch for a control cabinet.



Note: DI accepts DC type signal and supports isolated input circuit with Digital High Level input 11 VDC to 30 VDC and Digital Low Level input 0 VDC to 10 VDC. Do not apply voltage higher than the specification as it may cause internal circuit damage or a wrong action of DI.

2.2. ICRL-M-16RJ45/4CP-G-DIN Procedures

Use the following subsections to begin installation on the ICRL-M-16RJ45/4CP-G-DIN.

- *Connect the Power and Ground (ICRL-M-16RJ45/4CP-G-DIN)* on Page 13
- *Connect the Relay Output Contacts (ICRL-M-16RJ45/4CP-G-DIN)* on Page 14

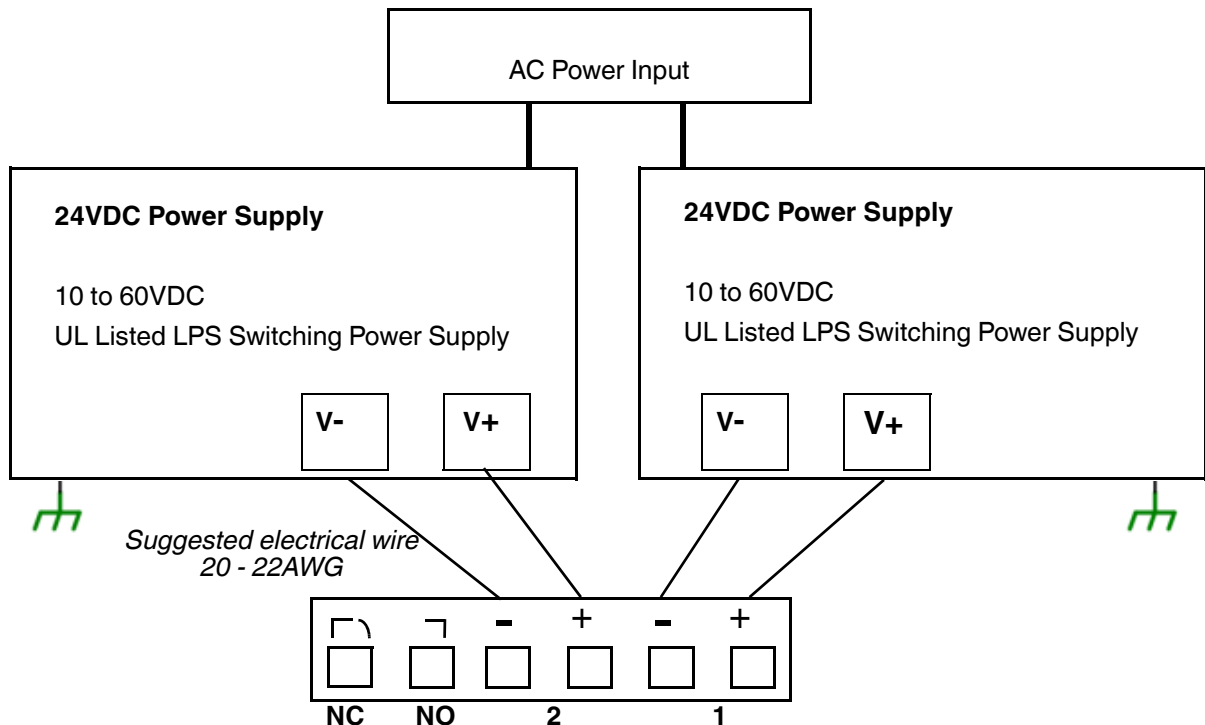
To complete installation, use the common procedures below:

- *Connect the Ethernet Ports* on Page 16
- *Connect SFP Transceivers* on Page 17
- *LED Descriptions* on Page 17
- *Reset Button* on Page 18

2.2.1. Connect the Power and Ground (ICRL-M-16RJ45/4CP-G-DIN)

Use the following procedure to connect the ICRL-M-16RJ45/4CP-G-DIN power and ground.

1. Connect the DC power inputs by inserting the positive and negative wires (20 - 22AWG) into the PW+ and PW- contacts.
 - PW1 and PW2 support power redundancy and reverse polarity protection.
 - Accepts a positive or negative power source but PW1 and PW2 must apply to the same mode.
 - If both power inputs are connected, the ICRL-M-16RJ45/4CP-G-DIN is powered from the highest connected voltage.
 - The ICRL-M-16RJ45/4CP-G-DIN can emit an alarm if PW1 or PW2 are no longer receiving power. See the *Warning* discussion on Page 140 to configure an alarm.



Note: Power should be disconnected from the power supply before connecting it to the switch. Otherwise, your screw driver blade can inadvertently short your terminal connections to the grounded enclosure.

4/21/20

Tighten the wire-clamp screws to prevent the wires from coming loose.

2. Connect a ground wire between the chassis and earth ground using 12-24AWG wire to ensure that the ICRL-M-16RJ45/4CP-G-DIN is not damaged by noise or electrical shock.
 - a. Loosen the ground screw on the back of the ICRL-M-16RJ45/4CP-G-DIN.
 - b. Insert the ground wire.
 - c. Tighten the ground screw after the ground wire is connected.

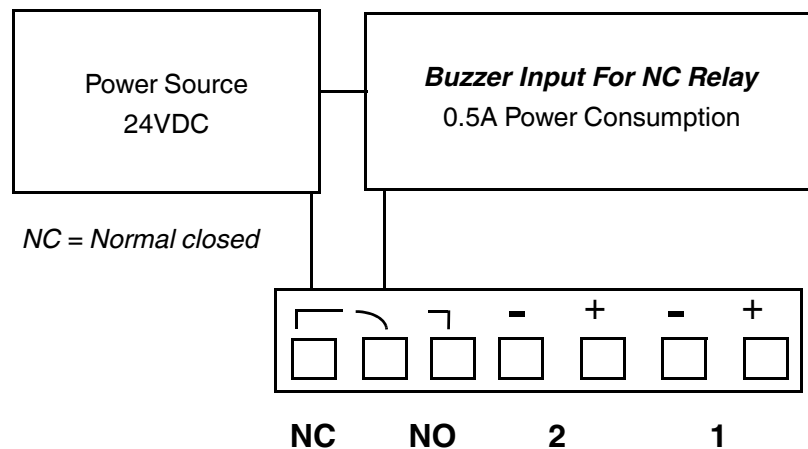
2.2.2. Connect the Relay Output Contacts (ICRL-M-16RJ45/4CP-G-DIN)

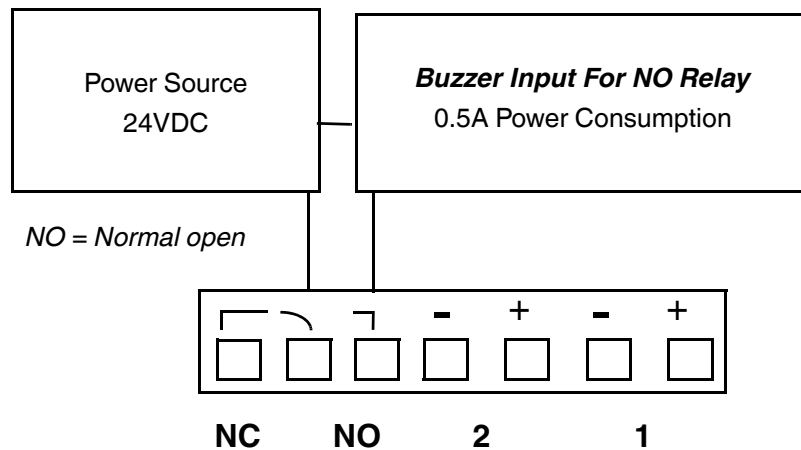
If desired, connect the Relay Output contacts located on the 6-pin terminal block connector on the front of the ICRL-M-16RJ45/4CP-G-DIN. The relay output is controlled by the predefined operating rules. To activate relay output functions, refer to *Fault Relay* on Page 140.

Digital output relay contacts are energized (open) for normal operation and close for fault conditions. The fault conditions include:

- Power failure
- Link failure
- Ring
- Ping failure
- Ping reset
- Dry output

Note: *The relay contact supports 0.5A at 24VDC. Do not apply voltage and current that exceeds these specifications.*

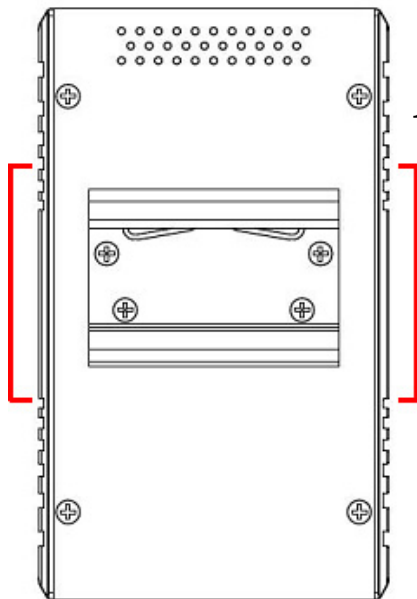




2.3. Mount the ICRL-M

You can use the following procedure to mount the ICRL-M on a DIN rail.

The DIN rail clip is already attached to the ICRL-M. If the DIN rail clip is not screwed onto the ICRL-M, follow the instructions and the figure below to attach DIN rail clip to the ICRL-M.



DIN Rail Mounting

1. If necessary, use the screws to attach DIN rail clip to the rear panel of the ICRL-M. (To remove DIN rail clip, reverse Step 1.)
2. Insert the upper end of DIN rail clip into the back of DIN rail track from its upper side.
3. Lightly push the bottom of DIN rail clip into the track.
4. Verify that the DIN rail clip is tightly attached on the track.
5. To remove the ICRL-M from the track, reverse the steps above.

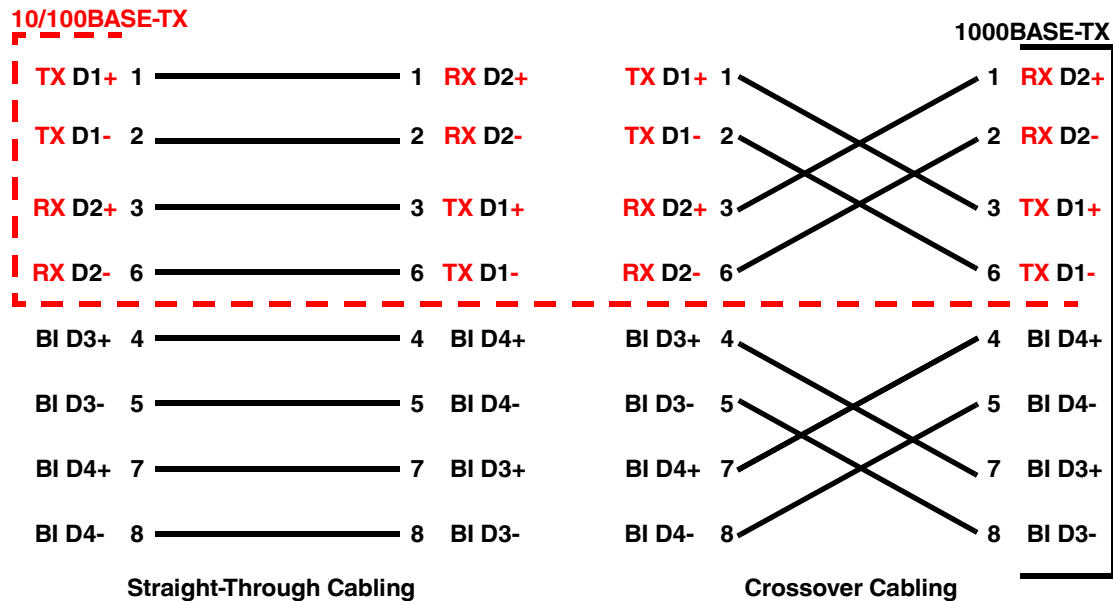
2.4. Connect the Ethernet Ports

You can use the following information to connect standard Ethernet cables between the ICRL-M Ethernet ports and the network nodes.

- ICRL-M-8RJ45/4SFP-G-DIN: Ports 1-8 are gigabit copper RJ45 ports and Ports 9-12 are gigabit SFPs
- ICRL-M-16RJ45/4CP-G-DIN: Ports 1-16 are gigabit copper RJ45 ports with combination Ports 17-20, which have 4 gigabit RJ45 ports and 4 gigabit SFP ports

See *Connect SFP Transceivers* on Page 17 for information about SFP installation.

All of the Ethernet ports automatically detect the signal from the connected devices to negotiate the link speed and duplex mode (half- or full-duplex). Auto MDI/MDIX allows you to connect another switch, hub, or workstation without changing straight-through or crossover cables. Crossover cables cross-connect the transmit lines at each end to the received lines at the opposite end.



Connect one side of an Ethernet cable into any switch port and connect the other side to your attached device. The **LNK/ACT** LED is lit when the cable is correctly connected. Always make sure that the cables between the switches and attached devices (for example, switch, hub, or workstation) are less than 100 meters (328 feet) and meet these requirements.

- **10/100BASE-TX:** Category 5 cable
- **1000BASE-TX:** Category 5 or 5e cable

2.5. Connect SFP Transceivers

The ICRL-M provides four SFP ports, The SFP ports accept standard mini GBIC SFP transceivers, that support 1000BASE-X (1000BASE-SX/LX/LHX/XD/ZX).

The ICRL-M-16RJ45/4CP-G-DIN SFP ports are combined with the RJ45 Ports 17-20.

To ensure system reliability, Pepperl+Fuchs recommends using Pepperl+Fuchs certified SFPs.

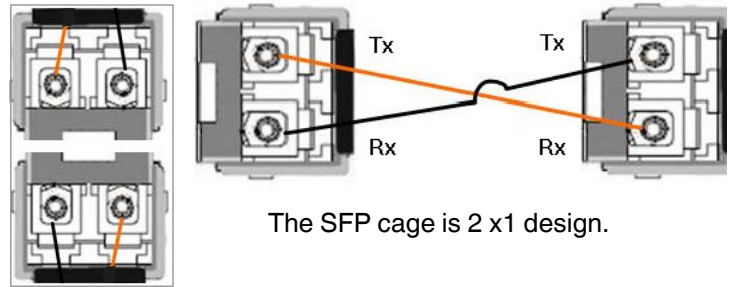
1. Plug the SFP transceiver into the SFP fiber transceiver.
2. Connect the transmit channel to the receive channel at each end.
3. Check the direction/angle of the fiber transceiver and the fiber cable.

Note: This is a Class 1 Laser/LED product. Do not stare at the Laser/LED Beam.

The SFP port does not function until the fiber cable is linked to another active device.

The SFP and corresponding RJ45 ports on the ICRL-M-16RJ45/4CP-G-DIN work in an exclusive mode. Traffic sent or received through the SFP module has priority thus no traffic is sent or received over the corresponding RJ45 connection. To use the RJ45 connection, remove the corresponding SFP.

Multi-Mode cables should not exceed 2KM and Single-Mode cables should not exceed 30km.



2.6. LED Descriptions

This subsection provides information about the ICRL-M LEDs. You can also refer to *Device Front Panel* on Page 154 for information about using the web user interface to remotely view LED information.

LED	LED Lit	LED Blinking	LED Off
Sys	System is ready	Firmware is uploading	System not ready
PWR 1/2	Power is on	Not applicable	Power is not applied
RS (Ring Status)	Green: Ring is normal Amber: Abnormal Ring	Green: Ring with the wrong port Amber: The device's ring port failed	Switch working in slave mode
DO (Red)	Relay is active and contacts have been shorted	Not applicable	DO not activated
DI (Green) ICRL-M-8RJ45/4SFP-G-DIN	High digital signal is detected	Not applicable	DI not activated
LINK/ACT	Port is linked	Port active	Port link down or port not connected
1000M	Port is linked at 1000Mbps	Not applicable	Not applicable

LEDs	Function	Description
Link/Act	Indicates the traffic and link status.	On: Port is linked to another device Blinking: The traffic is active Off: Port not connected.
Speed	Indicates the copper port link speed.	On: Port link is 1000Mbps Off: Port link is 100Mbps or 10Mbps
1000	SFP transceiver speed indicator.	On: The SFP supports 1000Mbps Gray: Plugged in but not linked up, yet

2.7. Reset Button

The ICRL-M has a reset button that you can use to reboot the ICRL-M or reset the configuration to the factory default.

Reset Button	Description
Depress 5 Seconds	This reboots the ICRL-M without changing the configuration.
Depress > 10 Seconds	This loads the factory default configuration values into the ICRL-M including the IP address.

The **Reset** button is located on the front panel of the ICRL-M-8RJ45/4SFP-G-DIN above **Console** port.

3. Using PortVision DX

Note: The ICRL-M-16RJ45/4CP-G-DIN and ICRL-M-8RJ45/4SFP-G-DIN are simply referred to as ICRL-M in the remainder of this chapter.

There are several ways to configure network information. Pepperl+Fuchs Technical Support recommends connecting the ICRL-M to a PC or laptop running Windows and installing *PortVision DX* for initial configuration.

This section shows how to use PortVision DX for initial network configuration and discusses how to:

- Install PortVision DX (Page 20)
- Configure the network address (Page 23)
- Check the firmware and bootloader version on the ICRL-M to verify that the latest versions are loaded (Page 26) before configuration
- Download the latest version firmware and bootloader and upload it to the ICRL-M (Page 27)
- Perform other PortVision DX tasks, such as:
 - Uploading firmware to multiple ICRL-M switches (Page 28)
 - Adding a new RocketLinx (managed or unmanaged) or a third party device to PortVision DX to maintain device information on your network (Page 29)
 - Using configuration files for use in configuring multiple installations with the same features (Page 30)
 - Using the LED Tracker (Page 31)
- Organize how PortVision DX displays your Pepperl+Fuchs Control Ethernet attached products (Page 30)

Optionally, you can use the web user interface or the CLI to perform these tasks on the ICRL-M using these subsections:

- *IP Configuration* on Page 39
- *Firmware Upgrade* on Page 55
- *Basic Settings (CLI)* on Page 174

3.1. PortVision DX Overview

PortVision DX automatically detects Pepperl+Fuchs Control Ethernet attached products physically attached to the local network segment so that you can configure the network address, upload firmware, and manage the following products:

- RocketLinx ICRL-M switches
- ICDM-RX/TCP series
- ICDM-RX/EN | EN1 | MOD | PN | PN1 Industrial Gateway series
- IO-Link Master (ICE2 | ICE3) series

In addition to identifying Pepperl+Fuchs Control Ethernet attached products, you can use PortVision DX to display any third-party switch and hardware that may be connected directly to those devices. All non-Pepperl+Fuchs products and unmanaged RocketLinx switches are treated as non-intelligent devices and have limited feature support. For example, you cannot configure or update firmware on a third-party switch.

3.2. PortVision DX Requirements

Use PortVision DX to identify, configure, update, and manage the ICRL-M on Windows XP SP3 through Windows 10 operating systems including Windows Server 2019 (at the time of publication).

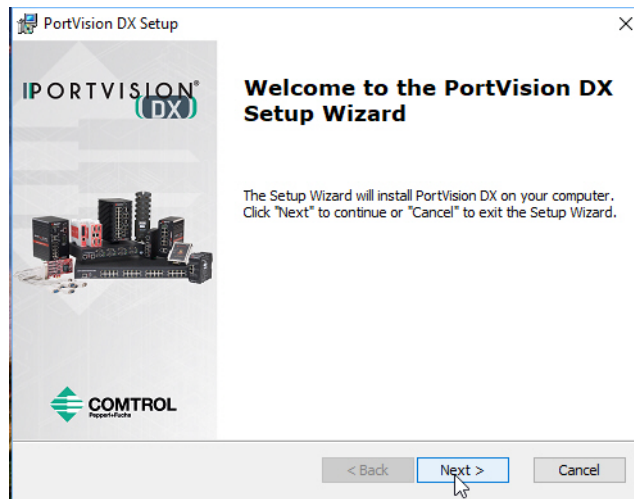
PortVision DX requires that you connect the Pepperl+Fuchs Control Ethernet attached product to the same network segment as the Windows host system if you want to be able to scan and locate it automatically during the configuration process.

3.3. Installing PortVision DX

During initial configuration, PortVision DX automatically detects and identifies ICRL-M switches, if they are in the same network segment.

You can download the latest version of PortVision DX from <https://www.pepperl-fuchs.com>.

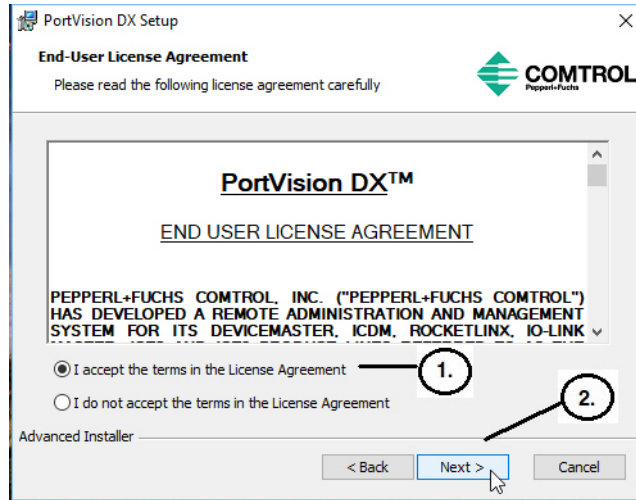
1. If necessary, unzip PortVision DX and then execute the **PortVision_DX[version].msi** file.



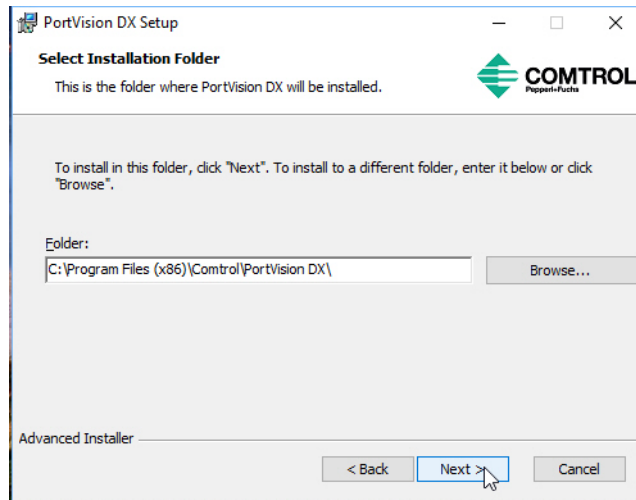
Note: Depending on your operating system, you may need to respond to a Security Warning to permit access.

2. Click **Next** on the *Welcome* screen.

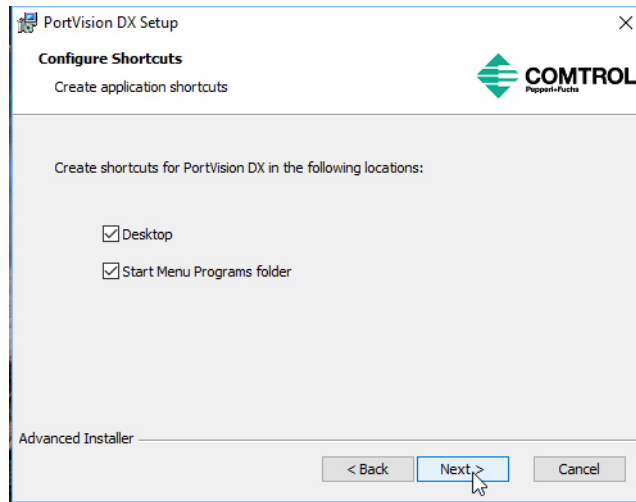
3. Click **I accept the terms in the License Agreement** and **Next**.



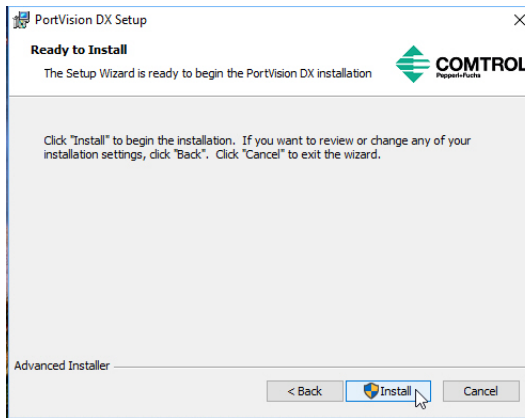
4. Click **Next** or optionally, browse to a different location and then click **Next**.



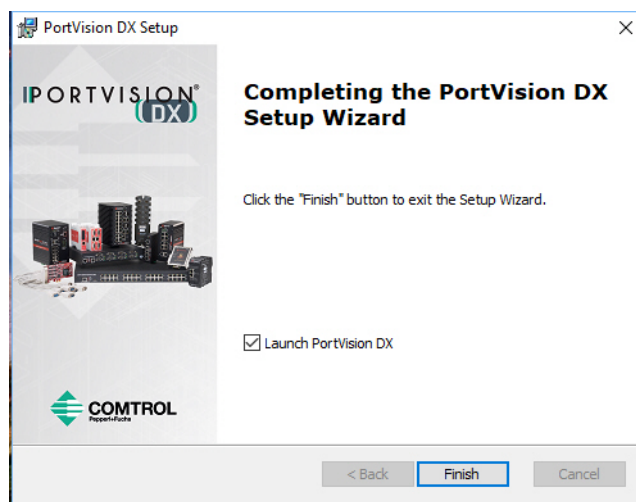
5. Click **Next** to configure the shortcuts.



6. Click **Install**.



7. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to install software on this computer?* query.
8. Click **Launch PortVision DX** and **Finish** in the last installation screen.



4/21/20

- Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.
- Go the next subsection to use PortVision DX to program the network information.

3.4. Configuring the Network Settings

The ICRL-M has the following default values when shipped from the factory:

- IP address: 192.168.250.250
- Subnet mask: 255.255.255.0
- Gateway address: 192.168.250.1

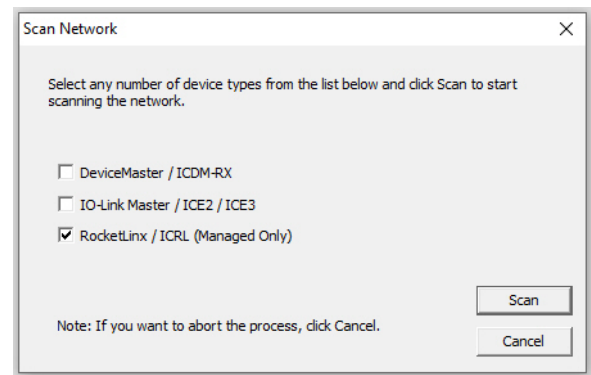
Use the following procedure to change the default network settings on the ICRL-M for your network.

- If necessary, start PortVision DX using the **PortVision DX** desktop shortcut or from the **Start** button, click **Pepperl+Fuchs Control > PortVision DX > PortVision DX**.

Note: Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.

- Click the **Scan** button in the *Toolbar*.
- Select the Pepperl+Fuchs Control Ethernet attached products that you want to locate and then click **Scan**.

Note: If the Pepperl+Fuchs Control Ethernet attached product is not on the local segment and it has been programmed with an IP address, it will be necessary to manually add the Pepperl+Fuchs Control Ethernet attached product to PortVision DX.



4. Highlight the ICRL-M for which you want to program network information and open the **Properties** screen using one of these methods.
 - Double-click the ICRL-M in the *Device Tree* or *Device List* pane.
 - Highlight the ICRL-M in the *Device Tree* or *Device List* pane and click the **Properties** button.
 - Right-click the ICRL-M in the *Device Tree* or *Device List* pane and click **Properties** in the popup menu
 - Highlight the ICRL-M, click the **Manage** menu and then **Properties**.

The contents of this folder are displayed below in the Device List pane

You can expand the tree and also view the devices in the Device Tree pane

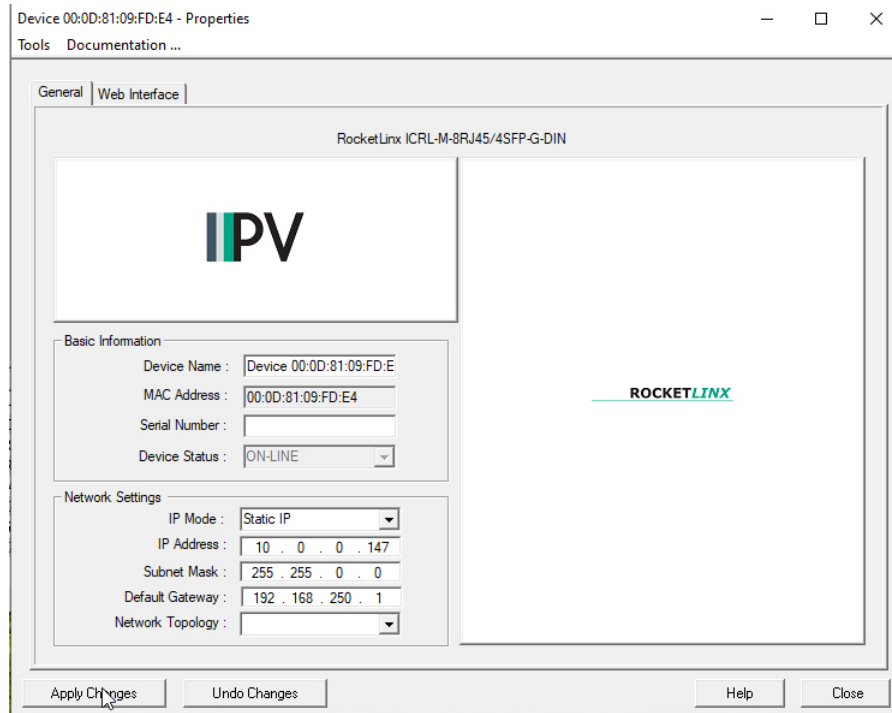
Device Tree Pane

Device Name	Model	IP Address	MAC Address	Software Version	Status
Device 00:0D:81:09:FD:E4	ICRL-M-8RJ45/4SFP-G-DIN		FD:E4	v1.0 (b1.0.0.1)	ON-LINE
Device 00:0D:81:09:FD:E5	ICRL-M-16RJ45/4CP-G-DIN		FD:E5	v1.0_b4 (b1.0.0.1)	ON-LINE
Device 9710-000064	ICE2-8IOL-K45P-RJ45		DC:8A	EtherNet/IP 1.5.39-mqtt-13b	ON-LINE
Device 9708-000061	ICE2-8IOL-G65L-V1D		C1:29	EtherNet/IP 1.5.39	ON-LINE
Device 9706-000036	ICE3-8IOL-K45S-RJ45		CD:08	PROFINET IO 1.5.39-mqtt-13b	ON-LINE
Device 00:0D:81:09:0B:9E	MOD-DB9/RJ45-DIN		DB:9E	Modbus Router 7.05	ON-LINE
Device 00:0D:81:09:08:CC	PN-ST/RJ45-DIN		08:CC	PROFINET IO V 3.4.2	ON-LINE
Device 00:0D:81:09:09:FE	ICDM-RX/TCP-DB9/RJ45-PM		09:FE	NS-Link 11.37	ON-LINE (Remote)
Device 00:0D:81:09:0A:AE	EN-4DB9/2RJ45-DIN		0A:AE	EtherNet/IP 7.12	ON-LINE

Device List Pane

View & Edit the existing properties of the device

5. *Optionally*, rename the ICRL-M in the **Device Name** field for a PortVision DX friendly name. The default name displays as *Device* and the MAC address.



Note: The MAC address and Device Status fields are automatically populated and you cannot change these values.

6. *Optionally*, enter the serial number, which is on a label on the ICRL-M.
7. Select **DHCP IP** or **Static IP** for the *IP Mode*.
 - If you select **DHCP IP**, go to Step 8.
 - If you select **Static IP**:
 - Enter a unique **IP address** as required for your site.
 - Enter a valid **Subnet Mask** value for your network.
 - Enter a valid **Default Gateway** value for your network.
8. *Optionally*, select the **Network Topology** type, which is an informational field.
9. Click **Apply Changes** to update the network information on the ICRL-M.

Note: If you are deploying multiple ICRL-M switches that share common values, you can save the configuration file and load that configuration onto other ICRL-M switches. See *Using Configuration Files* on Page 30 for more information.
10. Click **Close** to exit the *Properties* window.
11. You should verify that you have the latest firmware loaded on the ICRL-M because a newer version typically includes feature enhancements and bug fixes. Refer to *Checking the Firmware Version* on Page 26 and if necessary, *Uploading the Latest Firmware or Bootloader* on Page 27.
12. If you have the latest firmware, you can begin feature configuration, see one of these sections:
 - *Configuration - Web User Interface* on Page 33
 - *Configuration - Command Line Interface (CLI)* on Page 159
 - Right-click the ICRL-M in the *Device List* pane and click **Webpage** in the popup menu.

Note: The default User Name and Password are both **admin**.

3.5. Checking the Firmware Version

Checking your web interface and bootloader versions is easy in PortVision DX.

Pepperl+Fuchs recommends loading the latest firmware and bootloader so that you have all of the latest feature enhancements and bug fixes.

1. If the ICRL-M is not displayed in PortVision DX, click the **Scan** button.
2. Select the Pepperl+Fuchs Control Ethernet attached product type and click the **Scan** button.
3. Locate the ICRL-M in the *Device List* pane. Under *Software Version*: The first number reflects the firmware version and the second number displays the bootloader version.

You can customize and organize your view using PortVision DX.
 In addition, you can save and reload different sessions.
 The first number is the firmware version and (second number) is the bootloader version on the switch.

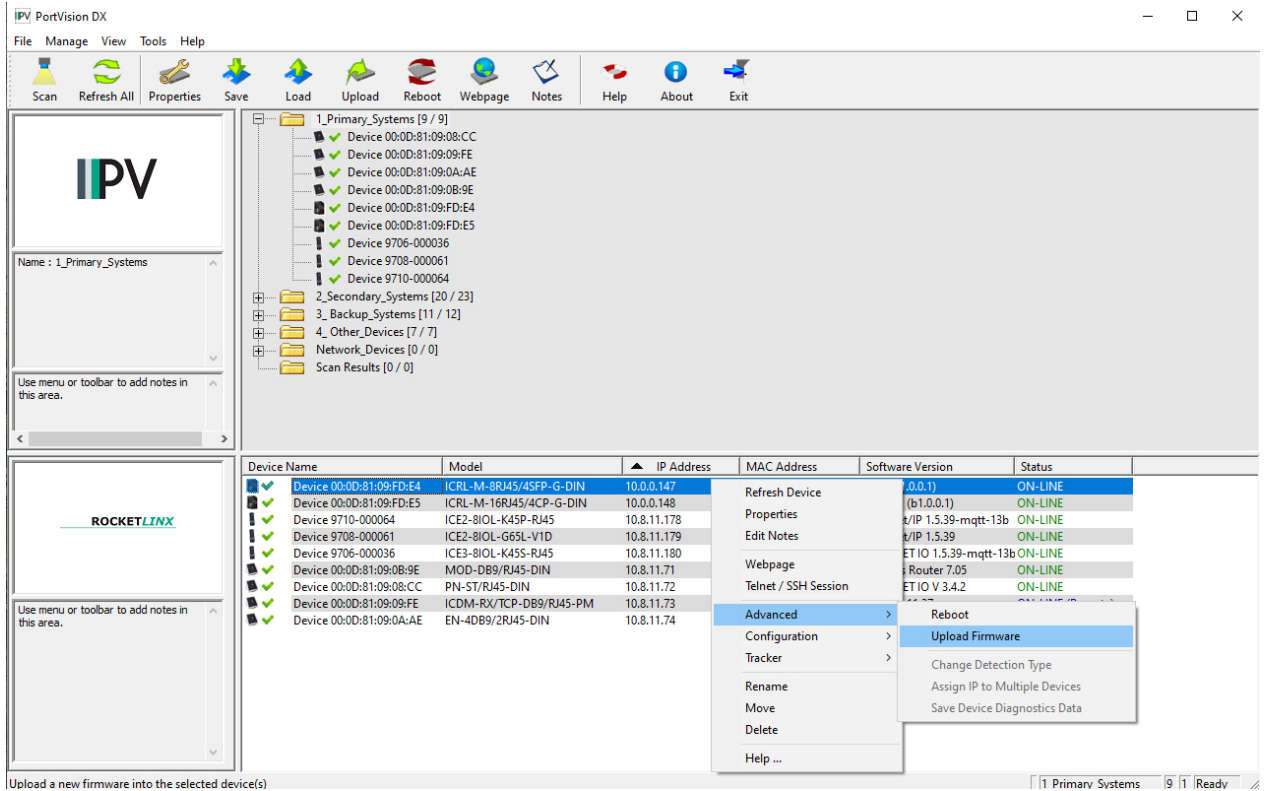
Device Name	Model	IP Address	MAC Address	Software Version	Status
Device 00:0D:81:09:FD:E4	ICRL-M-8RJ45/4SFP-G-DIN	10.0.0.147	00:0D:81:09:FD:E4	v1.0 (b1.0.0.1)	ON-LINE
Device 00:0D:81:09:FD:E5	ICRL-M-16RJ45/4CP-G-DIN	10.0.0.148	00:0D:81:09:FD:E5	v1.0_b4 (b1.0.0.1)	ON-LINE
Device 9710-000064	ICE2-8IOL-K45P-RJ45	10.8.11.178	00:0D:81:09:0C:8A	EtherNet/IP 1.5.39-mqtt-13b	ON-LINE
Device 9708-000061	ICE2-8IOL-G65L-V1D	10.8.11.179	00:0D:81:08:C:129	EtherNet/IP 1.5.39	ON-LINE
Device 9706-000036	ICE3-8IOL-K45S-RJ45	10.8.11.180	00:0D:81:08:C:D08	PROFINET IO 1.5.39-mqtt-13b	ON-LINE
Device 00:0D:81:09:0B:9E	MOD-DB9/RJ45-DIN	10.8.11.71	00:0D:81:09:0B:9E	Modbus Router 7.05	ON-LINE
Device 00:0D:81:09:08:CC	PN-ST/RJ45-DIN	10.8.11.72	00:0D:81:09:08:CC	PROFINET IO V 3.4.2	ON-LINE
Device 00:0D:81:09:09:FE	ICDM-RX/TCP-DB9/RJ45-PM	10.8.11.73	00:0D:81:09:09:FE	NS-Link 11.37	ON-LINE (Remote)
Device 00:0D:81:09:0A:AE	EN-4DB9/2RJ45-DIN	10.8.11.74	00:0D:81:09:0A:AE	EtherNet/IP 7.12	ON-LINE

4. Check <https://www.pepperl-fuchs.com> for the latest firmware and bootloader. Simply, click your product type and click the **Software** link and check the latest version against the version on the ICRL-M. Use the next subsection for procedures to upload the firmware (web interface) and bootloader.

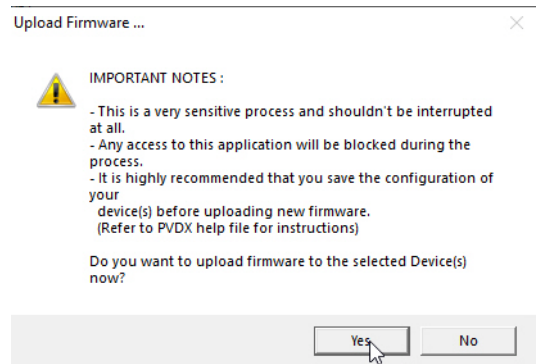
3.6. Uploading the Latest Firmware or Bootloader

You can use the following procedure to upload the latest firmware or bootloader.

1. If you have not done so, download the latest firmware and bootloader using the previous subsection.
2. Right-click the ICRL-M in the *Device List* pane that you want to update, click **Advanced --> Upload firmware**.



3. Navigate to the location of the firmware files, select the appropriate file, and then click **Open**.
4. Click **Yes** to the *Upload Firmware* message.
5. Click **Ok** to the message notifying you that you should wait to use the ICRL-M when the status returns to **ON-LINE**.
6. Right-click the ICRL-M in the *Device List* pane and click **Refresh**. Optionally, you can click the **Refresh** button in the *Toolbar* and that refreshes all devices in PortVision DX.
7. Verify that the version change is reflected in under the *Software Version*.



3.7. Uploading Firmware to Multiple ICRL-M Switches

You can use this procedure if your ICRL-M is connected to the host PC, laptop, or if the ICRL-M resides on the local network segment.

Note: *Technical support does not advise uploading bootloader to multiple ICRL-M switches. Remember that uploading firmware reboots the ICRL-M, which depending on your network connections may cause firmware uploading to fail on another ICRL-M.*

1. If the ICRL-M is not displayed in PortVision DX, click the **Scan** button.
2. Select the Pepperl+Fuchs Control Ethernet attached product type and click the **Scan** button.
3. Shift-click the multiple ICRL-M switches on the **Main** screen that you want to update and right-click and then click **Advanced > Upload Firmware**.
4. Browse, click the firmware (**.bin**) file, **Open** (*Please locate the new firmware*), and then click **Yes** (*Upload Firmware*).

It may take a few minutes for the firmware to upload onto all of the ICRL-M switches. The ICRL-M reboots itself during the upload process.

5. Click **Ok** to the advisory message about waiting to use the device until the status reads **ON-LINE**.

In the next polling cycle, PortVision DX updates the *Device List* pane and displays the new firmware version.

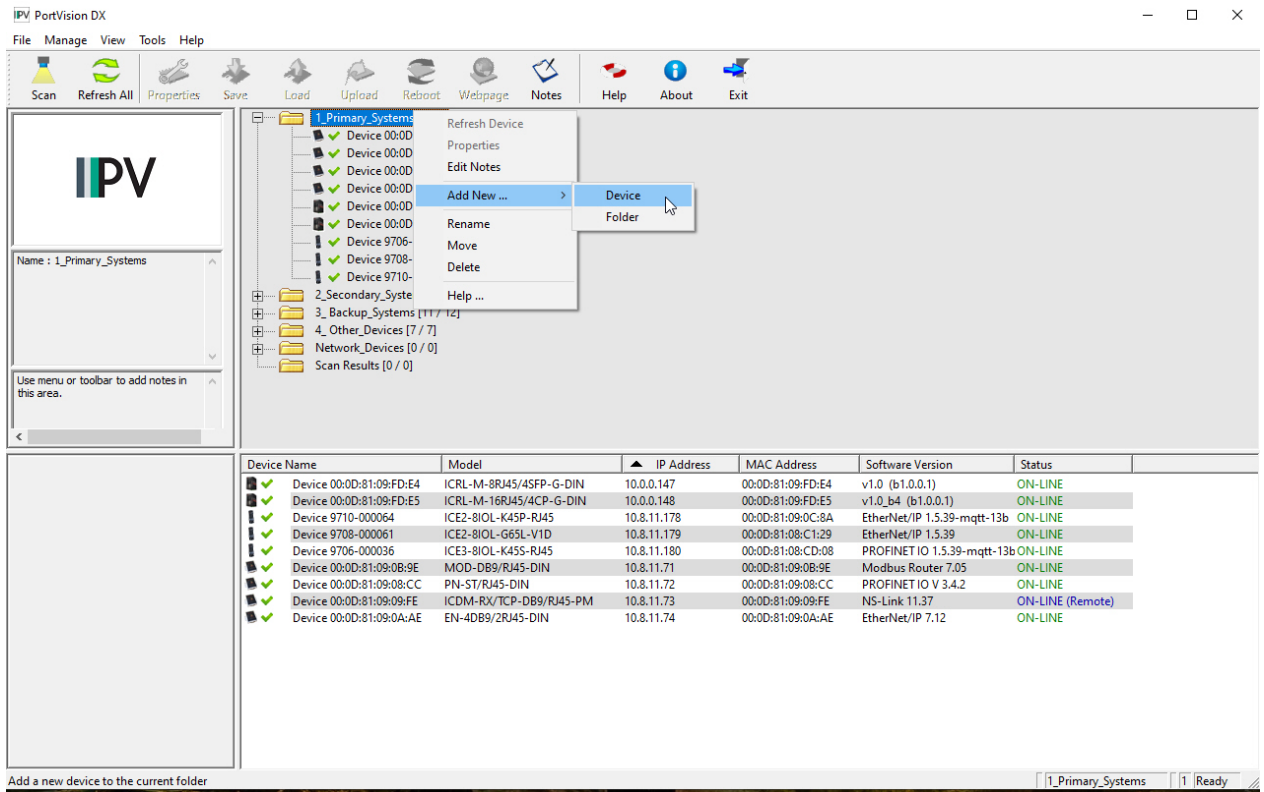
3.8. Adding a New Device in PortVision DX

You can add a new ICRL-M manually, if you do not want to scan the network to locate it or you want to pre-configure an ICRL-M before connecting it to the network. Optionally, you can also add unmanaged devices or RocketLinx switches to maintain information about devices on the network.

See the PortVision DX help system for additional information about adding unmanaged RocketLinx switches or third party devices or switches.

Use the following procedure to add a remote ICRL-M to PortVision DX.

1. Access the *New Device* window using one of these methods:
 - Click **Add New > Device** in the *Manage* menu.
 - Right-click a folder or a RocketLinx switch in the *Device Tree* pane and click **Add New > Device**.



2. Select the appropriate RocketLinx in the **Device Type** drop list.
3. Select the appropriate model in the **Device Model** drop list.
4. Enter a friendly device name in the **Device Name** list box.
5. Optionally, enter the serial number in the **Serial Number** list box.

6. Enter the IP Address for the ICRL-M. It is not necessary to enter the Subnet Mask and Default Gateway
7. Click **OK** to close the *Add New Device* window. It may take a few moments to save the ICRL-M.
8. If necessary, click **Refresh** for the new RocketLinx to display in the *Device Tree* or *Device List* panes. The RocketLinx shows OFF-LINE if it is not connected to the local network or if an incorrect IP address was entered.

3.9. Using Configuration Files

If you are deploying multiple ICRL-M switches that share common firmware values, you can save the configuration file (.dc) from the *Main* screen in PortVision DX and load that configuration onto other ICRL-M switches.

3.9.1. Saving a Configuration File

Use this procedure to save a configuration file.

1. Highlight the ICRL-M in the *Device List* pane and use one of the following methods:
 - Click the **Save** button.
 - Right-click and then click **Configuration > Save**.
2. Browse to the location you want to save the file, enter a file name, and click **Save**.
3. Click **OK** to close the *Save Configuration Completed* message.

3.9.2. Loading a Configuration File

Use the following procedure to load a previously saved a ICRL-M configuration file. Load a configuration file and apply it to a selected ICRL-M switch or switches from the *Device List* pane.

Use this procedure to load a configuration file using the *Device List* pane to one or more ICRL-M switches.

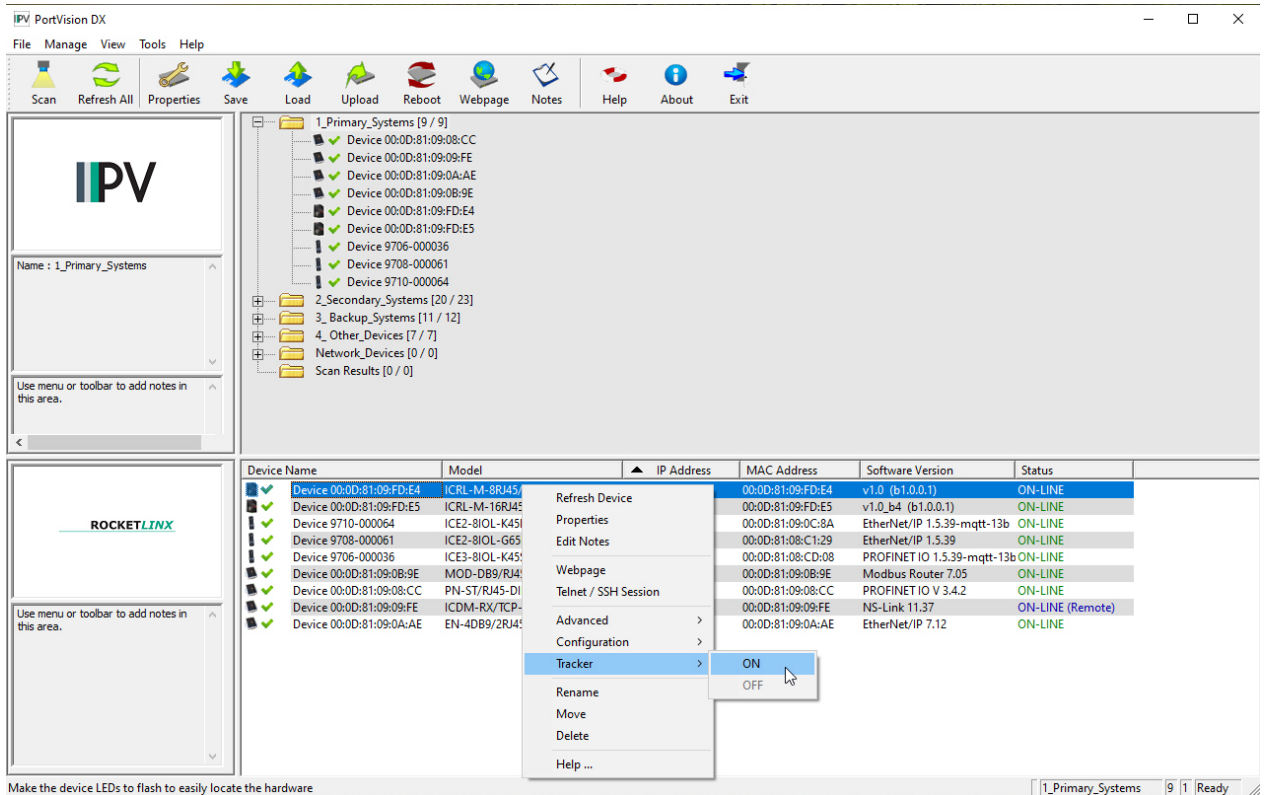
1. Highlight the device or devices in the *Device List* pane and use one of the following methods:
 - Click the **Load** button
 - Right-click and then click **Configuration > Load**
2. Click **Yes** to the warning that it will take 25 seconds per device and it may also reboot the devices.
3. Browse to the location of the configuration file, click the file name (.dc) and then **Open**.
4. Close the *Load Configuration* popup message.

3.10. Using the LED Tracker

RocketLinx managed switches support the LED Tracker feature, which allows you to toggle on/off the LEDs on a specific device so that you can locate the physical unit.

Use this procedure to toggle the **LED Tracker** feature on RocketLinx switches.

1. Right-click the ICRL-M in the *Device List* pane, click **Tracker**, and then click **ON**.
The ICRL-M **SYS** LED will flash for five seconds.



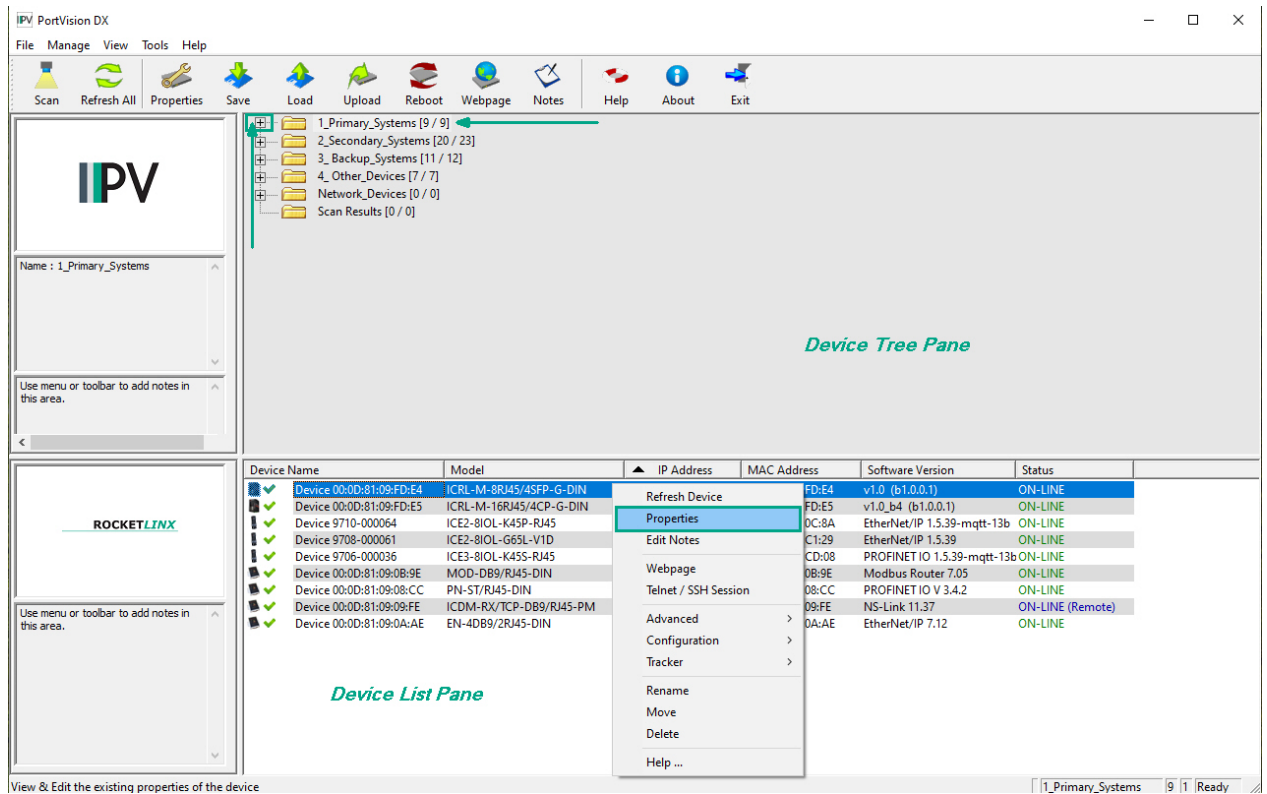
2. If necessary, you may need to click **Tracker** and **ON** several times to catch the flashing **SYS** LED.

3.11. Customizing PortVision DX

You can customize how PortVision DX displays the devices. You can even create sessions tailored for specific audiences. You can also add shortcuts to other applications using **Tools > Applications > Customize** feature.

The following illustrates how you can customize your view.

See the PortVision DX Help system for detailed information about modifying the view. For example, the above screen shot illustrates devices layered in folders.



4. Configuration - Web User Interface

Note: The ICRL-M-16RJ45/4CP-G-DIN and ICRL-M-8RJ45/4SFP-G-DIN are simply referred to as ICRL-M in the remainder of this chapter.

The ICRL-M provides in-band and out-band configuration methods:

- Out-band management means that you configure the ICRL-M using the RS-232 console cable and the Command Line Interface (CLI) to access the ICRL-M without attaching an admin PC to the network. You can use out-band management if you lose the network connection to the ICRL-M. The CLI and Telnet are discussed in *Configuration - Command Line Interface (CLI)* on Page 159.
- In-band management means that you connect remotely using the ICRL-M IP address through the network. You can remotely connect with the ICRL-M web user interface or a Telnet console and the CLI. The ICRL-M provides HTTP web user interface ([Page 34](#)) for web management.

4.1. Configuration Overview

This subsection discusses a minimum level of configuration required to operate the ICRL-M.

1. If you have not done so, install the hardware, see *Hardware Installation* on Page 9.
2. If you are planning on using in-band management, you need to program the ICRL-M IP address to meet your network requirements. The easiest way to configure the IP address is using a Windows system and PortVision DX, see *Configuring the Network Settings* on Page 23.
3. Configure other features as desired.
 - *Basic Settings* on Page 35
 - *Port Configuration* on Page 59
 - *Network Redundancy* on Page 69
 - *VLAN* on Page 88 and *Private VLAN* on Page 95
 - *Traffic Prioritization* on Page 101
 - *Multicast Filtering* on Page 106
 - *SNMP* on Page 111
 - *Security* on Page 114
 - *Warning* on Page 140
 - *Monitor and Diag* on Page 146
 - *Device Front Panel* on Page 154
 - *Save (to Flash)* on Page 156
 - *Logout* on Page 157

4.2. Web User Interface

You can use any standard web browser to configure and communicate with the ICRL-M from anywhere on the network.

The default IP address for the ICRL-M is **192.168.250.250**.

1. Open a command prompt window and ping the IP address for the ICRL-M to verify a normal response time.

Note: *If you did not program the IP address for your network using PortVision DX (Configuring the Network Settings on Page 23), you need to change your computer IP address to **192.168.250.x** (Network Mask: 255.255.255.0).*

```

Command Prompt
(c) 2015 Microsoft Corporation. All rights reserved.

C:\>ping 192.168.250.250

Pinging 192.168.250.250 with 32 bytes of data:
Reply from 192.168.250.250: bytes=32 time=3ms TTL=255
Reply from 192.168.250.250: bytes=32 time=4ms TTL=255
Reply from 192.168.250.250: bytes=32 time<1ms TTL=255
Reply from 192.168.250.250: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.250.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

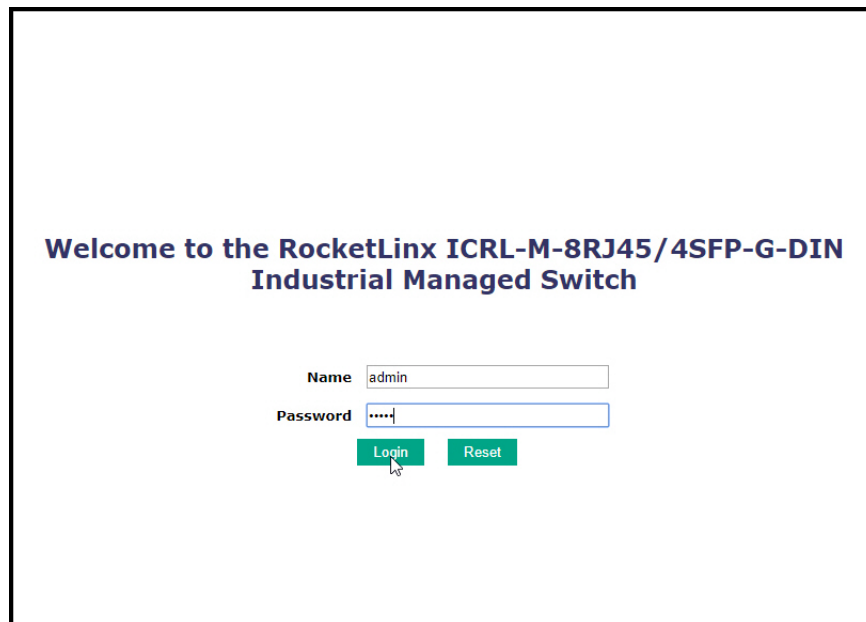
C:\>
    
```

2. Launch the web browser on the PC using one of these methods:

- Right-click the ICRL-M in PortVision DX and click **Webpage**.
- Open your browser, enter the IP address of the switch, and then press **Enter**. For example: **http://10.0.0.147**.

Note: *You will need to load a valid certificate to use an https connection.*

3. Enter the user name, the password, and click **OK**. The default user name and password are both **admin**.



4. If you have not done so, you can change the ICRL-M IP address to meet your network environment.
 - a. Double-click **Basic Setting**.
 - b. Click **IP Configuration**.
 - To use static addressing, enter a valid IP address, subnet mask and default gateway.
 - To use DHCP, click **Enable** in the **DHCP Client** drop list.
 - c. Click **Apply**.

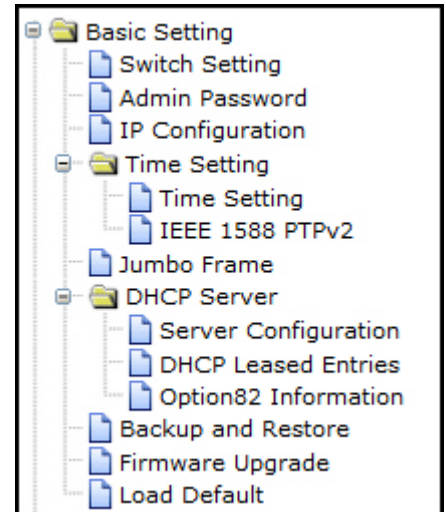
4.3. Basic Settings

The *Basic Setting* group allows you the ability to configure switch information, IP address, User name/ Password of the system. It also allows you to do firmware upgrade, backup and restore configuration, reload factory default, and reboot the system.

The following web pages are included in this group:

- *Switch Setting* on Page 36
- *Admin Password* on Page 37
- *IP Configuration* on Page 39
- *Time Setting* on Page 41
- *Jumbo Frame* on Page 45
- *DHCP Server Configuration* on Page 47
 - *DHCP Leased Entries* on Page 50
 - *Option82 Information Page* on Page 51
- *Backup and Restore* on Page 53
- *Firmware Upgrade* on Page 55
- *Load Default* on Page 57

Optionally, you can use the CLI for configuration, see *Basic Settings (CLI)* on Page 174.



4.3.1. Switch Setting

You can assign the **System Name**, **Location**, **Contact** and view ICRL-M information.



Switch Setting Page	
System Name	You can assign a name to the ICRL-M with up to 64 characters. After you configure the name, the CLI system selects the first 12 characters as the name in CLI system.
System Location	You can specify the ICRL-M physical location with up to 64 characters.
System Contact	You can specify contact people with up to 64 characters by typing the Administer's name, mail address or other information.
System OID	The SNMP Object ID of the ICRL-M. You can follow the path to find its private MIB in an MIB browser. Note: When you attempt to view private MIB, you should first compile private MIB files into your MIB browser.
System Description	ICRL-M Industrial Managed Ethernet Switch
Firmware Version	Displays the firmware version installed in this ICRL-M.
Device MAC	Displays a unique hardware address (MAC address) assigned at the factory.
Serial Number	Displays the serial number of the ICRL-M.
Manufacture Date	Displays the date of manufacture.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.3.2. Admin Password

You can change the user name and the password here to enhance security.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
 - Switch Setting
 - Admin Password
 - IP Configuration
 - Time Setting
 - Jumbo Frame
 - DHCP Server
 - Backup and Restore
 - Firmware Upgrade
 - Load Default
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

Admin Password Help

Name:

Privilege:

New Password:

Confirm Password:

Apply Cancel

Local User List

Select	User	Privilege
<input type="checkbox"/>	admin	15

Remove User Cancel

RADIUS Server

RADIUS Server IP:

Shared Key:

Server Port:

Secondary RADIUS Server

RADIUS Server IP:

Shared Key:

Server Port:

Apply

Primary TACACS+ Server

TACACS+ Server IP:

Shared Key:

Server Port:

Secondary TACACS+ Server

TACACS+ Server IP:

Shared Key:

Server Port:

TACACS+ Setting

Auth Type:

Server timeout(s):

Apply

Authentication Order

Auth order:

Apply

Admin Password Page	
Administrator	
Name	You can enter a new user name here. The default name is admin .
Privilege	0 or 15. 0 is a read-only privilege. 15 is a read/write privilege.
New Password	You can enter a new password here. The default password is admin .
Confirm Password	You need to type the new password again to confirm it.
Local User List	
Select	Click the check box and click Remove User if you want to remove a user.
RADIUS Server	
RADIUS Server IP	The IP address of the RADIUS server.
Shared Key	The password for communication between switch and RADIUS Server.
Server Port	The UDP port of the RADIUS server.
Secondary RADIUS Server	
RADIUS Server IP	The IP address of the RADIUS server.
Shared Key	The password for communication between switch and RADIUS Server.
Server Port	The UDP port of the RADIUS server.
Primary TACACS+ Server	
TACACS+ Server IP	The IP address of the primary TACACS+ server.
Shared Key	The password for communication between switch and primary TACACS+ Server.
Server Port	The UDP port of the primary TACACS+ server.
Secondary TACACS+ Server	
TACACS+ Server IP	The IP address of the secondary TACACS+ server.
Shared Key	The password for communication between switch and secondary TACACS+ Server.
Server Port	The UDP port of the secondary TACACS+ server.
TACACS+ Setting	
Auth Type	Select the appropriate authentication type: ASCII, PAP, or CHAP.
Server timeout(s)	TACACS+ server timeout in seconds.
Authentication Order	
Auth Order	Choose the order for user login process: Local, RADIUS--> Local or TACACS+ --> Local. The default is local.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.3.3. IP Configuration

This web page allows you to configure the ICRL-M's IP address settings.

PEPPERL+FUCHS
ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
 - Switch Setting
 - Admin Password
 - IP Configuration
 - Time Setting
 - Jumbo Frame
 - DHCP Server
 - Backup and Restore
 - Firmware Upgrade
 - Load Default
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

IP Configuration Help

DHCP Client Disable

IPv4 Configuration

IP Address	10.0.0.147
Subnet Mask	255.255.0.0
Default Gateway	192.168.250.1
DNS Server 1	
DNS Server 2	

IPv6 Configuration

IPv6 Address	Prefix Length
<input type="text"/>	<input type="text"/>

IPv6 Default Gateway

IPv6 Address
<input type="checkbox"/> fe80::20d:81ff:fe09:fde4/64

IPv6 Neighbor Table

Neighbor	Interface	MAC Address	State

Copyright (c) Peppert+Fuchs All Rights Reserved.

IP Configuration Page	
DHCP Client	You can select to Enable or Disable the DHCP Client function. When the DHCP Client function is enabled, an IP address is assigned to the switch from the network's DHCP server. In this mode, the default IP address is replaced by the one assigned by DHCP server. If DHCP Client is disabled, then the IP address that you specified is used.
IP Address Default: 192.168.250.250	You can assign the IP address reserved by your network for the ICRL-M. If the DHCP Client function is enabled, you do not need to assign an IP address to the ICRL-M, because it is overwritten by the DHCP server and displays here.
Subnet Mask Default: 255.255.255.0	You can assign the subnet mask for the IP address here. If the DHCP Client function is enabled, you do not need to assign the subnet mask. . Note: In the CLI, the enabled bit of the subnet mask is used to represent the number displayed in the web management interface. For example, 8 represents: 255.0.0.0, 16 represents: 255.255.0.0, 24 represents: 255.255.255.0.
Default Gateway Default: 192.168.250.1	You can assign the gateway for the switch here. Note: In the CLI, use 0.0.0.0/0 to represent the default gateway.
DNS Server 1/2	The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.
IPv6 Address	You can enter an IPv6 address for the ICRL-M. An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:), and the length of IPv6 address is 128bits. The 64-bit interface identifier is automatically generated from the MAC address for the ICRL-M using the modified EUI-64 format.
Prefix Length	This IPv6 prefix specifies the size of a network or subnet. The default is 64.
IPv6 Default Gateway	The IPv6 default gateway IP address identifies the gateway (for example, a router) that receives and forwards those packets whose addresses are unknown to the local network. The agent uses the default gateway address when sending alert packets to the management workstation on a network other than the local network.
IPv6 Address	This table shows the IPv6 addresses that have been added to the management VLAN. To remove an entry, click the check box next to it and then click the Remove button. To reload the list, click the Reload button.
IPv6 Neighbor Table	
Neighbor	The <i>IPv6 Neighbor Table</i> lists neighbors of the ICRL-M.
Interface	The interface connected to the neighbor.
MAC address	This is the MAC address of the neighbor.
State	This displays the Neighbor Unreachability Detection (NUD) state of the neighbor entry.
Remove	Click the Remove button to remove an IPv6 configuration or IPv6 Neighbor Table entry.
Reload	Click the Reload button to reload IPv6 configuration.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4/21/20

4.3.4. Time Setting

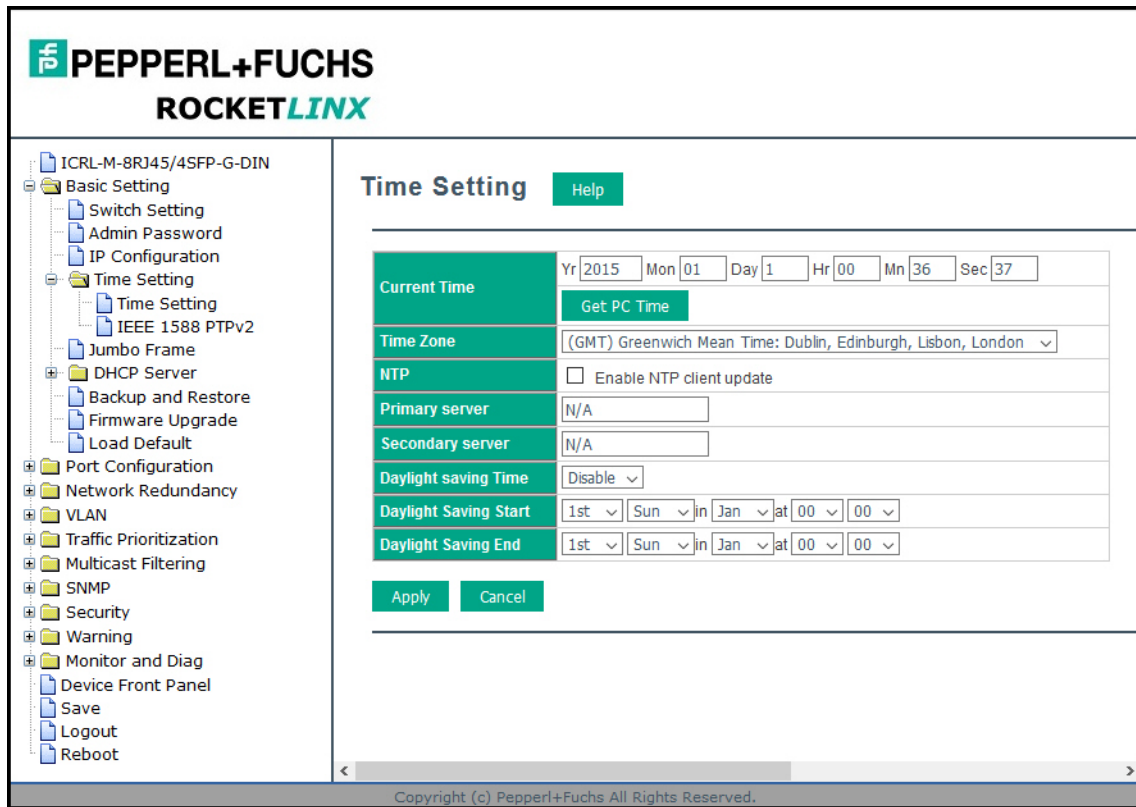
Time Setting page allows you to set the time manually or through the NTP server. Network Time Protocol (NTP) is used to synchronize computer clocks on the internet. You can configure NTP settings here to synchronize the clocks of several switches on the network.

The IEEE1588 PTP (Precision Time Protocol) supports very precise time synchronization in an Ethernet network. There are two clocks, Master and Slave. The master device periodically launches an exchange of messages with slave devices to help each slave clock re-compute the offset between its clock and the master's clock.

Note: Enable one synchronization protocol (PTP/NTP) only.

4.3.4.1. Time Setting Page

Time Setting allows you to set the time manually or through a Network Time Protocol (NTP) server. NTP is used to synchronize computer clocks on the Internet. You can configure NTP settings here to synchronize the clocks of several switches on the network. The ICRL-M also provides Daylight Saving functionality.



Time Setting Page	
Current Time	<p>Manual Setting: Click the Get PC Time button to get PC's time setting for the ICRL-M or enter the appropriate information in the fields provided.</p> <p>NTP client: Click Time Setting Source if you want the NTP client to permit the ICRL-M to enable the NTP client service. NTP client is automatically enabled if you change the Time Setting Source to NTP Client. The system sends a request packet to acquire current time from the NTP server you assign.</p>

4/21/20

Time Setting Page (Continued)	
Time Zone	Select the time zone where the ICRL-M is located. The following table lists the time zones for different locations for your reference. The default time zone is (GMT) Greenwich Mean Time.
NTP	Click this check box to enable NTP (Network Time Protocol).
Primary/Secondary Server	The Primary Server is the primary NTP server for which you want to synchronize time. The Secondary Server is the back up NTP server to use if the Primary Server becomes unavailable.
Daylight Saving Time	You can enable Daylight Saving Time and then set the Daylight Saving Time Start and End times. During Daylight Saving Time, the ICRL-M time is one hour earlier than the actual time.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

Switch(config)# clock timezone

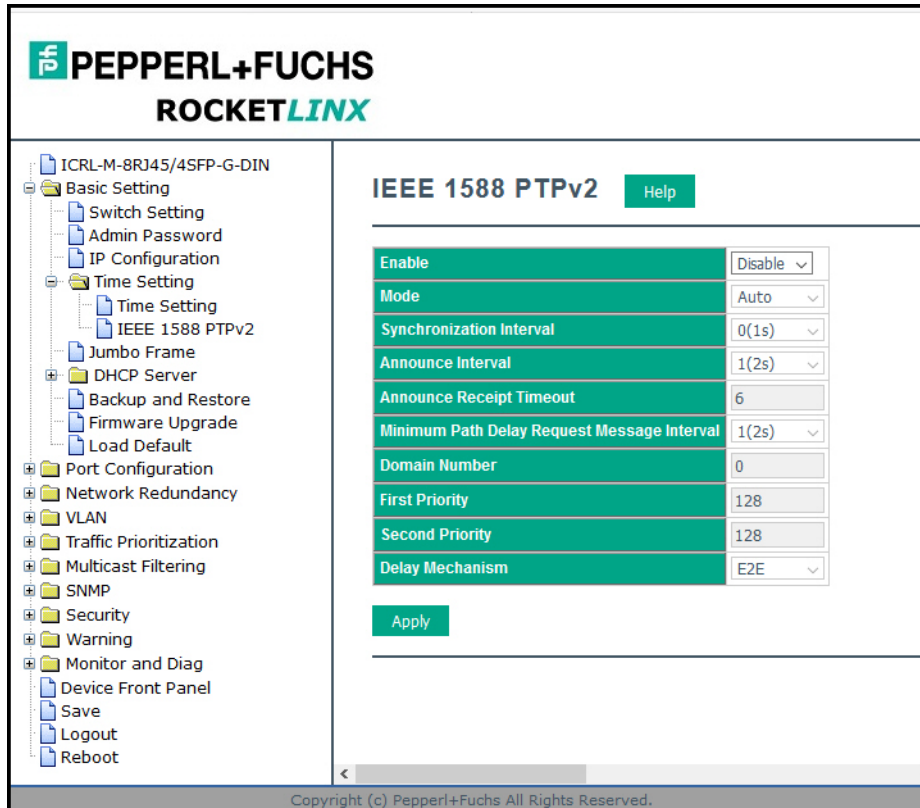
- 01 (GMT-12:00) Eniwetok, Kwajalein
- 02 (GMT-11:00) Midway Island, Samoa
- 03 (GMT-10:00) Hawaii
- 04 (GMT-09:00) Alaska
- 05 (GMT-08:00) Pacific Time (US & Canada), Tijuana
- 06 (GMT-07:00) Arizona
- 07 (GMT-07:00) Mountain Time (US & Canada)
- 08 (GMT-06:00) Central America
- 09 (GMT-06:00) Central Time (US & Canada)
- 10 (GMT-06:00) Mexico City
- 11 (GMT-06:00) Saskatchewan
- 12 (GMT-05:00) Bogota, Lima, Quito
- 13 (GMT-05:00) Eastern Time (US & Canada)
- 14 (GMT-05:00) Indiana (East)
- 15 (GMT-04:00) Atlantic Time (Canada)
- 16 (GMT-04:00) Caracas, La Paz
- 17 (GMT-04:00) Santiago
- 18 (GMT-03:00) Newfoundland
- 19 (GMT-03:00) Brasilia
- 20 (GMT-03:00) Buenos Aires, Georgetown
- 21 (GMT-03:00) Greenland
- 22 (GMT-02:00) Mid-Atlantic
- 23 (GMT-01:00) Azores
- 24 (GMT-01:00) Cape Verde Is.
- 25 (GMT) Casablanca, Monrovia
- 26 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
- 27 (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
- 28 (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
- 29 (GMT+01:00) Brussels, Copenhagen, Madrid, Paris
- 30 (GMT+01:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb
- 31 (GMT+01:00) West Central Africa
- 32 (GMT+02:00) Athens, Istanbul, Minsk
- 33 (GMT+02:00) Bucharest

4/21/20

- 34 (GMT+02:00) Cairo
- 35 (GMT+02:00) Harare, Pretoria
- 36 (GMT+02:00) Helsinki, Riga, Tallinn
- 37 (GMT+02:00) Jerusalem
- 38 (GMT+03:00) Baghdad
- 39 (GMT+03:00) Kuwait, Riyadh
- 40 (GMT+03:00) Moscow, St. Petersburg, Volgograd
- 41 (GMT+03:00) Nairobi
- 42 (GMT+03:30) Tehran
- 43 (GMT+04:00) Abu Dhabi, Muscat
- 44 (GMT+04:00) Baku, Tbilisi, Yerevan
- 45 (GMT+04:30) Kabul
- 46 (GMT+05:00) Ekaterinburg
- 47 (GMT+05:00) Islamabad, Karachi, Tashkent
- 48 (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi
- 49 (GMT+05:45) Kathmandu
- 50 (GMT+06:00) Almaty, Novosibirsk
- 51 (GMT+06:00) Astana, Dhaka
- 52 (GMT+06:00) Sri Jayawardenepura
- 53 (GMT+06:30) Rangoon
- 54 (GMT+07:00) Bangkok, Hanoi, Jakarta
- 55 (GMT+07:00) Krasnoyarsk
- 56 (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
- 57 (GMT+08:00) Irkutsk, Ulaan Bataar
- 58 (GMT+08:00) Kuala Lumpur, Singapore
- 59 (GMT+08:00) Perth
- 60 (GMT+08:00) Taipei
- 61 (GMT+09:00) Osaka, Sapporo, Tokyo
- 62 (GMT+09:00) Seoul
- 63 (GMT+09:00) Yakutsk
- 64 (GMT+09:30) Adelaide
- 65 (GMT+09:30) Darwin
- 66 (GMT+10:00) Brisbane
- 67 (GMT+10:00) Canberra, Melbourne, Sydney
- 68 (GMT+10:00) Guam, Port Moresby
- 69 (GMT+10:00) Hobart
- 70 (GMT+10:00) Vladivostok
- 71 (GMT+11:00) Magadan, Solomon Is., New Caledonia
- 72 (GMT+12:00) Auckland, Wellington
- 73 (GMT+12:00) Fiji, Kamchatka, Marshall Is.
- 74 (GMT+13:00) Nuku'alofa

4.3.5. IEEE 1588 PTPv2

The IEEE1588 PTP (Precision Time Protocol) supports very precise time synchronization in an Ethernet network. There are two clocks, Master and Slave. The master device periodically launches an exchange of messages with slave devices to help each slave clock re-compute the offset between its clock and the master's clock.



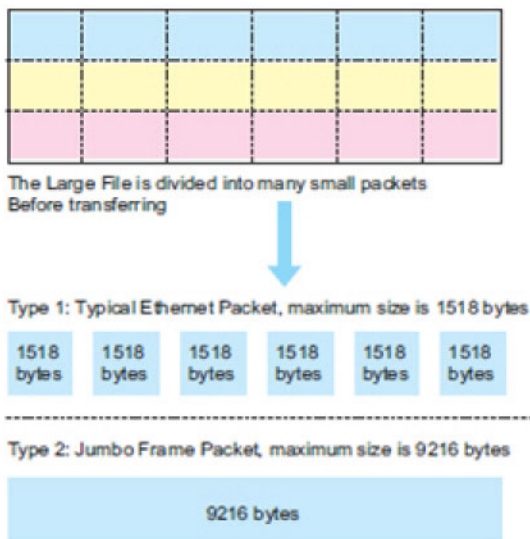
IEEE 1588 PTPv2 Page	
Enable	To enable IEEE 1588, select Enable in PTP Status and choose Auto, Master or Slave Mode. After time synchronized, the system time will display the correct time of the PTP server.
Mode	<ul style="list-style-type: none"> • Auto mode: the switch performs PTP Master and slave mode. • Master mode: switch performs PTP Master only. • Slave mode: switch performs PTP slave only.
Synchronization Interval	Select items: -3(128ms) -2(256ms) -1(512ms) 0(1s) 1(2s) 2(4s) 3(8s) 4(16s)
Announce Interval	Select items:0(1s) 1(2s) 2(4s) 3(8s) 4(16s)
Announce Receipt Timeout	Select items:<2-10>
Minimum Path Delay Request Message Interval	Select items: -1(512ms) 0(1s) 1(2s) 2(4s) 3(8s) 4(16s)
Domain Number	Select items:<0-3>
First Priority	First priority Select items:<0-255>
Second Priority	Second priority Select items:<0-255>

4/21/20

IEEE 1588 PTPv2 Page (Continued)	
Delay Mechanism	E2E: End-to-End PTP: Peer-to-Peer
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

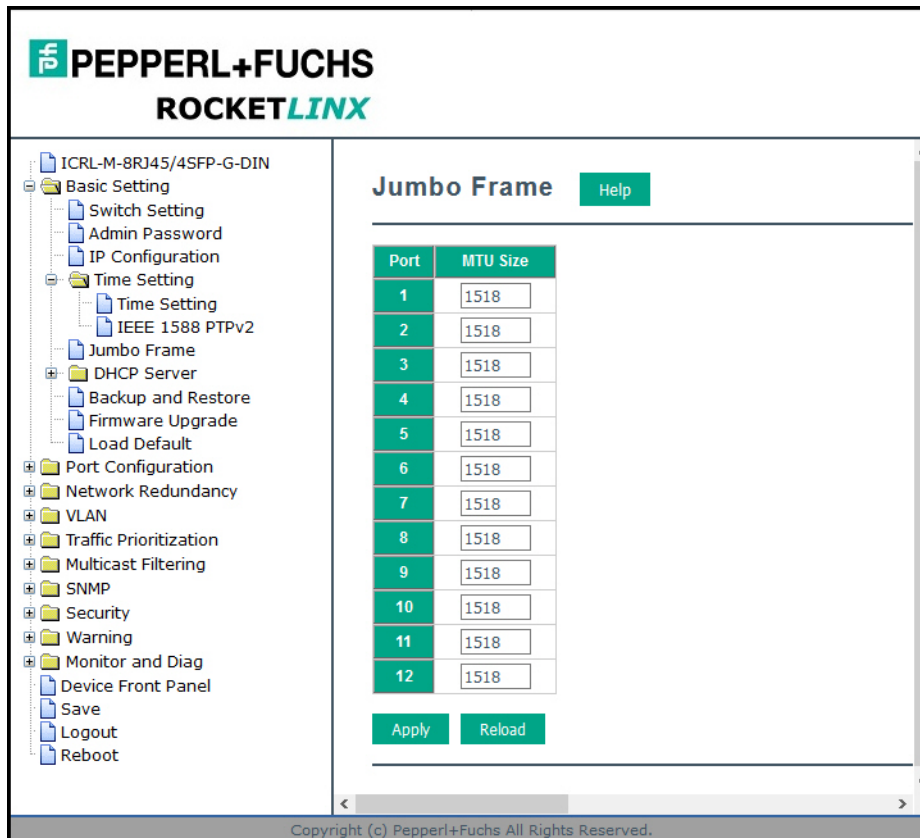
4.3.6. Jumbo Frame

The typical Ethernet frame range is from 64 to 1500. The Jumbo Frame feature allows this switch to send and receive Ethernet frames that are 64 to 9216 bytes on its interfaces.



Jumbo Frame supports 1,518 bytes (default) to 9,216 bytes. This is sufficient for general usages. However, when users want to transmit large files, the files may be divided into many small size packets. When the transmission speed becomes slow, long size Jumbo frame may solve the issue.

The ICRL-M allows you configure the size of the Maximum Transmission Unit (MTU). You can increase the MTU size to support jumbo frames on all interfaces by setting the Jumbo Frame MTU. You can freely change the available packet size.



Jumbo Frame	Description
MTU Size	Change the MTU size for all Gigabit Ethernet interfaces on the switch stack. The range is 1518 to 9216 bytes; the default is 1518 bytes.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.
Reset	Click to Reset the MTU to the default value.

4.3.7. DHCP Server Configuration

Use this page to configure DHCP server services.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Switch Setting
- Admin Password
- IP Configuration
- Time Setting
 - Time Setting
 - IEEE 1588 PTPv2
- Jumbo Frame
- DHCP Server
 - Server Configuration
 - DHCP Leased Entries
 - Option82 Information
 - Backup and Restore
 - Firmware Upgrade
 - Load Default
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

DHCP Server Configuration Help

Global Setting Disable

Address Pool Setting

Pool Name

Network

Mask

Default Gateway

Lease Time
(60~31536000 seconds)

Excluded Address List

Excluded IP

Index	IP Address

Static Port IP Binding List

Port

IP Address

Index	Port	IP Address

Static MAC IP Binding List

MAC Address

IP Address

Index	MAC Address	IP Address

Option82 IP Binding List

Circuit ID

Remote ID

IP Address

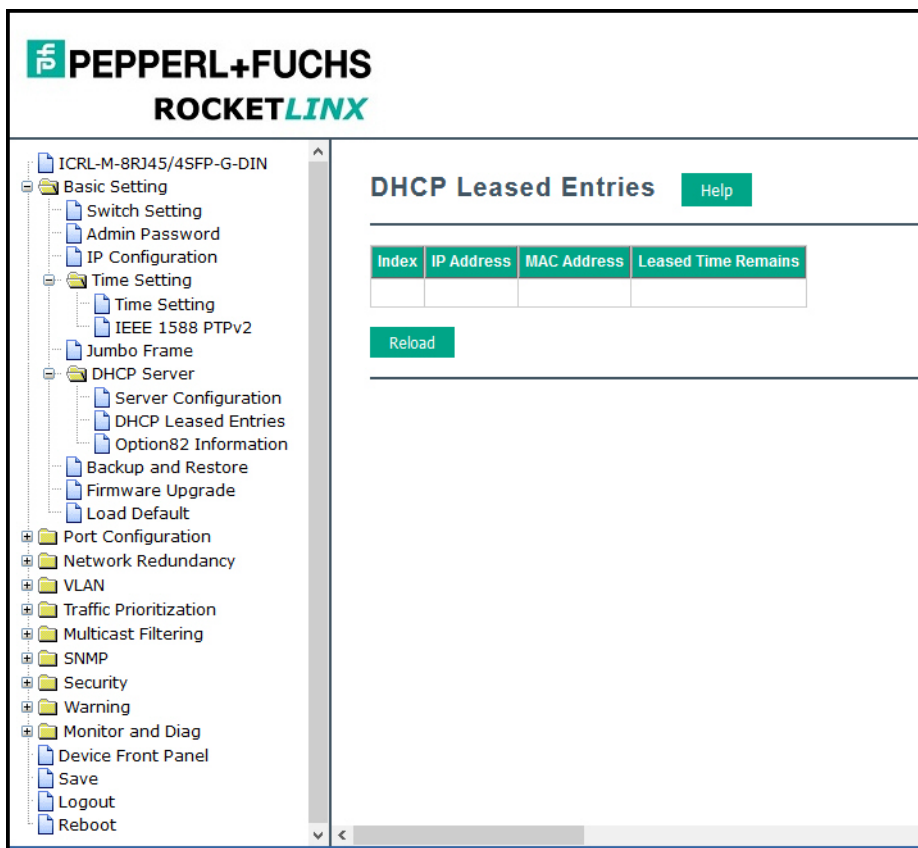
Index	Circuit ID	Remote ID	IP Address

DHCP Server Configuration Page	
Global Setting	You can select to Enable or Disable the DHCP Server function. The ICRL-M assigns a new IP address to link partners.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.
Address Pool Setting	
Pool Name	Enter a pool name.
Network	Enter the IPv4 address for the DHCP server.
Subnet Mask	Enter the subnet mask for the DHCP server.
Default Gateway	Enter the IP gateway address for the DHCP server.
Lease Time	Enter the Lease Time in seconds for the client.
Excluded Address List	
Excluded IP	You can type a specific address into the Excluded IP field for the DHCP server reserved IP address. The IP addresses listed in the Excluded Address List Table are not assigned to the network devices. Add or remove an IP address from the Excluded Address List by clicking Add or Remove . Note: By default, only the table heading are displayed until an IP address is entered in the Excluded IP field and added using the Add button.
Static Port/IP Binding List	
Port	Enter the client port number for the DHCP server.
IP Address	Enter the client IP address for the DHCP server. After entering the port number and IP address, click Add . To remove a port and associated IP address, click Remove . Click Reload to reload selected port and IP address entries. Note: By default, only the table heading are displayed until information is entered in the Port and IP Address fields and added using the Add button.
Static MAC/IP Binding List	
IP Address	The ICRL-M provides an IP address binding and removing function. Enter the specified IP address, and then click Add to add a new IP address binding rule for a specified link partner, like a PLC, or any device without DHCP client function. To remove an IP address from the Manual Binding List, highlight the rule and click Remove .

DHCP Server Configuration Page (Continued)	
MAC Address	<p>The ICRL-M provides a MAC address binding and removing function. Enter the specified MAC address, and then click Add to add a new MAC address binding rule for a specified link partner, like a PLC, or any device without DHCP client function.</p> <p>The MAC address format is xxxx.xxxx.xxxx.</p> <p>To remove a MAC address from the Static MAC/IP Binding List, highlight the rule and click Remove.</p> <p>Note: <i>By default, only the table heading are displayed until information is entered in the IP Address and MAC Address fields and added using the Add button.</i></p>
Option82/IP Binding List	
Circuit ID	The Circuit ID of the Option82 IP address configuration.
Remote ID	<p>The Remote ID of the Option82 IP address configuration.</p> <p>After entering the IP Address, Circuit ID, and Remote ID, click Add.</p> <p>Click the Remove button to remove selected Option82 IP Address table entries.</p> <p>Click the Reload button to reload selected Option82 IP Address table entries.</p>
IP Address	<p>Option 82 IP Address Configuration: fully supports DHCP relay function.</p> <p>The IP address of the Option82 IP address configuration.</p> <p>Note: <i>By default, only the table heading are displayed until information is entered in the Circuit ID, Remote ID, and IP Address fields and added using the Add button.</i></p>

4.3.8. DHCP Leased Entries

The ICRL-M provides a table that displays assigned IP addresses.



DHCP Leased Entries Page	
Index	Index of DHCP leased entries.
IP Address	The IP address of the leased entry.
MAC Address	The MAC Address of the leased entry.
Lease Time(s)	The lease time of the leased entry (in seconds).
Reload	Click to reload DHCP leased entries.

Note: By default, only the table heading are displayed until there is data to display.

4.3.9. Option82 Information Page

This subsection discusses the *Option82 Information* page.

The screenshot shows the 'Option82 Information' configuration page. On the left is a navigation tree with 'Option82 Information' selected. The main content area has the following sections:

- DHCP Relay Agent:** A dropdown menu set to 'Disable' and an 'Apply' button.
- Helper Address:** A text input field for 'Helper Address', an 'Add' button, and a list of four 'Helper Address' entries (1-4) with checkboxes and input fields. A 'Remove' button is below.
- Relay Policy:** Radio buttons for 'Replace', 'Keep', and 'Drop', with an 'Apply' button.
- Circuit ID:** A dropdown menu, radio buttons for 'Default (VLAN/Port)' and 'User Defined', and an 'Apply' button.
- Table:** A table with 3 columns: 'Port', 'Circuit ID', and 'HEX value'. It contains 12 rows for ports 1 through 12.
- Remote ID:** Radio buttons for 'Default (MAC Address)', 'IP Address', and 'User Defined', with an 'Apply' button.
- Table:** A table with 2 columns: 'Remote ID' and 'HEX value', with one row for input.

At the bottom, there is a footer: 'Copyright (c) Pepperl+Fuchs All Rights Reserved.'

4/21/20 **Note:** You must **Save** the settings (Page 156), to maintain these settings if the ICRL-M is powered off.

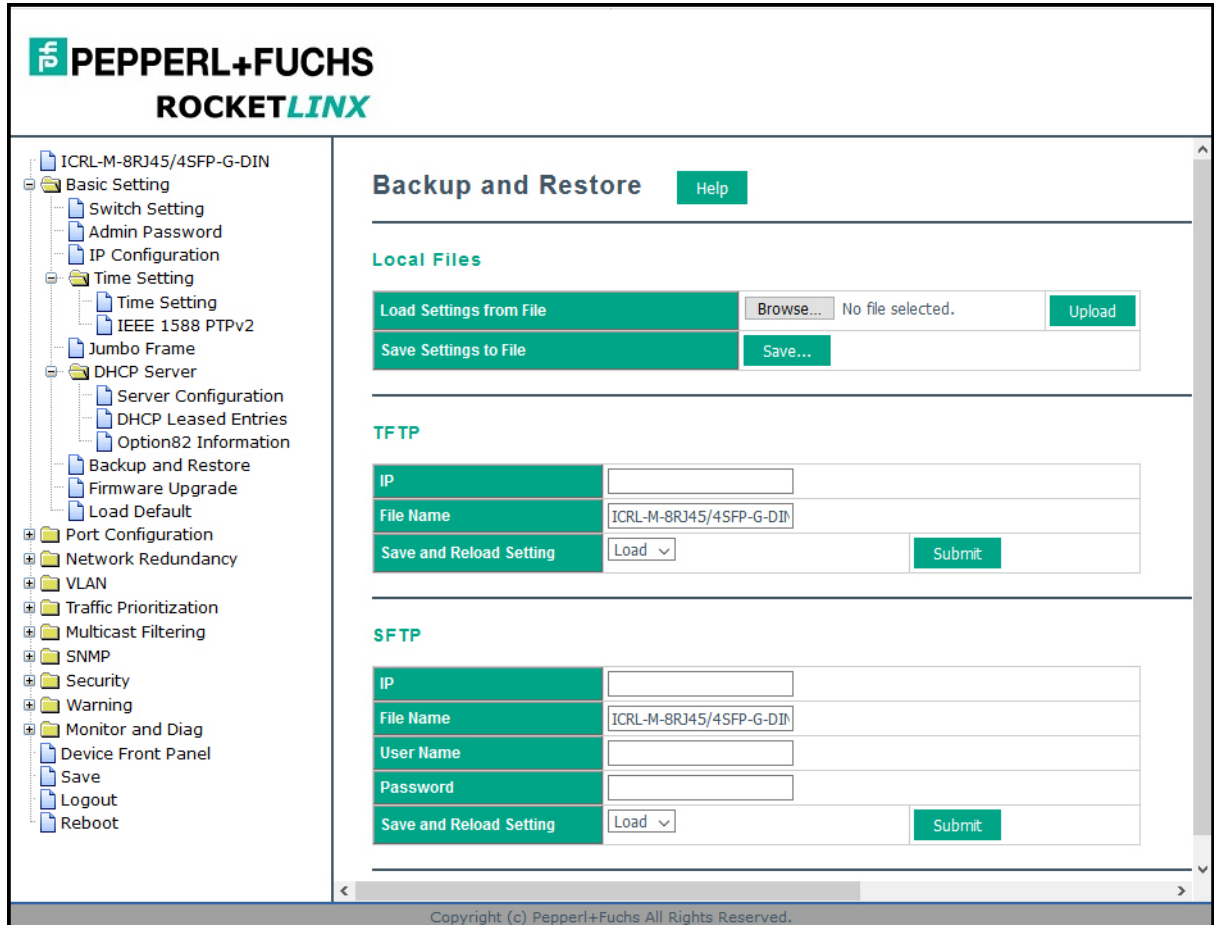
Option82 Information Page	
DHCP Relay Agent	You can select to Enable or Disable the DHCP Option82 Relay function, which assigns a new IP address to link partners.
Helper Address	
Helper Address	Enter the DHCP Server address for the Relay Agent and click Add . The Helper Addresses appear in the table below.
Helper Address 1-4	DHCP Server addresses for the Relay Agent.
Relay Policy	<ul style="list-style-type: none"> • Replace: Replaces the existing option 82 field and adds new option 82 field. This is the default when the DHCP Relay Agent is enabled. • Keep: Keeps the original option 82 field and forwards to server. • Drop: Drops the option 82 field and do not add any option 82 field.
Circuit ID	<ul style="list-style-type: none"> • Default: Default value of the Circuit-ID. • Port: Port of the switch. • Circuit ID: The Circuit ID includes information specific to which circuit the request came in on. It is an identifier that is specific to the relay agent, so the type of circuit varies depending on the relay agent.
Remote ID	<ul style="list-style-type: none"> • Default: Default value of the Remote-ID. • IP Address: IP Address of the switch. • Remote ID: The Remote-ID carries information relating to the remote host end of the circuit, which is the MAC address of the relay.

4.3.10. Backup and Restore

You can use the **Backup** option to save the current configuration saved in the ICRL-M flash to a PC or laptop, your TFTP server, or SFTP server.

This allows you to use the **Restore** option to restore a configuration file back to the ICRL-M or load the same settings to another ICRL-M. Before you can restore a configuration file, you must first save the backup configuration file to a local system, TFTP, or SFTP server. The ICRL-M then can download this file back into the flash.

The ICRL-M configuration file is a standard text file. You can open the file with WordPad or Notepad. You can also modify the file, add/remove the configuration settings, and then restore the file back to the ICRL-M.



Optionally, you can use PortVision DX to back up and restore configuration files.

Backup & Restore Page	
Local Files	<p>In this mode, the switch acts as the file server. You can browse the target folder and then type the file name to backup the configuration. You can also browse the target folder and select an existing configuration file to restore the configuration back to the ICRL-M. This mode is only provided by web user interface.</p> <p>Load Settings from File: Click the Browse button to select the previously saved backup configuration file. After locating the configuration file, click the Upload button.</p> <p>Save Settings to File: Click the Save button to save the configuration file.</p> <p>Note: Pointing to the wrong file causes the entire configuration to be skipped.</p>

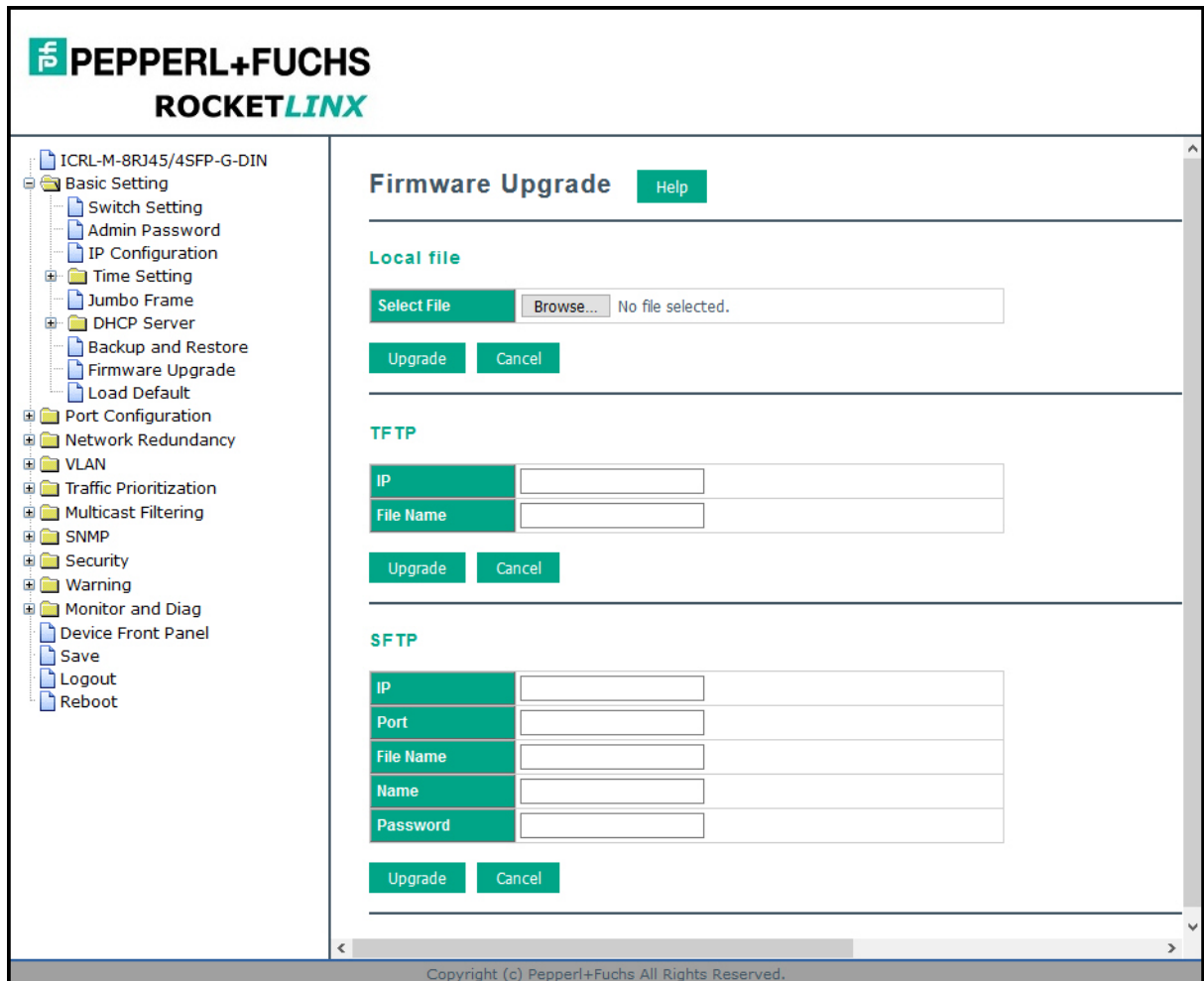
4/21/20

Backup & Restore Page (Continued)	
TFTP	<p>In this mode, the ICRL-M acts as a TFTP client. Before you do so, make sure that your TFTP server is ready. Enter the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and web user interface.</p> <p>IP: This is the IP address of the TFTP server where your configuration file has been previously saved or can be saved.</p> <p>File Name: This is the file name of configuration file to be saved.</p> <p>Load/Save Settings: Select Load to load the configuration from the TFTP server onto the switch.</p> <p>Click Submit to load or save the configuration.</p>
SFTP	<p>In this mode, the switch acts as SFTP client. Before you do so, make sure that your SFTP server is ready. Enter the IP address of SFTP Server and Backup configuration file name. This mode can be used in both CLI and web user interface.</p> <p>IP: This is the IP address of the SFTP server where your configuration file has been previously saved or can be saved.</p> <p>File Name: This is the file name of configuration file to be saved.</p> <p>User Name: Insert the User name for SFTP</p> <p>Password: Insert the password of SFTP</p> <p>Load/Save Settings: Select Load to load the configuration from the TFTP server onto the switch.</p> <p>Click Submit to load or save the configuration.</p>
<ul style="list-style-type: none"> • The ICRL-M provides a default configuration file in the ICRL-M. To load the default configuration file, you can use the Reset on the <i>Load Default</i> page on Page 57 or the Reload command in the CLI (Page 179). • You can use the CLI to view the latest settings running in the ICRL-M. The information are the settings you have configured but have not yet saved to the flash. The settings must be saved to the flash in order to work after a power recycle. Use the running-config command to view the configuration file, see <i>Show Running Config</i> on Page 179. • After you save the running-config to flash, the new settings are kept and work after the power is cycled. Use the show startup-config to view it in the CLI. The Backup command can only backup the configuration file to your PC or TFTP server. 	

4.3.11.Firmware Upgrade

Use this section to update the ICRL-M with the latest firmware. Pepperl+Fuchs provides the latest firmware on <https://www.pepperl-fuchs.com>. Updated firmware may include new features, bug fixes, or other software changes. Pepperl+Fuchs Technical Support suggests you use the latest firmware before installing the ICRL-M at a customer site.

Note: *Optionally, you can use PortVision DX to upload the latest firmware. If you need to upload a new version of the Bootloader, you must use PortVision DX or the CLI. You cannot use the web user interface to upload the Bootloader.*



Firmware Upgrade Page	
Local File	<p>This option allows you to upload a firmware image that is stored locally on your computer.</p> <p>Select File: Select a firmware image from your computer. Click Upgrade to begin upgrading the firmware.</p> <p>Click Cancel to clear the selected file.</p> <p>After the firmware has upgraded the switch reboots automatically. You may want to remind the attached network users before you perform this function.</p>

4/21/20

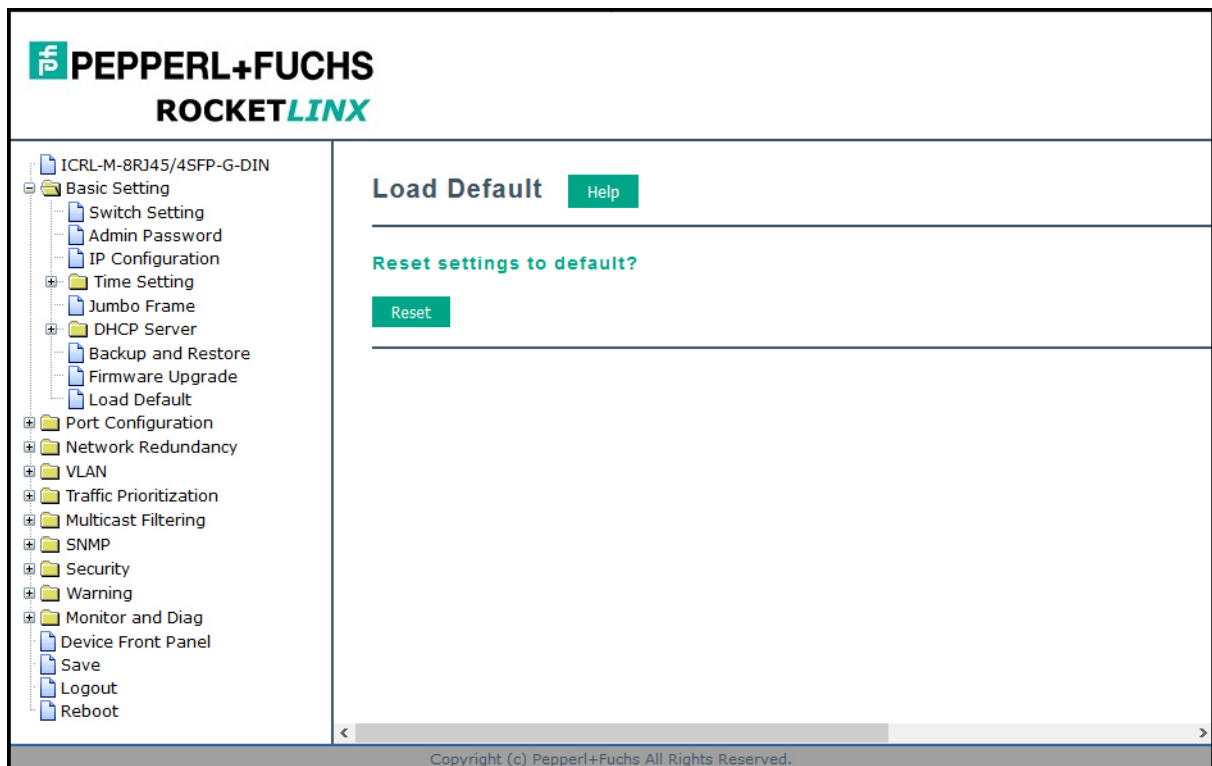
Firmware Upgrade Page (Continued)	
TFTP	<p>This option allows you to upload a firmware image that is stored on a TFTP server.</p> <p>IP: This is the IP address of the TFTP server where your firmware image is stored.</p> <p>File Name: This is the file name of the firmware image.</p> <p>Click Upgrade to begin upgrading the firmware.</p> <p>Click Cancel to clear the selected file.</p> <p>After the firmware has upgraded the switch reboots automatically. You may want to remind the attached network users before you perform this function.</p>
SFTP	<p>This option allows you to upload a firmware image that is stored on a SFTP server.</p> <p>IP: This is the IP address of the SFTP server where your firmware image is stored.</p> <p>Port: Insert the TCP Port number.</p> <p>File Name: This is the file name of the firmware image.</p> <p>Name: Insert the User name for SFTP</p> <p>Password: Insert the password of SFTP</p> <p>Click Upgrade to begin upgrading the firmware. Click Cancel to clear the selected file.</p> <p>After the firmware has upgraded the switch will reboot automatically. You may want to remind the attached network users before you perform this function.</p>

4.3.12. Load Default

You can reset the ICRL-M configuration values to default settings, excluding the network information. Optionally, you can use the *Reset Button* on Page 18, which also resets the IP address with the default configuration values.

Note: You can also use *PortVision DX* to reset the switch to the default configuration values (excluding the network settings.).

1. Click the **Reset** button, if you want the ICRL-M to reset all configurations to factory default settings.



The system displays a popup message window after finishing. The default settings work after rebooting the ICRL-M.

2. Click **OK** in the popup message to reset the configuration to the defaults.
3. Click **OK** to the *Please reboot the switch to reload default settings except IP address* message.

4. Go to the **Reboot** page, click the **Yes** button.

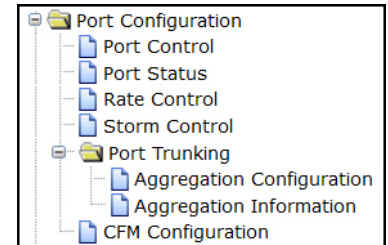
The screenshot displays the web management interface for a PEPPERL+FUCHS ROCKETLINX device. The left sidebar contains a navigation menu with the following items: ICRL-M-8RJ45/4SFP-G-DIN, Basic Setting, Switch Setting, Admin Password, IP Configuration, Time Setting, Jumbo Frame, DHCP Server, Backup and Restore, Firmware Upgrade, Load Default, Port Configuration, Network Redundancy, VLAN, Traffic Prioritization, Multicast Filtering, SNMP, Security, Warning, Monitor and Diag, Device Front Panel, Save, Logout, and Reboot. The main content area is titled "Reboot" and contains the question "Do you want to reboot?" followed by a green "Yes" button. At the bottom of the interface, there is a copyright notice: "Copyright (c) Pepper+Fuchs All Rights Reserved."

4.4. Port Configuration

The *Port Configuration* group allows you to enable/disable port state, or configure port auto-negotiation, speed, duplex, flow control, port aggregation settings (port trunking), and rate limit control. It also allows you to view port status and aggregation information. The following pages are included in this group:

- *Port Control*
- *Port Status* on Page 61
- *Rate Control* on Page 63
- *Storm Control* on Page 64
- *Port Trunking* on Page 65

Optionally, you can use the CLI for configuration, see *Port Configuration (CLI)* on Page 180.



4.4.1. Port Control

The *Port Control* page allows you to enable/disable port state, or configure the port auto-negotiation, speed, duplex, and flow control.

Select the port you want to configure and make changes to the port. The following table provides information about the different port control options.

Note: *If both ends are not at the same speed, they cannot link with each other. If both ends are not in the same duplex mode, they are connected by half-duplex mode.*

- ICRL-M-8RJ45/4SFP-G-DIN
- Basic Setting
- Port Configuration
 - Port Control
 - Port Status
 - Rate Control
 - Storm Control
- Port Trunking
 - CFM Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

Port Control Help

Port	State	Speed/Duplex	Flow Control	Description
1	Enable	AutoNegotiation	Disable	
2	Enable	AutoNegotiation	Disable	
3	Enable	AutoNegotiation	Disable	
4	Enable	AutoNegotiation	Disable	
5	Enable	AutoNegotiation	Disable	
6	Enable	AutoNegotiation	Disable	
7	Enable	AutoNegotiation	Disable	
8	Enable	AutoNegotiation	Disable	
9	Enable	AutoNegotiation	Disable	
10	Enable	AutoNegotiation	Disable	
11	Enable	AutoNegotiation	Disable	
12	Enable	AutoNegotiation	Disable	

Apply
Cancel

Copyright (c) Pepperl+Fuchs All Rights Reserved.

Port Configuration Page	
State	You can enable or disable the state of this port. Once you click Disable , the port stops to link to the other end and stops to forward any traffic. The default setting is Enable which means all the ports are workable when you receive the ICRL-M.
Speed/Duplex	<p>You can configure port speed and duplex mode of each Gigabit port.</p> <p>Below are the selections you can choose for the RJ45 ports:</p> <ul style="list-style-type: none"> • Auto Negotiation (default) • 10M full-duplex (10 Full) • 10M half-duplex (10 Half) • 100M full-duplex (100 Full) • 100M half-duplex (100 Half) <p>Below are the selections you can choose for the SFP ports:</p> <ul style="list-style-type: none"> • Auto Negotiation (default) • 100M full-duplex (100 Full) <p>ICRL-M-16RJ45/4CP-G-DIN provides four RJ45/SFP combination ports. By default the RJ45 (C) ports are disabled. If you want to use both the RJ45 copper ports and the SFP (F) ports, you must enable the copper port. If both ports are accessed at the same time, the SPF takes priority.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> Enable ▾ C: AutoNegotiation ▾ Disable ▾ F: AutoNegotiation ▾ </div>
Flow Control	<p>Enable means that you need to activate the flow control function of the remote network device in order to let the flow control of that corresponding port on the switch to work.</p> <p>Disable (default) means that you do not need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the switch works.</p>
Description	Click this field if you want to enter a port description.
Apply	<p>Click Apply to apply the settings.</p> <p>Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.</p>

4.4.2. Port Status

Note: The *Port Status* page displays the current port status, including Small Form Factory (SFP) fiber transceivers with Digital Diagnostic Monitoring (DDM) functionality that provides real time information of SFP transceiver and allows you to diagnose the optical fiber signal received and launched. *The web user interface can display the vendor name, wave length and distance of all Pepperl+Fuchs Gigabit SFP transceivers. If you see Unknown information, it may mean that the vendor doesn't provide their information or that the information of their transceiver can't be read.*

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
 - Port Control
 - Port Status
 - Rate Control
 - Storm Control
 - Port Trunking
 - CFM Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
 - Device Front Panel
 - Save
 - Logout
 - Reboot

Port Status Help

Port	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	Up	Enable	100 Full	Disable	---	---	---
2	Down	Enable	---	Disable	---	---	---
3	Down	Enable	---	Disable	---	---	---
4	Down	Enable	---	Disable	---	---	---
5	Down	Enable	---	Disable	---	---	---
6	Down	Enable	---	Disable	---	---	---
7	Down	Enable	---	Disable	---	---	---
8	Down	Enable	---	Disable	---	---	---
9	Down	Enable	---	Disable	---	---	---
10	Down	Enable	---	Disable	---	---	---
11	Up	Enable	1000 Full	Disable	Optech	850 nm	550 m
12	Down	Enable	---	Disable	---	---	---

SFP DDM

Port	SFP Scan/Eject	SFP DDM	Temperature (degree)		Tx Power (dBm)		Rx Power (dBm)	
			Current	Range	Current	Range	Current	Range
9	---	Enable	---	---	---	---	---	---
10	---	Enable	---	---	---	---	---	---
11	---	Enable	45.00	-15.00 - 85.00	-6.2	-10.5 - -3.0	-8.8	-17.0 - -3.0
12	---	Enable	---	---	---	---	---	---

Reload Apply Scan All Eject All

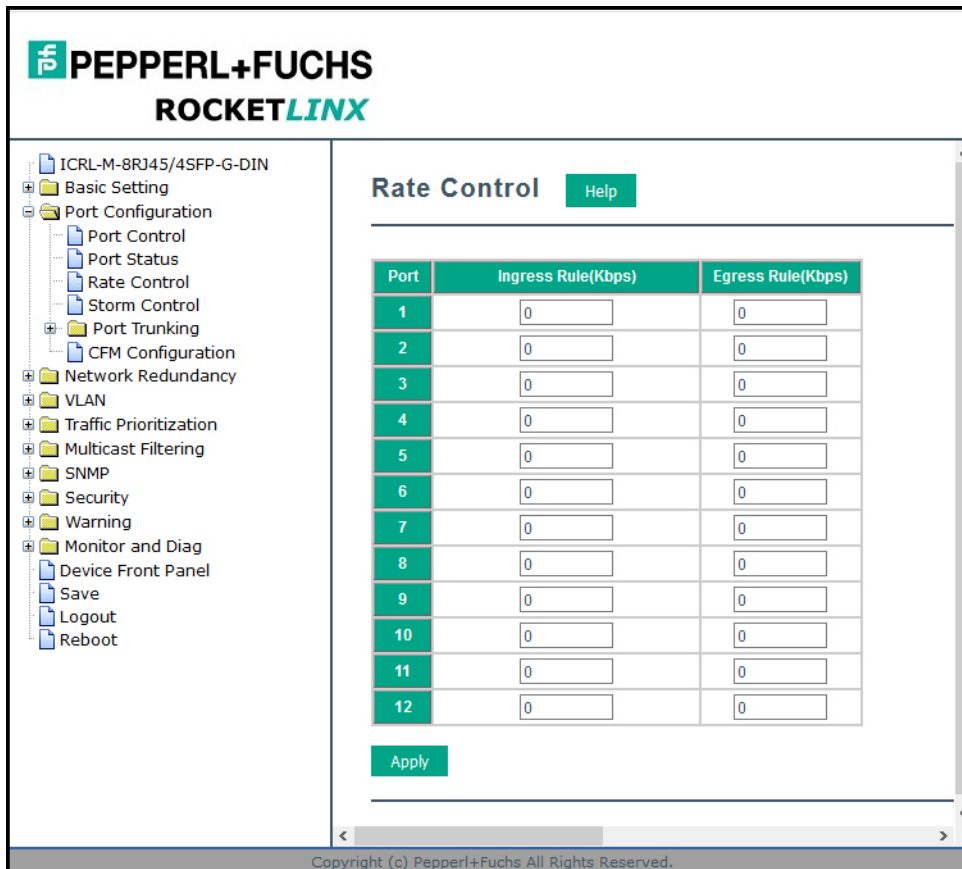
Copyright (c) Pepperl+Fuchs All Rights Reserved.

Port Status Page	
Link	Shows link status; Up means the link is up and Down means that the link is down.
State	Shows the port state. If the state is enabled it displays Enable . If the port is disabled or shutdown, it displays Disable .
Speed/Duplex	Current working status of the port.
Flow Control	The state of the flow control.
SFP Vendor	Vendor name of the SFP transceiver that is plugged into the SFP port or ports.
Wavelength	The wave length of the SFP transceiver that is plugged into the SFP port or ports.
Distance	The distance of the SFP transceiver that is plugged into the SFP port or ports.
SFP Scan/Eject	You can choose from these options: <ul style="list-style-type: none"> • Scan: Scan the SFP transceiver and display the information. • Eject: Eject the SFP transceiver that you have selected. You can eject one port or eject all by click the Eject All button.
SFP DDM	When you select, enable, this scans a SFP DDM transceiver and displays the information.
SFP Scan/Eject	Click the Scan / Eject button to scan or safely remove the SFP.
SFP DDM	Click the Enable / Disable button to enable or disable the SFP DDM function.
Temperature	Displays the current temperature detected and acceptable temperature range for the DDM SFP transceiver.
Tx Power (dBm)	Displays the current transmit power detected and acceptable Tx power range for the DDM SFP transceiver.
Rx Power (dBm)	Displays the current received power and acceptable Rx power range for the DDM SFP transceiver.
Reload	Click to reload the port status.
Scan All	Click the Scan All button to scan for all SFPs.
Eject All	You can eject one or all of the DDM SFP transceivers. To eject all of the SFPs, click Eject All .

Note: Most of the SFP transceivers provide vendor information that allows the ICRL-M to read it. The web interface can display vendor name, wave length, and distance of all Pepperl+Fuchs SFP transceiver models. If you see *Unknown info*, it may mean that the vendor does not provide their information or that the information of their transceiver cannot be read. If the plugged DDM SFP transceiver is not certified by Pepperl+Fuchs, the DDM function is not supported, but the communication is not disabled.

4.4.3. Rate Control

Rate limiting is used to control the rate of traffic that is sent or received on a network interface. For ingress rate limiting, traffic that is less than or equal to the specified rate is received, whereas traffic that exceeds the rate is dropped. For egress rate limiting, traffic that is less than or equal to the specified rate is sent, whereas traffic that exceeds the rate is dropped.



Rate Control Page	
Ingress Rule (Kbps)	Ingress rate in Kbps, the rate range is from 1 Kbps to 1000000 Kbps and zero means no limit. The default value is no-limit.
Egress Rule (Kbps)	Egress rate in Kbps, the rate range is from 1 Kbps to 1000000 Kbps and zero means no limit. The default value is no-limit. Egress rate limiting has an effect on all types of packet types, including Unknown Unicast, Multicast, and Broadcast.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.4.4. Storm Control

Storm Control is similar to Rate Control. Rate Control filters all the traffic over the threshold you input by the user interface. Storm Control allows you to define the rate for specific Packet Types.

PEPPERL+FUCHS
ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
 - Port Control
 - Port Status
 - Rate Control
 - Storm Control
 - Port Trunking
 - CFM Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

Storm Control Help

Port	Broadcast	Rate(packet/sec)	DLF	Rate(packet/sec)	Multicast	Rate(packet/sec)
1	Disable	0	Disable	0	Disable	0
2	Disable	0	Disable	0	Disable	0
3	Disable	0	Disable	0	Disable	0
4	Disable	0	Disable	0	Disable	0
5	Disable	0	Disable	0	Disable	0
6	Disable	0	Disable	0	Disable	0
7	Disable	0	Disable	0	Disable	0
8	Disable	0	Disable	0	Disable	0
9	Disable	0	Disable	0	Disable	0
10	Disable	0	Disable	0	Disable	0
11	Disable	0	Disable	0	Disable	0
12	Disable	0	Disable	0	Disable	0

Apply

Copyright (c) Pepperl+Fuchs All Rights Reserved.

Storm Control Page

Broadcast	Enable or disable broadcast storm control on the corresponding port. The Broadcast rate limit range is from 2 to 262142 packet/sec, and zero means no limit.
DLF	To enable or disable destination lookup failure storm control on the corresponding port. The Destination lookup failure rate limit range is from 2 to 262142 packet/sec, and zero means no limit.
Multicast	To enable or disable multicast storm control on this port. The Multicast rate limit range is from 2 to 262142 packet/sec, zero means no limit.
Apply	Click Apply to apply the settings. It may take some time and the web user interface may become slow, this is normal condition. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.4.5. Port Trunking

Port Trunking allows you to group multiple Ethernet ports in parallel to increase link bandwidth. The aggregated ports can be viewed as a physical port that has a bandwidth equal to the combined bandwidth of each trunked port. The member ports of the same trunk group can balance the loading and backup for each other. The Port Trunking feature is usually used when you need higher bandwidth for the network backbone. This is an inexpensive way for you to transfer more data.

The aggregated ports can interconnect to the another switch that also supports Port Trunking. Pepperl+Fuchs supports two types of port trunking:

- Static Trunk
- IEEE 802.3ad

There are some different descriptions for the port trunking. Different manufacturers may use different descriptions for their products, like Link Aggregation Group (LAG), Link Aggregation Control Protocol, Ethernet Trunk, or Ether Channel.

When the other end uses IEEE 802.3ad LACP, you should assign IEEE 802.3ad LACP to the trunk. When the other end uses non-802.3ad, you can then use Static Trunk.

There are two pages for port trunking, *Aggregation Configuration* on Page 66 and *Aggregation Information* on Page 67.

4.4.5.1. Aggregation Configuration

Use the *Port Trunk - Aggregation Configuration* page to set up port trunking.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

Basic Setting

Port Configuration

Port Control

Port Status

Rate Control

Storm Control

Port Trunking

Aggregation Configuration

Aggregation Information

CFM Configuration

Network Redundancy

VLAN

Traffic Prioritization

Multicast Filtering

SNMP

Security

Warning

Monitor and Diag

Device Front Panel

Save

Logout

Reboot

Port Trunking - Aggregation Configuration Help

Aggregation Configuration

Port	Group ID	Trunk Type
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	0	
11	0	
12	0	

Load Balance Setting

Group ID	Type
1	src-dst-mac
2	src-dst-mac
3	src-dst-mac
4	src-dst-mac
5	src-dst-mac
6	src-dst-mac
7	src-dst-mac
8	src-dst-mac

Apply Reload

Copyright (c) Pepperl+Fuchs All Rights Reserved.

Aggregation Setting Page

Group ID	Group ID is the ID for the port trunking group. Ports with same group ID are in the same group.
Trunk Type	Static or LACP . Each trunk group can only support Static or 802.3ad LACP. Non-active ports cannot be setup here.

Aggregation Setting Page (Continued)	
Load Balance Type	<p>There are several load balance types</p> <ul style="list-style-type: none"> • dst-ip (Destination IP) • dst-mac (Destination MAC) • src-dst-ip (Source and Destination IP) • src-dst-mac (Source and Destination MAC) • src-ip (Source IP) • src-mac (Source MAC)
Apply	<p>Click Apply to apply the settings.</p> <p>Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.</p>

4.4.5.2. Aggregation Information

The *Port Trunk - Aggregation Information* page shows the status of port aggregation. Once the aggregation ports are negotiated, you see the following status.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
 - Port Control
 - Port Status
 - Rate Control
 - Storm Control
 - Port Trunking
 - Aggregation Configuration
 - Aggregation Information
 - CFM Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

Port Trunking - Aggregation Information [Help](#)

Group ID	Type	Aggregated Ports	Individual Ports	Link Down Ports
1	N/A			
2	N/A			
3	N/A			
4	N/A			
5	N/A			
6	N/A			
7	N/A			
8	N/A			

[Reload](#)

Copyright (c) Pepperl+Fuchs All Rights Reserved.

Aggregation Status Page	
Group ID	Displays Trunk 1 to Trunk 8 set up.
Type	The Type is Static or LACP . Static means that LACP is disabled and configured statically by the Administrator.
Aggregated Ports	When LACP links, you can see the member ports in the Aggregated column.

4/21/20

Aggregation Status Page (Continued)	
Individual Ports	When LACP is enabled, member ports of LACP group that are not connected to the correct LACP member ports are displayed in the Individual column.
Link Down Ports	When LACP is enabled, member ports of LACP group that are not linked up are displayed in the Link Down column.
Reload	Click Reload to reload aggregation settings.

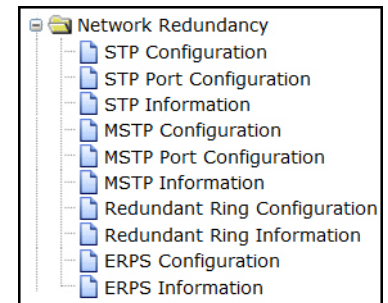
4.5. Network Redundancy

It is critical for industrial applications that the network remains running at all times. The ICRL-M supports:

- *Standard Rapid Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP)*
The ICRL-M supports RSTP versions IEEE 802.1D-2004, IEEE 802.1D-1998 STP, and IEEE 802.1w RSTP.
- *Multiple Spanning Tree Protocol (MSTP)*
MSTP implements IEEE 802.1s, which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs. MSTP was originally defined in the IEEE 802.1s and later merged into the IEEE 802.1Q-2003 specification.
- *Redundant Ring*
The Redundant Ring features 0 ms for restore and about several milliseconds for fail over for copper.
- *Rapid Dual Homing (RDH)*
Advanced RDH technology allows the ICRL-M to connect with a core managed switch easily. With RDH technology, you can also couple several Rapid Super Rings or RSTP groups together, which is also known as Auto Ring Coupling.

The following pages are included in this group:

- *STP Configuration on Page 70*
- *STP Port Configuration on Page 72*
- *STP Information on Page 73*
- *MSTP Configuration on Page 75*
- *MSTP Port Configuration on Page 78*
- *MSTP Information on Page 79*
- *Redundant Ring Configuration on Page 81*
- *Redundant Ring Information on Page 83*
- *ERPS Configuration on Page 84*
- *ERPS Information on Page 87*



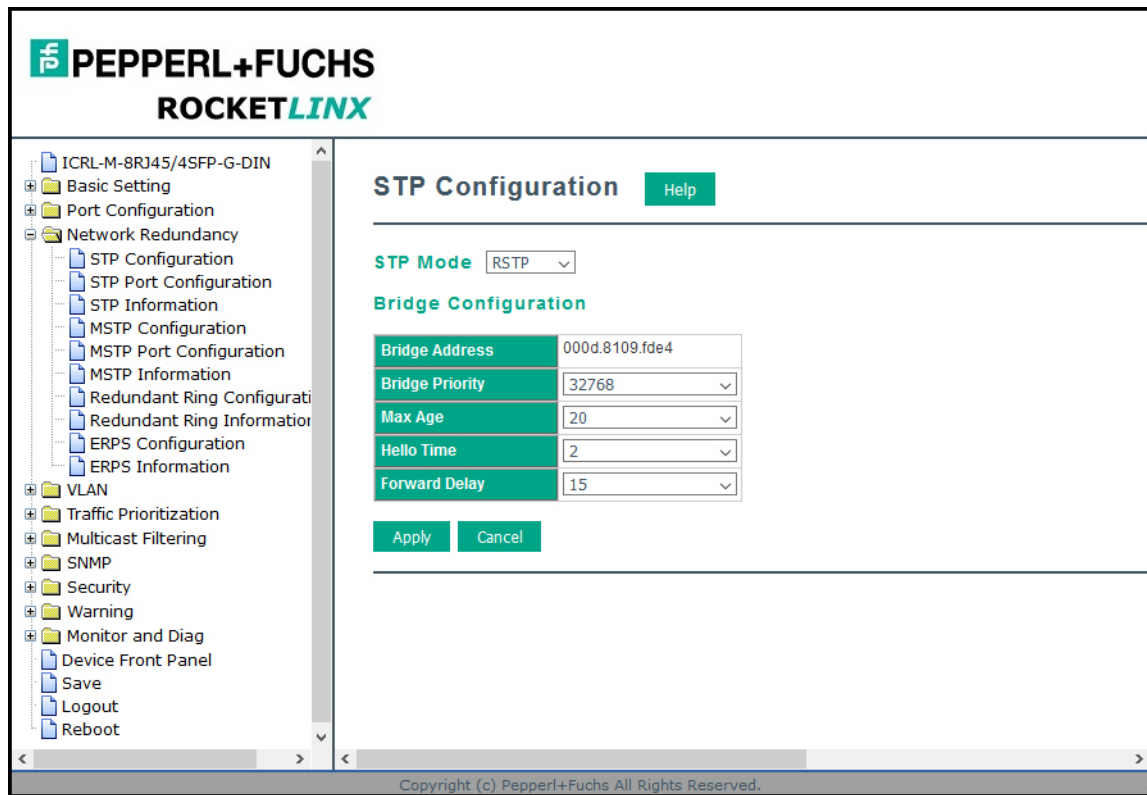
Optionally, you can use the CLI to configure these features, see *Network Redundancy (CLI)* on Page 184.

4.5.1. STP Configuration

This page allows you to select the STP mode and configure the global STP/RSTP bridge configuration. Spanning Tree Protocol (STP; IEEE 802.1D) provides a loop-free topology for any LAN or bridged network.

Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) is an evolution of the Spanning Tree Protocol (STP), and was introduced with the IEEE 802.1w standard, and provides faster spanning tree convergence after a topology change. In most cases, IEEE 802.1w can also revert back to IEEE 802.1D in order to interoperate with legacy bridges on a per-port basis. The new edition of the IEEE 802.1D standard, IEEE 802.1D-2004, incorporates the IEEE 802.1t-2001 and IEEE 802.1w standards.

Multiple Spanning Tree Protocol (MSTP; IEEE 802.1s) which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides a loop-free topology with load balancing while reducing the number of spanning-tree instances required to support a large number of VLANs. MSTP was originally defined in the IEEE 802.1s and later merged into the IEEE 802.1Q-2003 specification.

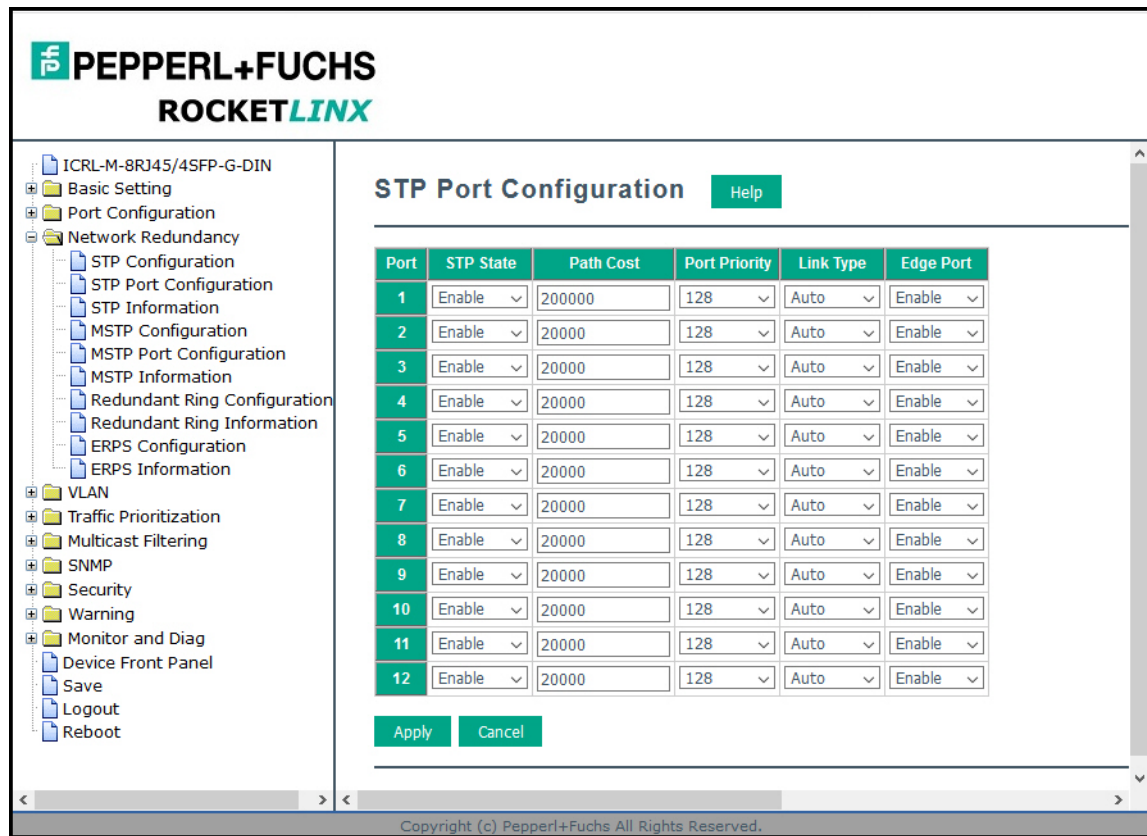


STP Configuration Page	
STP Mode	Select the spanning tree protocol: STP, RSTP or MSTP or disable STP.
Bridge Configuration	
Bridge Address	A value used to identify the bridge. This item cannot be modified.

STP Configuration Page (Continued)	
Bridge Priority	<p>RSTP uses a bridge ID to determine the root bridge. The bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. So that the bridge with the highest priority becomes the highest bridge ID. If all of the bridge IDs have the same priority, the bridge with the lowest MAC address then becomes the root bridge.</p> <p>Note: <i>The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority. For example: 4096 is higher than 32768.</i></p> <p><i>The web user interface allows you to select the priority number directly. When you configure the value through the CLI or SNMP, you may need to type the value directly. You will need to follow the $n \times 4096$ rules for the Bridge Priority.</i></p>
Max Age (See Note)	<p>This value represents the time that a bridge waits without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.</p> <p>If the ICRL-M is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then the ICRL-M reconfigures itself as a root bridge. Once two or more devices on the network are recognized as a root bridge, the devices will renegotiate to set up a new spanning tree topology.</p> <p>The MAX Age value affects the maximum volume of the RSTP loop. In the RSTP BPDU packet, there is one field, message age which starts from 0, add 1 after passed one hop in the RSTP loop. When the message age is larger than MAX Age, the BPDU is ignored and the lower switches are separated to a different RSTP domain. The switches in other RSTP domain cannot be managed through the upper switch.</p> <p>Since different RSTP-aware switches may have their own mechanism to calculate the message age an interoperate issue may occur with different vendors' RSTP-aware switches. The maximum volume of the RocketLinx RSTP domain is 23, so make sure that you configure the MAX Age lower than 23.</p>
Hello Time (See Note)	This is a periodic timer that drives the ICRL-M to send out BPDU (Bridge Protocol Data Unit) packet to check current STP status. Enter a number of 1 through 10.
Forward Delay (See Note)	The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a number 4 - 30.
Apply	<p>Click Apply to apply the settings.</p> <p>Note: <i>You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.</i></p>
<p>Note: <i>$2 \times (\text{Forward Delay Time} - 1 \text{ second})$ should be greater than or equal to the Max Age. The Max Age should be greater than or equal to $2 \times (\text{Hello Time} + 1 \text{ sec})$.</i></p>	

4.5.2. STP Port Configuration

This page allows you to configure the port parameter after you have enabled STP, RSTP, or MSTP.

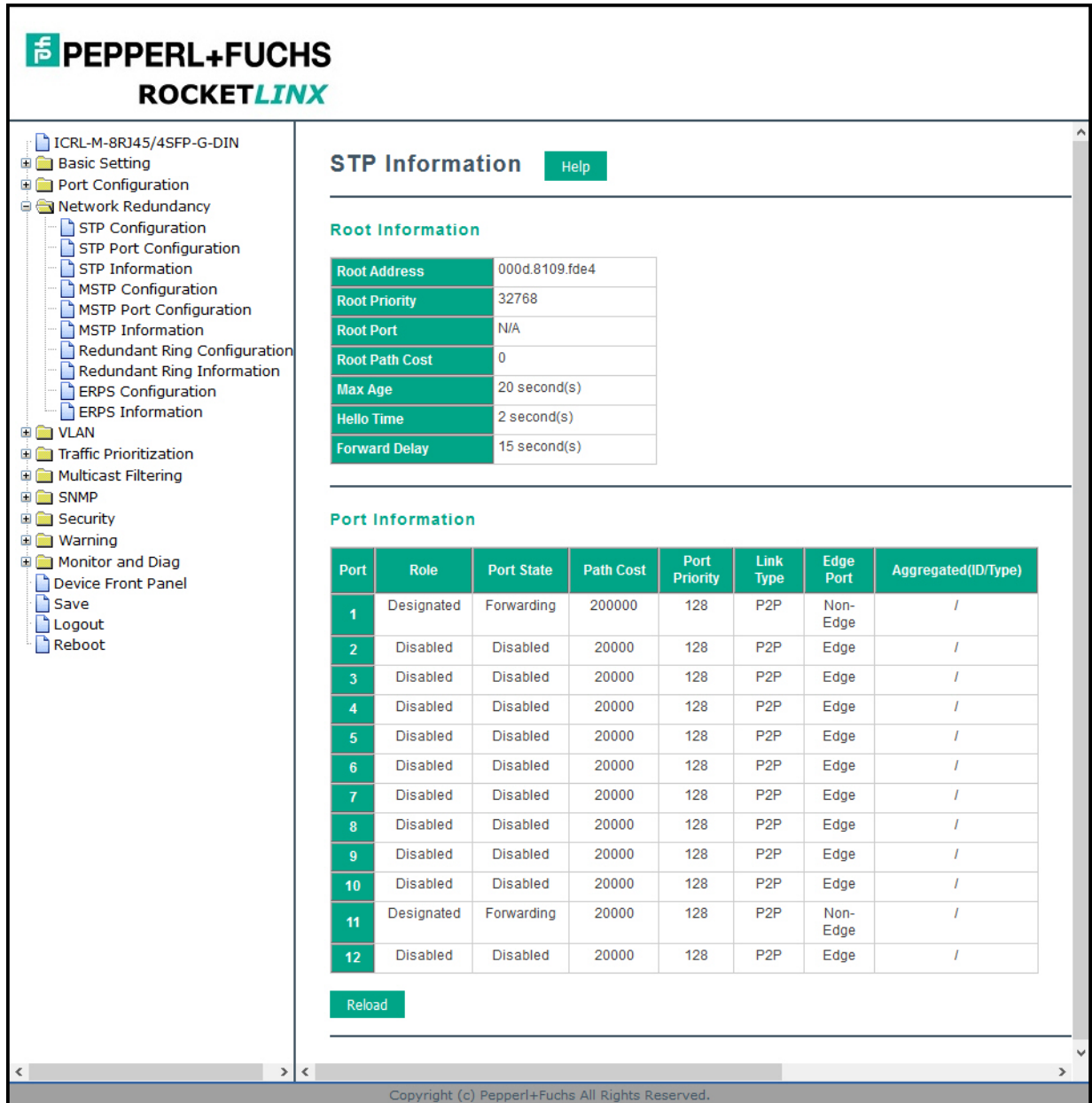


STP Port Configuration Page	
STP State	You can enable/disable STP/RSTP/MSTP on a port by port basis. You can disable the STP state when connecting a device in order to avoid STP waiting periods.
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number from 1 through 200,000,000.
Port Priority	Decide which port should be blocked by priority on your LAN. Enter a number from 0 - 240 in increments of 16.
Link Type	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port in question is connected to exactly one other bridge (that is, it is served by a point-to-point LAN segment), or if it is connected to two or more bridges (that is., it is served by a shared medium LAN segment). This configuration allows the P2P status of the link to be controlled by an administrator.
Edge Port	Present in implementations that support the identification of edge ports. All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, and skipping the listening and learning stages. When a non-bridge device connects an edge port, this port is in a blocking state and turn to forwarding state in 2 x Hello Time seconds. When the bridge device connects an edge port, this port is a non-edge port automatic.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4/21/20

4.5.3. STP Information

The *STP Information* page allows you to see the ICRL-M root information and port status.



PEPPERL+FUCHS
ROCKETLINX

STP Information [Help](#)

Root Information

Root Address	000d.8109.fde4
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age	20 second(s)
Hello Time	2 second(s)
Forward Delay	15 second(s)

Port Information

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port	Aggregated(ID/Type)
1	Designated	Forwarding	200000	128	P2P	Non-Edge	/
2	Disabled	Disabled	20000	128	P2P	Edge	/
3	Disabled	Disabled	20000	128	P2P	Edge	/
4	Disabled	Disabled	20000	128	P2P	Edge	/
5	Disabled	Disabled	20000	128	P2P	Edge	/
6	Disabled	Disabled	20000	128	P2P	Edge	/
7	Disabled	Disabled	20000	128	P2P	Edge	/
8	Disabled	Disabled	20000	128	P2P	Edge	/
9	Disabled	Disabled	20000	128	P2P	Edge	/
10	Disabled	Disabled	20000	128	P2P	Edge	/
11	Designated	Forwarding	20000	128	P2P	Non-Edge	/
12	Disabled	Disabled	20000	128	P2P	Edge	/

[Reload](#)

Copyright (c) Pepperl+Fuchs All Rights Reserved.

STP Information Page

Root Information

Root Address	Root bridge address, which is the bridge with the smallest (lowest) bridge ID.
Root Priority	Root bridge priority, the bridge with the lowest value has the highest priority and is selected as the root.
Root Port	Root port of this bridge.
Root Path Cost	Root path cost.

4/21/20

STP Information Page (Continued)	
Max Age	The number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting to reconfigure.
Hello Time	The number of seconds between the transmissions of Spanning-Tree Protocol configuration messages.
Forward Delay	The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state.
Port Information	
Role	Descriptive information about the STP/RSTP switch port role. Role: Root, Designated, Alternate, Backup, Disabled, Unknown.
Port State	Descriptive information about the STP/RSTP switch port state. State: Blocking, Listening, Learning, Forwarding, Disabled, Unknown.
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Path cost range is 1 through 200,000,000.
Port Priority	Decide which port should be blocked by priority in your LAN. Range is 0 through 240 in increments of 16.
Link Type	Operational link type. Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port in question can be concerned to exactly one other bridge (that is, it is served by a point-to-point LAN segment), or can be connected to two or more bridges (that is, it is served by a shared medium LAN segment).
Edge Port	Operational edge port state. Present in implementations that support the identification of edge ports. All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages. When the non-bridge device connects an edge port, this port is in blocking state and turn to forwarding state in 2*Hello Time seconds. When the bridge device connects an edge port, this port is a non-edge port automatic.
Aggregated (ID/Type)	This is the aggregated port information. The ID is the aggregation ID (Trunk ID) and the Type is either Static or LACP.
Reload	Click the Reload button to reload STP information.

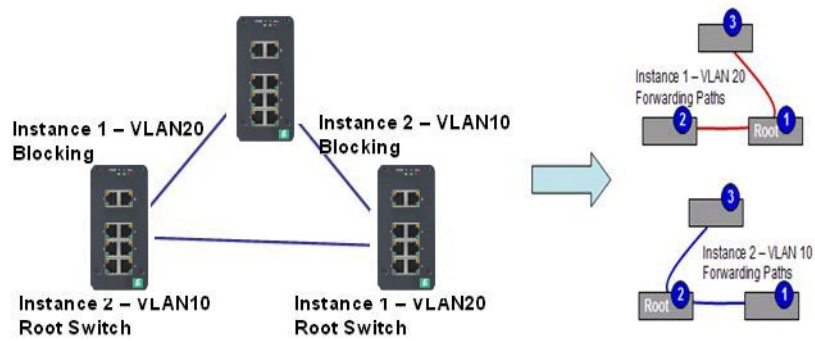
4.5.4. MSTP Configuration

Multiple Spanning Tree Protocol (MSTP) is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, creates a faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

While using MSTP, there are some new concepts of network architecture. A switch may belong to different groups, act as root or designate switch, or generate BPDU packets for the network to maintain the forwarding table of the spanning tree. MSTP can also provide load balancing between switches.

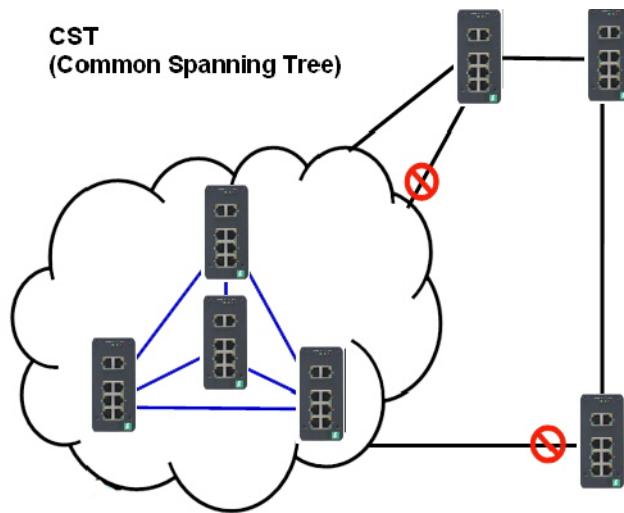
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). The maximum number of instances that the ICRL-M supports is 16, with a range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. An MST Region may contain multiple MSTP instances.

The following figure shows a MSTP instance with two VLANs. Each instance has a root node and forwarding paths.

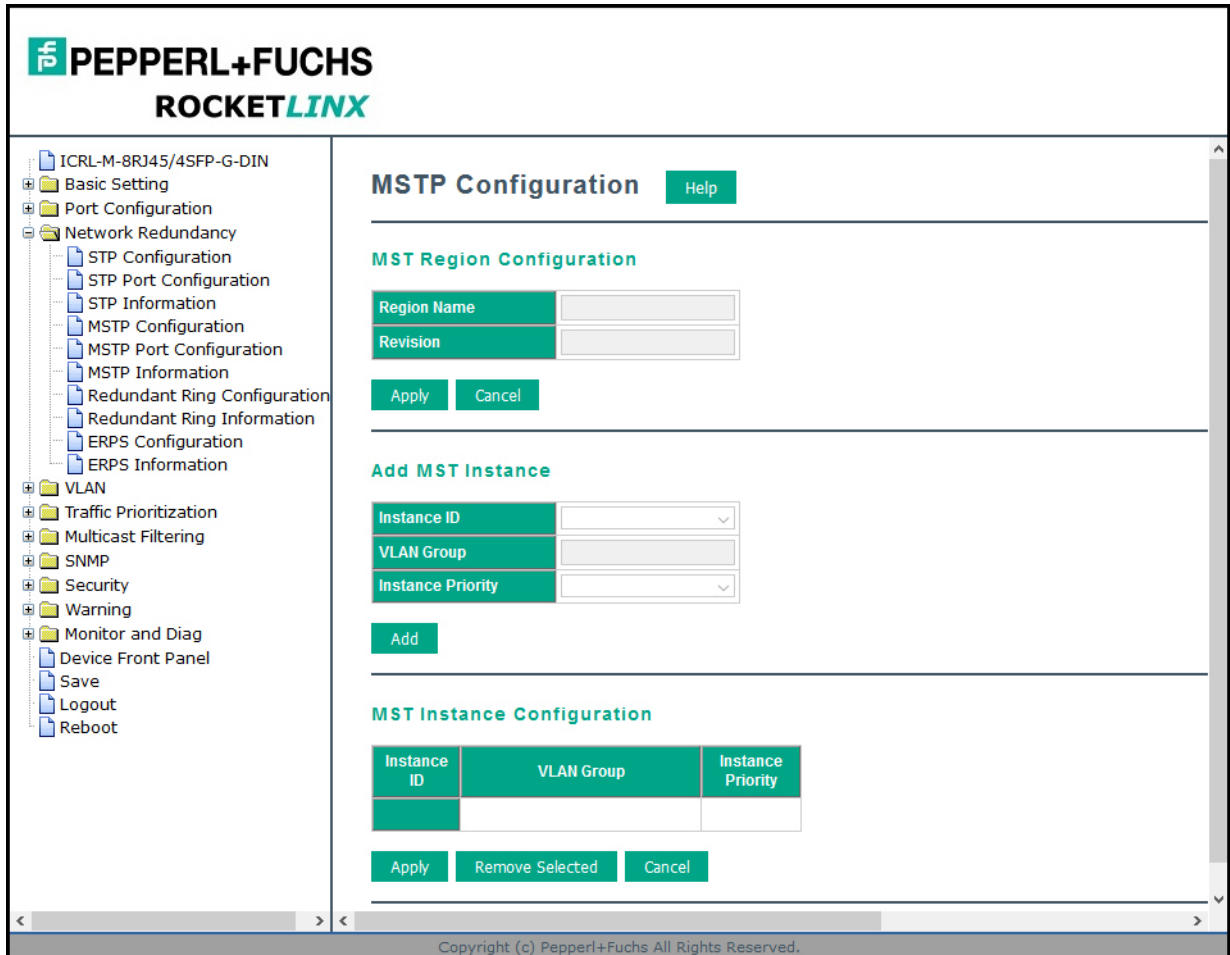


A Common Spanning Tree (CST) interconnects all adjacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, or MSTP protocols.

The following diagram shows a CST attached to a larger network. In this network, a Region may have different instances and its own forwarding path and table, however, the CST acts as a single bridge.



This is the *MSTP Configuration* page.



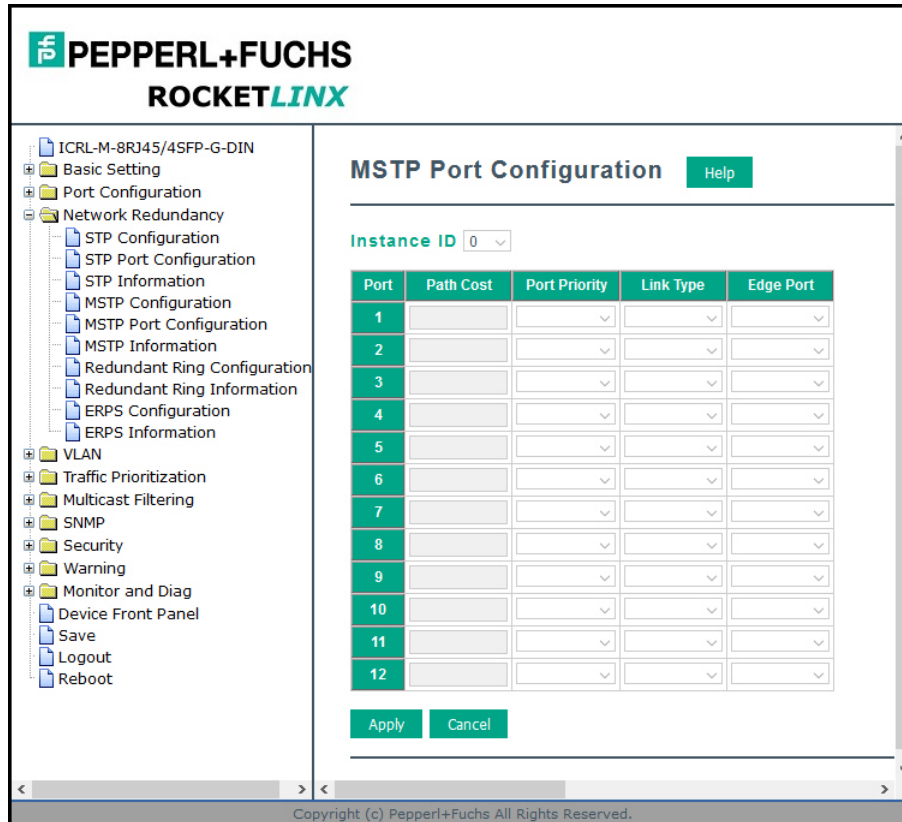
MSTP Configuration Page	
MST Region Configuration	
Region Name	A name used to identify the MST Region. Maximum length: 32 characters.
Revision	A value used to identify the MST Region. Range: 0-65535; Default: 0).
Apply	Click the Apply button to apply the MST Region Configuration .
New MST Instance	
Instance ID	A value used to identify the MST instance, valid value are 1 through 15. Instance 0 (CIST, Common Internal Spanning Tree) is a special instance of spanning-tree known as IST or Internal Spanning Tree (=MSTI00).
VLAN Group	Give a VLAN group to map this MST instance. Use a VLAN number (for example, 10), range (for example:1-10) or mixing format (for example: 2,4,6,4-7,10).
Instance Priority	A value used to identify the MST instance. The MST instance with the lowest value has the highest priority and is selected as the root. Enter a number 0 through 61440 in increments of 4096.
Add	Click the Add button to add the New MST Instance .

4/21/20

MSTP Configuration Page (Continued)	
Current MST Instance Configuration	
Instance ID	A value used to identify the MST instance. Instance 0 (CIST, Common Internal Spanning Tree) is a special instance of spanning-tree known as IST or Internal Spanning Tree (=MSTI00).
VLAN Group	Provide a VLAN group to map this MST instance. Use the VLAN number, for example: 10. You can set a range, for example: 1-10) or set specific VLANs, for example: 2,4,6,4-7.
Instance Priority	A value used to identify the MST instance. The MST instance with the lowest value has the highest priority and is selected as the root. Enter a number 0 through 61440 in increments of 4096.
Apply	Click the Apply button to apply the current MST instance configuration . Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.5.5. MSTP Port Configuration

This page allows you to configure the port settings. Choose the Instance ID that you want to configure.




MSTP Port Configuration Page	
Instance ID	Select an Instance ID to display and modify MSTP instance setting.
Port Configuration	
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number from 1 through 200,000,000.
Port Priority	Decide which port should be blocked by priority on your LAN. Enter a number from 0 through 240 in increments of 16.
Link Type	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port in question is connected to exactly one other bridge (that is, it is served by a point-to-point LAN segment), or if it's connected to two or more bridges (that is, it is served by a shared medium LAN segment). This configuration allows the P2P status of the link to be controlled by an administrator.
Edge Port	Present in implementations that support the identification of edge ports. All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, and skipping the listening and learning stages. When the non-bridge device connects an edge port, this port is in a blocking state and turn to forwarding state in 2 x Hello Time seconds. When the bridge device connects an edge port, this port is a non-edge port automatic.
Apply	Click the Apply button to apply the configuration. Note: You must Save the settings (Page 156) to maintain these settings if the ICRL-M is powered off.

4/21/20

4.5.6. MSTP Information

This page allows you to see the current MSTP information. Choose the Instance ID first. If the instance is not added, the information remains blank.



- ICRL-M-8RJ45/4SFP-G-DIN
 - Basic Setting
 - Port Configuration
 - Network Redundancy
 - STP Configuration
 - STP Port Configuration
 - STP Information
 - MSTP Configuration
 - MSTP Port Configuration
 - MSTP Information
 - Redundant Ring Configuration
 - Redundant Ring Information
 - ERPS Configuration
 - ERPS Information
 - VLAN
 - Traffic Prioritization
 - Multicast Filtering
 - SNMP
 - Security
 - Warning
 - Monitor and Diag
 - Device Front Panel
 - Save
 - Logout
 - Reboot

MSTP Information Help

Instance ID

Root Information

Root Address	--
Root Priority	--
Root Port	--
Root Path Cost	--
Max Age	--
Hello Time	--
Forward Delay	--

Port Information

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

Reload

MSTP Information Page	
Instance ID	Select an instance ID to display MSTP instance information. Instance 0 (CIST, Common Internal Spanning Tree) is a special instance of spanning-tree known as IST or Internal Spanning Tree (=MSTI00).
Root Information	
Root Address	Root bridge address, which is the bridge with the smallest (lowest) bridge ID.
Root Priority	Root bridge priority, the bridge with the lowest value has the highest priority and is selected as the root.
Root Port	Root port of this bridge.
Root Path Cost	Root path cost.
Max Age	The number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting to reconfigure.
Hello Time	The number of seconds between the transmissions of Spanning-Tree Protocol configuration messages.
Forward Delay	The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state.
Port Information	
Port Role	Descriptive information about the MSTP switch port role. Role: Master, Root, Designated, Alternate, Backup, Boundary, Disabled, Unknown.
Port State	Descriptive information about the MSTP switch port state. State: Blocking, Listening, Learning, Forwarding, Disabled, Unknown.
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Path cost range is 1 through 200,000,000.
Port Priority	Decide which port should be blocked by priority in your LAN. The range is 0 through 240 in increments of 16.
Link Type	Operational link type. Some of the rapid state transactions that are possible within MSTP are dependent upon whether the port in question can be concerned to exactly one other bridge (that is, it is served by a point-to-point LAN segment), or can be connected to two or more bridges (that is, it is served by a shared medium LAN segment).
Edge Port	Operational edge port state. Present in implementations that support the identification of edge ports. All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages. When the non-bridge device connects an edge port, this port is in blocking state and turn to forwarding state in 2*Hello Time seconds. When the bridge device connects an edge port, this port is a non-edge port automatic.
Reload	Click the Reload button to reload MSTP instance information.

4.5.7. Redundant Ring Configuration

The most common industrial network redundancy is to form a ring or loop. Typically, managed switches are connected in series and the last switch is connected back to the first one. In such connection, you can implement Redundant Ring technology.

The screenshot shows the 'Redundant Ring Configuration' page in the ROCKETLINX interface. On the left is a navigation tree with categories like Basic Setting, Port Configuration, Network Redundancy, VLAN, Traffic Prioritization, Multicast Filtering, SNMP, Security, Warning, Monitor and Diag, Device Front Panel, Save, Logout, and Reboot. The main content area is titled 'Redundant Ring Configuration' and includes a 'Help' button. Below the title is an 'Add Ring' section with a 'Ring ID' dropdown menu set to '0' and a 'Name' text input field, followed by an 'Add' button. The 'Ring Configuration' section contains a table with columns: Ring ID, Name, Version, Device Priority, Ring Port1, Path Cost, Ring Port2, Path Cost, Rapid Dual Homing, RDH Ext. ID, and Ring Status. Below this table are 'Apply', 'Remove Selected', and 'Cancel' buttons. The 'Super Chain Configuration' section has a table with columns: Ring ID, Role, and Edge Port, with 'Apply' and 'Cancel' buttons below. The 'Rapid Dual Homing Port Configuration' section has a table with columns: Ring ID, Auto Detect, and 12 numbered ports (1-12), with 'Apply' and 'Cancel' buttons below.

Redundant Ring Page	
Ring ID/Name	To create a Redundant Ring select the Ring ID, which has range from 0 to 31. If the name field is left blank, the name of this ring is automatically named with the Ring ID. The maximum number of rings is 32. Note: Once a ring is created, you cannot change it.
Ring Configuration	
Ring ID	Once a Ring is created, the Ring ID appears, and cannot be changed. In multiple ring environments, the traffic can only be forwarded under the same Ring ID. Remember to check the Ring ID when there are more than one ring in existence.
Name	This field shows the name of the Ring. If it is not entered when creating, it is automatically named by the rule <i>RingID</i> .
Version	The version of Ring can be changed here, the choices are Rapid Super Ring or Super Chain .
Device Priority	The switch with highest priority (highest value) is automatically selected as the Ring Master (RM) . When one of the ring ports on this switch becomes a forwarding port and the other one becomes a blocking port. If all of the switches have the same priority, the switch with the highest MAC address is selected as the Ring Master.

4/21/20

Redundant Ring Page (Continued)	
Ring Port1	In a Rapid Super Ring environment, you should have two Ring ports. Whether this switch is a Ring Master or not. When configuring Rapid Super Rings , two ports should be selected to be Ring ports. For a Ring Master, one of the Ring Ports becomes the forwarding port and the other one becomes the blocking port.
Path Cost	Change the Path Cost of Ring Port1, if this switch is the Ring Master of a Ring, then it determines the blocking port. The port with higher Path Cost in the two Ring Ports becomes the blocking port, If the Path Cost is the same, the port with larger port number becomes the blocking port.
Ring Port2	Assign another port for ring connection.
Path Cost	Change the Path Cost of Ring Port2.
Rapid Dual Homing	Rapid Dual Homing is an important feature of Rapid Super Ring redundancy technology. When you want to connect multiple RSR or form redundant topology with other vendors, RDH allows you to have a maximum of seven multiple links for redundancy without any problem. In RDH, you do not need to configure a specific port to connect to other protocol. The RDH selects the fastest link for the primary link and blocks all the other links to avoid a loop. If the primary link failed, RDH automatically forwards the secondary link for a network redundant. If there are more connections, they are standby links and are recovered if both primary and secondary links are broken.
RDH Ext ID	This is the Rapid Dual Homing Extension ID. The Extension ID and Ring ID cannot be the same, when dual home to the same external network. The Extension ID range is from 0 to 7. With the combination of Extension ID (0 to 7) and Ring ID (0 to 31), the ICRL-M supports up to 256 (8 x 32) different dual homing rings.
Ring status	To Enable/Disable the Ring, remember to enable the Ring after you add it.
Super Chain Configuration	
ID	The Ring Identifier referring to this Ring (Chain).
Role	Super Chain has two node roles, Border and Member . Border is the node, which connects to an external network. Member is the node except the Border node in the Super Chain.
Edge Port	Edge Port is one of ring ports of Border node. It is used to connect to an external network.
Rapid Dual Homing Port Configuration	
Ring ID	The Ring Identifier referring to this Ring.
Auto Detect	Enable Rapid Dual Homing (RDH) auto detect RDH port mode.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.5.8. Redundant Ring Information

This page shows Redundant Ring information.

Redundant Ring Information Page	
Ring ID	The Ring ID.
Version	Displays the ring version, this field could be Rapid Super Ring or Super Chain.
Role	This ICRL-M is the RM (Ring Master) or nonRM (non-ring master).
Status	If this field is Normal it means the redundancy is approved. If any one of the link in this Ring is broken, then the status is Abnormal .
RM MAC	The MAC address of Ring Master of this Ring, which helps to find the redundant path.
Blocking Port	Shows which is blocked port of RM.
Role Transition Count	Shows how many times this ICRL-M has changed its Role from nonRM to RM or from RM to nonRM.
Ring State Transition Count	Shows how many times the Ring status has been transformed between Normal and Abnormal state.
Reload	Click to reload redundant ring information.

4.5.9. ERPS Configuration

Ethernet Ring Protection Switching (ERPS) implements the ITU-T (G.8032) recommendation to provide sub-50ms recovery for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.

The primary advantage of this feature is that it is an industry standard ring technology so that you can drop the ICRL-M into a G.8032 ring with other manufacturers' switches.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
 - STP Configuration
 - STP Port Configuration
 - STP Information
 - MSTP Configuration
 - MSTP Port Configuration
 - MSTP Information
 - Redundant Ring Configuration
 - Redundant Ring Information
 - ERPS Configuration
 - ERPS Information
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

ERPS Configuration [Help](#)

Add ERPS Instance

Instance ID	VLAN Group
0	

[Add](#)

ERPS Instance Configuration

Instance ID	VLAN group

[Apply](#) [Remove Selected](#) [Cancel](#)

Add ERPS Ring

Ring ID
0

[Add](#)

ERPS Ring Configuration

Ring ID	Version	Ring State	Node Role	Control Channel	Sub Ring Without Virtual Channel	Virtual Channel of Sub Ring	Ring Port 1	Ring Port 2	Ring Port 1 RMEP ID	Ring Port 2 RMEP ID	RPL port	Revertive Mode	Instance	Manual Switch	Force Switch

[Apply](#) [Remove Selected](#) [Clear Selected](#) [Cancel](#)

ERPS Timer Configuration

Ring ID	Guard Timer	WTR Timer

[Apply](#) [Cancel](#)

Copyright (c) Pepperl+Fuchs All Rights Reserved.


ERPS Configuration Page	
Add ERPS Instance	
Instance ID	The ERPS instance identity. Valid values range from 0 to 15.
VLAN Group	The VLAN ID members of the Instance ID. Click the Add button to add this ERPS Instance.
ERPS Instance Configuration	
Instance ID	The ERPS instance identity. Valid values range from 0 to 15.
VLAN Group	The VLAN ID members of the Instance ID. <ul style="list-style-type: none"> Click the Add button to add the ERPS Instance. To remove an MST instance check the checkbox of the Instance ID you want to remove and click the Remove Selected button. Click the Cancel button to reload the current settings.
Add ERPS Ring	
Ring ID	The ERPS Ring identity. Valid values are 0 to 31. Click the Add to add the ERPS Ring.
ERPS Ring Configuration	
Ring ID	The ERPS Ring identity.
Version	ERPS has version 1 and 2.
Ring State	The current state of ring, Disable, Major or Sub.
Node Role	The role of the node, RPL Owner and Ring Node . The RPL owner is an Ethernet ring node adjacent to the RPL.
Control Channel	Control Channel to provide a communication channel for ring automatic protection switching (R-APS) transmission.
Sub Ring Without Virtual Channel	Select to use virtual channel to transmit sub-ring ring automatic protection switching (R-APS) or not.
Virtual Channel of Sub Ring	Control Channel to provide a communication channel for sub-ring ring automatic protection switching (R-APS) transmission.
Ring Port	A ring link is bounded by two adjacent nodes and a port for a ring link is called a ring port.
RMEP ID	The remote Maintenance association End Point (MEP) ID of ring port.
RPL Port	The ring protection link (RPL) is the ring link which under normal conditions, that is, without any failure or request, is blocked for traffic channel, to prevent the formation of loops.
Revertive Mode	In revertive mode, all ring links and nodes have recovered, the block link will revert to RPL link. In non-revertive mode, the ring does not automatically revert.
Instance	Select one ERPS instance to control it.
Manual Switch	Allows the operator to manually block a particular ring port.
Force Switch	Allows the operator to forcefully block a particular ring port.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4/21/20

ERPS Configuration Page	
Remove Selected	Select the ring and then click this button to remove a ring.
Clear Selected	Select the ring and click this button to cancel an existing FS or MS command on the ring port.
Cancel	Click this button to cancel this modification.
ERPS Ring Configuration	
Ring ID	The ERPS Ring identity.
Guard Timer	The Guard Timer. Valid values are 10 to 2000 ms, default is 100 ms.
WTR Timer	The WTR (Wait-to-restore) Timer. Valid values are 1 to 12 minutes, default is 5 minutes.
Cancel	Click this button to cancel this modification.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.5.10. ERPS Information

This page provides information about ERPS.



- ICRL-M-8RJ45/4SFP-G-DIN
- Basic Setting
- Port Configuration
- Network Redundancy
 - STP Configuration
 - STP Port Configuration
 - STP Information
 - MSTP Configuration
 - MSTP Port Configuration
 - MSTP Information
 - Redundant Ring Configuration
 - Redundant Ring Information
 - ERPS Configuration
 - ERPS Information
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

ERPS Configuration Help

Add ERPS Instance

Instance ID	VLAN Group
0	

Add

ERPS Instance Configuration

Instance ID	VLAN group

Apply
Remove Selected
Cancel

Add ERPS Ring

Ring ID
0

Add

ERPS Ring Configuration

Ring ID	Version	Ring State	Node Role	Control Channel	Sub Ring Without Virtual Channel	Virtual Channel of Sub Ring	Ring Port 1	Ring Port 2	Ring Port 1 RMEP ID	Ring Port 2 RMEP ID	RPL port	Revertive Mode	Instance	Manual Switch	Force Switch

Apply
Remove Selected
Clear Selected
Cancel

ERPS Timer Configuration

Ring ID	Guard Timer	WTR Timer

Apply
Cancel

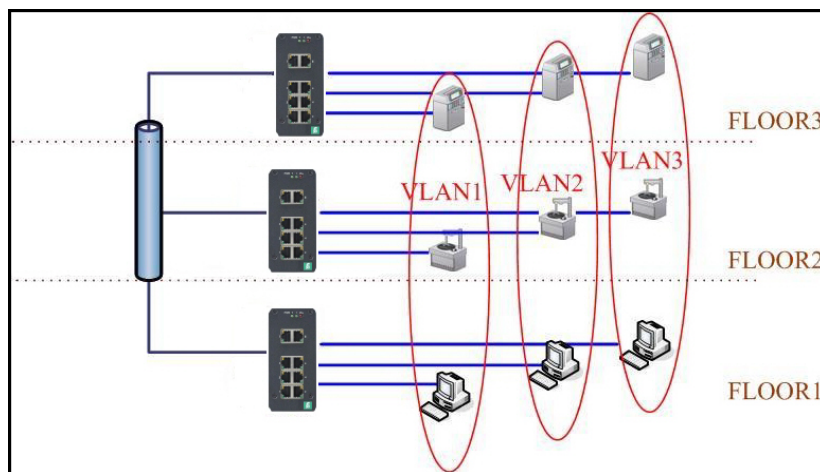
Copyright (c) Pepperl+Fuchs All Rights Reserved.

4.6. VLAN

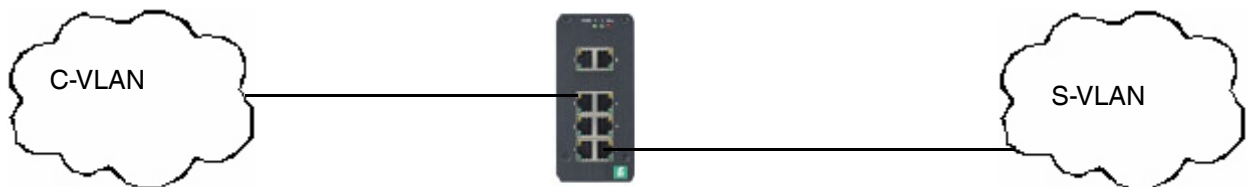
A Virtual LAN (VLAN) is a logical grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members. The VLAN allows you to isolate network traffic so that only members of the VLAN could receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is the logical equivalent of physically reconnecting a group of network devices to another Layer 2 switch, without actually disconnecting these devices from their original switches.

The ICRL-M supports IEEE 802.1Q VLAN, which is also known as Tag-Based VLAN. This Tag-Based VLAN allows a VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame's tag, without the need to dissect the contents of the frame, this saves a lot of computing resources within the ICRL-M.

The following figure displays an IEEE 802.1Q VLAN.



The ICRL-M supports VLAN tunneling (QinQ), which expands the number of VLANs by adding a tag to the 802.1Q packets. The original VLAN is usually identified as Customer VLAN (C-VLAN) and the new VLAN is Service VLAN (S-VLAN). By adding the additional tag, QinQ increases the possible number of VLANs. After QinQ is enabled, the ICRL-M can reach up to 256 x 256 VLANs. With different standard tags, it also improves network security.

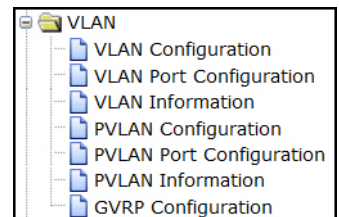


802.1Q Tunnel

802.1Q Tunnel Uplink

VLAN Configuration pages allow you to add and remove a VLAN, configure port Ingress/Egress parameters, and view the VLAN table. The following pages are included in this group:

- *VLAN Configuration* on Page 89
- *VLAN Configuration* on Page 89
- *VLAN Information* on Page 94
- *Private VLAN* on Page 95
- *PVLAN Configuration* on Page 96



- *PVLAN Port Configuration* on Page 97
- *PVLAN Information* on Page 98
- *GVRP Configuration* on Page 99

Optionally, you can use the CLI for configuration, see *VLAN (CLI)* on Page 191.

4.6.1. VLAN Configuration

Use this page to assign the Management VLAN, create the static VLAN, and assign the Egress rule for the member ports of the VLAN.

PEPPERL+FUCHS ROCKETLINX

VLAN Configuration Help

Management VLAN ID

Apply

Static VLAN

VLAN ID	Name
<input type="text"/>	<input type="text"/>

Add

Static VLAN Configuration

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/> 1	<input type="text" value="VLAN1"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>	<input type="text" value="U"/>

Apply Remove Selected Reload

Copyright (c) Pepperl+Fuchs All Rights Reserved.

VLAN Configuration Page	
Management VLAN ID	<p>The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch. The default management VLAN ID is 1.</p> <p>Click Apply after you enter the VLAN ID.</p>
Static VLAN	<p>You can assign a VLAN ID and VLAN Name for the new static VLAN.</p> <ul style="list-style-type: none"> VLAN ID: This is used by the switch to identify different VLANs. A valid VLAN ID is between 1 and 4,094, 1 is the default VLAN. VLAN Name: This is a reference for the network administrator to identify different VLANs. The VLAN name may up to 12 characters in length. If you do not provide a VLAN name, the system automatically assigns a VLAN name. The rule is VLAN (VLAN ID). <p>Click Add to create a new VLAN. The new VLAN displays in the <i>Static VLAN Configuration</i> table. After creating the VLAN, the status of the VLAN remains Unused, until you add ports to the VLAN.</p> <p>Note: Before changing the management VLAN ID by web or Telnet, remember that the port attached by the administrator should be the member port of the management VLAN; otherwise the administrator cannot access the switch through the network. The ICRL-M supports a maximum of 256 VLANs.</p>
Static VLAN Configuration	<ul style="list-style-type: none"> VLAN ID: The VLAN identifier for this VLAN. Name: The name of the VLAN. 1 - 20: The corresponding port number on the VLAN. <ul style="list-style-type: none"> -- Not available U Untag, indicates that egress/outgoing frames are not VLAN tagged. T Tag, indicates that egress/outgoing frames are LAN tagged. Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off. Click Remove Selected to remove the selected static VLAN. Click Reload to reload static VLAN configuration.

The following figure shows a static VLAN configuration table. Two new VLANs were created (VLAN2 and Test). Egress rules of the ports are not configured.

Static VLAN Configuration													
VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/> 1	VLAN1	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾
<input type="checkbox"/> 2	VLAN2	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾
<input type="checkbox"/> 3	Test	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾

Apply Remove Selected Reload

The following figure displays how to configure the Egress rule of the ports.

Use the following steps to configure Egress rules:

1. Assign Egress rule of the ports to **U** or **T**.
2. Press **Apply** to apply the setting.

Static VLAN Configuration

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/> 1	VLAN1	U	U	U	U	U	U	U	U	U	U	U	U
<input type="checkbox"/> 2	VLAN2	--	--	--	--	--	--	--	--	--	--	--	--
<input checked="" type="checkbox"/> 3	Test	--	--	--	U	--	--	--	--	--	--	--	--

--
U
 T

If you want to remove one VLAN, select the VLAN entry and then click the **Remove** button.

4.6.2. VLAN Port Configuration

The *VLAN Port Configuration* page allows you to configure VLAN port parameters on a specific port. Tag-based VLANs are based on the IEEE 802.1Q specification. Traffic is forwarded to VLAN member ports based on identifying VLAN tags in data packets. You can also configure the switch to inter-operate with existing tag-based VLAN networks and legacy non-tag networks.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
 - VLAN Configuration
 - VLAN Port Configuration
 - VLAN Information
 - PVLAN Configuration
 - PVLAN Port Configuration
 - PVLAN Information
 - GVRP Configuration
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
 - Device Front Panel
 - Save
 - Logout
 - Reboot

VLAN Port Configuration Help

Port	PVID	Tunnel Mode	EtherType	Accept Frame Type	Ingress Filtering
1	1	None	0x8100	Admit All	Disable
2	1	None	0x8100	Admit All	Disable
3	1	None	0x8100	Admit All	Disable
4	1	None	0x8100	Admit All	Disable
5	1	None	0x8100	Admit All	Disable
6	1	None	0x8100	Admit All	Disable
7	1	None	0x8100	Admit All	Disable
8	1	None	0x8100	Admit All	Disable
9	1	None	0x8100	Admit All	Disable
10	1	None	0x8100	Admit All	Disable
11	1	None	0x8100	Admit All	Disable
12	1	None	0x8100	Admit All	Disable

Apply

Copyright (c) Pepperl+Fuchs All Rights Reserved.

VLAN Port Configuration Page	
PVID	Enter the port VLAN ID (PVID). The PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs. The default Port VID, the VLAN ID assigned to an untagged frame or a Priority-Tagged frame received on the port. The valid range is from 1 to 4094. Enter the PVID you want to configure.
Tunnel Mode	<p>None - IEEE 802.1Q tunnel mode is disabled.</p> <p>802.1Q Tunnel: QinQ is applied to the ports which connect to the C-VLAN. The port receives a tagged frame from the C-VLAN. You need to add a new tag (Port VID) as an S-VLAN VID. When the packets are forwarded to the C-VLAN, the S-VLAN tag is removed. After 802.1Q Tunnel mode is assigned to a port, the egress setting of the port should be <i>Untag</i>, it indicates that the egress packet is always untagged. This is configured in the Static VLAN Configuration table (Page 89).</p> <p>802.1Q Tunnel Uplink: QinQ is applied to the ports which connect to the S-VLAN. The port receives a tagged frame from the S-VLAN. When the packets are forwarded to the S-VLAN, the S-VLAN tag is kept. After 802.1Q Tunnel Uplink mode is assigned to a port, the egress setting of the port should be <i>Tag</i>, it indicates that the egress packet is always tagged. This is configured in the Static VLAN Configuration table (Page 89). For example, if the VID of S-VLAN/Tunnel Uplink is 10, the VID of C-VLAN/Tunnel is 5. The 802.1Q Tunnel port receives Tag 5 from C-VLAN and adds Tag 10 to the packet. When the packets are forwarded to S-VLAN, Tag 10 is kept.</p>
EtherType	This allows you to define the EtherType manually. This is an advanced QinQ parameter that allows you to define the transmission packet type.
Accept Frame Type	When you select Tag Only the device discards untagged frames or Priority-Tagged only frames received on this port. When you select Admit All , untagged frames or Priority-Tagged only frames received on this port are accepted and assigned to the PVID for this frame. This control does not affect VLAN independent BPDU frames, such as STP, GVRP and LACP. It does affect VLAN dependent BPDU frames, such as GMRP.
Ingress Filtering	<p>Ingress filtering instructs the VLAN engine to filter out undesired traffic on a port.</p> <ul style="list-style-type: none"> When you Enable Ingress Filtering, the port checks whether the incoming frames belong to the VLAN they claimed or not. The port then determines if the frames can be processed or not. For example, if a tagged frame from <i>TEST VLAN</i> is received, and Ingress Filtering is enabled, the ICRL-M determines if the port is on the <i>TEST VLAN</i>'s Egress list. If it is, the frame can be processed. If it is not, the frame is dropped. When you select Disable, the port accepts all incoming frames regardless of its VLAN classification. This control does not affect VLAN independent BPDU frames, such as Super Ring, STP, GVRP and LACP. It does affect VLAN dependent BPDU frames, such as GMRP.
Apply	<p>Click Apply to apply the settings.</p> <p>Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.</p>

4.6.3. VLAN Information

The *VLAN Information* page displays the current settings of your VLAN table, including VLAN ID, Name, Status, and Egress rule of the ports.

PEPPERL+FUCHS
ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
 - VLAN Configuration
 - VLAN Port Configuration
 - VLAN Information
 - PVLAN Configuration
 - PVLAN Port Configuration
 - PVLAN Information
 - GVRP Configuration
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

VLAN Information [Help](#)

VLAN ID	Name	Status	1	2	3	4	5	6	7	8	9	10	11	12
1	VLAN1	Static	U	U	U	U	U	U	U	U	U	U	U	U
2	VLAN2	Unused	-	-	-	-	-	-	-	-	-	-	-	-
3	Test	Static	-	-	-	U	-	-	-	-	-	-	-	-

[Reload](#)

Copyright (c) Pepperl+Fuchs All Rights Reserved.

VLAN Information Page	
VLAN ID	The ID of the VLAN.
Name	The name of the VLAN.
Status	<p>Static means that this is a manually configured static VLAN.</p> <p>Unused means this VLAN is created by web user interface/CLI and has no member ports and the VLAN is not workable yet.</p> <p>Dynamic means this VLAN was learned by GVRP.</p> <ul style="list-style-type: none"> -- No VLAN setting. T A Trunk Link is a LAN segment used for multiplexing VLANs between VLAN bridges. All the devices that connect to a Trunk Link must be IEEE 802.1Q VLAN-aware, which sends and receives frames with IEEE 802.1Q tags. U An Access Link is a LAN segment for IEEE 802.1Q VLAN-unaware devices into a Port of a VLAN Bridge. Devices that are connected to an Access Link sends and receives frames without IEEE 802.1Q tagging, which is the identification of the VLAN it belongs to.

4.7. Private VLAN

A private VLAN helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. The private VLAN features provides primary and secondary VLANs within a single switch.

Primary VLAN: The uplink port is usually a member of the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with Secondary VLANs.

The screenshot shows the PEPPERL+FUCHS ROCKETLINX web interface. The left sidebar contains a navigation tree with the following items: ICRL-M-8RJ45/4SFP-G-DIN, Basic Setting, Port Configuration, Network Redundancy, VLAN (expanded), VLAN Configuration, VLAN Port Configuration, VLAN Information, PVLAN Configuration, PVLAN Port Configuration, PVLAN Information, GVRP Configuration, Traffic Prioritization, Multicast Filtering, SNMP, Security, Warning, Monitor and Diag, Device Front Panel, Save, Logout, and Reboot. The main content area is titled "Private VLAN Configuration" and includes a "Help" button. Below the title is a table with two columns: "VLAN ID" and "Private VLAN Type". The table contains two rows: VLAN ID 2 with Primary type, and VLAN ID 3 with Isolated type. An "Apply" button is located below the table. At the bottom of the interface, there is a copyright notice: "Copyright (c) Pepperl+Fuchs All Rights Reserved."

VLAN ID	Private VLAN Type
2	Primary
3	Isolated

Secondary VLAN: The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated and Community VLANs. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other, however, the isolated VLAN ports cannot.

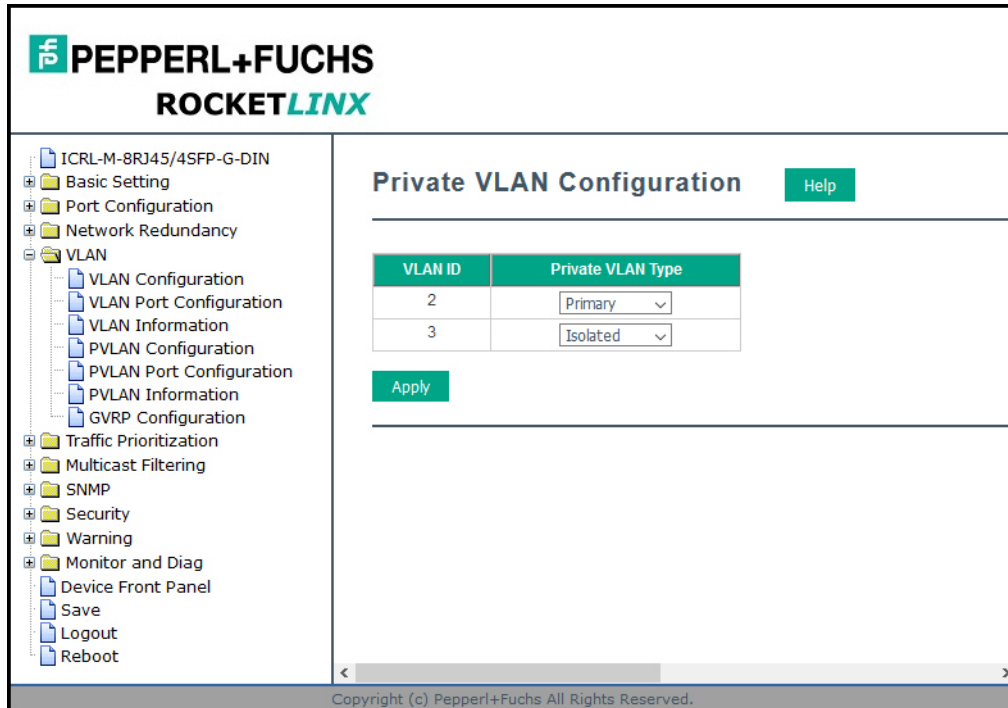
This figure shows a typical private VLAN network. A SCADA/Public Server or NMS workstation is usually located in a primary VLAN. Client PCs and rings are usually located within the secondary VLAN.

Optionally, you can use the CLI for configuration, see *Private VLAN (CLI)* on Page 195.

4.7.1. PVLAN Configuration

PVLAN Configuration allows you to assign a private VLAN type. Choose the private VLAN types for each VLAN you want configure.

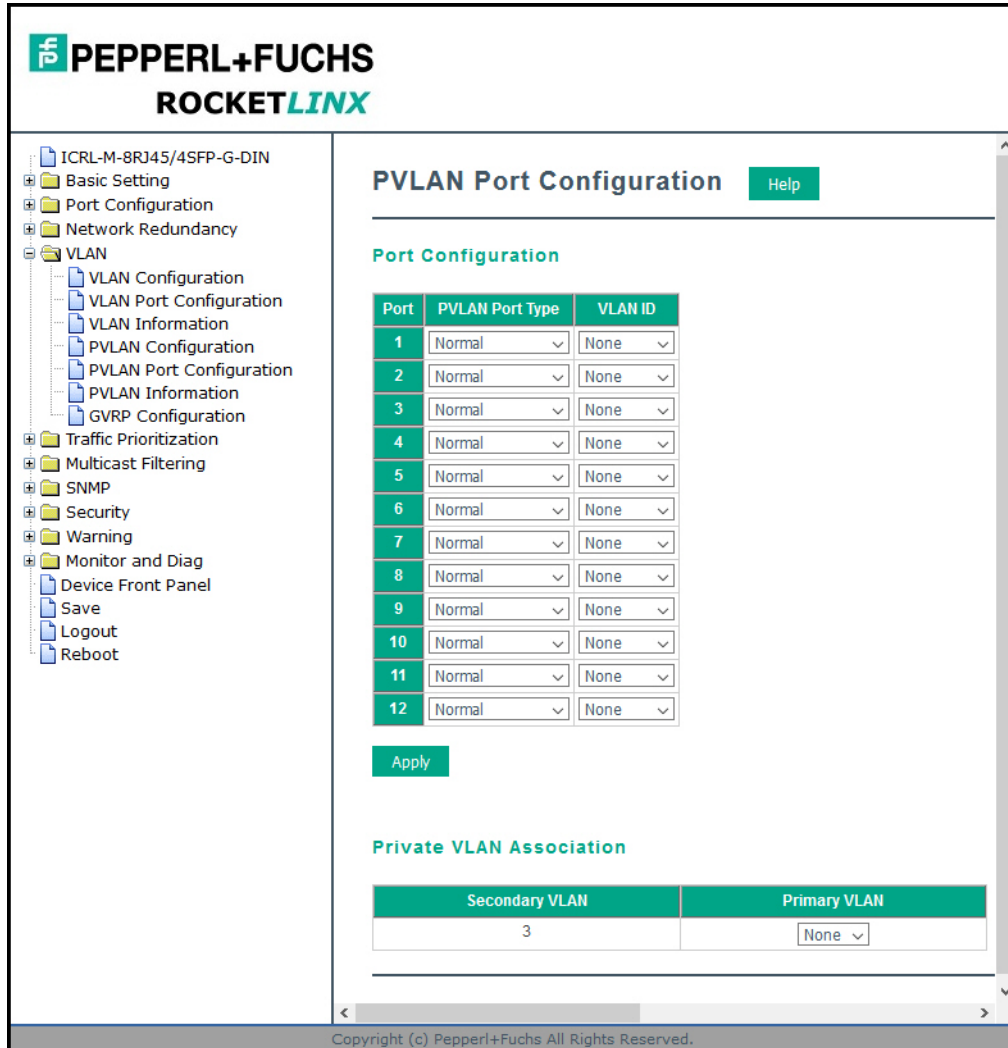
Note: You must have previously configured a VLAN in the VLAN Configuration screen. Refer to VLAN Configuration on Page 89 for information.



Private VLAN Configuration Page	
VLAN ID	<ul style="list-style-type: none"> Primary VLAN - The uplink port is usually the primary VLAN. Ports within a primary VLAN can communicate with ports in a secondary VLAN Secondary VLAN - The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLANs. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other. However, the isolated VLAN ports cannot.
Private VLAN Type	<ul style="list-style-type: none"> None: The VLAN is not included in private VLAN. Primary: A primary VLAN contains promiscuous ports that can communicate with the secondary VLANs. Isolated: The member ports of the VLAN are isolated. Community: The member ports of the VLAN can communicate with each other.
Apply	<p>Click Apply to apply the settings.</p> <p>Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.</p>

4.7.2. PVLAN Port Configuration

The *PVLAN Port Configuration* page allows you to configure the port configuration and private VLAN associations.



Private VLAN Port Configuration Page	
PVLAN Port Type	<p>The following options are available:</p> <p>Normal: Normal ports remain in their original VLAN configuration.</p> <p>Host: Host ports can be mapped to the secondary VLAN.</p> <p>Promiscuous: Promiscuous ports can be associated to the primary VLAN.</p>
VLAN ID	<p>After assigning the port type, this displays the available VLAN ID for which the port can associate.</p>

Private VLAN Port Configuration Page (Continued)	
Private VLAN Association	
Secondary VLAN	After the isolated and community VLANs are configured in the <i>Private VLAN Configuration</i> page, the VLANs belonging to the second VLAN are displayed.
Primary VLAN	After the Primary VLAN Type is assigned in <i>Private VLAN Configuration</i> page, the secondary VLAN can associate to the primary VLAN ID. Note: Before configuring PVLAN port type, the private VLAN Association should be done first.

4.7.3. PVLAN Information

The *PVLAN Information* page allows you to see the private VLAN information. Click **Reload** to refresh the page contents.

PEPPERL+FUCHS
ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
 - VLAN Configuration
 - VLAN Port Configuration
 - VLAN Information
 - PVLAN Configuration
 - PVLAN Port Configuration
 - PVLAN Information
 - GVRP Configuration
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

PVLAN Information [Help](#)

Primary VLAN	Secondary VLAN	Secondary VLAN Type	Port
2	--	--	--
--	3	Isolated	--

[Reload](#)

Copyright (c) Pepperl+Fuchs All Rights Reserved.

4.7.4. GVRP Configuration

GARP VLAN Registration Protocol (GVRP) allows you to set-up VLANs automatically rather than manual configuration on every port on every switch in the network. GVRP conforms to the IEEE 802.1Q specification. This defines a method of tagging frames with VLAN configuration data that allows network devices to dynamically exchange VLAN configuration information with other devices.

GARP (Generic Attribute Registration Protocol), a protocol that defines procedures by which end stations and switches in a local area network (LAN) can register and de-register attributes, such as identifiers or addresses, with each other. Every end station and switch thus has a current record of all the other end stations and switches that can be reached. GVRP, like GARP, eliminates unnecessary network traffic by preventing attempts to transmit information to unregistered users. In addition, it is necessary to manually configure only one switch and all the other switches are configured accordingly.

Port	State	Registration	Join Timer	Leave Timer	Leave All Timer
1	Disable	Normal	20	60	1000
2	Disable	Normal	20	60	1000
3	Disable	Normal	20	60	1000
4	Disable	Normal	20	60	1000
5	Disable	Normal	20	60	1000
6	Disable	Normal	20	60	1000
7	Disable	Normal	20	60	1000
8	Disable	Normal	20	60	1000
9	Disable	Normal	20	60	1000
10	Disable	Normal	20	60	1000
11	Disable	Normal	20	60	1000
12	Disable	Normal	20	60	1000

GVRP Configuration Page	
GVRP Protocol	Allows you to Enable/Disable GVRP globally.
State	After enabling GVRP globally, you can still Enable/Disable GVRP by port.
Registration	This value sets the registration mode of GVRP (default is Normal mode).
Join Timer	Controls the interval of sending the GVRP Join BPDU (Bridge Protocol Data Unit). An instance of this timer is required on a per-port, per-GARP participant basis.

4/21/20

GVRP Configuration Page (Continued)	
Leave Timer	Controls the time to release the GVRP reservation after having received the GVRP Leave BPDU. An instance of the timer is required for each state machine that is in the LV state.
Leave All Timer	Controls the period to initiate the garbage collection of registered VLAN. The timer is required on a per-port, per-GARP participant basis.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

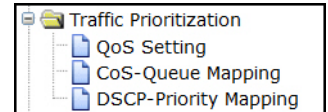
4.7. Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization mechanism which allows you to deliver better service to certain flows. QoS can also help to alleviate congestion problems and ensure high-priority traffic is delivered first. This section allows you to configure *Traffic Prioritization* settings for each port with regard to setting priorities.

The ICRL-M QoS supports four physical queues, weighted fair queuing (WRR) and Strict Priority scheme, that follows the IEEE 802.1p CoS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

The following web pages are included in this group:

- *QoS Setting*
- *CoS-Queue Mapping* on Page 104
- *DSCP-Queue Mapping* on Page 105



Optionally, you can use the CLI for configuration, see *Traffic Prioritization (CLI)* on Page 199.

4.7.1. QoS Setting

Use this subsection to set up QoS settings for the ICRL-M.

PEPPERL+FUCHS ROCKETLINX

QoS Setting [Help](#)

QoS Trust Mode

- 802.1P priority tag
- DSCP/TOS code point

Queue Scheduling

- Round Robin Scheme
- Strict Priority Scheme
- Weighted Round Robin Scheme
- Weighted Deficit Round Robin Scheme

Queue	0	1	2	3	4	5	6	7
Weight	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Port Setting

Port	Queue
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>
9	<input type="text"/>
10	<input type="text"/>
11	<input type="text"/>
12	<input type="text"/>

[Apply](#)

Copyright (c) Pepperl+Fuchs All Rights Reserved.

QoS Setting Page	
Queue Trust Mode	
802.1P Priority Tag	If 802.1P is selected the ICRL-M relies on a packet's CoS information to determine priority. This is related to the settings in the <i>CoS-Queue Mapping</i> page.
DSCP/TOS Code Point	If DSCP/TOS is selected the switch relies on a packets differentiated services code point information to determine the priority. This is related to the settings in the <i>DSCP-Priority Mapping</i> page.
Queue Scheduling	
Round Robin Scheme	The Round Robin scheme means all the priority has the same privilege, the traffic is forward cyclic from highest to lowest.
Strict priority scheme	Packets with higher priority in the queue are always processed first, except that there is no packet with higher priority.
Use Weighted Round Robin scheme	This scheme allows users to assign new weight ratio for each class. The 10 is the highest ratio. The ratio of each class is as below: $Wx / W0 + W1 + W2 + W3 + W4 + W5 + W6 + W7$ (Total volume of Queue 0-7)
Weighted Deficit Round Robin Scheme	This scheme allows you to assign a new weight ratio for each class. The weight: 2032 is the maximum, the weight: 0 is the minimum and it has to be even. A setting of 0 establishes pure priority scheduling. The programmable weight setting ranges from 1 to 127. Total volume of Queue 0-7.
Port Setting	
Queue	Choose the Queue value of each port, the port then has its default priority. The Queue 7 is the highest port-based queue, 0 is the lowest queue. The traffic injected to the port follows the queue level to be forwarded, but the outgoing traffic does not bring the queue level to next switch.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.7.2. CoS-Queue Mapping

Use this page to change the CoS values into the Physical Queue mapping table. Since the switch fabric of ICRL-M supports four queues, Lowest, Low, Middle, and High users should therefore assign how to map the CoS value to the level of the physical queue.

You can assign the mapping table or follow the suggestion of the IEEE 802.1p standard. The ICRL-M uses IEEE 802.1p suggestion as default values. CoS Values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS Values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. CoS Values 4 and 5 are mapped to physical Queue 2, the middle physical queue. CoS Values 6 and 7 are mapped to physical Queue 3, the high physical queue.

Class of service (CoS) is a 3 bit field within a layer two Ethernet frame header defined by IEEE 802.1p when using IEEE 802.1Q tagging. The field specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic.

While CoS operates only on Ethernet at the data link layer, other QoS mechanisms (such as DiffServ) operate at the network layer and higher. Others operate on other physical layers. Although IEEE 802.1Q tagging must be enabled to communicate priority information from switch to switch, some switches use CoS to internally classify traffic for QoS purposes.

Differentiated Services (DiffServ) is a model where traffic is treated by intermediate systems with relative priorities based on the type of services (ToS) field. Defined in RFC2474 and RFC2475, the DiffServ standard supersedes the original specification for defining packet priority described in RFC791. DiffServ increases the number of definable priority levels by reallocating bits of an IP packet for priority marking. The DiffServ architecture defines the DiffServ field, which supersedes the ToS field in IPv4 to make per-hop behavior (PHB) decisions about packet classification and traffic conditioning functions, such as; metering, marking, shaping, and policing.

The screenshot shows the web interface for configuring CoS-Queue Mapping. The navigation tree on the left includes categories like VLAN, Traffic Prioritization, and Security. The main content area is titled 'CoS-Queue Mapping' and contains a table with the following structure:

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

Below the table, there is a note: "Note- Queue 7 is the highest priority queue in using Strict Priority scheme". At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons.

After configuration, press **Apply** to enable the settings.

Note: You must **Save** the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.7.3. DSCP-Queue Mapping

Use this page to change DSCP values to Physical Queue mapping table. Since the switch fabric of the ICRL-M only supports four queues. Lowest, Low, Middle and High users should therefore assign how to map DSCP values to the level of the physical queue. You should therefore assign how to map DSCP value to the level of the queue. You can change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.

After configuration, press **Apply** to enable the settings.

The screenshot shows the 'DSCP-Priority Mapping' configuration page in the PEPPERL+FUCHS ROCKETLINX web interface. The left sidebar contains a navigation tree with the following items: ICRL-M-8RJ45/4SFP-G-DIN, Basic Setting, Port Configuration, Network Redundancy, VLAN, VLAN Configuration, VLAN Port Configuration, VLAN Information, PVLAN Configuration, PVLAN Port Configuration, PVLAN Information, GVRP Configuration, Traffic Prioritization, QoS Setting, CoS-Queue Mapping, DSCP-Priority Mapping, Multicast Filtering, SNMP, Security, Warning, Monitor and Diag, Device Front Panel, Save, Logout, and Reboot. The main content area is titled 'DSCP-Priority Mapping' and includes a 'Help' button. Below the title is a table with 8 columns representing DSCP values (0-7) and 8 rows representing Queue numbers (0-7). Each cell in the table contains a dropdown menu. The current configuration shows Queue 0 mapped to DSCP 0-7, Queue 1 to 8-15, Queue 2 to 16-23, Queue 3 to 24-31, Queue 4 to 32-39, Queue 5 to 40-47, Queue 6 to 48-55, and Queue 7 to 56-63. At the bottom of the table are 'Apply' and 'Cancel' buttons. A copyright notice 'Copyright (c) Pepperl+Fuchs All Rights Reserved.' is visible at the very bottom of the interface.

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

Note: You must **Save** the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.8. Multicast Filtering

For multicast filtering, the ICRL-M uses IGMP (Internet Group Management Protocol) Snooping technology. IGMP is an Internet protocol that provides a way for Internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the network device to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computer's data.

Multicasting is useful for applications where the same data needs to be sent to multiple destinations such as multimedia streaming or organization wide software updates.

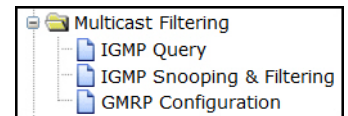
In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown in the following table.

Messages	
Query	A message sent from the querier (an IGMP router or a switch) that asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

You can enable **IGMP Snooping** and **IGMP Query** functions. This section illustrates the information of the IGMP Snooping function, including different multicast groups' VID and member ports, and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255.

The following web pages are included in this group:

- *IGMP Query* on Page 107
- *IGMP Snooping & Filtering* on Page 108
- *GMRP Configuration* on Page 110

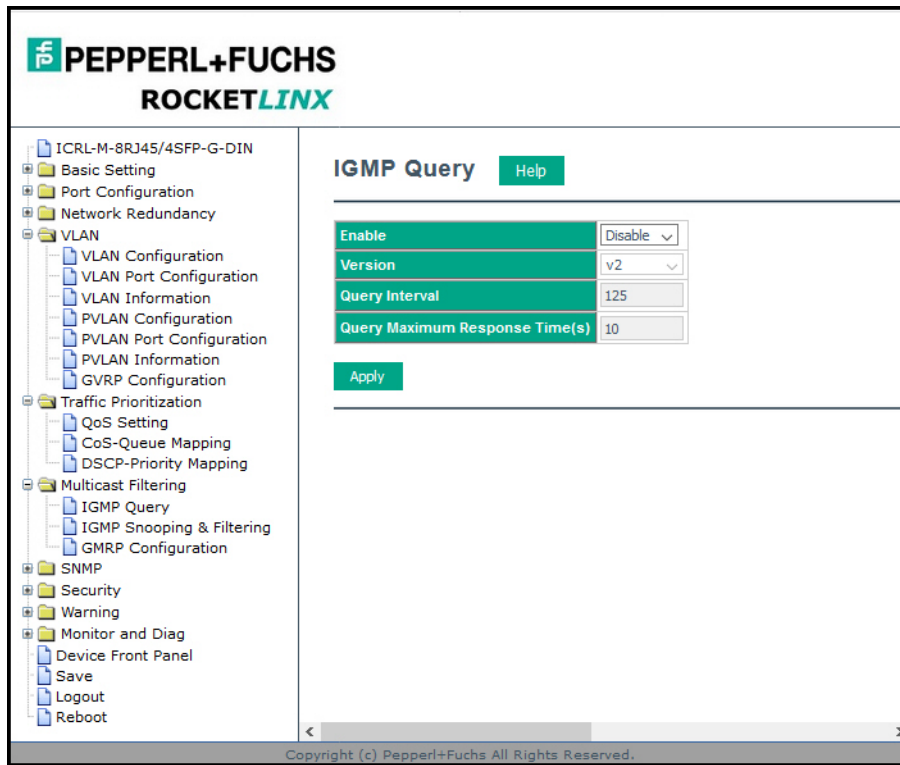


Optionally, you can use the CLI for configuration, see *Multicast Filtering (CLI)* on Page 202.

4.8.1. IGMP Query

Use this page to configure the *IGMP Query* feature. Since the ICRL-M can only be configured by member ports of the management VLAN, the IGMP Query can only be enabled on the management VLAN. If you want to run IGMP Snooping feature in several VLANs, first check to see whether each VLAN has its own IGMP Querier.

The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.



IGMP Query Page	
Enable	By default, IGMP Query is disable
Version	Select Version 1 , Version 2 or Disable . <ul style="list-style-type: none"> Version 1 means IGMP V1 General Query Version 2 means IGMP V2 General Query. The query is forwarded to all multicast groups in the VLAN. Disable allows you to disable IGMP Query.
Query Interval(s)	The period of query (seconds) sent by querier. Enter a number between 1 and 65,535.
Query Maximum Response Time	This option is available when you select Version 2 . The span querier detect (seconds) to confirm there are no more directly connected group members on a LAN. Enter a number between 1 and 25.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.8.2. IGMP Snooping & Filtering

Use this page to enable the IGMP Snooping feature, assign IGMP Snooping for specific VLANs, and view the *IGMP Snooping Table* from a dynamic learned or static that you provide.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
 - QoS Setting
 - CoS-Queue Mapping
 - DSCP-Priority Mapping
- Multicast Filtering
 - IGMP Query
 - IGMP Snooping & Filtering
 - GMRP Configuration
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

IGMP Snooping & Filtering Help

IGMP Snooping Global Setting Disable ▾

Apply

IGMP Snooping VLAN Setting

VLAN	IGMP Snooping	Immediate-leave	Last Member Query Interval	Filtering Mode
1	Disable ▾	Disable ▾	100	Broadcast Unknown ▾
2	Disable ▾	Disable ▾	100	Broadcast Unknown ▾
3	Disable ▾	Disable ▾	100	Broadcast Unknown ▾

Apply

IGMP Snooping Table

Multicast Address	VLAN ID	Interface

Reload

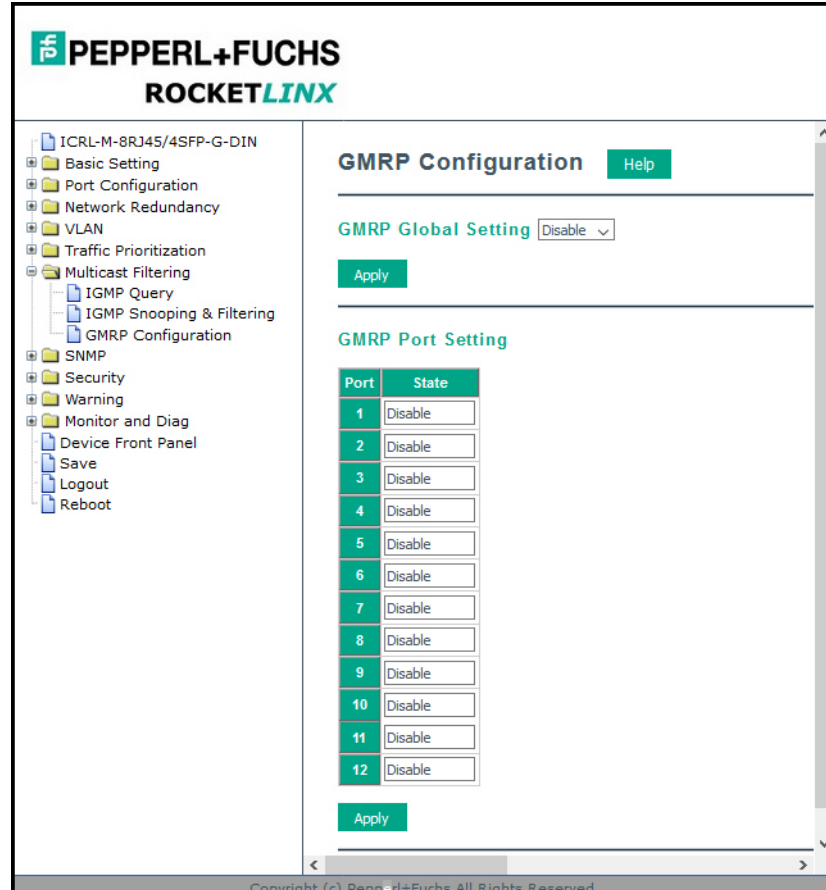
Copyright (c) Pepper+Fuchs All Rights Reserved.

IGMP Snooping Page	
IGMP Snooping Global Setting	You can select to Enable or Disable IGMP Snooping. After enabling IGMP Snooping, you can then enable IGMP Snooping for specific VLAN using the <i>IGMP Snooping VLAN Setting</i> table.
IGMP Snooping VLAN Setting	
VLAN	Refers to the VLAN number that was configured using the <i>VLAN Configuration</i> page.
IGMP Snooping	Select Enable to start IGMP snooping on the selected VLAN.
Immediate-leave	Leave group when receive a leave message.
Last Member Query Interval (centiseconds)	The interval for which the switch waits before updating the table entry.
Filtering Mode	The available filtering modes are: <ul style="list-style-type: none"> • Broadcast-Unknown- The unknown multicast is broadcast to all ports even if they are not member ports of the groups. • Discard-Unknown - The unknown multicast is discarded. Non-member ports do not receive the unknown multicast streams. • Source-only-learning - This is forwarding unknown multicast traffic to all ports that are already members of a multicast group.
IGMP Snooping Table	This table displays the multicast group IP address, VLAN ID it belongs to, and the member ports of the multicast group. The ICRL-M supports 256 multicast groups. Click Reload to refresh the table.

Note: You must **Save** the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.8.3. GMRP Configuration

GARP Multicast Registration Protocol (GMRP) is a Generic Registration Protocol (GARP) application that provides a multicast traffic management facility at Layer 2 similar to what IGMP provides at Layer 3. GMRP and GARP are industry-standard protocols first introduced as part of IEEE 802.1D.



GMRP Configuration	
GMRP Global Setting	Enable/Disable GMRP protocol.
State	The state of the GMRP operation on a selected port. The value enabled indicates that the GMRP is enabled on this port as long as the GMRP protocol is also enabled for this device. When disabled, but the GMRP protocol is still enabled for the device, GMRP is disabled on the selected port.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

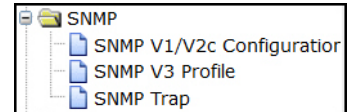
4.9. SNMP

Simple Network Management Protocol (SNMP) is a protocol to exchange management information between network devices. SNMP is a member of the TCP/IP protocol suite. The ICRL-M supports SNMP v1 and v2c and v3.

An SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP compatible format. The manager is the console through the network.

The following web pages are included in this group:

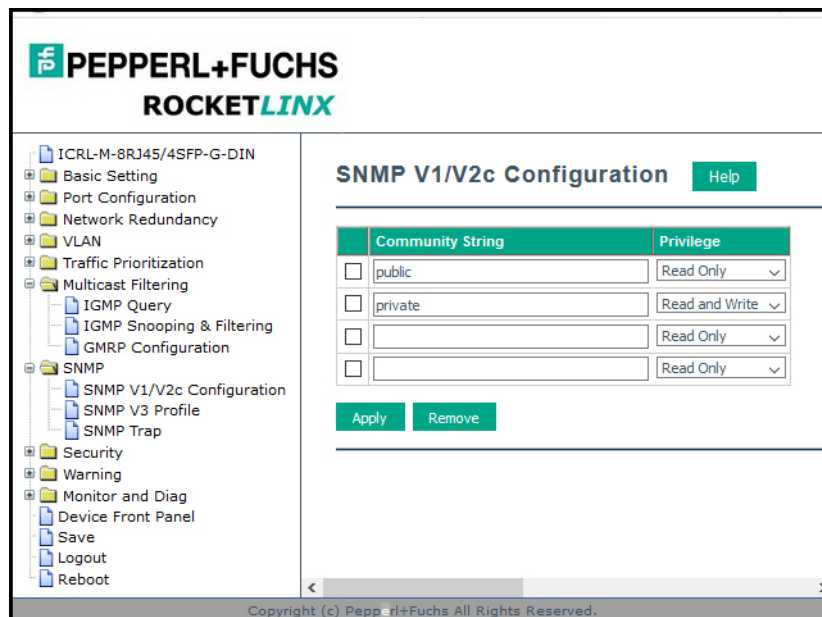
- *SNMP Configuration*
- *SNMP V3 Profile* on Page 112
- *SNMP Traps* on Page 113



Optionally, you can use the CLI for configuration, see *SNMP (CLI)* on Page 206.

4.9.1. SNMP Configuration

Use this page to configure the SNMP v1/v2c Community. The community string can be viewed as the password because SNMP v1/v2c does not request you to enter a password before you try to access the SNMP agent.



The community includes two privileges:

- **Read Only** privilege, you only have the ability to read the values of MIB tables. The default community string is **public**.
- **Read and Write** privilege, you have the ability to read and set the values of MIB tables. The default community string is **private**.

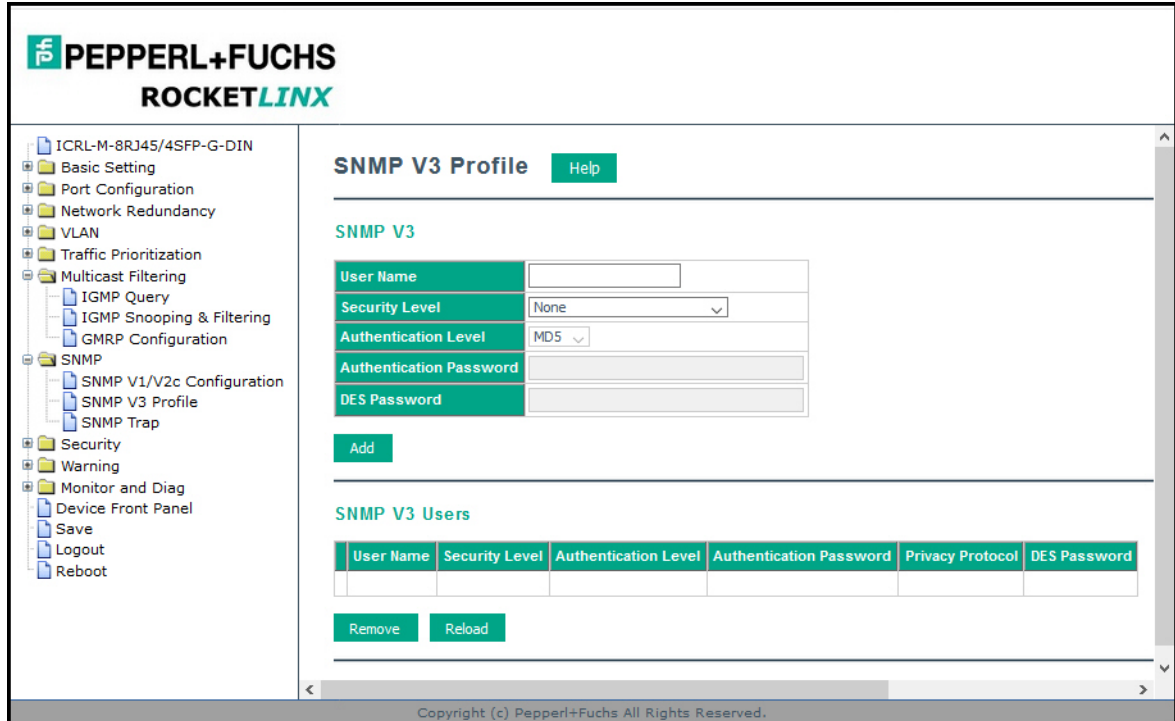
The ICRL-M allows you to assign four community strings. Type the community string, select the privilege, and then click **Apply**.

Note: When you first install the device in your network, we recommend that you change the community string. Most SNMP management applications use public and private as the default community name, this could be a network security leak.

4/21/20

4.9.2. SNMP V3 Profile

SNMP v3 can provide more security functions when you perform remote management through SNMP protocol. It delivers SNMP information to the administrator with user authentication; all of data between the ICRL-M and the administrator are encrypted to ensure secure communication.



SNMP V3 Profile Page	
User Name	SNMP v3 user name.
Security Level	Select the following levels of security: None , Authentication , and Authentication and Privacy .
Authentication Level	Select either MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm). <ul style="list-style-type: none"> MD5 is a widely used cryptographic hash function with a 128-bit hash value. SHA functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. <p>The ICRL-M provides two user authentication protocols in MD5 and SHA. You need to configure SNMP v3 parameters for your SNMP tool with the same authentication method.</p>
Authentication Password	Enter the SNMP v3 user authentication password.
DES Password	Enter the password for SNMP v3 user DES Encryption.
Add	Click to add an SNMP v3 user.
SNMP V3 Users	This table provides SNMP v3 user information. Click Remove to remove a selected SNMP v3 user. Click Reload to reload SNMP v3 user information.

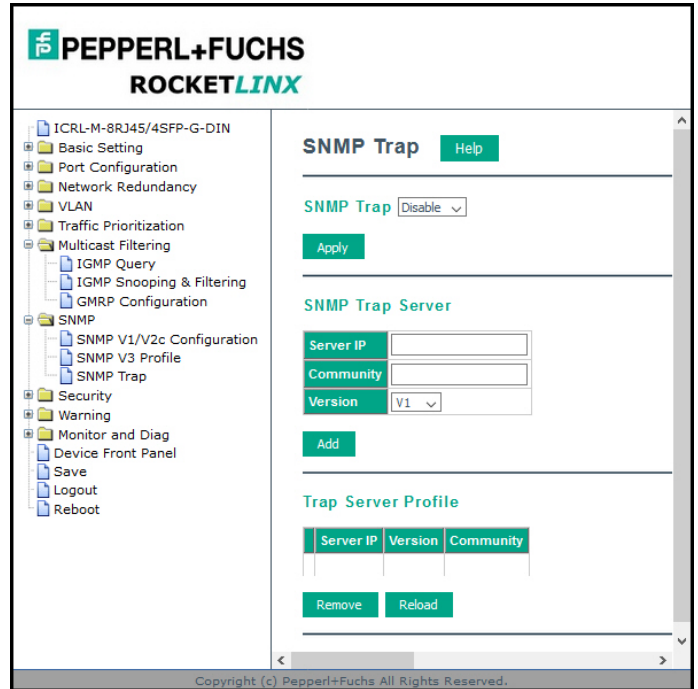
Note: You must **Save** the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4/21/20

4.9.3. SNMP Traps

SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap information. So you do not need to install new applications to read the notification information.

You can see the change of the SNMP predefined standard traps and Pepperl+Fuchs pre-defined traps. The pre-defined traps can be found in the MIB file for your ICRL-M at <https://www.pepperl-fuchs.com>.



SNMP Trap Page	
SNMP Trap	Click Enable or Disable SNMP trap functionality.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.
SNMP Trap Server	
Server IP	The SNMP trap server IP address.
Community	The SNMP trap server community string.
Version	The SNMP trap version, V1 or V2c.
Add	Click the Add button to add a SNMP server.
Trap Server Profile	
Server IP	The SNMP trap server IP address
Community	The SNMP trap server community string.
Version	The SNMP trap version, V1 or V2c.
Remove	Click Remove to remove selected SNMP server.
Reload	Click the Reload button to reload SNMP server information.

Note: You must **Save** the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

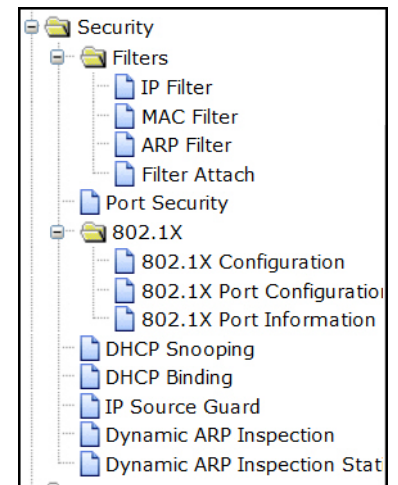
4/21/20

4.10. Security

The ICRL-M provides several security features for you to secure your connection. The following pages are included in this group:

- *Filter Set (Access Control List)*
 - *IP Filter* on Page 116
 - *MAC Filter (Port Security)* on Page 118
 - *ARP Filter*
 - *Filter Attach* on Page 122
- *Port Security*
- *802.1X Configuration* on Page 125
- *802.1X Port Configuration* on Page 127
- *802.1X Port Information* on Page 129
- *DHCP Snooping* on Page 130
- *DHCP Binding Configuration* on Page 132
- *IP Source Guard* on Page 134
- *Dynamic ARP Inspection* on Page 136
- *Dynamic ARP Inspection Status* on Page 138

Optionally, you can use the CLI for configuration, see *Security (CLI)* on Page 207.



4.10.1. Filter Set (Access Control List)

The Filter Set is known as Access Control List (ACL) feature. There are two major types:

- *IP Filter* on Page 116, which is called IP security in other RocketLinx models and supports the IP Standard access list, and advanced IP based access lists.
- *MAC Filter (Port Security)* on Page 118, which is called Port Security in other RocketLinx switches. It allows you to define the access rule based on the MAC address.

You can use Access Control Entry (ACE) to define a Permit or Deny rule for specific IP or MAC address, or IP groups by network mask in each ACE. One ACL may include several ACEs. The system checks the ACEs one after another and forwards the data based on the result.

If the rules conflict, the oldest entry is selected.

4.10.1.1. IP Filter

Click **IP Filter** and type the **ID/Name** to configure security using IP addresses. Click **Reload** to refresh settings and **Delete** to remove one of the entries.

PEPPERL+FUCHS ROCKETLINX

IP Filter [Help](#)

IP Filter Group

(1-99) IP Standard Access List
(100-199) IP Extended Access List
(1300-1999) IP Standard Access List (expanded range)
(2000-2699) IP Extended Access List (expanded range)

[Add](#)

Select	Group Number	Type
<input type="checkbox"/>		

[Delete](#) [Reload](#)

IP Filter Setting

Group Number	<input type="text"/>
Protocol	IP <input type="text"/>
Source IP	<input type="text"/>
Source Wildcard	any <input type="text"/>
Source Port	<input type="text"/>
Destination IP	<input type="text"/>
Destination Wildcard	any <input type="text"/>
Destination Port	<input type="text"/>
Egress Port	-- <input type="text"/>
Action	<input type="radio"/> Permit <input type="radio"/> Deny

[Add](#)

IP Filter List

Select	Group Number	Type	Protocol	Source IP	Source Wildcard	Source Port	Destination IP	Destination Wildcard	Destination Port	Action	Egress Port
<input type="checkbox"/>											

[Delete](#)

Copyright (c) Pepperl+Fuchs. All Rights Reserved.

IP Filter Page	
IP Filter Group	
IP Filter Group	<p>Enter an applicable Group Number to specify whether it is an IP Standard and IP Extended access list.</p> <ul style="list-style-type: none"> IP Standard Access List This type of ACL allows you to define filter rules according to the source IP address. IP Extended Access List This type of ACL allows you to define filter rules according to the source IP address, destination IP address, Source TCP/UDP port, destination TCP/UDP port and ICMP type and code.
Add	After entering an IP filter group number, click Add .
Select	Select this field to delete or reload this entry.
Group Number	This is the number that represents the Filter Group.
Type	This is the Filter Group type (standard or extended).
Delete	Deletes the selected rule table.
Reload	Reloads the rule table.

Highlight an IP Filter ID/Name and click **Edit** to configure the IP Filter Rules.

IP Filter Setting	
Group Number	This is the Filter Group number.
Protocol	This is the IP protocol (IP) or L4 protocol (TCP/UDP/ICMP).
Source IP	Type the source IP address of the packet.
Source Wildcard	This is the mask of the source IP address.
Source Port	This is the source port of L4 protocol (TCP/UDP).
Destination IP	This is the destination IP address of the packet.
Destination Wildcard	This is the mask of the destination IP address.
Destination Port	This is the destination port of L4 protocol (TCP/UDP).
Egress Port	This is the outgoing (exiting) port number.
Action	This is the filter action, which is to deny or permit the packet.
Add	Adds the rule to the Filter.
IP Filter List	
Delete	Removes the selected rule from the Filter.

4.10.1.2. MAC Filter (Port Security)

The MAC Filter allows you to define the Access Control List for a specific MAC address or a group of MAC addresses. Packet filtering can help limit network traffic and restrict network use by certain users or devices. The Add Filters feature filters traffic as it passes through a switch and permits or denies packets crossing specified interfaces. MAC Filters can filter layer 2 traffic.

PEPPERL+FUCHS
ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
 - Filters
 - IP Filter
 - MAC Filter
 - ARP Filter
 - Filter Attach
 - Port Security
 - 802.1X
 - DHCP Snooping
 - DHCP Binding
 - IP Source Guard
 - Dynamic ARP Inspection
 - Dynamic ARP Inspection Stati
- Warning
- Monitor and Diag
 - Device Front Panel
 - Save
 - Logout
 - Reboot

MAC Filter [Help](#)

MAC Filter Group

[Add](#)

Select	Group Name
<input type="checkbox"/>	

[Delete](#) [Reload](#)

MAC Filter Setting

Group Name	<input type="text"/>
Source MAC	<input type="text"/>
Source Wildcard	<input type="text" value="any"/>
Destination MAC	<input type="text"/>
Destination Wildcard	<input type="text" value="any"/>
Egress Port	<input type="text" value="--"/>
Action	<input type="radio"/> Permit <input type="radio"/> Deny

[Add](#)

MAC Filter List

Select	Group Name	Source MAC	Source Wildcard	Destination MAC	Destination Wildcard	Action	Egress Port
<input type="checkbox"/>							

[Delete](#)

Copyright (c) Pepperl+Fuchs All Rights Reserved.

MAC Filter Page	
MAC Filter Group	The name for this MAC Filter entry.
Select	If you select this and click the Delete button, the corresponding Filter Group is deleted.
Group Name	This is the MAC group name
Reload	Click Reload to reload the Filter Group table.
MAC Filter Setting	
Group Name	This is the MAC Filter Group name.
Source MAC	Type the MAC address that you want to configure. The format is AABB.CCDD.EE FF.
Source Wildcard	You can define a single host or a group of hosts based on the wildcard. Some of the allowance examples are shown in the following table.
Destination MAC	Type the MAC address that you want to configure. The format is AABB.CCDD.EE FF.
Destination Wildcard	You can define a single host or a group of hosts based on the wildcard. Some of the allowance examples are shown in the following table.
Egress Port	This is the outgoing (exiting) port number.
Action	Select Permit to allow traffic from specified sources or Deny traffic from those sources.
MAC Filter List	
Group Name	This is the Filter Group number.
Source MAC	Type the source MAC address of the packet.
Source Wildcard	This is the mask of the MAC address.
Destination MAC	This is the destination MAC address of the packet.
Destination Wildcard	This is the mask of the destination MAC address.
Action	This is the filter action, which is to deny or permit the packet.
Egress Port	This is the outgoing (exiting) port number
Delete	Removes the selected rule from the Filter.

Once you finish configuring the MAC settings, click **Add** to apply your configuration.

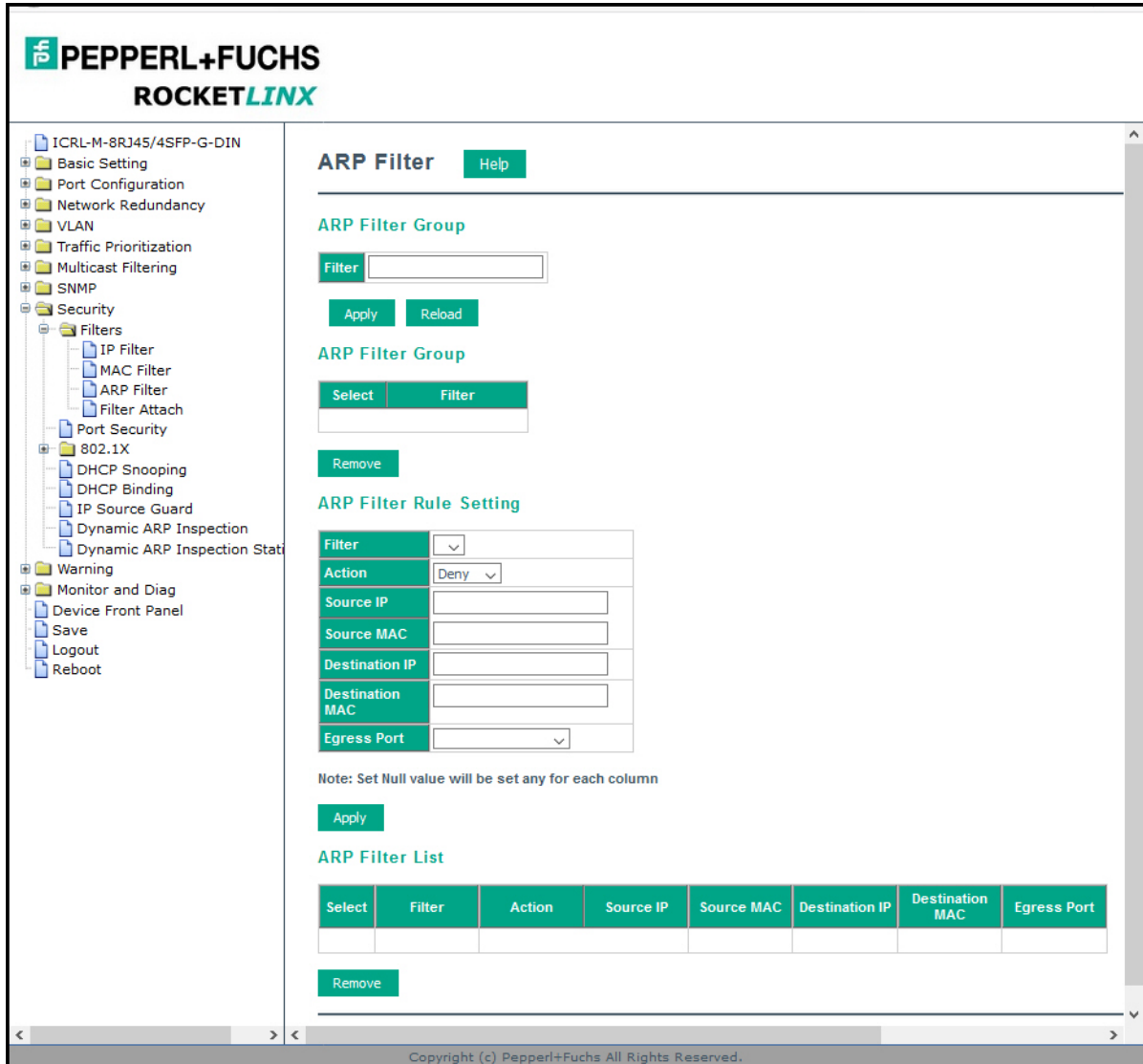
Note: You must **Save** the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

In the **Source MAC/ Destination MAC** field, type the MAC address you want configure, the format is **AABB.CCDD.EE FF**. For example: **Source to Destination** is **0012.7700.0000 to 0012.7700.0002**. The **Source Wildcard /Destination Wildcard** field allows you to define a single host or a group of hosts based on the wildcard. Some of the allowance examples are illustrated below:

Wildcard	Bit	Number of Allowances	Note
Any	1111.1111.1111	All	
Host		1	Only the source or destination
0000.0000.0003	0000.0000.000(00000011)	3	
0000.0000.0007	0000.0000.000(00000111)	7	
0000.0000.000F	0000.0000.000(11111111)	15	
....			

4.10.1.3. ARP Filter

ARP filtering can help limit ARP traffic and restrict network use by certain users or devices. The **Add Filters** feature filters ARP as it passes through a switch and permits or denies packets crossing specified interfaces.



ARP Filter Page

ARP Filter Group

Filter	This is name that represents the Filter Group.
Apply	This saves the Filter Group.
Reload	This reloads the selected Filter Group.

ARP Filter Group

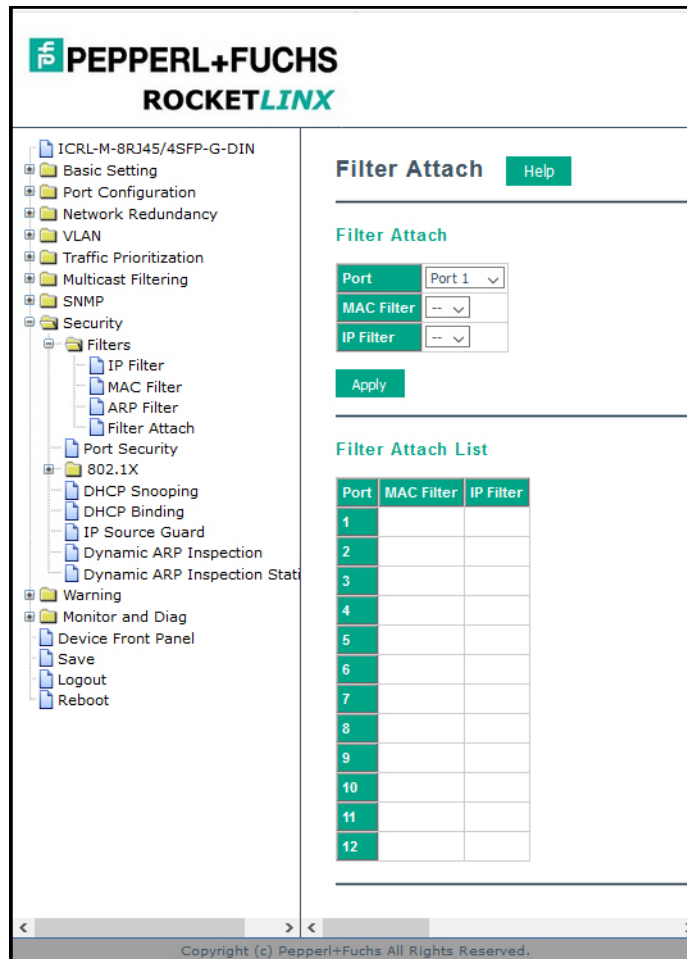
Select	Select this field to delete the entry and then click the Remove button.
Filter	This is name that represents the Filter Group.

4/21/20

ARP Filter Page (Continued)	
Remove	Click the Remove button to remove the Filter Group.
ARP Filter Rule Setting	
Filter	Name of the Filter Group.
Action	This is the filter action, which is to deny or permit the packet.
Source IP	This is the source IP address of the packet.
Source MAC	This for the source MAC of the packet.
Destination IP	This is the destination IP address of the packet.
Destination MAC	This is the destination MAC of the packet.
Egress Port	This is the outgoing (exiting) port.
Apply	Click the Apply button to add a new ARP Filter rule.
ARP Filter List	
Select	Selected for delete.
Filter	Name of the Filter Group.
Action	This is the filter action, which is to deny or permit the packet.
Source IP	This is the source IP address of the packet.
Source MAC	This for the source MAC of the packet.
Destination IP	This is the destination IP address of the packet.
Destination MAC	This is the destination MAC of the packet.
Egress Port	This is the outgoing (exiting) port number
Remove	Click the Remove button to remove the Filter you selected.

4.10.1.4. Filter Attach

This page allows you to attach filters created on the IP Filter and MAC Filter pages to ports on the switch.



Filter Attach Page	
Port	The port you want to attach a filter to.
MAC Filter	Select a MAC address based filter to attach to the interface. Select "--" to remove an attached MAC address filter.
IP Filter	Select an IP address based filter to attach to the interface. Select "--" to remove an attached IP address filter.
Apply	Click the Apply button to apply the Filter configurations.

Note: You must **Save** the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.10.2. Port Security

Use the *Port Security* page to configure security on a port-by-port basis.

PEPPERL+FUCHS ROCKETLINX

Port Security [Help](#)

Port	Security	Sticky	Auto Learn	Shutdown Time	Shutdown Status	Shutdown Elapsed Time
1	Disable	Enable	0	0	Up	0
2	Disable	Enable	0	0	Up	0
3	Disable	Enable	0	0	Up	0
4	Disable	Enable	0	0	Up	0
5	Disable	Enable	0	0	Up	0
6	Disable	Enable	0	0	Up	0
7	Disable	Enable	0	0	Up	0
8	Disable	Enable	0	0	Up	0
9	Disable	Enable	0	0	Up	0
10	Disable	Enable	0	0	Up	0
11	Disable	Enable	0	0	Up	0
12	Disable	Enable	0	0	Up	0

[Apply](#)

Add Port Security Entry

Port	VID	MAC Address
Port 1		

[Add](#)

Show Port Security List

Port	Address Type	VID	MAC Address

[Remove](#) [Reload](#)

Copyright (c) Pepperl+Fuchs All Rights Reserved.

Port Security Page	
Port	The port identifier.
Security	Enable or disable port security on this port.
Sticky	Enable or disable sticky on this port.
Auto Learn	It specifies maximum number of MAC addresses that can be dynamically learned on the port, valid range is 0-10.
Shutdown Time	It specifies for how long to shutdown the port, valid range is 0-86400 seconds, if a security violation occurs.

Port Security Page (Continued)	
Shutdown Status	It displays the port is shutdown or not.
Shutdown Elapsed Time	It displays the elapsed time of port shutdown.
Apply	Click the Apply button to apply Port Security State configurations.
Add Port Security Entry	
Port	The port id, if you want to insert a new MAC entry, the port ID must be correct when creating a new entry.
VID	The VLAN id, if you want to insert a new MAC entry, the VLAN id must be correct when creating a new entry.
MAC Address	MAC address of the entry.
Add	Click the Add button to add a Port Security Entry.
Show Port Security List	
Port	The port id of the entry.
Address Type	Type of Security MAC address. Security is static security MAC address. Security is auto learned MAC address.
VID	The VLAN ID of the entry.
MAC Address	MAC address of the entry.
Remove	Click the Remove button to remove the selected Port Security Entry.

4.10.3. 802.1X Configuration

IEEE 802.1X is the protocol that performs authentication to obtain access to IEEE 802 LANs. It is port-base network access control. With the function, the ICRL-M could control which connection is available or not.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
 - Filters
 - IP Filter
 - MAC Filter
 - ARP Filter
 - Filter Attach
 - Port Security
 - 802.1X
 - 802.1X Configuration
 - 802.1X Port Configuration
 - 802.1X Port Information
 - DHCP Snooping
 - DHCP Binding
 - IP Source Guard
 - Dynamic ARP Inspection
 - Dynamic ARP Inspection Sta
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

802.1X Configuration Help

System Auth Control Disable

Authentication Method RADIUS

Apply

RADIUS Server

RADIUS Server IP

Shared Key

Server Port

Accounting Port

Secondary RADIUS Server

RADIUS Server IP

Shared Key

Server Port

Accounting Port

Apply

Local RADIUS User

User Name	Password	VID
<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply

Local RADIUS User List

Delete	Name	Password	VID
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Delete

Copyright (c) Pepperl+Fuchs. All Rights Reserved.

IEEE 802.1x Page	
System Auth Control	Enable or Disable the IEEE 802.1x authentication.
Authentication Method	RADIUS is an authentication server that provides a key for authentication. When you use this method, you must connect the switch to the server. If you select Local for the authentication method, the switch uses the local user database that can be created in this page for authentication.
RADIUS Server	
RADIUS Server IP	The IP address of the RADIUS server.
Shared Key	The password used to communicate between the ICRL-M and the RADIUS Server.
Server Port	The UDP port of the RADIUS server.
Accounting Port	The port for packets that contains the account login or logout information.
Secondary RADIUS Server	
RADIUS Server IP	You can set a Secondary RADIUS Server, if the primary RADIUS server goes down.
Shared Key	The password used to communicate between the ICRL-M and the secondary RADIUS Server.
Server Port	The UDP port of the secondary RADIUS server.
Accounting Port	The port for packets that contains the account login or logout information for the secondary server.
Local RADIUS User	
User Name	The user name of the local RADIUS user.
Password	The password of the local RADIUS user.
VID	The password of the local RADIUS user.
Apply	Click the Apply button to add a local RADIUS user.
Local RADIUS User List	
Delete	This is the selection item for the local RADIUS user delete.
Name	This is the name of the local RADIUS user.
Password	This is the password of the local RADIUS user.
VID	This is the VLAN ID of the local RADIUS user.
Delete	Click the Delete button to remove selected local RADIUS users.

4.10.4. 802.1X Port Configuration

After configuring the **RADIUS Server** or **Local RADIUS User List**, you also need to configure the authentication mode, authentication behavior, applied VLAN for each port, and permitted communications.

The screenshot displays the configuration interface for 802.1X on a PEPPERL+FUCHS device. The left sidebar shows a navigation tree with '802.1X Port Configuration' selected. The main area is divided into two sections: '802.1X Port Configuration' and '802.1X Timeout Configuration'.

802.1X Port Configuration

Port	Port Control	MAB	Re-authentication	Max Request	Guest VLAN	Host Mode	Admin Control Direction
1	Force Authorize	Disable	Disable	2	0	Single	Both
2	Force Authorize	Disable	Disable	2	0	Single	Both
3	Force Authorize	Disable	Disable	2	0	Single	Both
4	Force Authorize	Disable	Disable	2	0	Single	Both
5	Force Authorize	Disable	Disable	2	0	Single	Both
6	Force Authorize	Disable	Disable	2	0	Single	Both
7	Force Authorize	Disable	Disable	2	0	Single	Both
8	Force Authorize	Disable	Disable	2	0	Single	Both
9	Force Authorize	Disable	Disable	2	0	Single	Both
10	Force Authorize	Disable	Disable	2	0	Single	Both
11	Force Authorize	Disable	Disable	2	0	Single	Both
12	Force Authorize	Disable	Disable	2	0	Single	Both

Buttons: Apply Selected, Initialize Selected, Reauthenticate Selected, Default Selected

802.1X Timeout Configuration

Port	Re-Auth Period(s)	Quiet Period(s)	Tx period(s)	Supplicant Timeout(s)	Server Timeout(s)
1	3600	60	30	30	30
2	3600	60	30	30	30
3	3600	60	30	30	30
4	3600	60	30	30	30
5	3600	60	30	30	30
6	3600	60	30	30	30
7	3600	60	30	30	30
8	3600	60	30	30	30
9	3600	60	30	30	30
10	3600	60	30	30	30
11	3600	60	30	30	30
12	3600	60	30	30	30

Button: Apply

802.1x Port Configuration Page	
802.1X Port Configuration	
Port control	Force Authorized means that this port is authorized; the data is free to move in/out. Force unauthorized is just the opposite, the port is blocked. To control this port with a RADIUS server, select Auto for port control.
MAB	If this field is enabled, the functional MAC Address will bypass to the RADIUS Server for authentication.
Reauthentication	If this field is enabled, the ICRL-M requests the client to re-authenticate. The default time interval is 3600 seconds.
Max Request	This is the maximum times that the ICRL-M allows a client request.
Guest VLAN	The permitted range for this field is 0 to 4094. If this field is set to 0, that means the port is blocked after an authentication failure. Otherwise, the port is set to Guest VLAN.
Host Mode	If there is more than one device connected to this port, set the Host Mode to Single , which means only the first PC to authenticate successfully can access this port. If this port is set to Multi , all of the devices can access this port once any one of them passes the authentication.
Admin Control Direction	Use this to determine which devices can only send data or both send and receive data.
Apply	Click Apply to apply the settings.
Initialize Selected	Click to set the authorization state of the selected port to initialize status.
Reauthenticate Selected	Click to send an EAP Request to the requestor to request reauthentication.
Default Selected	Click to reset the configurable IEEE 802.1x parameters of selected port to the default values.
802.1x Timeout Configuration	
Re-Auth Period(s)	Controls the re-authentication time interval (seconds), you can enter a range of 1 - 65535.
Quiet Period(s)	When authentication fails, the ICRL-M waits for a period and then tries to communicate with the RADIUS server again.
Tx Period(s)	The time interval of the authentication request.
Supplicant Timeout(s)	The timeout for the client authentication.
Sever Timeout(s)	The timeout for the server response for authentication.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.10.5. 802.1X Port Information

Use the *802.1X Port Information* page to observe the port status for **Port Control Status**, **Authorize Status**, **Authorized Supplicant**, and **Oper Control Direction** for each port.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
 - Filters
 - IP Filter
 - MAC Filter
 - ARP Filter
 - Filter Attach
 - Port Security
 - 802.1X
 - 802.1X Configuration
 - 802.1X Port Configuration
 - 802.1X Port Information
 - DHCP Snooping
 - DHCP Binding
 - IP Source Guard
 - Dynamic ARP Inspection
 - Dynamic ARP Inspection Status
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

802.1X Port Information Help

Port	Port Control	MAB	Port Status	Supplicant MAC Address	Oper Control Direction
1	Force Authorized	Disable	Authorized	NONE	Both
2	Force Authorized	Disable	Authorized	NONE	Both
3	Force Authorized	Disable	Authorized	NONE	Both
4	Force Authorized	Disable	Authorized	NONE	Both
5	Force Authorized	Disable	Authorized	NONE	Both
6	Force Authorized	Disable	Authorized	NONE	Both
7	Force Authorized	Disable	Authorized	NONE	Both
8	Force Authorized	Disable	Authorized	NONE	Both
9	Force Authorized	Disable	Authorized	NONE	Both
10	Force Authorized	Disable	Authorized	NONE	Both
11	Force Authorized	Disable	Authorized	NONE	Both
12	Force Authorized	Disable	Authorized	NONE	Both

Reload

802.1X Port Information Page	
Port	The port identifier.
Port Control	Force Authorized means that this port is Authorized and the data is free to travel in and out. Force unauthorized is just the opposite and the port is blocked.
Authorized Status	The authorize status of the port.
Authorized Supplicant	The MAC address of the authorized supplicant.
Oper Control Direction	Whether an unauthenticated port disables income and outgoing traffic or only incoming traffic. Both means income and outgoing traffic are blocked. In means incoming traffic is blocked.
Reload	Click Reload to reload 802.1X port status

4.10.6. DHCP Snooping

DHCP Snooping is a series of techniques applied to the security of an existing DHCP network . With the DHCP Snooping feature, the DHCP Server manages the network access and permits the access with specific IP and specific MAC address from a specific ICRL-M port that can access the network. It also provides the protection to avoid the intruder-added fake DHCP server into a secure network that tries to take over the DHCP process. Once the ICRL-M detects the phenomena, the port that the intruder connected to will be locked to protect network access.

Note: DHCP snooping provides a valuable security function and is required to support IP Source Guard.

PEPPERL+FUCHS ROCKETLINX

DHCP Snooping [Help](#)

DHCP Snooping ▾

MAC Verify ▾

VLAN ID	DHCP Snooping
1	<input type="button" value="Disable"/> ▾
2	<input type="button" value="Disable"/> ▾
3	<input type="button" value="Disable"/> ▾

Note- Before setting VLAN Snooping, you should enable DHCP Snooping first

DHCP Snooping Statistics

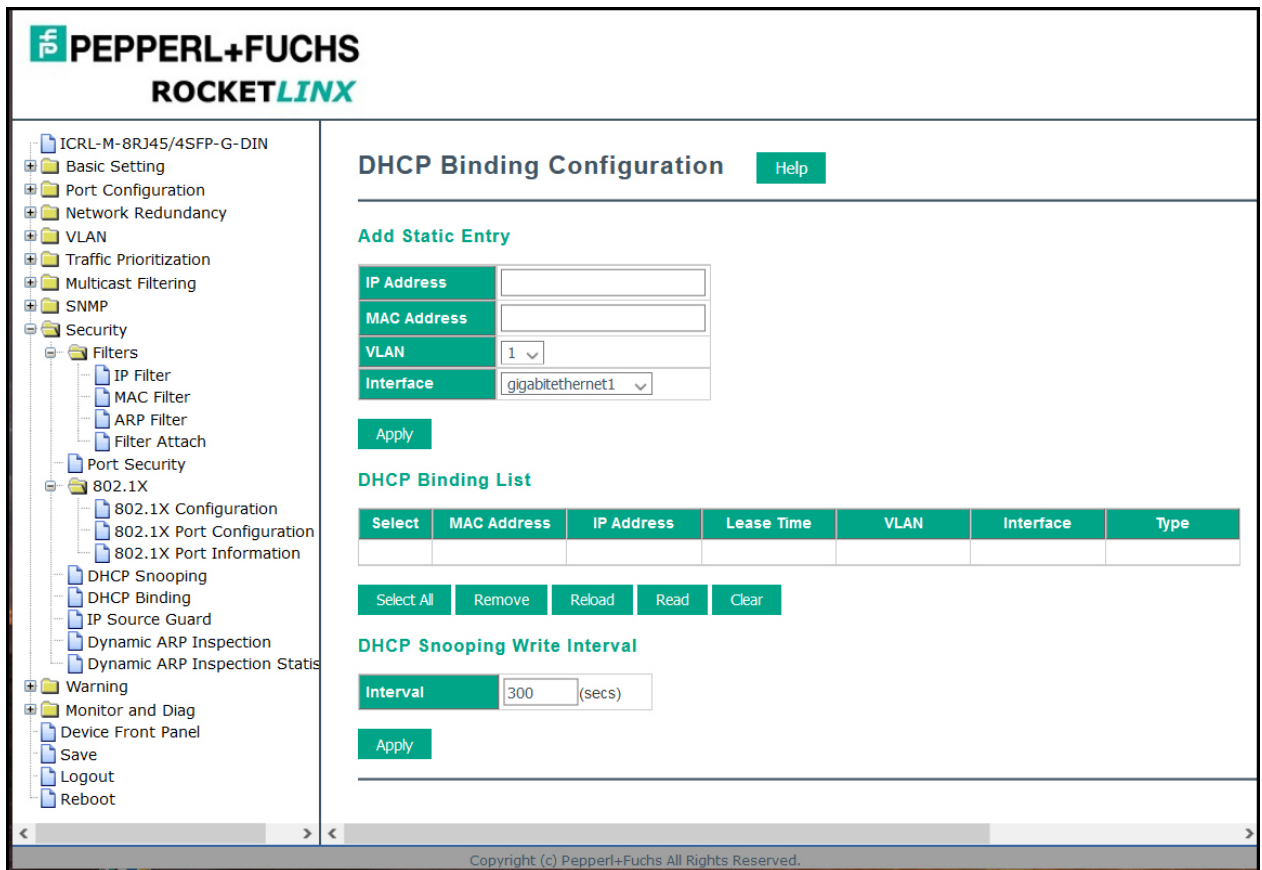
Drop Type	Drop Packets
Total received	0
Dropped (MAC verification failed)	0
Dropped (Interface invalid)	0
Dropped (Binding not matched)	0
Dropped (Relay Agent address error)	0
Dropped (Total dropped)	0

Copyright (c) Pepperl+Fuchs All Rights Reserved.

DHCP Snooping Page	
DHCP Snooping	Enables/Disables DHCP snooping globally.
MAC Verify	Enables/Disables MAC Verify globally. If this option is enabled, the Layer 2 DHCP Snooping module will verify the source MAC address against the client hardware address in the received DHCP packets.
Apply	Click the Apply button to apply the configurations.
DHCP Snooping Statistics	
Total received	The number of snooping packets which is received.
MAC verification failed	The number of MAC verification failed packets.
Interface invalid	Request packet is not matched to it's interface.
Binding not matched	Counts the packets which the binding is not matched.
Relay Agent address error	Counts the relay agent address error packets.
Total dropped	The number of snooping packets which is dropped.
Clear	Click the Clear button to clear the drop-packet count.
Reload	Click the Reload button to refresh the drop-packet count.

4.10.7. DHCP Binding Configuration

DHCP Binding Configuration shows the snooping binding table. In addition, you can add a static entry.



DHCP Binding Configuration Page	
Add Static Entry	
IP Address	IP of the entry.
MAC Address	MAC of the entry.
VLAN	VLAN of the entry.
Interface	Interface of the entry.
Apply	Click the Apply button to add a static entry.
DHCP Binding List	
MAC Address	Shows the MAC of the entry.
IP Address	Shows the IP of the entry.
Lease Time	The Lease time of the entry.
VLAN	The entry belong VLAN's ID.
Interface	Interface of the entry.
Type	The entry entry type: Static/Dynamic.
Select All	Click the Select All button to select all the entries.

4/21/20

DHCP Binding Configuration Page (Continued)	
Remove	Click the Remove button to remove the selected entries.
Reload	Click the Reload button to load the temporary entries.
Read	Click the Read button to load the entries of DHCP binding database.
Clear	Click the Clear button to clear all entries and binding database.
DHCP Snooping Write Interval:	
Interval	Writes the current binding table to system. (secs.)
Apply	Click the Apply button to apply change write interval.

4.10.8. IP Source Guard

IP Source Guard is a security feature that restricts IP traffic on an untrusted switch Layer 2 port by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
 - Filters
 - IP Filter
 - MAC Filter
 - ARP Filter
 - Filter Attach
 - Port Security
 - 802.1X
 - 802.1X Configuration
 - 802.1X Port Configuration
 - 802.1X Port Information
 - DHCP Snooping
 - DHCP Binding
 - IP Source Guard
 - Dynamic ARP Inspection
 - Dynamic ARP Inspection Status
- Warning
- Monitor and Diag
 - Device Front Panel
 - Save
 - Logout
 - Reboot

IP Source Guard Help

IP Source Guard Configuration

Port	Trust	IP Source Guard	Packet-discarded
1	Trust	Disable	0
2	Trust	Disable	0
3	Trust	Disable	0
4	Trust	Disable	0
5	Trust	Disable	0
6	Trust	Disable	0
7	Trust	Disable	0
8	Trust	Disable	0
9	Trust	Disable	0
10	Trust	Disable	0
11	Trust	Disable	0
12	Trust	Disable	0

Apply Clear Packet-discarded Reload

Check Period

Check period (mins)

Apply

Copyright (c) Pepperl+Fuchs All Rights Reserved.

IP Source Guard Page	
IP Source Guard Configuration	
Trust	Enables/Disable Trust on each Port.
IP Source Guard	Configure the interface as Enables IPSPG or Disables IPSPG. If IP source guard is enabled on a interface, incoming IP traffic on an interface are allowed when there is a matching entry in IP source binding database. Else, all incoming IP traffic on an interface are allowed irrespective of the IP binding database.
Packet-discarded	Shows discard packets for each port.
Apply	Click the Apply button to apply the configurations.
Clear Packet-discarded	Click the Clear Packet-discarded button to clear packet discarded count.
Check Period	
Check Period	The timer for update discard-packet. It will calculate and accumulate to discard-packet in the duration.
Apply	Click the Apply button to apply the Check Period configurations.

4.10.9. Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that prevents ARP attack. The ICRL-M receives one ARP packet on an untrusted port, the ICRL-M compares the IP-to-MAC address binding with entries from the DHCP Snooping database or ARP access-lists. If there is no match, the ARP packet will be dropped by the ICRL-M to ensure network performance.

Dynamic ARP Inspection Help

VLAN Configuration

VLAN	Configuration	Operation	Gateway Verify	Gateway IP	ACL-Match
1	Disable	Inactive	Disable	0.0.0.0	
2	Disable	Inactive	Disable	0.0.0.0	
3	Disable	Inactive	Disable	0.0.0.0	

Apply

Interface Configuration

Port	Trust	pps
1	Untrusted	15
2	Untrusted	15
3	Untrusted	15
4	Untrusted	15
5	Untrusted	15
6	Untrusted	15
7	Untrusted	15
8	Untrusted	15
9	Untrusted	15
10	Untrusted	15
11	Untrusted	15
12	Untrusted	15

Apply

Check Period

Check period: (mins)

Apply

Copyright (c) Pepper+Fuchs All Rights Reserved.

Dynamic ARP Inspection Page	
VLAN Configuration	
VLAN	Shows the VLAN index.
Configuration	Enable or disable DAI for each VLAN.
Operation	Shows the DAI operation state.
Gateway Verify	Enable/disable verify Gateway .
Gateway IP	Gateway IP address .
ACL-Match	Select the one of the ARP filter rule, the blank blank column is not to set the APR rule.
Interface Configuration	
Trust	Set Trust or Untrust for DAI for each port.
pps	Packet per second.
Apply	Click the Apply button to apply change configuration.
Check Period	
Check Period	The timer for update discard-packet. It will calculate and accumulate to discard-packet in the duration.
Apply	Click the Apply button to apply the Check Period configurations.

4.10.10. Dynamic ARP Inspection Status

This page displays DAI statistics for the specified VLAN and port.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
 - Filters
 - IP Filter
 - MAC Filter
 - ARP Filter
 - Filter Attach
 - Port Security
 - 802.1X
 - 802.1X Configuration
 - 802.1X Port Configuration
 - 802.1X Port Information
 - DHCP Snooping
 - DHCP Binding
 - IP Source Guard
 - Dynamic ARP Inspection
 - Dynamic ARP Inspection Status
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout
- Reboot

Dynamic ARP Inspection Statistics Help

Interface Statistics

Port	Received	Forwarded	Dropped	Invalid IP	Mismatch MAC	DHCP Dropped	Invalid GW IP	Invalid Opcode	Mismatch Src Port	No Dst Port	ACL Dropped
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0

Clear Statistics Reload

VLAN Statistics

VLAN	Forwarded	Dropped	DHCP Dropped	ACL Dropped	DHCP Permits	ACL Permits	Source MAC Dropped	Destination MAC Dropped	Invalid IP
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0

Clear Statistics Reload

Copyright (c) Pepperl+Fuchs All Rights Reserved.

Dynamic ARP Inspection Statistics Page	
Interface statistics	
Port	This is the port identifier.
Received	The count of ARP packet received.
Forwarded	The count of ARP packet forwarded.
Dropped	The count of ARP packet dropped.
Invalid IP	The count of packet mismatch target IP address on DHCP binding table.
Mismatch MAC	The count of source MAC address of Ethernet header not same as sender MAC address.
DHCP Dropped	The count of ARP packet dropped by DHCP binding table mismatch.
Invalid GW IP	The count of invalid gateway IP address.
Invalid Opcode	The count of invalid opcode received .
Mismatch Src Port	The count of source port mismatch on DHCP binding table.

4/21/20

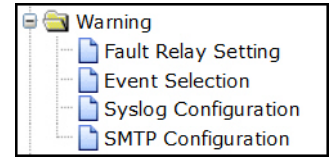
Dynamic ARP Inspection Statistics Page (Continued)	
No Dst Port	The count of packet dropped by destination port not found.
ACL Dropped	The count of ARP packet dropped by ACL setting.
Clear	Click the Clear Statistics button to clear the interface statistics.
Reload	Click the Reload button to reload the statistics.
VLAN statistics	
VLAN	This is the VLAN identifier.
Forwarded	The count of ARP packet forwarded.
Dropped	The count of ARP packet dropped.
DHCP Dropped	The count of ARP packet dropped by DHCP binding table mismatch.
ACL Dropped	The count of ARP packet dropped by ACL setting.
DHCP Permits	The count of ARP packet permits by DHCP binding table.
ACL Permits	The count of ARP packet permits by ACL setting.
Src MAC Dropped	The count of source MAC address of Ethernet header not same as sender MAC address.
Dest MAC Dropped	The count of ARP packet dropped by mismatch destination MAC address.
Invalid IP	The count of packet mismatch target IP address on DHCP binding table.
Clear Statistics	Click the Clear Statistics button to clear the VLAN statistics.
Reload	Click the Reload button to reload the statistics.

4.11. Warning

The ICRL-M provides several types of warning features for you to remotely monitor the status of the attached devices or changes in your network. The features include Fault Relay, System Log, and SMTP Email Alert.

The following web pages are included in this group:

- *Fault Relay*
- *Event Selection* on Page 142
- *SysLog Configuration* on Page 144
- *SMTP Configuration* on Page 145



Optionally, you can use the CLI for configuration, see *Warnings (CLI)* on Page 211.

4.11.1. Fault Relay

The ICRL-M provides one alarm relay output (DO) that can support multiple fault conditions. The relay contacts are energized (open) for normal operation and close under fault conditions. The fault conditions include power failure, Ethernet port link faults, Ring topology changes, Ping failures, DI state changes or ping remote IP address failure.

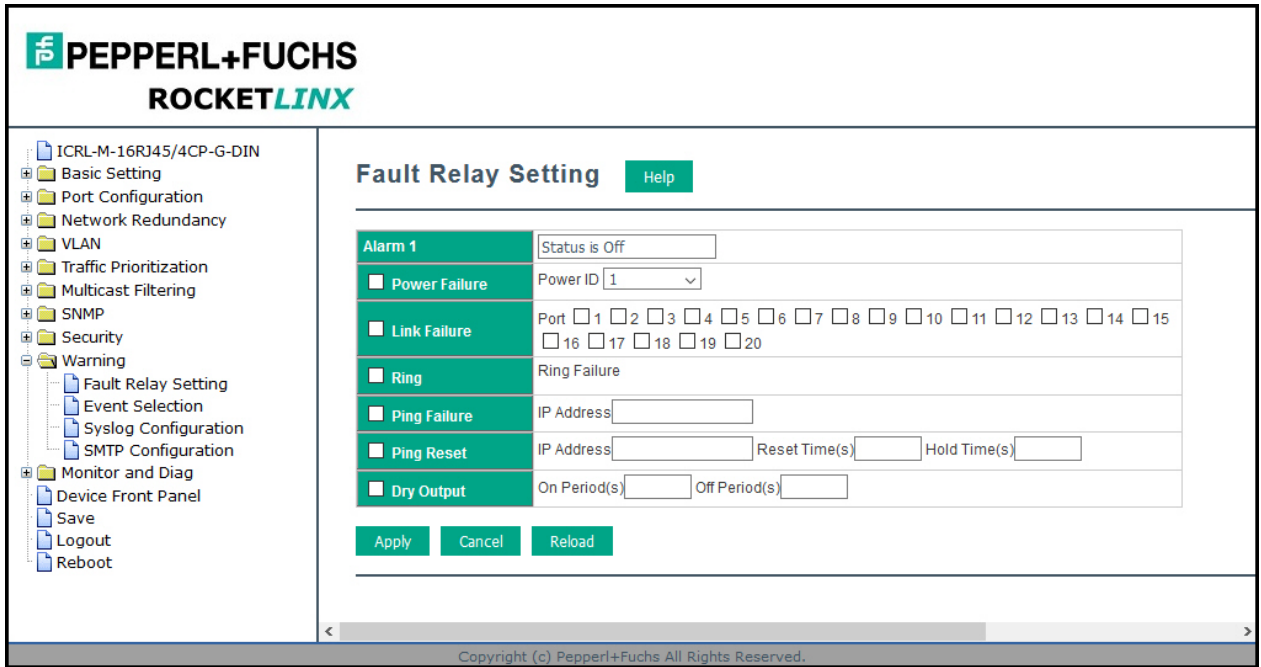
PEPPERL+FUCHS ROCKETLINX

Fault Relay Setting Help

Alarm 1	Status is Off
<input type="checkbox"/> Power Failure	Power ID <input type="text" value="1"/>
<input type="checkbox"/> Link Failure	Port <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12
<input type="checkbox"/> Ring	Ring Failure
<input type="checkbox"/> Ping Failure	IP Address <input type="text"/>
<input type="checkbox"/> Ping Reset	IP Address <input type="text"/> Reset Time(s) <input type="text"/> Hold Time(s) <input type="text"/>
<input type="checkbox"/> Dry Output	On Period(s) <input type="text"/> Off Period(s) <input type="text"/>
<input type="checkbox"/> DI State	DI ID <input type="text" value="1"/> DI State <input type="text" value="Low"/>

Apply Cancel Reload

Copyright (c) Pepperl+Fuchs All Rights Reserved.



The following table describes Fault Relay conditions.

Fault Relay Page	
Alarm 1	This displays whether the alarm status is on or off. You must select a fault relay option and click Apply for the status to display as on.
Power Failure	Detects power input status on the selected power source or sources.
Link Failure	Monitors port link down events for the selected ports.
Ring	Monitors ring topology changes.
Ping Failure	If the target IP address does not reply to the ping request, the fault relay is enabled.
Ping Reset	<p>Pings target device and triggers the relay to emulate to emulate a power reset on the remote device if the remote system crashes.</p> <ul style="list-style-type: none"> IP Address: Remote device IP address whose power wiring is connected with relay output. Reset Time (Sec): Duration that the relay contact is opened to emulate the power switch is off. After the reset time, the relay closes to emulate that the power switch is on. Hold Time (Sec): Boot time that the remote device requires. After the relay contact closes the ICRL-M starts pinging after the hold time.
Dry Output	<p>The relay continuously opens and closes the contacts. The available range is 0-65535 seconds.</p> <p>Note: Do not use this function with any other event.</p> <ul style="list-style-type: none"> On Period: Duration of the relay output short (closed). Off Period: Duration of the relay output open.

Fault Relay Page (Continued)	
DI State (ICRL-M-8RJ45/4SFP-G-DIN)	Relay triggered when DI changes state to high or low.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.11.2. Event Selection

Event Types can be divided into two basic groups: System Events and Port Events. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of specific ports.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
 - Fault Relay Setting
 - Event Selection
 - Syslog Configuration
 - SMTP Configuration
- Monitor and Diag
 - Device Front Panel
 - Save
 - Logout
 - Reboot

Event Selection Help

System Event Selection

- Device Cold Start
- Authentication Failure
- Power 1 Failure
- Fault Relay 1
- DI 1 Change
- Ring Event
- SFP Event
- DHCP Snooping Event
- DAI Event
- Device Warm Start
- Time Synchronization Failure
- Power 2 Failure
- IPSPG Event

Port Event Selection

Port	Link State
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable
11	Disable
12	Disable

Port Security Selection

Port	Security
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable
11	Disable
12	Disable

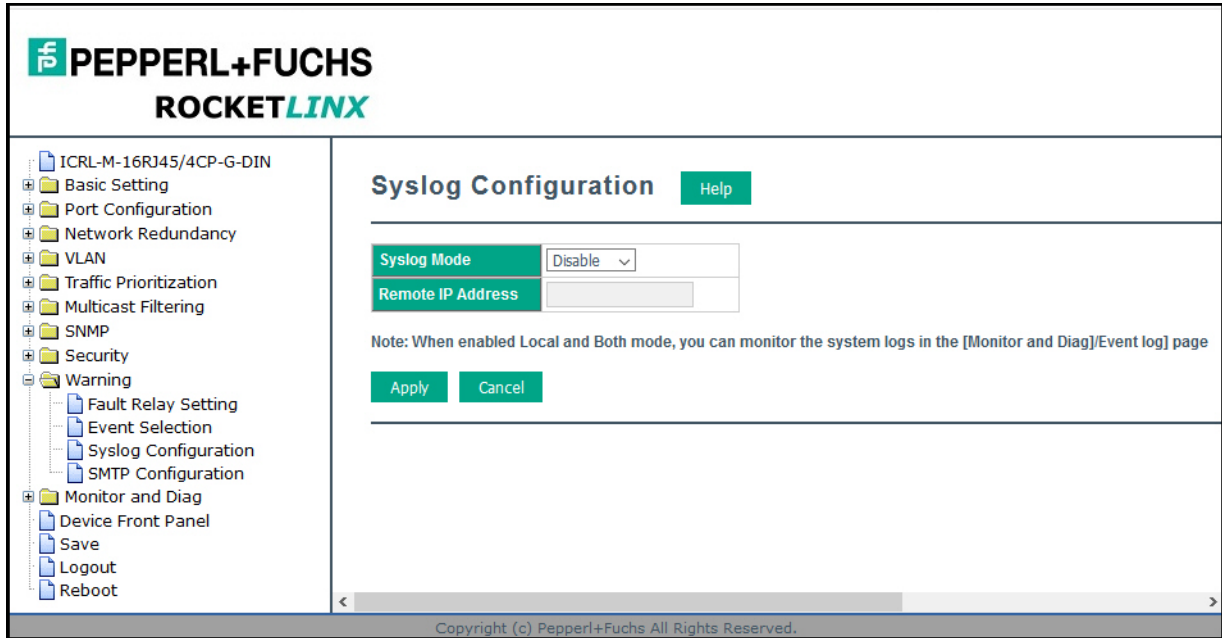
Apply Cancel

Copyright (c) Pepperl+Fuchs All Rights Reserved.

Event Selection Page	
System Event Selection	Warning is sent when....
Device Cold Start	Power is cut off and then reconnected.
Device Warm Start	Reboot the device by CLI or web user interface.
Authentication failure	An incorrect password or SNMP Community String is entered.
Time Synchronize Failure	Accessing the NTP Server is failing.
Power 1 Failure	PW1 power failure.
Power 2 Failure	PW2 power failure.
Fault Relay 1	A Fault Relay has occurred.
DI 1 Change	The Digital Input#1 status has changed.
Ring Event	A ring event has occurred.
SFP Event	The information read from the DDM SFP transceiver is over temperature or out the range of TX/RX power.
DHCP Snooping Event	When selected, the switch generates a notification if the state of an DHCP Snooping changes.
DAI Event	When selected, the switch generates a notification if the state of an DAI statistics changes.
IPSG Event	When selected, the switch generates a notification if the state of an IPSG statistics changes.
Port Event Selection	Warning is sent when.....
Link-Up	The port is connected to another device.
Link-Down	The port is disconnected. For example, the cable is pulled out or the opposing devices is down.
Both	The link status changed.
Port Security Selection	Warning is sent when.....
Port	The associated port number.
Security	Select Disable or Enable to generate a Port Security event, when this event occurs, the switch sends notification.
Both	The link status changed.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.11.3. SysLog Configuration

The *System Log* page provides the system administrator ICRL-M events history. There are two System Log modes provided by the ICRL-M, **Local** mode and **Remote** mode.

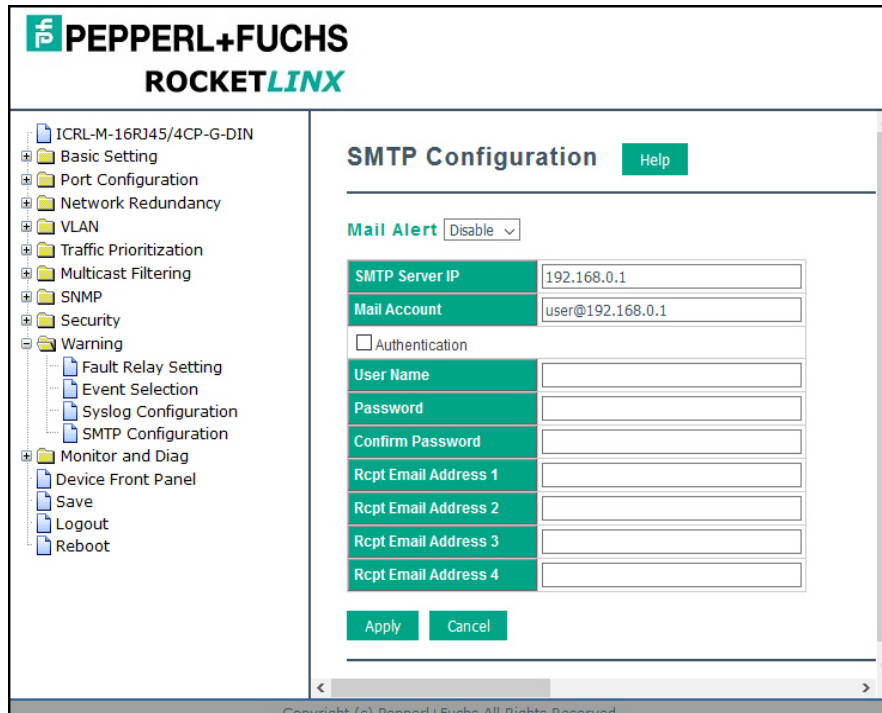


Warning - SysLog Configuration Page	
Syslog Mode	<p>There are two system logs available:</p> <ul style="list-style-type: none"> Local Mode: The ICRL-M prints the events that have been selected in the Event Selection page to the System Log table of the ICRL-M. You can monitor the system logs in the <i>Monitor and Diag /Event Log</i> page. Remote Mode: Assign the IP address of the System Log server. The ICRL-M sends the events that occurred in the selected in <i>Event Selection</i> page to System Log server that you assign. Both: This enables both Local and Remote modes.
Remote IP Address	The IP address of the System log server.
Apply	<p>Click Apply to apply the settings.</p> <p>Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.</p>

When enabling **Local** or **Both** modes, you can monitor the system logs in the *Monitor and Diag /Event Log* page.

4.11.4. SMTP Configuration

The ICRL-M supports an email alert feature. The ICRL-M sends the events that have occurred to a remote email server. The email warning conforms to the SMTP standard. The *E-mail Alert* page allows you to assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If the SMTP server requests authentication, you can set up the user name and password.



SMTP Configuration Page	
SMTP Server IP Address	Enter the IP address of the email server.
Mail Account	The mail account for the SMTP server.
Authentication	Click the check box to enable password.
User Name	Enter an email account name (maximum 40 characters).
Password	Enter the password of the email account.
Confirm Password	Re-type the password of the email account.
<i>You can set up to 4 email addresses to receive email alarm from the ICRL-M.</i>	
Rcpt E-mail Address 1	The first email address to receive an email alert from the ICRL-M (maximum 40 characters).
Rcpt E-mail Address 2	The second email address to receive an email alert from the ICRL-M (maximum 40 characters).
Rcpt E-mail Address 3	The third email address to receive an email alert from the ICRL-M (maximum 40 characters).
Rcpt E-mail Address 4	The fourth email address to receive an email alert from the ICRL-M (maximum 40 characters).
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

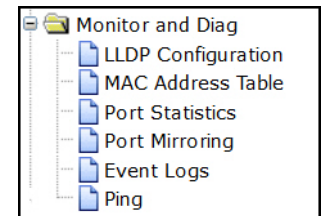
4/21/20

4.12. Monitor and Diag

The ICRL-M provides several web user interface pages for you to monitor the status of the switch or diagnostics when encountering problems related to the ICRL-M. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log, and Ping.

The following web pages are included in this group:

- *LLDP Configuration* on Page 146
- *MAC Address Table*
- *Port Statistics* on Page 150
- *Port Mirroring* on Page 151
- *Event Logs* on Page 152
- *Ping* on Page 153



Optionally, you can use the CLI for configuration, see *Monitor and Diag (CLI)* on Page 214.

4.12.1. LLDP Configuration

The ICRL-M supports topology discovery using LLDP (IEEE 802.1AB Link Layer Discovery Protocol). LLDP allows network devices to advertise their identities and capabilities to other devices on the same network segment.

LLDP allows network monitoring systems to learn the network topology and display information about managed switches such as port descriptions and VLAN IDs. .

PEPPERL+FUCHS ROCKETLINX

ICRL-M-16RJ45/4CP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
 - Fault Relay Setting
 - Event Selection
 - Syslog Configuration
 - SMTP Configuration
- Monitor and Diag
 - LLDP Configuration
 - MAC Address Table
 - Port Statistics
 - Port Mirroring
 - Event Logs
 - Ping
- Device Front Panel
- Save
- Logout
- Reboot

LLDP Configuration Help

LLDP Disable ▾

LLDP Timer

LLDP Hold Time

Apply Cancel

LLDP Port State

Local Port	Neighbor ID	Neighbor IP	Neighbor VID

Reload

Copyright (c) Pepperl+Fuchs All Rights Reserved.

LLDP Configuration Page	
LLDP Configuration	
LLDP	Select Enable/Disable to enable/disable LLDP function.
LLDP timer	This is the interval time of each LLDP in seconds; valid values are from 5 to 254. The default is seconds when LLDP is enabled.
LLDP hold time	The Time to Live (TTL) timer. The LLDP state expires when the LLDP is not received by the hold time. The default is 120 seconds when LLDP is enabled. and the range is from 10 to 255.
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.
LLDP Port State	
Local Port	The current port number that linked with neighbor network device.
Neighbor ID	The MAC address of neighbor device on the same network segment.
Neighbor IP	The IP address of neighbor device on the same network segment.
Neighbor VID	The VLAN ID of neighbor device on the same network segment.
Reload	Click Reload to reload the LLDP Port State Table.

4.12.2. MAC Address Table

The ICRL-M provides 16K entries in the *MAC Address Table*. You can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports.

PEPPERL+FUCHS ROCKETLINX

ICRL-M-8RJ45/4SFP-G-DIN

- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
 - LLDP Configuration
 - MAC Address Table
 - Port Statistics
 - Port Mirroring
 - Event Logs
 - Ping
- Device Front Panel
- Save
- Logout
- Reboot

MAC Address Table Help

Aging Time(secs) Apply

Static Unicast MAC Address

MAC Address	VID	Port
<input type="text"/>	<input type="text"/>	Port 1 <input type="button" value="v"/>

Add

Static Multicast MAC Address

Multicast MAC Address	VID	Port
<input type="text"/>	<input type="text"/>	Port 1 <input type="button" value="v"/>

Add

MAC Address Table All

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/> 00c0.4e5e.0003	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e5b.0001	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e54.0079	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e38.0002	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e32.0422	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e5f.0068	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e21.05cd	Dynamic Unicast	1	V											
<input type="checkbox"/> 0030.18a7.85c2	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e5c.000b	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e40.005d	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e3a.000d	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e29.fff5	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e6c.0030	Dynamic Unicast	1	V											
<input type="checkbox"/> 000d.8109.fde5	Dynamic Unicast	1											V	
<input type="checkbox"/> 00c0.4e39.010c	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e51.ffff	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e36.0002	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e59.ffd5	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e69.0001	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e38.0067	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e07.ffff	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e17.ffff	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e15.047a	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e35.0009	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e3c.0002	Dynamic Unicast	1	V											
<input type="checkbox"/> 0025.6439.26b4	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e40.0098	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e1c.ffff	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e48.0569	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e07.4384	Dynamic Unicast	1	V											
<input type="checkbox"/> 00c0.4e42.fff8	Dynamic Unicast	1	V											

Remove Reload

MAC Address Table Page	
Aging Time (Sec)	<p>Each switch fabric has a size limit to write the learned MAC address. To save more entries for a new MAC address, the switch fabric ages out a non-used MAC address entry per the Aging Time timeout.</p> <p>This value determines the interval that an automatically learned MAC address entry remains valid in the forwarding database, since its last access as a source address, before being purged. The value should be increments of 15 in seconds.</p> <p>The minimum age time is 15 seconds. The maximum age time is 3825 seconds or almost 64 minutes. The default Aging Time is 300 seconds.</p> <p>If the value is set to 0, the aging function is disabled and all learned addresses remain in the database forever.</p>
Static Unicast MAC Address	<p>Some applications may require that you type in the static Unicast MAC address to its MAC address table. Type the MAC address (format: xxxx.xxxx.xxxx), select its VID, and Port ID, and then click Add to add it to MAC Address Table.</p>
Static Multicast MAC Address	<p>This section allows you to manually add multicast MAC addresses to the FIB. Manually entered addresses do not expire like automatically learned addresses do.</p> <ul style="list-style-type: none"> • Multicast MAC Address: The multicast MAC address you want to manually enter into the FIB. • VID: The VLAN you want to add the MAC address to. • Port: The port you want the MAC address to be associated with. <p>Click the Add button to add the static multicast MAC address to the FIB.</p>
MAC Address Table	<p>This displays all the MAC addresses learned by the switch fabric.</p> <p>The packet types include Management Unicast, Static Unicast, Dynamic Unicast, Static Multicast, and Dynamic Multicast.</p> <p>The table allows you to sort the address by the packet types and port.</p>
Address Types	<ul style="list-style-type: none"> • Management Unicast means the MAC address of the switch. It belongs only to the CPU port. • Static Unicast MAC addresses can be added and deleted. • Dynamic Unicast MAC is a MAC address learnt by the switch Fabric. • Static Multicast can be added by the CLI and can be deleted using the web user interface and CLI. • Dynamic Multicast appears after you enabled IGMP and the switch learnt IGMP report. • Management Multicast - multicast address that is configured for management purposes, such as GVRP and so on. Management entries are read-only. <p>Dynamic and static entries can be removed.</p>
Remove	<p>Click to remove the static Unicast/Multicast MAC address.</p>
Reload	<p>Click to reload to refresh the table. The new learnt Unicast/Multicast MAC address are updated in the <i>MAC Address Table</i>.</p>
Apply	<p>Click Apply to apply the settings.</p> <p>Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.</p>

4.12.3. Port Statistics

Use this page to view operation statistics for each port. The statistics that can be viewed include **Link Type**, **Link State**, **Rx Good**, **Rx Bad**, **Rx Abort**, **Tx Good**, **Tx Bad** and **Collisions**.

Note: If you see an increase of Bad, Abort or Collision counts, that may mean the network cable is not properly connected or the network performance of the port is poor. Check your network cable, the network interface card of the connected device, the network application, or reallocate the network traffic.

The following information provides a view of the current port statistic information.

Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
1	100	Connected	Enable	72292276	0	64463	38098841	0	0
2	0	Disconnected	Enable	0	0	0	0	0	0
3	0	Disconnected	Enable	0	0	0	0	0	0
4	0	Disconnected	Enable	0	0	0	0	0	0
5	0	Disconnected	Enable	0	0	0	0	0	0
6	0	Disconnected	Enable	0	0	0	0	0	0
7	0	Disconnected	Enable	0	0	0	0	0	0
8	0	Disconnected	Enable	0	0	0	0	0	0
9	0	Disconnected	Enable	0	0	0	0	0	0
10	0	Disconnected	Enable	0	0	0	0	0	0
11	1000	Connected	Enable	6466529	0	0	61929625	0	0
12	0	Disconnected	Enable	0	0	0	0	0	0

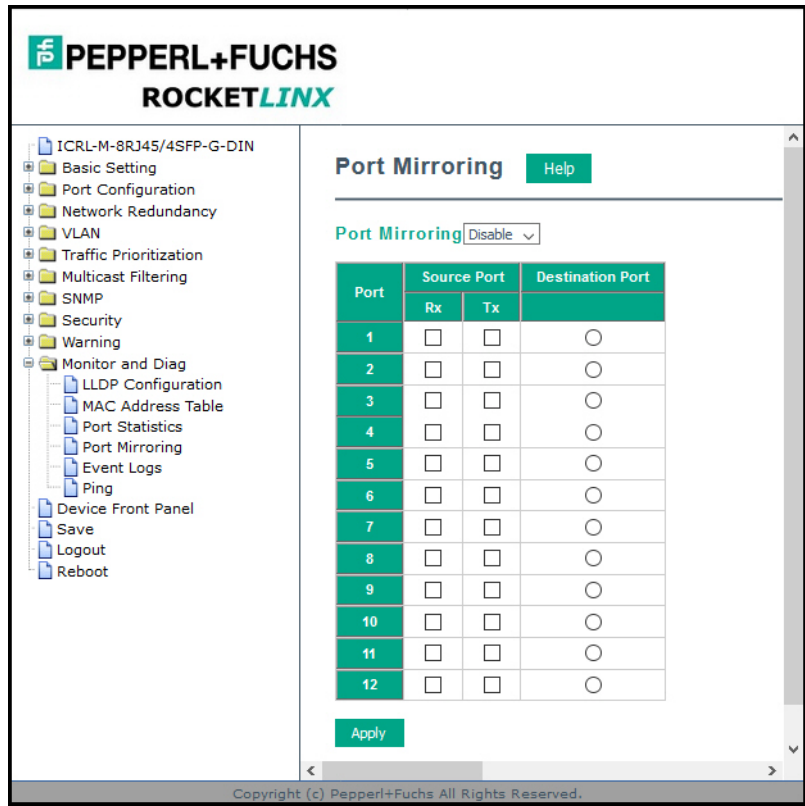
Port Statistics Page	
Type	Indicates the port type.
Link	Indicates the link status; Up or Down .
State	Indicates the link state; Enable or Disable .
Rx Good	The count of good frames received, which is the total number of received unicast, broadcast, multicast, and pause frames.
Rx Bad	The count of bad frames received, which is the total number of undersized, fragments, oversized, jabber, receive errors (RxErr), and frame check sequence errors (FCSErr) frames.
Rx Abort	The count of abort frames received, which is the total number of discarded and filtered frames.
Tx Good	The count of good frames transmitted, which is the total number of transmitted unicast, broadcast, multicast and pause frames.
Tx Bad	The count of FCSErr frames transmitted.
Collision	The count of collision frames, including single, multiple, excessive, and late collisions frames.
Clear Selected	Click to clear selected port counts.

4/21/20

Port Statistics Page (Continued)	
Clear All	Click to clear all counts.
Reload	Click to reload all counts.

4.12.4. Port Mirroring

Port mirroring (also called *port spanning*) is a tool that allows you to mirror the traffic from one or more ports onto another port, without disrupting the flow of traffic on the original port. Any traffic that goes into or out of the **Source Ports** is duplicated at the **Destination Ports**. This traffic can then be analyzed at the Destination Port using a monitoring device or application. The network administrator typically utilizes this tool for diagnostics, debugging, or fending off attacks.



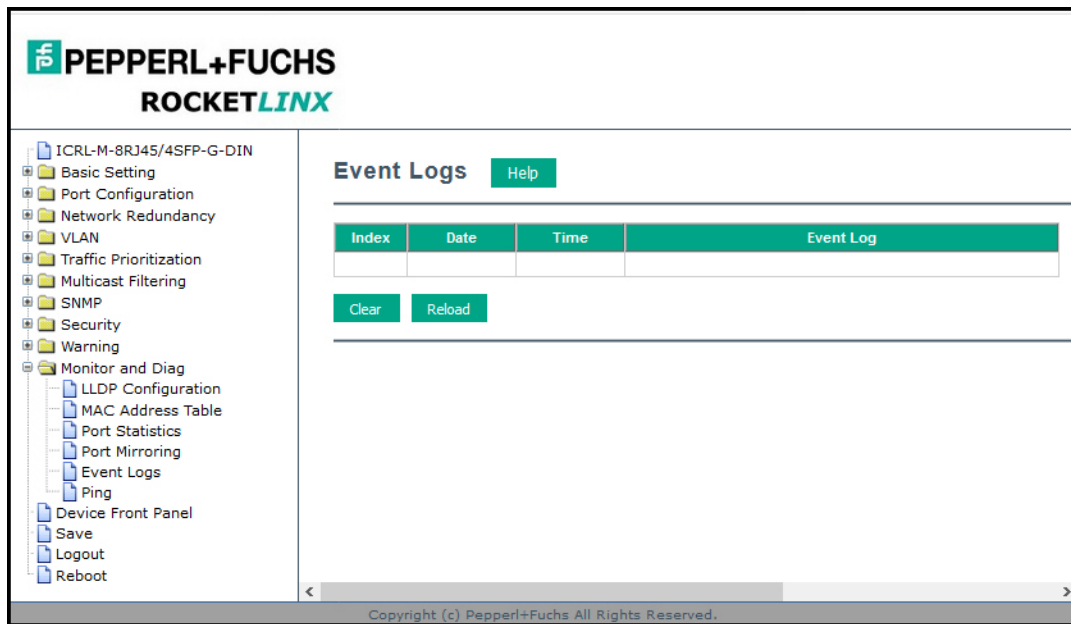
Port Mirroring Mode Page	
Port Mirror Mode	Select Enable or Disable to enable/disable port mirroring.
Source Port	This is also known as <i>Monitor Port</i> . These are the ports that you want to monitor. The traffic of all source/monitor ports is copied to destination/analysis ports. You can choose a single port, or any combination of ports, but you can only monitor them in Rx or TX only. Click the check box of the Port ID , Rx , Tx or both to select the source ports.
Destination Port	This is also known as <i>Analysis Port</i> . You can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port or ports being monitored. Only one RX/TX of the destination port can be selected. The network administrator typically connects a LAN analyzer or Netxray device to this port.

4/21/20

Port Mirroring Mode Page (Continued)	
Apply	Click Apply to apply the settings. Note: You must Save the settings (Page 156), if you want to maintain these settings if the ICRL-M is powered off.

4.12.5. Event Logs

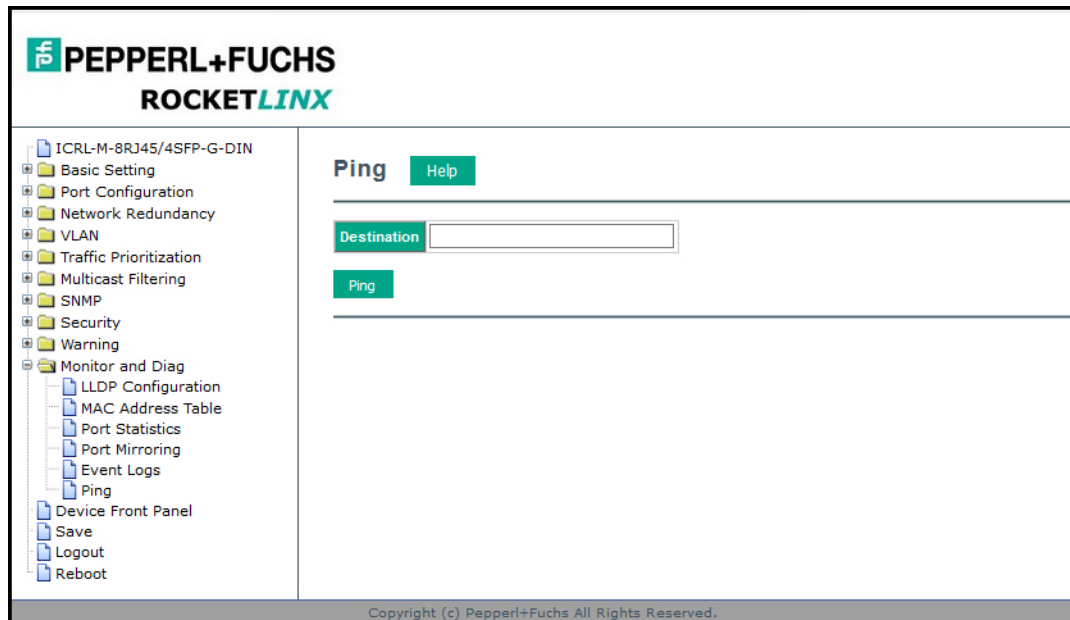
The System Log feature was introduced in *SysLog Configuration* on Page 144. When **System Log Local** mode is selected, the ICRL-M records events that occurred in the local log table. This page shows the log table. The entry includes the index, occurred data and time, and content of the events.



Click **Clear** to clear the entries. Click **Reload** to refresh the table.

4.12.6. Ping

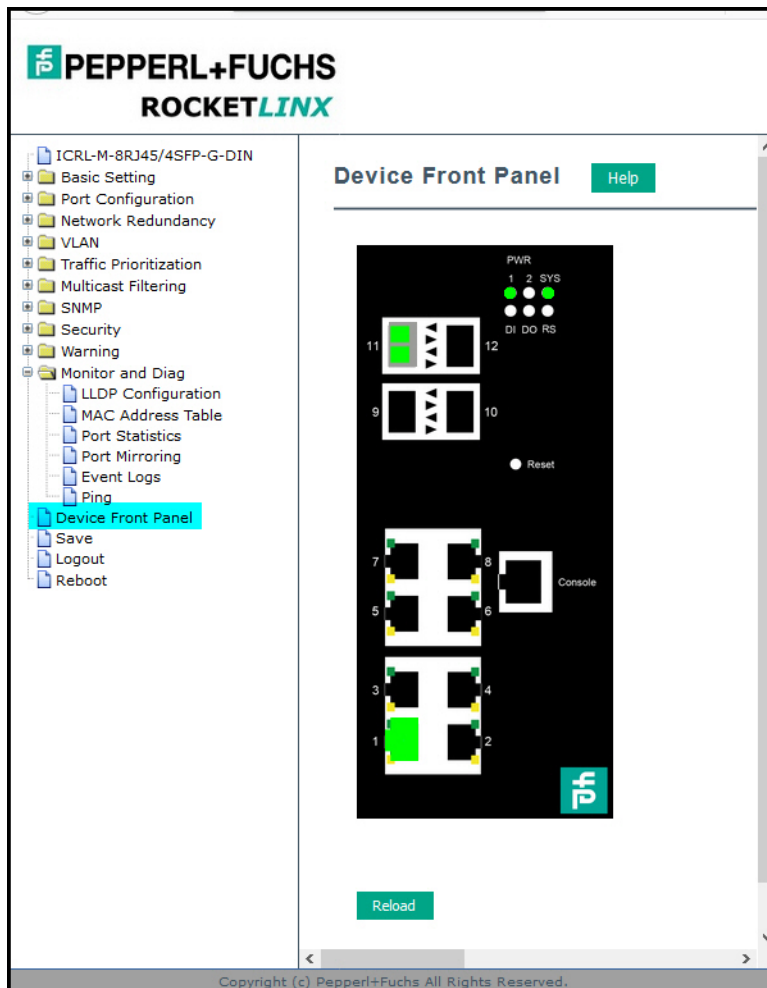
This page provides a **Ping Utility** to ping a remote device and check whether the device is alive or not. Type the **Target IP** address of the target device and click **Start** to start the ping.



After few seconds, you can see the result in the **Result** field.

4.13. Device Front Panel

The **Device Front Panel** allows you to see the LED status of the ICRL-M.



Note: There is not a CLI command for this feature. If you can view the physical LEDs, you can use the LED Descriptions on Page 17, which provide detailed LED information. If you need to locate your ICRL-M in a rack, you can use the LED Tracker feature in PortVision DX.

The screenshot displays the web management interface for a PEPPERL+FUCHS ROCKETLINX device. The left sidebar contains a navigation menu with the following items:

- ICRL-M-16RJ45/4CP-G-DIN
 - Basic Setting
 - Port Configuration
 - Network Redundancy
 - VLAN
 - Traffic Prioritization
 - Multicast Filtering
 - SNMP
 - Security
 - Warning
 - Fault Relay Setting
 - Event Selection
 - Syslog Configuration
 - SMTP Configuration
 - Monitor and Diag
 - LLDP Configuration
 - MAC Address Table
 - Port Statistics
 - Port Mirroring
 - Event Logs
 - Ping
 - Device Front Panel
 - Save
 - Logout
 - Reboot

The main content area is titled "Device Front Panel" and includes a "Help" button. It features a detailed diagram of the device's front panel with the following components:

- Port 1: Console port (RJ45)
- Ports 2-5: SFP ports (SFP1-4)
- Ports 6-16: RJ45 ports (1-16)
- Ports 17-18: SFP ports (SFP5-6)
- Ports 19-20: RJ45 ports (17-20)
- Power LEDs: PWR (green), -1 (red), 2 (green), SYS (green)
- DO RS: Diagnostic LEDs
- Buttons: Reload (green)
- Logo: PEPPERL+FUCHS

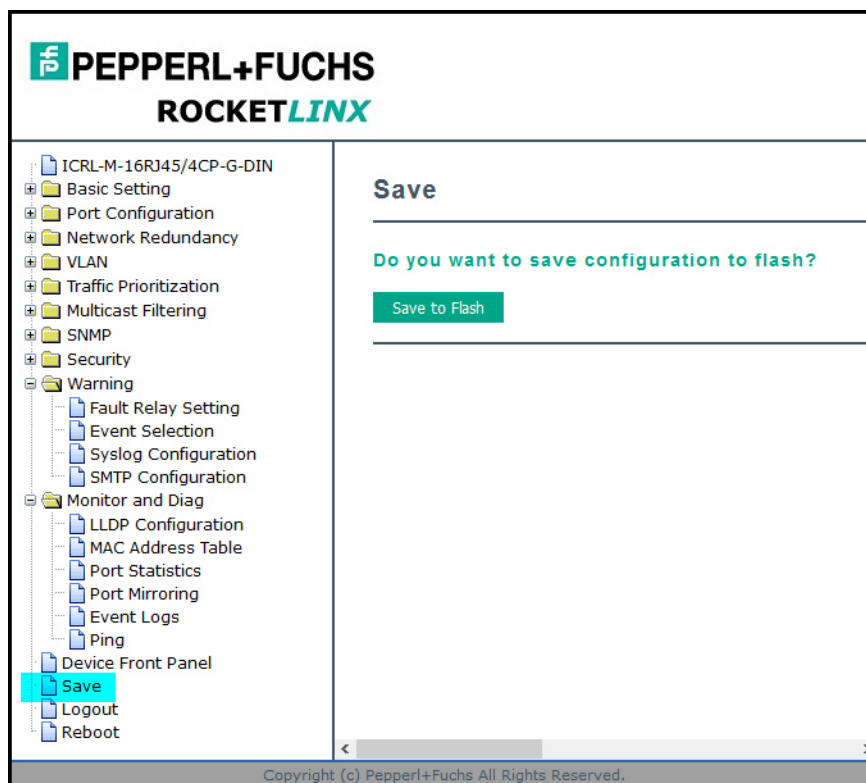
At the bottom of the interface, the copyright notice reads: "Copyright (c) Pepperl+Fuchs All Rights Reserved."

4.14. Save (to Flash)

The **Save** page saves any changes to the configuration to the flash.

Changes made to a switch's configuration are initially stored in volatile memory, which causes them to be lost if the switch loses power or is rebooted. Saving the settings to flash stores them in non-volatile memory, which preserves them if the switch loses power or is rebooted.

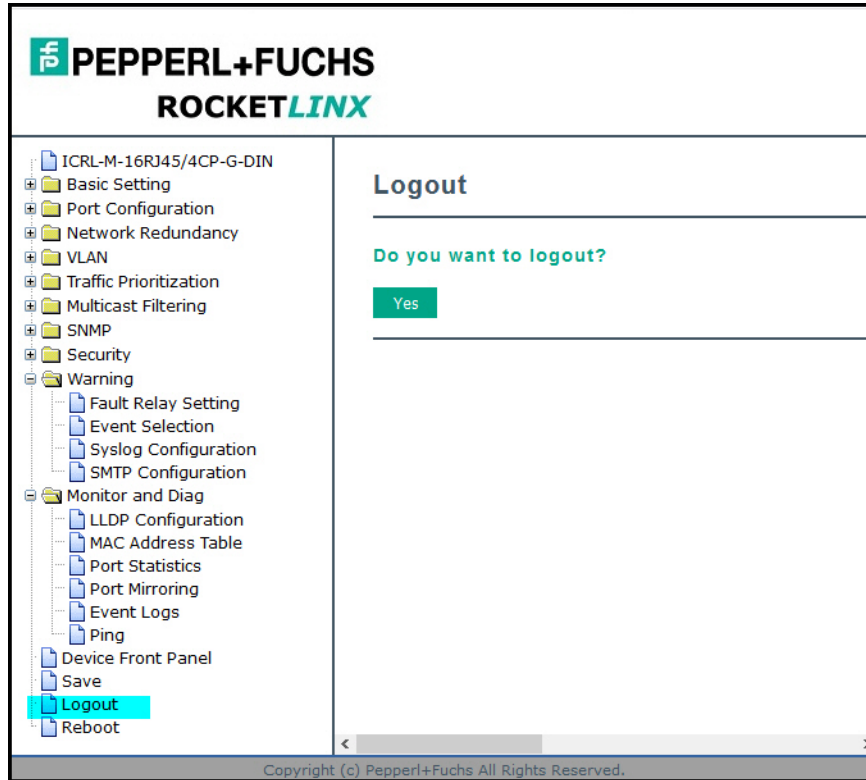
After selecting **Save Configuration**, click **Save to Flash** to save your new configuration.



Optionally, you can use the CLI, see *Saving to Flash (CLI)* on Page 217.

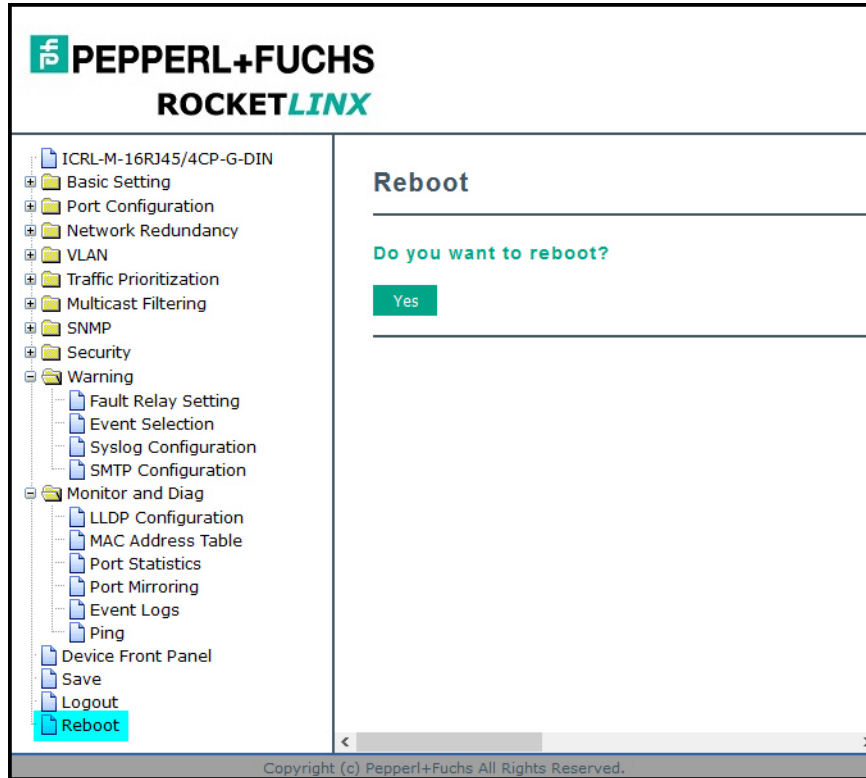
4.15. Logout

Click the **Logout** option in the web user interface to manually logout the web connection.
Click **Yes** to logout.



4.16. Reboot

Use this page to reboot the ICRL-M - make sure that you have saved your changes or they will be lost.



5. Configuration - Command Line Interface (CLI)

5.1. Overview

The ICRL-M provides in-band and out-band configuration methods:

- Out-band management means that you configure the ICRL-M using the RS-232 console cable and the Command Line Interface (CLI) to access the ICRL-M without attaching an admin PC to the network. You can use out-band management if you lose the network connection to the ICRL-M.
- In-band management means that you connect remotely using the ICRL-M IP address through the network. You can remotely connect with the ICRL-M embedded web user interface or a Telnet console and the CLI.

If you are planning on using in-band management, you need to program the ICRL-M IP address to meet your network requirements. The easiest way to configure the IP address is using a Windows system and PortVision DX, which is discussed in *Configuring the Network Settings* on Page 23.

If you want to use the web user interface for configuration, see *Configuration - Web User Interface* on Page 33.

Use the following procedures to access the ICRL-M using the CLI:

- *Using the Serial Console*
- *Using a Telnet/SSH Console*

This section contains information about the following groups of commands:

- *Basic Settings (CLI)* on Page 174
- *Port Configuration (CLI)* on Page 180
- *Network Redundancy (CLI)* on Page 184
- *VLAN (CLI)* on Page 191 and *Private VLAN (CLI)* on Page 195
- *Traffic Prioritization (CLI)* on Page 199
- *Multicast Filtering (CLI)* on Page 202
- *SNMP (CLI)* on Page 206
- *Security (CLI)* on Page 207
- *Warnings (CLI)* on Page 211
- *Monitor and Diag (CLI)* on Page 214
- *Saving to Flash (CLI)* on Page 217
- *Logging Out (CLI)* on Page 217
- *Service (CLI)* on Page 217

5.1.1. Using the Serial Console

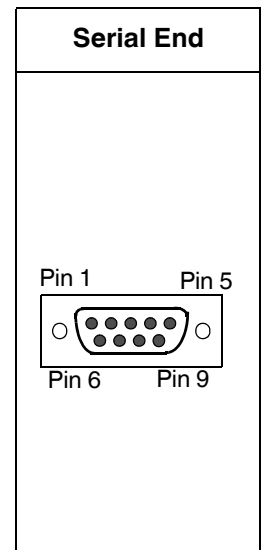
Pepperl+Fuchs provides one RS-232 RJ45 (ICRL-M-8RJ45/4SFP-G-DIN) and one RS-232 DB9 (ICRL-M-16RJ45/4CP-G-DIN) console cable.

Note: A system COM port is required to use a serial console connection. If you do not have an available COM port, use the Using a Telnet/SSH Console procedure on [Page 163](#).

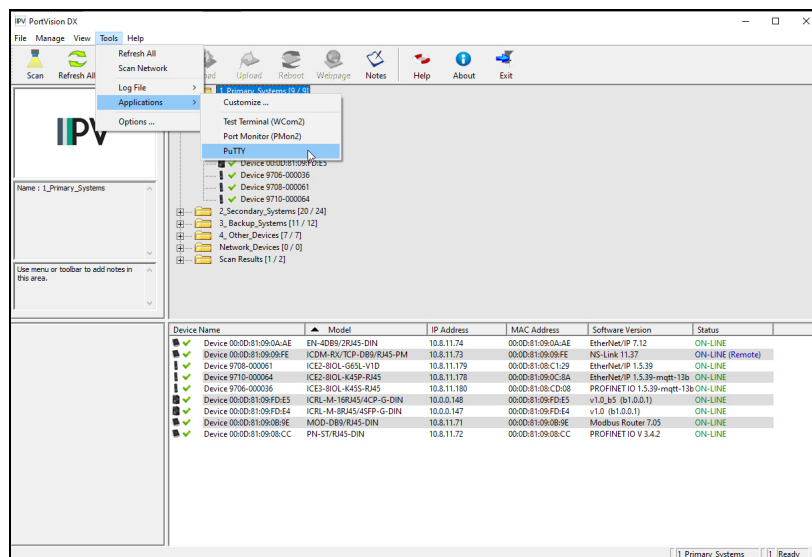
1. Attach the RS-232 connector (RJ45 or DB9 female) to your PC COM port and connect the other end to the **Console** port of the ICRL-M. If you misplace the cable, you can use the appropriate console cable pin assignment or purchase a null-modem cable. If building a replacement cable, at a minimum, you need to connect Tx, Rx, and ground signals.

RJ45 Pin	RJ45 Signal
5	DTR
7	Tx
6	Rx
3	DSR
4	Gnd
1	CTS
8	RTS
2	CD

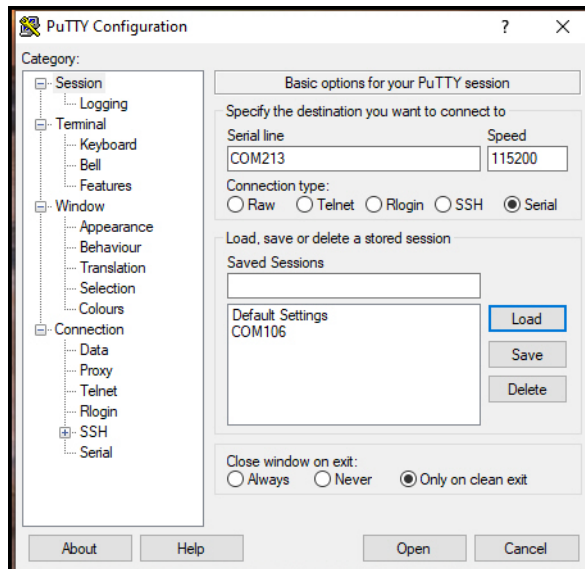
DB9F Pin	DB9 Signal
1	CD
2	Rx
3	Tx
4	DTR
5	Gnd
6	Not Used
7	RTS
8	CTS
9	RI



2. Start a terminal program such as HyperTerminal or use PuTTY, which is included with PortVision DX. The following example illustrates using PuTTY.
3. Open PortVision DX, click **Tools | Applications | PuTTY**.



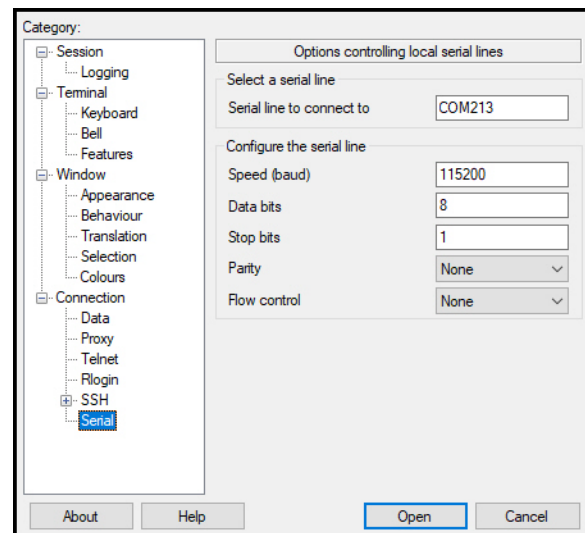
4. Click **Serial** for the **Connection type**.
5. Type a **Host Name** to represent the COM port.



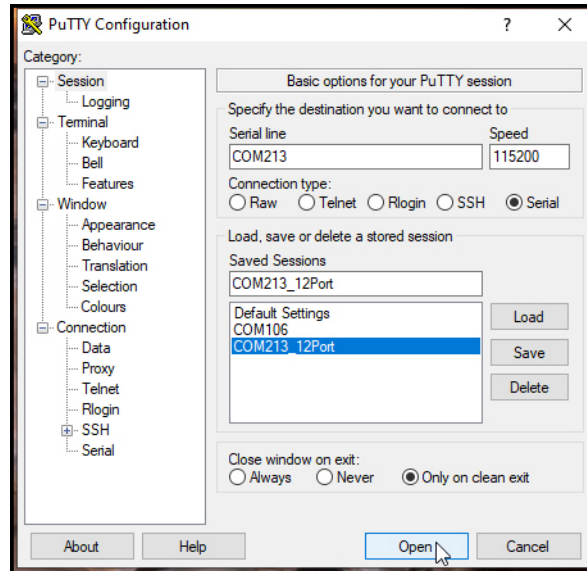
6. Click **Serial** on the left side under **Category**.
7. Configure the serial line with the following characteristics.

Serial Settings	Value
Baud Rate	115200
Data bits	8
Stop Bit	1
Parity	None
Flow Control	None

8. Click **Session** under **Category** in the menu.



9. Type an appropriate **Saved Session** name and click **Save**.



10. Click **Open**.
11. Press **Enter**.
12. Log in to the switch. The default user name is **admin**, password, **admin**.
 - a. Type the login and press the **Enter** key.
 - b. Type the password and press the **Enter** key.

```
Switch login: admin
Password:

ICRL-M-8RJ45/4SFP-G-DIN (version 1.0-20200131-16:50:50).
Copyright Pepperl+Fuchs
```

Note: The following examples illustrate the ICRL-M-8RJ45/4SFP-G-DIN but note that the ICRL-M-16RJ45/4CP-G-DIN is similar.

13. If necessary, configure the IP address for your network. The following example shows how to program an IP address of 192.168.11.252 with a Class B subnet mask (255.255.0.0).

```
Switch> enable
Switch# configure terminal
Switch(config)# int vlan1
Switch(config-if)# ip address 192.168.11.252/16
```

For more information about using the CLI, see *Command Line Interface Introduction* on Page 165.

5.1.2. Using a Telnet/SSH Console

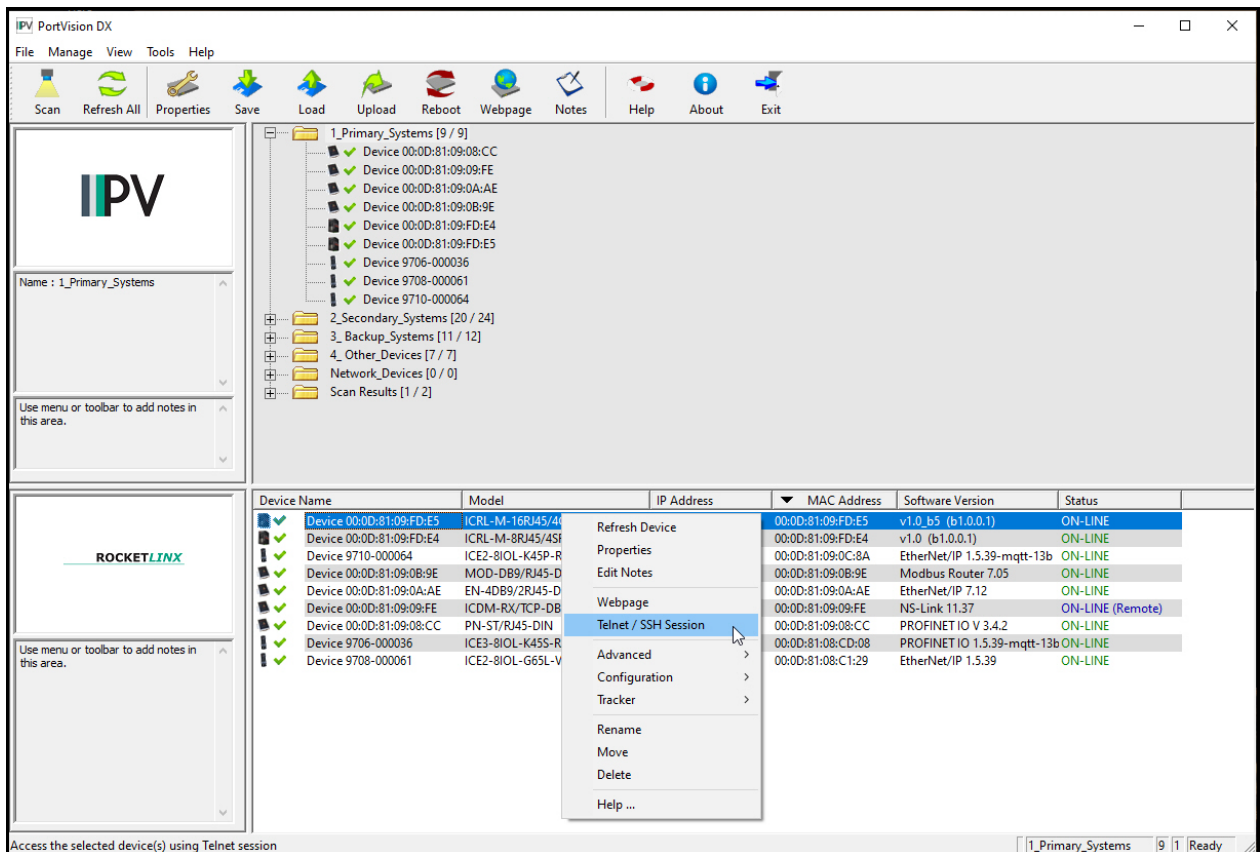
The ICRL-M supports a Telnet console or SSH console with the Command Line Interface (CLI), which is the same as what you see using the RS-232 console port. The SSH connection can secure all the configuration commands you send to the ICRL-M.

SSH is a client/server architecture while the ICRL-M is the SSH server. When you want to make SSH connection with the ICRL-M, you can use PortVision DX or download an SSH client tool.

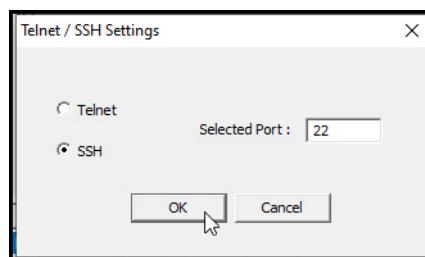
The next discussion provides procedures to use PortVision DX with a Telnet or SSH connection.

You can use PortVision DX to access the CLI using the following procedure.

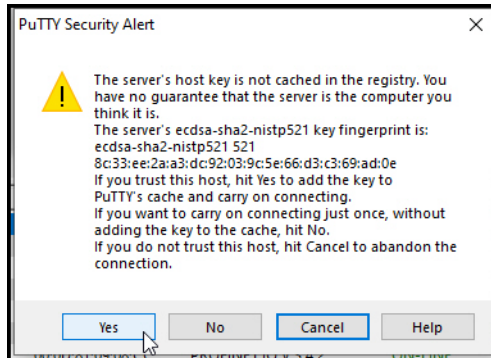
1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 20).
2. Start PortVision DX.
3. Right-click the ICRL-M in the *Device List* pane (lower) and click **Telnet/SSH**.



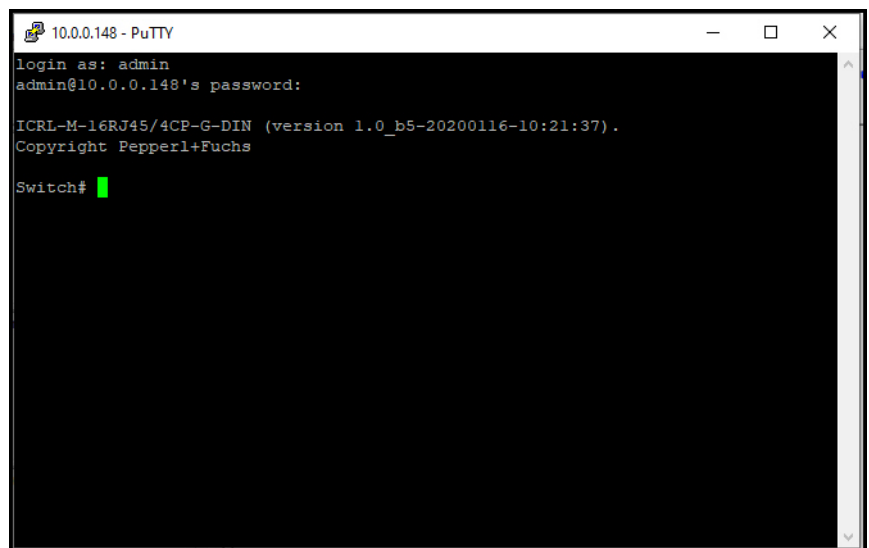
4. Select either Telnet or SSH and leave the default port number.



If you selected **SSH**, click **Yes**.



- Enter the user name (default = **admin**).
- Enter the password (default = **admin**).



If you selected **Telnet**:

- Enter the user name (default = **admin**).
- Enter the password (default = **admin**).

All the commands you see in SSH are the same as the CLI commands you see through the RS-232 console.

For more information about using the CLI, see *Command Line Interface Introduction* on Page 165.

5.2. Command Line Interface Introduction

The Command Line Interface (CLI) is the user interface to the ICRL-M embedded software. You can view the system information, show the status, configure the switch, and receive a response back from the system by keying in a command.

There are several different command modes. Each command mode has its own access ability, available command lines and uses different command lines to enter and exit. These modes are:

- *User EXEC Mode* on Page 168, which includes commands to ping or telnet to a remote device, and show some basic information and to access *Privileged EXEC* mode
- *Privileged EXEC Mode* on Page 169, which provides a view current configuration, reset default, reload switch, show system information, save configuration, and access *Global Configuration* mode
- *Global Configuration Mode* on Page 169, which you can use configure all ICRL-M features and access to one of the *Interface Configuration* modes
- *(Port) Interface Configuration* on Page 171, which can be used to configure port settings
- *(VLAN) Interface Configuration* on Page 172, which can be used to configure the settings for a specific VLAN

Refer to *Configuration - Command Line Interface (CLI)* on Page 159 to access the CLI.

5.3. Accessing the Options for a Command

The following example illustrates how to view the description and options for a command. This example illustrates the **show** command and the firmware version displayed may not reflect your firmware version.

Note: *The ? does not appear on the screen.*

1. If you type **show?** (without a space between **show** and the **?**; do not press the **Enter** key) the ICRL-M provides a basic description of that command.

```
Switch login: admin
Password:

ICRL-M-8RJ45/4SFP-G-DIN (version 1.0-20200131-16:50:50).
Copyright Pepperl+Fuchs

switch# show
show Show running system information
```

Note: *The firmware version may not reflect your RocketLinx model.*

2. If you type **show ?** (with a space between **show** and the **?**; do not press the **Enter** key) the ICRL-M provides information about the options for that command.

```

switch# show
acceptable      Get the information of acceptable frame type
arp             Address Resolution Protocol
auth           Authentication
cfm            IEEE 802.1ag - Connectivity Fault Management
clock          Display time-of-day clock
debugging      Debugging functions (see also 'undebug')
dot1q-tunnel    802.1Q tunnel characteristics
dot1x          Get IEEE 802.1x information
erps           Ethernet Ring Protection Switching (ITU-T G.8032)
ethernet-ip     Show Ethernet/IP information
event-log      Event log
garp           General Attribute Registration Protocol
gmrp           GMRP
gvrp           GARP VLAN Registration Protocol information
hardware       Hardware information
ingress        Get the information of ingress filtering
interface      Interface status and configuration
ip             IP interface commands
ipv6           IPv6
l2_interface    Interface status and configuration
lACP           Link Aggregation Control Protocol
lldp           Show LLDP information
mac            MAC interface commands
mac-address-table MAC address table
memory         Memory statistics
mirror         Port mirroring
modbus         Modbus TCP Slave
nameserver     DNS Server
ntp            Network time protocol
port-security  Port Security
process        Process
ptp            IEEE1588 Precision Time Protocol
qos            Quality of Service (QoS)
rate-limit     Rate limit configuration
redundant-ring The Redundant Ring protocol
relay          relay output type information
rmon           Remote monitoring
running-config Current operating configuration
service        System service
sfp            Small form factor pluggable information
smtp-server    SMTP server configuration
snmp-server    The SNMP server
spanning-tree  The spanning-tree protocol
startup-config Contentes of startup configuration
storm-control  Enables packets flooding rate limiting features
tftp           Show tftp status
trunk          Trunk group information
users          Users information
version        Displays ISS version
vlan           vlan
warning-event  Warning event
    
```

3. Type **show ip ?** (with a space between **show** and the **?**, do not press the **Enter** key) to review the options for **ip**.

```
switch# show ip
access-group      IP access-group configuration commands
access-list       List IP access lists
arp               Address Resolution Protocol
dhcp              DHCP Protocol
forwarding        IP forwarding status
igmp              IGMP information
route             IP routing table
verify           Verify
```

4. Type **show ip route** and press the **Enter** key to view the IP routing tables for the ICRL-M.

```
Switch> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      IA - OSPF inter area, E1 - OSPF external type 1,
      E2 - OSPF external type 2,
      B - BGP, > - selected route, * - FIB route

S 0.0.0.0/0 [1/10] via 192.168.250.1 inactive
C>* 10.0.0.0/16 is directly connected, vlan1
```

5. If you type **list** and press **Enter**, the ICRL-M provides you information about all of the commands and options for a mode. The following example shows the available commands and their options for *User EXEC* mode.

```
switch# disable
switch> list
enable
exit
list
ping A.B.C.D
ping WORD
ping X:X::X:X
quit
show gvrp statistics [IFNAME]
show ip forwarding
show ip route
show ip route A.B.C.D
show ip route A.B.C.D/M
show ip route supernets-only
show memory
show users
show version
telnet WORD
telnet WORD PORT
traceroute WORD
switch>
```

5.3.1. User EXEC Mode

When you login to the ICRL-M with the CLI, you are in *Privileged EXEC* mode. To access User EXEC mode, you must type `disable`.

In *User EXEC* mode, you can ping, telnet to a remote device, and show some basic information.

Type the command and press **Enter**:

- **enable** to access *Privileged EXEC* mode (*Privileged EXEC Mode* on Page 169).
- **exit** to logout.
- **?** to see the command list.
- **list** to review the *User EXEC* mode commands and corresponding options.

switch# disable	
switch>	
enable	Turn on privileged mode command
exit	Exit current mode and down to previous mode
list	Print command list
ping	Send echo messages
quit	Exit current mode and down to previous mode
show	Show running system information
telnet	Open a telnet connection
traceroute	Trace route to destination

For the complete list of commands with options, refer to *User EXEC Mode* on Page 218.

5.3.2. Privileged EXEC Mode

In this mode (default mode upon logging in) the ICRL-M allows you to view current configuration, reset default, reload switch, show system information, save configuration, and enter *Global Configuration* mode.

Type the following commands and press the **Enter** key:

- **configure terminal** to access *Global Configuration* mode (*Global Configuration Mode* on Page 169).
- **exit** to close the CLI.
- **?** to see the command list.
- **list** to review the *Privileged EXEC* mode commands and corresponding options.

For the complete list of commands and options, refer to *Privileged EXEC Mode* on Page 219.

switch#	
archive	Manage archive files
clear	Reset functions
clock	Configure time-of-day clock
configure	Configuration from vty interface
copy	Copy from one file to another
debug	Debugging functions (see also 'undebug')
disable	Turn off privileged mode command
dot1x	IEEE 802.1x standard access security control
end	End current mode and change to enable mode
exit	Exit current mode and down to previous mode
list	Print command list
mac	MAC interface commands
no	Negate a command or set its defaults
pager	Terminal pager
ping	Send echo messages
quit	Exit current mode and down to previous mode
read	Read from flash
reboot	Reboot system
reload	copy a default-config file to replace the current one
show	Show running system information
telnet	Open a telnet connection
traceroute	Trace route to destination
write	Write running configuration to memory, network, or terminal

5.3.3. Global Configuration Mode

If you type **configure terminal** in *Privileged EXEC* mode, you can then access *Global Configuration* mode. In *Global Configuration* mode, you can configure all ICRL-M features. Type the following commands and press the **Enter** key:

- **interface IFNAME/VLAN**, to access the corresponding *Interface Configuration* mode.
- **exit** to return to *Privileged EXEC* mode.
- **?** to see the command list.
- **list** to review the *Global Configuration* mode commands and corresponding options.

The following is a list of available command lists of *Global Configuration* mode. For the complete list of commands and options, refer to *Global Configuration Mode* on Page 226..

switch#	config term
switch(config)#	
access-list	Add an access list entry
arp	ARP
auth	authentication
cfm	IEEE 802.1ag - Connectivity Fault Management
clock	Configure time-of-day clock
default	Set a command to its defaults
dot1x	IEEE 802.1x standard access security control
end	End current mode and change to enable mode
erps	Ethernet Ring Protection Switching (ITU-T G.8032)
ethernet-ip	Ethernet/IP Protocol
exit	Exit current mode and down to previous mode
gmrp	GMRP protocol
gvrp	GARP VLAN Registration Protocol
hostname	Set system's network name
interface	Select an interface to configure
ip	Global IP configuration subcommands
ipv6	IP information
lacp	Link Aggregation Control Protocol
list	Print command list
lldp	Link Layer Discovery Protocol
log	Logging control
mac	Global MAC configuration subcommands
mac-address-table	mac address table
mirror	Port mirroring
modbus	Modbus TCP Slave
nameserver	DNS Server
no	Negate a command or set its defaults
ntp	Configure NTP
ptp	IEEE1588 PTPv2
qos	Quality of Service (QoS)
redundant-ring	Configure Redundant Ring
relay	relay output type information
router	Enable a routing process
service	System service
sfp	Small form-factor pluggable
smtp-server	SMTP server configuration
snmp-server	the SNMP server
spanning-tree	the spanning tree algorithm
tftp	tftp switch to enable/disable tftp
trunk	Trunk group configuration
username	Add or setup existing user account, password or privilege
vlan	Virtual LAN
warning-event	Warning event selection
write-config	Specify config files to write to

5.3.4. (Port) Interface Configuration

When you type **interface IFNAME** in *Global Configuration* mode, you can access *Interface Configuration* mode. In this mode you can configure port settings.

Type the interface name, for example `gi1`, when you want to enter a certain interface configuration mode. Type the following commands and press the **Enter** key:

- **exit** to return to *Privileged EXEC* mode.
- **?** to see the command list.
- **list** to review the *Interface Configuration* mode commands and corresponding options. The following list is the available commands for the *Port Interface Configuration* mode.

For the complete list of commands and options, refer to **Port Interface Configuration Mode** on Page 234.

switch(config)# interface gi1	
switch(config-if)#	
acceptable	Configures the 802.1Q acceptable frame types of a port.
description	Interface specific description
dot1x	IEEE 802.1x standard access security control
duplex	Specifies the duplex mode of operation for a port
end	End current mode and change to enable mode
ethertype	Ethertype
exit	Exit current mode and down to previous mode
flowcontrol	Sets the flow-control value for an interface
garp	General Attribute Registration Protocol
ingress	802.1Q ingress filtering features
ip	Interface Internet Protocol config commands
lacp	Link Aggregation Control Protocol
list	Print command list
loopback	Specifies the loopback mode of operation for a port
mac	MAC interface commands
media-type	Specify media type
mtu	Specifies the MTU on a port.
no	Negate a command or set its defaults
qos	Quality of Service (QoS)
quit	Exit current mode and down to previous mode
rate-limit	Rate limit configuration
sfp	Small form-factor pluggable
shutdown	Shutdown the selected interface
spanning-tree	the spanning-tree protocol
speed	Specifies the speed of a Fast Ethernet port or a Gigabit Ethernet port.
storm-control	Enables packets flooding rate limiting features
switchport	Set switching mode characteristics

5.3.5. (VLAN) Interface Configuration

If you type **interface VLAN VLAN-ID** in *Global Configuration* mode, you can access *VLAN Interface Configuration* mode. In this mode, you can configure the settings for the specific VLAN.

The VLAN interface name of VLAN 1 is VLAN 1, VLAN 2 is VLAN 2.

Type **exit** to return to the previous mode. Type **?** to see the available command list.

switch# config term	
switch(config)# interface vlan 1	
switch(config-if)#	
description	Interface specific description
end	End current mode and change to enable mode
exit	Exit current mode and down to previous mode
ip	Interface Internet Protocol config commands
ipv6	Interface Internet Protocol config commands
list	Print command list
no	Negate a command or set its defaults
quit	Exit current mode and down to previous mode
shutdown	Shutdown the selected interface

For the complete list of commands and options, refer to *VLAN Interface Configuration Mode* on Page 237.

5.4. Command Mode Summary

This table is a summary of the five command modes.

Mode: Main Function	Access and Exit Mode	Prompt
User EXEC: This is the first level of access. You can ping, telnet a remote device, and show some basic information.	<ul style="list-style-type: none"> Access <i>User EXEC</i> mode: Login successfully and type disable to access <i>User EXEC</i> mode. Exit: exit to logout. Next mode: Type enable to re-enter <i>Privileged EXEC</i> mode. 	Switch>
Privileged EXEC: Allows you to view current configuration, reset the default values, reload the switch, show system information, save configuration and enter <i>Global Configuration</i> mode.	<ul style="list-style-type: none"> Access <i>Privileged EXEC</i> mode: Login successfully. Type enable if returning from <i>User EXEC</i> mode. Exec: Type disable to exit to <i>User EXEC</i> mode. Type exit to logout. Next mode: Type configure terminal to enter <i>Global Configuration</i> mode. 	Switch#
Global Configuration: Configure all of the features that the ICRL-M provides.	<ul style="list-style-type: none"> Access <i>Global Configuration</i> mode: Type configure terminal in <i>Privileged EXEC</i> mode. Exit: Type exit or end or press Ctrl-Z to exit. Next mode: Type interface IFNAME/ VLAN VID to enter <i>Interface Configuration</i> mode. 	Switch(config)#
Port Interface Configuration: Configure port related settings.	<ul style="list-style-type: none"> Access <i>Port Interface Configuration</i> mode: Type interface IFNAME in global configuration mode. Exit: Type exit or Ctrl+Z to <i>Global Configuration</i> mode. Type end to return to <i>Privileged EXEC</i> mode. 	Switch(config-if)#

4/21/20

Mode: Main Function	Access and Exit Mode	Prompt
VLAN Interface Configuration: Configure settings for a specific VLAN.	<ul style="list-style-type: none"> Access <i>VLAN Interface Configuration</i> mode: Type interface VLAN VID in <i>Global Configuration</i> mode. Exit: Type exit or Ctrl+Z to return to <i>Global Configuration</i> mode. Type end to return to <i>Privileged EXEC</i> mode. 	Switch(config-vlan)#

The following are useful commands to save you typing time and to avoid typing errors.

Press **?** to see all of the available commands in a mode. It helps you to see the next command you can type.

```
switch(config)# interface (?)
IFNAME      Interface's name
vlan        Select a vlan to configure
```

Type a *Character?* (shown below) to see all of the available commands starting with this character.

```
switch(config)# a?
access-list  Add an access list entry
administrator Administrator account setting
auth         Authentication
```

Press the **Tab** key, which helps you to input the command quicker. If there is only one available command in the next, click the **Tab** key to help finish the typing.

```
switch# co (tab) (tab)
switch# configure terminal

switch(config)# ad (tab)
switch(config)# administrator
```

Key Combination	Function
Ctrl+C	To stop executing the unfinished command.
Ctrl+S	To lock the screen of the terminal - you cannot input any command.
Ctrl+Q	To unlock the screen which is locked by Ctrl+S .
Ctrl+Z	To exit <i>Configuration</i> mode.

5.5. Basic Settings (CLI)

The *Basic Setting* group provides you with the ability to configure switch information, IP address, User name/ Password of the system. It also allows you to do firmware upgrade, backup and restore configuration, reload factory default, and reboot the system.

Optionally, you can use the web user interface for configuration, see *Basic Settings* on Page 35.

This table provides detailed information about the CLI commands for basic settings.

Switch Setting	
System Name	Switch(config)# hostname DWORD Network name of this system Switch(config)# hostname ICRL-M Switch(config)#
System Location	Switch(config)# snmp-server location Minnesota
System Contact	Switch(config)# snmp-server contact info@de.pepperl-fuchs.com
Display	Switch# show snmp-server name ICRL-M Switch# show snmp-server location DLR lab Switch# show snmp-server contact drada switch# show version Hardware Information : Product Name : ICRL-M-8RJ45/4SFP-G-DIN Serial Number : RDSAMPLE561201 MAC Address : 000D8109FDE4 Manufacturing Date : 2019/08/10 HW Code : 20 Software Information : Loader Version : 1.0.0.1 Firmware Version : 1.0-20200131-16:50:50 System OID : 1.3.6.1.4.1.2882.2.5.0 Switch# show hardware mac MAC Address: 00:0D:81:09:FD:E4
Admin Password	
User Name and Password	Switch(config)# administrator NAME Administrator account name Switch(config)# administrator admin PASSWORD Administrator account password Switch(config)# administrator admin admin Change administrator account admin and password admin success.
Display	Switch# show administrator Administrator account information name: admin password: admin

4/21/20

IP Configuration	
<p>IP Address/Mask (192.168.250.250, 255.255.255.0)</p> <p>The enabled bit of the subnet mask is used to represent the number displayed in the web user interface. For example, 8 represents: 255.0.0.0, 16 represents: 255.255.0.0, 24 represents: 255.255.255.0.</p>	<pre>Switch(config)# int vlan 1 Switch(config-if)# ip address dhcp Switch(config-if)# ip address 192.168.250.8/24 Switch(config-if)# ip dhcp client Switch(config-if)# ip dhcp client renew Switch(config-if)# ipv6 address ; IPv6 configuration X::X::X/M IPv6 address (e.g. 3ffe:506::1/48) Switch(config-if)# ipv6 address 3ffe:506::1/48</pre>
Gateway	Switch(config)# ip route 0.0.0.0/0 192.168.250.254/24
Remove Gateway	Switch(config)# no ip route 0.0.0.0/0 192.168.250.254/24
Display	<pre>Switch# show running-config ! interface vlan1 ip address 192.168.250.8/24 no shutdown ! ip route 0.0.0.0/0 192.168.250.254/24 !</pre>
Time Setting	
NTP Server	<pre>Switch(config)# ntp peer enable disable primary secondary Switch(config)# ntp peer primary IPADDR Switch(config)# ntp peer primary 192.168.250.250</pre>
Time Zone	<pre>Switch(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London</pre> <p>Note: By typing <code>clock timezone?</code>, you can see the <code>timezone</code> list. Then choose the number of the <code>timezone</code> you want to select.</p>

Time Setting (Continued)	
Display	Switch # sh ntp associations Network time protocol Status: Disabled Primary peer: N/A Secondary peer: N/A Switch # show clock Sun Jan 1 04:14:19 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London Switch # show clock timezone clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Jumbo Frame	
Jumbo Frame	Switch(config-if)# mtu 9216
DHCP Server	
DHCP Server configuration	Enable DHCP Server on ICRL-M Switch Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Configure DHCP network address pool Switch(config-dhcp)#network 50.50.50.0/4 -(network/mask) Switch(config-dhcp)#default-router 50.50.50.1
Lease time configure	Switch(config-dhcp)#lease 300 (300 sec)

DHCP Server (Continued)	
DHCP Relay Agent	<pre> Enable DHCP Relay Agent Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Switch(config-dhcp)# ip dhcp relay information option Enable DHCP Relay policy Switch(config-dhcp)# ip dhcp relay information policy <u>replace</u> drop Relay Policy keep Drop/Keep/Replace option 82 field replace Switch(config-dhcp)# ip dhcp relay information option <cr> circuit-id Configure Circuit-ID remote-id Configure Remote-ID Switch(config-dhcp)# ip dhcp relay information option option Option82 Switch(config-dhcp)# ip dhcp relay information option </pre>
Show DHCP server information	<pre> Switch# show ip dhcp server statistics DHCP Server ON Address Pool 1 network:192.168.17.0/24 default-router:192.168.17.254 lease time:300 Excluded Address List IP Address ----- (list excluded address) Manual Binding List IP Address MAC Address ----- (list IP & MAC binding entry) Leased Address List IP Address MAC Address Leased Time Remains ----- (list leased Time remain information for each entry) </pre>

DHCP Server (Continued)	
DHCP Commands	<pre>Switch(config)# router dhcp Switch(config-dhcp)# default-router DHCP Default Router end Exit current mode and down to previous enable mode exit Exit current mode and down to previous mode ip IP protocol lease DHCP Lease Time list Print command list network dhcp network no Remove quit Exit current mode and down to previous mode service Enable service</pre>
DHCP Server Enable	<pre>Switch(config-dhcp)# service dhcp</pre>
DHCP Server IP Pool (Network/Mask)	<pre>Switch(config-dhcp)# network A.B.C.D/M network/mask ex. 10.10.1.0/24 Switch(config-dhcp)# network 192.168.10.0/24</pre>
DHCP Server – Default Gateway	<pre>Switch(config-dhcp)# default-router A.B.C.D address Switch(config-dhcp)# default-router 192.168.10.254</pre>
DHCP Server – lease time	<pre>Switch(config-dhcp)# lease TIME second Switch(config-dhcp)# lease 1000 (1000 second)</pre>
DHCP Server – Static IP and MAC binding	<pre>Switch(config-dhcp)# ip dhcp static MACADDR MAC address Switch(config-dhcp)# ip dhcp static 00:0D:81:09:FD:E4 .0001 A.B.C.D leased IP address Switch(config-dhcp)# ip dhcp static 00:0D:81:09:FD:E4 .0001 192.168.10.99</pre>
DHCP Relay – Enable DHCP Relay	<pre>Switch(config-dhcp)# ip dhcp relay information option Option82 policy Option82 Switch(config-dhcp)# ip dhcp relay information option</pre>
DHCP Relay – DHCP policy	<pre>Switch(config-dhcp)# ip dhcp relay information policy drop Relay Policy keep Drop/Keep/Replace option82 field replace Switch(config-dhcp)# ip dhcp relay information policy drop Switch(config-dhcp)# ip dhcp relay information policy keep Switch(config-dhcp)# ip dhcp relay information policy replace</pre>
DHCP Relay – IP Helper Address	<pre>Switch(config-dhcp)# ip dhcp helper-address A.B.C.D Switch(config-dhcp)# ip dhcp helper-address 192.168.10.200</pre>
Reset DHCP Settings	<pre>Switch(config-dhcp)# ip dhcp reset</pre>

Backup and Restore	
Backup Startup Configuration File	Switch# copy startup-config tftp: 192.168.250.33/default.conf Writing Configuration [OK] Note: <i>To backup the latest startup configuration file, you should save current settings to flash first. You can refer to Save (to Flash) on Page 156 to see how to save settings to the flash.</i> <i>In the example above, 192.168.250.33 is the TFTP server's IP and default.conf is name of the configuration file. Your environment may use different IP addresses or different file name. Type target TFTP server IP or file name in this command.</i>
Restore Configuration	Switch# copy tftp: 192.168.250.33/default.conf startup-config
Show Startup Config	Switch# show startup-config
Show Running Config	Switch# show running-config
Firmware Upgrade	
Firmware Upgrade	Switch# archive download-sw /overwrite tftp 192.168.11.33 ICRL-M.bin Firmware upgrading, don't turn off the switch! Tftping file ICRL-M.bin Firmware upgrading Firmware upgrade success!! Rebooting.....
Load Default	
Load Default	Switch# reload default-config file Reload OK! Switch# reboot
System Reboot	
Reboot	Switch# reboot

5.6. Port Configuration (CLI)

The Port Configuration group allows you to enable/disable port state, or configure port auto-negotiation, speed, duplex, flow control, rate limit control, and port aggregation settings. It also allows you to view port status and aggregation information.

Gigabit ports are identified as: gi1, gi2, gi3 and so forth.

Optionally, you can use the web user interface for configuration, see *Port Configuration* on Page 59.

This table provides detailed information about the CLI commands for port configuration.

Port Control	
Port Control – State	Switch(config-if)# shutdown -> Disable port state Port1 Link Change to DOWN interface gigabitethernet1 is shutdown now. Switch(config-if)# no shutdown -> Enable port state Port1 Link Change to DOWN Port1 Link Change to UP interface gigabitethernet1 is up now. Switch(config-if)# Port1 Link Change to UP Switch(config)# sfp ddm Digital diagnostic and monitoring eject Eject SFP scan Scan SFP Switch(config)# sfp ddm enable Enable DDM disable Disable DDM
Port Control – Auto Negotiation	Switch(config)# interface gi1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!
Port Control – Force Speed/ Duplex	Switch(config-if)# speed 100 Port1 Link Change to DOWN set the speed mode ok! Switch(config-if)# Port1 Link Change to UP Switch(config-if)# duplex full set the duplex mode ok!
Port Control – Flow Control	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!

Port Status	
Port Status	<pre> ICRL-M# show interface gi1 Interface gigabitethernet1 Description : N/A Administrative Status : Enable Operating Status : Connected Duplex : Auto (Full) Speed : Auto (100) MTU : 1518 Flow Control : off Default Port VLAN ID: 1 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Enable Loopback Mode : None STP Status: Forwarding Default CoS Value for untagged packets is 0. Medium mode is Copper. ICRL-M# show sfp ddm Port 9 Admin status : Enabled Temperature : N/A Tx power : N/A Rx power : N/A Port 10 Admin status : Enabled Temperature : N/A Tx power : N/A Rx power : N/A Port 11 Admin status : Enabled Temperature : 45.00 C (Range : -15.00 - 85.00) Tx power : -6.2 dBm (Range : -10.5 - -3.0) Rx power : -9.0 dBm (Range : -17.0 - -3.0) Port 12 Admin status : Enabled Temperature : N/A Tx power : N/A Rx power : N/A Note: Administrative Status -> Port state of the port. Operating status -> Current status of the port. Duplex -> Duplex mode of the port. Speed -> Speed mode of the port. Flow control -> Flow Control status of the port. </pre>

Port Status (Continued)	
Rate Control – Ingress or Egress	Switch(config-if)# rate-limit egress Outgoing packets ingress Incoming packets Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.
Rate Control – Filter Packet Type	Switch(config-if)# rate-limit ingress bandwidth Set bandwidth informational parameter Switch(config-if)# rate-limit ingress bandwidth Switch(config-if)# rate-limit ingress bandwidth 800 Set the ingress rate limit 800Kbps for Port 1.
Storm Control	
Storm Control – Packet Type	Switch(config-if)# storm-control broadcast :Broadcast packets dlf :Destination Lookup Failure multicast :Multicast packets
Storm Control - Rate	Switch(config)# storm-control broadcast <0-100000> Rate limit value 0~262143 packet/sec Switch(config)# storm-control broadcast 10000 limit_rate = 10000 packets/sec Set rate limit for Broadcast packets. Switch(config)# storm-control multicast 10000 limit_rate = 10000 packets/sec Set rate limit for Multicast packets. Switch(config)# storm-control dlf 10000 limit_rate = 10000 packets/sec Set rate limit for Destination Lookup Failure packets.
Port Trunking	
Display – LACP	Switch# show lacp internal LACP group 1 is inactive LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive LACP group 5 is inactive LACP group 6 is inactive LACP group 7 is inactive LACP group 8 is inactive
LACP	Switch(config)# lacp group 1 gi8-10 Group 1 based on LACP(802.3ad) is enabled!

Port Trunking (Continued)	
LACP – Port Setting	<pre> SWITCH(config-if)# lacp port-priority LACP priority for physical interfaces timeout assigns an administrative LACP timeout SWITCH(config-if)# lacp port-priority <1-65535> Valid port priority range 1 - 65535 (default is 32768) SWITCH(config-if)# lacp timeout long specifies a long timeout value (default) short specifies a short timeout value SWITCH(config-if)# lacp timeout short Set lacp port timeout ok. </pre>
Display – LACP	<pre> Switch# show lacp counters LACP statistical information group LACP group internal LACP internal information neighbor LACP neighbor information port-setting LACP setting for physical interfaces system-id LACP system identification system-priority LACP system priority Switch# show lacp port-setting LACP Port Setting : Port Priority Timeout ----- 1 32768 Long 2 32768 Long 3 32768 Long Switch# show lacp internal LACP group 1 internal information: LACP Port Admin Oper Port Port Priority Key Key State ----- 8 1 8 8 0x45 9 1 9 9 0x45 10 1 10 10 0x45 LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive </pre>
Display - Trunk	<pre> Switch# show trunk group 1 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group TGID Protocol Load-Balance Ports -----+-----+-----+----- 1 Static src-dst-mac 11(D) 12(P) </pre>

4/21/20

5.7. Network Redundancy (CLI)

It is critical for industrial applications that the network remains running at all times. The ICRL-M supports:

- Standard Rapid Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP)
The ICRL-M supports RSTP versions IEEE 802.1D-2004, IEEE 802.1D-1998 STP, and IEEE 802.1w RSTP.
- Multiple Spanning Tree Protocol (MSTP)
MSTP implements IEEE 802.1s, which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs. MSTP was originally defined in the IEEE 802.1s and later merged into the IEEE 802.1Q-2003 specification.
- Redundant Ring
The Redundant Ring features 0 ms for restore and about .
- Rapid Dual Homing (RDH)
Advanced RDH technology allows the ICRL-M to connect with a core managed switch easily and conveniently. With RDH technology, you can also couple several Rapid Super Rings or RSTP groups together, which is also known as Auto Ring Coupling.

Optionally, you can use the web user interface for configuration, see *Network Redundancy* on Page 69.

This table provides detailed information about the CLI command lines for network redundancy.

Global (STP, RSTP, and MSTP)	
Enable	Switch(config)# spanning-tree enable
Disable	Switch(config)# spanning-tree disable
Mode	Switch(config)# spanning-tree mode rst the rapid spanning-tree protocol (802.1w) stp the spanning-tree prtocol (802.1d) mst the multiple spanning-tree protocol (802.1s) Switch(config)# spanning-tree mode Switch(config)# spanning-tree mode mst Spanning-Tree Mode change to be MSTP (802.1s) Switch(config)# spanning-tree mode stp Spanning-Tree Mode change to be STP(802.1d) . Switch(config)# spanning-tree mode rst Spanning-Tree Mode change to be RSTP(802.1w) . Switch(config)# spanning-tree mode mst Spanning-Tree Mode change to be MSTP(802.1s).
Bridge Priority	Switch(config)# spanning-tree priority <0-61440> the value of bridge priority in multiple of 4096 Switch(config)# spanning-tree priority 4096
Bridge Times	Switch(config)# spanning-tree bridge-times (forward Delay) (max-age) (Hello Time) Switch(config)# spanning-tree bridge-times 15 20 2 This command allows you configure all the timing in one time.

4/21/20

Global (STP, RSTP, and MSTP) (Continued)	
Forward Delay	Switch(config)# spanning-tree forward-time <4-30> the value of forward delay time in seconds Switch(config)# spanning-tree forward-time 15
Max Age	Switch(config)# spanning-tree max-age <6-40> the value of message maximum age time in seconds Switch(config)# spanning-tree max-age 20
Hello Time	Switch(config)# spanning-tree hello-time <1-10> the value of hello time in seconds Switch(config)# spanning-tree hello-time 2
MSTP	
Enter the MSTP Configuration Tree	Switch(config)# spanning-tree mst MSTMAP the mst instance number or range configuration enter mst configuration mode forward-time the forward delay time hello-time the hello time max-age the message maximum age time max-hops the maximum hops sync sync port state of exist vlan entry Switch(config)# spanning-tree mst configuration Switch(config)# spanning-tree mst configuration Switch(config-mst)# abort exit current mode and discard all changes end exit current mode, change to enable mode and apply all changes exit exit current mode and apply all changes instance the mst instance list Print command list name the name of mst region no Negate a command or set its defaults quit exit current mode and apply all changes revision the revision of mst region show show mst configuration
Region Configuration	Region Name: Switch(config-mst)# name NAME the name string Switch(config-mst)# name Pepperl+Fuchs Region Revision: Switch(config-mst)# revision <0-65535> the value of revision Switch(config-mst)# revision 65535
Mapping Instance to VLAN (Ex: Mapping VLAN 2 to Instance 1)	Switch(config-mst)# instance <1-15> target instance number Switch(config-mst)# instance 1 vlan VLANMAP target vlan number(ex.10) or range(ex.1-10) Switch(config-mst)# instance 1 vlan 2

4/21/20

MSTP (Continued)	
Display Current MST Configuration	<pre>Switch(config-mst)# show current Current MST configuration Name [Pepperl+Fuchs] Revision 65535 Instance Vlans Mapped ----- 0 1,4-4094 1 2 2 3 ----- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D -----</pre>
Remove Region Name	<pre>Switch(config-mst)# no name name configure revision revision configure instance the mst instance Switch(config-mst)# no name</pre>
Remove Instance example	<pre>Switch(config-mst)# no instance <1-15> target instance number Switch(config-mst)# no instance 2</pre>
Show Pending MST Configuration	<pre>Switch(config-mst)# show pending Pending MST configuration Name [] (->The name is removed by no name) Revision 65535 Instance Vlans Mapped ----- 0 1,3-4094 1 2 (->Instance 2 is removed by no instance 2) ----- Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 -----</pre>
Apply the setting and go to the configuration mode	<pre>Switch(config-mst)# quit apply all mst configuration changes Switch(config)#</pre>
Apply the setting and go to the global mode	<pre>Switch(config-mst)# end apply all mst configuration changes Switch#</pre>

MSTP (Continued)	
<p>Abort the Setting and go to the configuration mode.</p> <p>Show Pending to see the new settings are not applied.</p>	<pre>Switch(config-mst)# abort discard all mst configuration changes Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name [Pepperl+Fuchs] (->The name is not applied after Abort settings.) Revision 65535 Instance Vlans Mapped ----- 0 1,4-4094 1 2 2 3 (-> The instance is not applied after Abort settings.) ----- Config HMAC-MD5 Digest: 0xAC36177F50283CD4B83821D8AB26DE62 -----</pre>
RSTP	
System RSTP Setting	The mode should be rstp, timings can be configured in the global settings listed in the previous examples.
Port Configuration Mode	
Port Configuration	<pre>Switch(config)# interface gi1 Switch(config-if)# spanning-tree bpdufilter a secure BPDU process on edge-port interface bpduguard a secure response to invalid configurations (received BPDU sent by self) cost change an interface's spanning-tree port path cost edge-port interface attached to a LAN segment that is at the end of a bridged LAN or to an end node link-type the link type for the Rapid Spanning Tree mst the multiple spanning-tree port-priority the spanning tree port priority stp-state the bridge port STP state</pre>
Port Path Cost	<pre>Switch(config-if)# spanning-tree cost <1-200000000> 16-bit based value range from 1-65535, 32-bit based value range from 1-200,000,000 Switch(config-if)# spanning-tree cost 200000</pre>
Port Priority	<pre>Switch(config-if)# spanning-tree port-priority <0-240> Number from 0 to 240, in multiple of 16 Switch(config-if)# spanning-tree port-priority 128</pre>
Link Type - Auto	Switch(config-if)# spanning-tree link-type auto
Link Type - P2P	Switch(config-if)# spanning-tree link-type point-to-point

Port Configuration Mode (Continued)	
Link Type – Share	Switch(config-if)# spanning-tree link-type shared
Edge Port	Switch(config-if)# spanning-tree edge-port enable Switch(config-if)# spanning-tree edge-port disable
MSTP Port Configuration	Switch(config-if)# spanning-tree mst MSTMAP cost <1-200000000> the value of mst instance port cost Switch(config-if)# spanning-tree mst MSTMAP port-priority <0-240> the value of mst instance port priority in multiple of 16
Global Information	
Active Information	<pre>Switch# show spanning-tree active Spanning-Tree : Enabled Protocol : RSTP Root Address : 000d.8109.fde4 Priority : 32768 Root Path Cost : 0 Root Port : N/A Root Times : max-age 20, hello-time 2, forward-delay 15 Bridge Address : 000d.8109.fde4 Priority : 32768 Bridge Times : max-age 20, hello-time 2, forward-delay 15 BPDU transmission-limit : 3 Port Role State Cost Prio.Nbr Type Aggregated ----- gi1 Designated Forwarding 200000 128.1 P2P(RSTP) N/A gi11 Designated Forwarding 20000 128.11 P2P(RSTP) N/A</pre>
RSTP Summary	<pre>Switch# show spanning-tree summary Spanning-Tree : Enabled Protocol : RSTP Root Address : 000d.8109.fde4 Priority : 32768 Root Path Cost : 0 Root Port : N/A Root Times : max-age 20, hello-time 2, forward-delay 15 Bridge Address 000d.8109.fde4 Priority : 32768 Bridge Times : max-age 20, hello-time 2, forward-delay 15 BPDU transmission-limit : 3 BPDU Skewing Detection : Disabled Backbonefast : Disabled Topology Change Flag : False Topology Change Detected Flag : False Topology Change Count : 75 Last Topology Change from : 0000.0000.0000 Timers: hello 1, topology change 0 Summary of connected spanning tree ports : Port-State Summary Blocking Listening Learning Forwarding Disabled ----- 0 0 0 2 10 Port Link-Type Summary AutoDetected PointToPoint SharedLink EdgePort ----- 12 0 0 10</pre>

4/21/20

Global Information (Continued)	
Port Info	<pre>Switch# show spanning-tree interface gi1 Interface gigabitethernet1 of Bridge is Enabled Port Role : Designated Port State : Forwarding Edge Port : Edge (Non-Edge) BPDU Filter : Disabled Link Type : Auto (Point-to-point) BPDU Guard : Disabled Timers : message-age 0, forward-delay 0 BPDUs : sent 390718, received 91 TCNs : sent 0, received 0 Message Expired Count : 0 Forward Transition Count : 1 Aggregation Group: N/A Type: N/A Aggregated with : N/A Port information port id 128.1 priority 128 cost 200000 Designated root address 000d.8109.fde4 priority 32768 cost 200000 Designated bridge address 000d.8109.fde4 priority 32768 port id 128.1</pre>
MSTP Information	
MSTP Configuration	<pre>Switch# show spanning-tree mst configuration Current MST configuration (MSTP is Stopped) Name [] Revision 0 Instance Vlans Mapped ----- 0 1-4094 ----- Config HMAC-MD5 Digest: 0xAC36177F50283CD4B83821D8AB26DE62 ----- -----</pre>

MSTP Information (Continued)	
Create or configure a Ring	Switch(config)# redundant-ring 1 Ring 1 created Switch(config-redundant-ring)# Note: 1 is the target Ring ID which is going to be created or configured.
Super Ring Version	Switch(config-redundant-ring)# version default set default to Redundant ring rapid-super-ring rapid super ring super-ring super ring Switch(config-redundant-ring)# version rapid-super-ring
Priority	Switch(config-redundant-ring)# priority <0-255> valid range is 0 to 255 default set default Switch(config-redundant-ring)# super-ring priority 100
Ring Port	Switch(config-redundant-ring)# port IFLIST Interface list, ex: gi1,gi3-5,gi8-10 cost path cost Switch(config-redundant-ring)# port 1,2
Ring Info	Switch# show redundant-ring [Ring ID] [Ring1] Ring1 Current Status : Disabled Role : Disabled Ring Status : Abnormal Ring Manager : 0000.0000.0000 Blocking Port : N/A Giga Copper : N/A Configuration : Version : Super Ring Priority : 128 Ring Port : gi1, gi2 Path Cost : 100, 200 Dual-Homing II : Disabled Statistics : Watchdog sent 0, received 0, missed 0 Link Up sent 0, received 0 Link Down sent 0, received 0 Role Transition count 0 Ring State Transition count 1 <i>Ring ID is optional. If the ring ID is typed, this command only displays the information of the target Ring.</i>

5.8. VLAN (CLI)

A Virtual LAN (VLAN) is a logical grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members. The VLAN allows you to isolate network traffic so that only members of the VLAN could receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is the logical equivalent of physically reconnecting a group of network devices to another Layer 2 switch, without actually disconnecting these devices from their original switches.

The ICRL-M supports IEEE 802.1Q VLAN, which is also known as Tag-Based VLAN. This Tag-Based VLAN allows a VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame's tag, without the need to dissect the contents of the frame, this also saves a lot of computing resources within the switch.

Optionally, you can use the web user interface for configuration, see *VLAN* on Page 88.

The following table provides detailed information about command lines for the VLAN.

VLAN Port Configuration	
VLAN Port PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
Port Accept Frame Type	Switch(config)# inter gi1 Switch(config-if)# acceptable frame type all any kind of frame type is accepted! Switch(config-if)# acceptable frame type vlantaggedonly only vlan-tag frame is accepted!
Ingress Filtering (for Fast Ethernet Port 1)	Switch(config)# interface gi1 Switch(config-if)# ingress filtering enable ingress filtering enable Switch(config-if)# ingress filtering disable ingress filtering disable
Egress rule – Untagged (for VLAN 2)	Switch(config-if)# switchport access vlan 2 switchport access vlan - success
Egress rule – Tagged (for VLAN 2)	Switch(config-if)# switchport trunk allowed vlan add 2

VLAN Port Configuration (Continued)	
Display – Port Ingress Rule (PVID, Ingress Filtering, Acceptable Frame Type)	<pre>ICRL-M# show interface gi1 Interface gigabitethernet1 Description : N/A Administrative Status : Enable Operating Status : Connected Duplex : Auto (Full) Speed : Auto (100) MTU : 1518 Flow Control : off Default Port VLAN ID: 1 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Enable Loopback Mode : None STP Status: Forwarding Default CoS Value for untagged packets is 0. Medium mode is Copper.</pre>
Display – Port Egress Rule (Egress rule, IP address, status)	<pre>Switch# show running-config ! interface gigabitethernet1 switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 interface vlan1 ip address 192.168.250.8/24 no shutdown</pre>
VLAN Configuration	
Create VLAN (2)	<pre>Switch(config)# vlan 2 vlan 2 success Switch(config)# interface vlan 2 Switch(config-if)#</pre> <p>Note: In the CLI configuration, you should first create a VLAN interface. Then you can start to add/remove ports. The default status of the created VLAN is unused until you add member ports to it.</p>
Remove VLAN	<pre>Switch(config)# no vlan 2 no vlan success</pre> <p>Note: You can only remove the VLAN when the VLAN is in unused mode.</p>

VLAN Configuration (Continued)	
VLAN Name	<pre>Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2 Switch(config-vlan)# no name</pre> <p>Note: Use no name to change the name to default name, VLAN VID.</p>
VLAN description	<pre>Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description this is the VLAN 2 Switch(config-if)# no description ->Delete the description.</pre>
IP address of the VLAN	<pre>Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.250.18/24 Switch(config-if)# no ip address 192.168.250.8/24 ->Delete the IP address</pre>
Create multiple VLANs (VLAN 5-8)	<pre>Switch(config)# interface vlan 5-8</pre>
Shutdown VLAN	<pre>Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->Turn on the VLAN</pre>
Display – VLAN table	<pre>Switch# sh vlan VLAN Name Status Trunk Ports Access Ports ----- - 1 VLAN1 Static - gi1-12 2 VLAN2 Unused -</pre>
Display – VLAN interface information	<pre>Switch# show interface vlan1 Interface vlan1 Description : N/A Administrative Status : Enable Operating Status : Up DHCP Client : Disable Primary IP Address : 10.0.0.147/16 IPv6 Address : fe80::20d:81ff:fe09:fde4/64</pre>

GVRP Configuration	
GVRP enable/ disable	<pre>Switch(config)# gvrp mode disable Disable GVRP feature globally on the switch enable Enable GVRP feature globally on the switch Switch(config)# gvrp mode enable Gvrp is enabled on the switch!</pre>
Configure GVRP timer Join timer /Leave timer/ LeaveAll timer	<pre>Switch(config)# inter gi1 Switch(config-if)# garp timer <10-10000> Switch(config-if)# garp timer 20 60 1000</pre> <p>Note: The unit of this timer is centiseconds.</p>
Management VLAN	
Management VLAN	<pre>Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# no shutdown</pre>
Display	<pre>Switch# show running-config ! interface vlan1 ip address 192.168.250.17/24 ip igmp no shutdown !</pre>

5.9. Private VLAN (CLI)

A private VLAN helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. The Private VLAN features provides primary and secondary VLANs within a single switch.

Primary VLAN: The uplink port is usually a member of the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with Secondary VLANs.

Secondary VLAN: The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated and Community VLANs. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other, however, the isolated VLAN ports cannot.

Optionally, you can use the web user interface for configuration, see *Private VLAN* on Page 95.

The following table provides detailed information about command lines for private VLAN port configuration, VLAN configuration, and VLAN table display.

Private VLAN Configuration	
Create VLAN	Switch(config)# vlan 2 vlan 2 success Switch(config-vlan)# end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list name Assign a name to vlan no no private-vlan Configure a private VLAN
Private VLAN Type	Go to the VLAN you want configure first. Switch(config)# vlan (VID)
Choose the Types	Switch(config-vlan)# private-vlan community Configure the VLAN as an community private VLAN isolated Configure the VLAN as an isolated private VLAN primary Configure the VLAN as a primary private VLAN
Primary Type	Switch(config-vlan)# private-vlan primary <cr>
Isolated Type	Switch(config-vlan)# private-vlan isolated <cr>
Community Type	Switch(config-vlan)# private-vlan community <cr>
Go to the port configuration	Switch(config)# interface (port_number, ex: gi1) Switch(config-if)# switchport private-vlan host-association Set the private VLAN host association mapping map primary VLAN to secondary VLAN
Private VLAN Port Type	Switch(config-if)# switchport mode private-vlan Set private-vlan mode Switch(config-if)# switchport mode private-vlan host Set the mode to private-vlan host promiscuous Set the mode to private-vlan promiscuous

4/21/20

Private VLAN Configuration (Continued)	
Promiscuous Port Type	Switch(config-if)# switchport mode private-vlan promiscuous <cr>
Host Port Type	Switch(config-if)# switchport mode private-vlan host <cr>
Private VLAN Port Configuration	Switch(config)# interface gi1
PVLAN Port Type	Switch(config-if)# switchport mode private-vlan host
Host Association primary to secondary (The command is only available for host port.)	Switch(config-if)# switchport private-vlan host-association <2-4094> Primary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 <2-4094> Secondary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 3
Mapping primary to secondary VLANs (This command is only available for promiscuous port)	Switch(config)# interface gi1 Switch(config-if)# switchport mode private-vlan promiscuous Switch(config-if)# switchport private-vlan mapping 2 add 3 Switch(config-if)# switchport private-vlan mapping 2 add 4 Switch(config-if)# switchport private-vlan mapping 2 add 5
Private VLAN Information	
Private VLAN Information	Switch# show vlan private-vlan FLAGS: I -> Isolated P -> Promiscuous C -> Community Primary Secondary Type Ports ----- 2 3 Isolated gi1(P),gi2(I) 2 4 Community gi2(P),gi3(C) 2 5 Community gi2(P),gi1(C),gi3(I) 10 - - -

Private VLAN Information (Continued)	
Running Config Information	Switch# show run Building configuration...
Private VLAN Type	Current configuration: hostname Switch vlan learning independent ! vlan 1 ! vlan 2 private-vlan primary ! vlan 3 private-vlan isolated ! vlan 4 private-vlan community ! vlan 5 private-vlan community ! interface gigabitethernet7 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 5 ! interface gigabitethernet switchport access vlan add 2,4 switchport trunk native vlan 4 switchport mode private-vlan host switchport private-vlan host-association 2 4 ! interface gigabitethernet9 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 3 ! interface gigabitethernet10 switchport access vlan add 2,5 switchport trunk native vlan 2 switchport mode private-vlan promiscuous switchport private-vlan mapping 2 add 3-5
Private VLAN Port Information	

Private VLAN Information (Continued)	
PVLAN Type	<pre>Switch# show vlan private-vlan type Vlan Type Ports ----- 2 primary gi3 3 isolated gi2 4 community gi1 5 community gi4,gi5 10 primary -</pre>
Host List	<pre>Switch# show vlan private-vlan port-list Ports Mode Vlan ----- 1 normal - 2 normal - 3 normal - 4 normal - 5 normal - 6 normal - 7 host 5 8 host 4 9 host 3 10 promiscuous 2</pre>

5.10. Traffic Prioritization (CLI)

Quality of Service (QoS) provides a traffic prioritization mechanism which allows you to deliver better service to certain flows. QoS can also help to alleviate congestion problems and ensure high-priority traffic is delivered first. This section allows you to configure Traffic Prioritization settings for each port with regard to setting priorities.

ICRL-M QoS supports four physical queues, weighted fair queuing (WRR) and Strict Priority scheme, that follows the IEEE 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

Optionally, you can use the web user interface for configuration, see *Traffic Prioritization* on Page 101. This table provides detailed information about command lines for traffic prioritization configuration

QoS Setting	
Queue Scheduling – Strict Priority	<pre>Switch(config)# qos queue-sched sp Strict Priority wrr Weighted Round Robin Switch(config)# qos queue-sched sp The queue scheduling scheme is setting to Strict Priority.</pre>
Queue Scheduling - WRR	<pre>Switch(config)# qos queue-sched wrr <1-10> Weights for COS queue 0 (queue_id 0) Switch(config)# qos queue-sched wrr 10 <1-10> Weights for COS queue 1 (queue_id 1) Switch(config)# qos queue-sched wrr 1 2 3 4 The queue scheduling scheme is setting to Weighted Round Robin. Assign the ratio for the 4 classes of service.</pre>
Port Setting – CoS (Default Port Priority)	<pre>Switch(config)# interface gi1 Switch(config-if)# qos priority <0-3> Assign a priority queue Switch(config-if)# qos priority 3 The priority queue is set 3 ok.</pre>
QoS Priority Mode	<pre>Switch(config)# qos priority cos CoS dscp DSCP/TOS port-based Port-based Switch(config)# qos priority dscp Switch# show qos priority QoS Priority Mode: DSCP</pre>

QoS Setting (Continued)	
Display – Port Priority Setting (Port Default Priority)	<pre>Switch# show qos port-priority Port Default Priority : Port Priority Queue -----+----- 1 7 2 0 3 0 4 0 5 0 205 0 26 0 27 0 28 0</pre>
CoS-Queue Mapping	
Format	<pre>Switch(config)# qos cos-map PRIORITY Assign an priority (3 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-3)</pre> <p>Note: Format: qos cos-map priority_value queue_value.</p>
Map CoS 0 to Queue 1	<pre>Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok.</pre>
Map CoS 1 to Queue 0	<pre>Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok.</pre>
Map CoS 2 to Queue 0	<pre>Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok.</pre>
Map CoS 3 to Queue 1	<pre>Switch(config)# qos cos-map 3 1 The CoS to queue mapping is set ok.</pre>
Map CoS 4 to Queue 2	<pre>Switch(config)# qos cos-map 4 2 The CoS to queue mapping is set ok.</pre>
Map CoS 5 to Queue 2	<pre>Switch(config)# qos cos-map 5 2 The CoS to queue mapping is set ok.</pre>
Map CoS 6 to Queue 3	<pre>Switch(config)# qos cos-map 6 3 The CoS to queue mapping is set ok.</pre>
Map CoS 7 to Queue 3	<pre>Switch(config)# qos cos-map 7 3 The CoS to queue mapping is set ok.</pre>

CoS-Queue Mapping (Continued)	
Display – CoS-Queue mapping	<pre>Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue ---- + ----- 0 1 1 0 2 0 3 1 4 2 5 2 6 3 7 3</pre>
DSCP-Queue Mapping	
Format	<pre>Switch(config)# qos dscp-map <0-63> Assign an priority (63 highest) Switch(config)# qos dscp-map 0 <0-3> Assign an queue (0-3)</pre> <p>Format: qos dscp-map priority_value queue_value</p>
Map DSCP 0 to Queue 1	<pre>Switch(config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.</pre>
Display – DSCO-Queue mapping	<pre>Switch# show qos dscp-map DSCP to Queue Mapping : (dscp = d1 d2) d2 0 1 2 3 4 5 6 7 8 9 d1 -----+----- 0 1 1 1 1 1 1 1 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 2 0 0 0 0 1 1 1 1 1 1 1 3 1 1 1 2 2 2 2 2 2 2 2 4 2 2 2 2 2 2 2 2 3 3 5 3 3 3 3 3 3 3 3 3 3 3 6 3 3 3 3</pre>

5.11. Multicast Filtering (CLI)

For multicast filtering, the ICRL-M uses IGMP (Internet Group Management Protocol) Snooping technology. IGMP is an internet protocol that provides a way for internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data.

Multicasting is useful for such applications as updating the address books of mobile computer users in the field, sending out newsletters to a distribution list, and broadcasting streaming media to an audience that has tuned into the event by setting up multicast group membership.

In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown in the following table.

Message	
Query	A message sent from the querier (an IGMP router or a switch) that asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

You can enable **IGMP Snooping** and **IGMP Query** functions. This section illustrates the information of the IGMP Snooping function, including different multicast groups' VID and member ports, and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255.

Optionally, you can use the web user interface for configuration, see *Multicast Filtering* on Page 106.

The following table provides detailed information about command lines for multicast filtering configuration.

IGMP Snooping	
IGMP Snooping - Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Specify on which vlans IGMP snooping enables
IGMP Snooping - VLAN	Switch(config)# ip igmp snooping vlan VLANLIST allowed vlan list all all existed vlan Switch(config)# ip igmp snooping vlan 1-2 IGMP snooping is enabled on VLAN 1-2.
Disable IGMP Snooping - Global	Switch(config)# no ip igmp snooping IGMP snooping is disabled globally ok.
Disable IGMP Snooping - VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.

IGMP Snooping (Continued)	
Display – IGMP Snooping Setting	<pre>Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv1 query-interval; 125s query-max-response-time: 10s Switch# sh ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled Vlan2 is IGMP snooping enabled Vlan3 is IGMP snooping disabled</pre>
Display – IGMP Table	<pre>Switch# sh ip igmp snooping multicast all VLAN IP Address Type Ports ----- 1 239.192.8.0 IGMP gi6, 1 239.255.255.250 IGMP gi6,</pre>
IGMP Query	
IGMP Query V1	<pre>Switch(config)# int vlan 1 Switch(config-if)# ip igmp v1</pre>
IGMP Query V2	<pre>Switch(config)# int vlan 1 Switch(config-if)# ip igmp</pre>
IGMP Query version	<pre>Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2</pre>
IGMP Query Interval	<pre>Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp Switch(config-if)# ip igmp query-interval 60 (Change query interval to 60 seconds, default value is 125 seconds)</pre>
IGMP Query Max Response Time	<pre>Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp Switch(config-if)# ip igmp query-max-response-time 15 (Change query max response time to 15 seconds, default value is 10 seconds)</pre>
Disable	<pre>Switch(config)# int vlan 1 Switch(config-if)# no ip igmp</pre>

IGMP Query (Continued)	
Display	<pre>Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config ! interface vlan1 ip address 192.168.250.17/24 ip igmp no shutdown !</pre>
Unknown Multicast	
Send Unknown Multicast to Query Ports	<pre>Switch(config)# ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning enabled</pre>
Send Unknown Multicast to All Ports	<pre>Switch(config)# no ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning disabled Switch(config)# no mac-address-table multicast filtering Flooding unknown multicast addresses ok!</pre>
Discard All Unknown Multicast	<pre>Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok!</pre>

GMRP Configuration	
Enable GMRP globally	Switch(config)# gmrp mode enable Gmrp is enabled on the switch!
Disable GMRP globally	Switch(config)# gmrp mode disable Gmrp is disabled on the switch!
Enable GMRP on a port	Switch(config)# gmrp mode enable gi1 Gmrp enabled on port 1 !
Disable GMRP on a port	Switch(config)# gmrp mode disable gi2 Gmrp disabled on port 2 !
Display	Switch# sh gmrp GMRP global enabled port 1 : enabled port 2 : enabled port 3 : disabled port 4 : disabled port 5 : disabled port 6 : disabled port 7 : disabled port 8 : disabled port 9 : disabled port 10 : disabled
Force Filtering	
Enable	Switch(config)# mac-address-table force filtering Filtering unknown multicast addresses ok!
Disable	Switch(config)# no mac-address-table force filtering Flooding unknown multicast addresses ok!

5.12. SNMP (CLI)

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. The ICRL-M supports SNMP v1 and v2c and V3.

An SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP compatible format. The manager is the console through the network.

Optionally, you can use the web user interface for configuration, see *SNMP* on Page 111.

The following table provides detailed information about command lines for SNMP configuration.

SNMP Community	
Read Only Community	Switch(config)# snmp-server community public ro community string add ok
Read Write Community	Switch(config)# snmp-server community private rw community string add ok
SNMP Trap	
Enable Trap	Switch(config)# snmp-server enable trap Set SNMP trap enable ok.
SNMP Trap Server IP without specific community name	Switch(config)# snmp-server host 192.168.250.33 SNMP trap host add OK.
SNMP Trap Server IP with version 1 and community	Switch(config)# snmp-server host 192.168.250.33 version 1 private SNMP trap host add OK. Note: Private is the community name, version 1 is the SNMP version.
SNMP Trap Server IP with version 2 and community	Switch(config)# snmp-server host 192.168.250.33 version 2 private SNMP trap host add OK.
Disable SNMP Trap	Switch(config)# no snmp-server enable trap Set SNMP trap disable ok.
Display	Switch# sh snmp-server trap SNMP trap: Enabled SNMP trap community: public Switch# show running-config snmp-server community public ro snmp-server community private rw snmp-server enable trap snmp-server host 192.168.250.33 version 2 admin snmp-server host 192.168.250.33 version 1 admin

5.13. Security (CLI)

The ICRL-M provides several security features for you to secure your connection. Optionally, you can use the web user interface for configuration, see *Security* on Page 114. This table provides information about the command lines for security configuration.

Securing Interfaces	
Display	Switch# show service Telnet : Disabled Http : Disabled
Telnet	Switch(config)# service telnet enable
HTTP	Switch(config)# service http enable
Port Security	
Add MAC access list	Switch(config)# mac access-list extended NAME access-list name Switch(config)# mac access-list extended server1 Switch(config-ext-macl)# permit Specify packets to forward deny Specify packets to reject end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode
Add IP Standard access list	Switch(config)# ip access-list extended Extended access-list standard Standard access-list Switch(config)# ip access-list standard <1-99> Standard IP access-list number <1300-1999> Standard IP access-list number (expanded range) WORD Access-list name Switch(config)# ip access-list standard 1 Switch(config-std-acl)# deny Specify packets to reject permit Specify packets to forward end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode remark Access list entry comment

Port Security (Continued)	
Add IP Extended access list	<pre>Switch(config)# ip access-list extended <100-199> Extended IP access-list number <2000-2699> Extended IP access-list number (expanded range) WORD access-list name Switch(config)# ip access-list extended 100 Switch(config-ext-acl)# deny Specify packets to reject permit Specify packets to forward end End current mode and down to previous mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode remark Access list entry comment</pre>
Example 1: Edit MAC access list	<pre>Switch(config-ext-macl)#permit MACADDR Source MAC address xxxx.xxxx.xxxx any any source MAC address host A single source host Switch(config-ext-macl)#permit host MACADDR Source MAC address xxxx.xxxx.xxxx Switch(config-ext-macl)#permit host 00:0D:81:09:FD:E4 .2233 MACADDR Destination MAC address xxxx.xxxx.xxxx any any destination MAC address host A single destination host Switch(config-ext-macl)#permit host 00:0D:81:09:FD:E4 .2233 host MACADDR Destination MAC address xxxx.xxxx.xxxx Switch(config-ext-macl)#permit host 00:0D:81:09:FD:E4 .2233 host 00:0D:81:09:FD:E4 .2234 [IFNAME] Egress interface name Switch(config-ext-macl)#permit host 00:0D:81:09:FD:E4 .2233 host 00:0D:81:09:FD:E4 .2234 gi25 MAC Rule: Permit/Deny wildcard Source_MAC wildcard Dest_MAC Egress_Interface.</pre>

Port Security (Continued)	
Example 1: Edit IP Extended access list	<pre>Switch(config)# ip access-list extended 100 Switch(config-ext-acl)#permit ip Any Internet Protocol tcp Transmission Control Protocol udp User Datagram Protocol icmp Internet Control Message Protocol Switch(config-ext-acl)#permit ip A.B.C.D Source address any Any source host host A single source host Switch(config-ext-acl)#permit ip 192.168.10.1 A.B.C.D Source wildcard bits Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 A.B.C.D Destination address any Any destination host host A single destination host Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 [IFNAME] Egress interface name Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 gi26</pre> <p>Note: Follow the below rules to configure ip extended access list.</p> <p>IP Rule: Permit/Deny Source_IP wildcard Dest_IP wildcard Egress_Interface</p> <p>TCP Rule: Permit/Deny tcp Source_IP wildcard Dest_IP wildcard eq Given_Port_Number Egress_Interface</p> <p>UDP Rule: Permit/Deny udp Source_IP wildcard Dest_IP wildcard eq Given_Port_Number Egress_Interface</p> <p>ICMP Rule: Permit/Deny icmp Source_IP wildcard Dest_IP wildcard ICMP_Message_Type ICMP_Message_Code Egress_Interface</p>
Add MAC	<pre>Switch(config)# mac-address-table static 00:0D:81:09:FD:E4 vlan 1 interface gi1 mac-address-table unicast static set ok!</pre>
Port Security	<pre>Switch(config)# interface gi1 Switch(config-if)# switchport port-security</pre> <p>Disables new MAC addresses learning and aging activities!</p> <p>Rule: Add the static MAC, VLAN and Port binding first, then enable the port security to stop new MAC learning.</p>
Disable Port Security	<pre>Switch(config-if)# no switchport port-security</pre> <p>Enable new MAC addresses learning and aging activities!</p>
Display	<pre>Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ----- 00:0D:81:09:FD:E4 Static 1 gi1</pre>

802.1x	
enable	Switch(config)# dot1x system-auth-control Switch(config)#
disable	Switch(config)# no dot1x system-auth-control Switch(config)#
authentic-method	Switch(config)# dot1x authentic-method local Use the local username database for authentication RADIUS Use the Remote Authentication Dial-In User Service (RADIUS) servers for authentication Switch(config)# dot1x authentic-method RADIUS Switch(config)#
RADIUS server-ip	Switch(config)# dot1x RADIUS Switch(config)# dot1x RADIUS server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.10.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
RADIUS server-ip	Switch(config)# dot1x RADIUS Switch(config)# dot1x RADIUS server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.10.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
RADIUS secondary-server-ip	Switch(config)# dot1x RADIUS secondary-server-ip 192.168.10.250 key 5678 Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) Secondary RADIUS Server IP : 192.168.10.250 Secondary RADIUS Server Key : 5678 Secondary RADIUS Server Port : 1812 Secondary RADIUS Accounting Port : 1813
User name/password for authentication	Switch(config)# dot1x username Pepperl+Fuchs passwd Pepperl+Fuchs vlan 1

5.14. Warnings (CLI)

The ICRL-M provides several types of warning features for you to remotely monitor the status of the attached devices or changes in your network. The features include Fault Relay, System Log and SMTP Email Alert.

Optionally, you can use the web user interface for configuration, see *Warning* on Page 140.

This table provides detailed information about the command lines of the warning configuration.

Fault Relay Output	
Relay Output	Switch(config)# relay 1 di DI State dry dry output ping ping failure port port link failure power power failure ring ring failure
DI State	Switch(config)# relay 1 di 1 DI number Switch(config)# relay 1 di 1 high high is abnormal low low is abnormal Switch(config)# relay 1 di 1 high
Dry Output	Switch(config)# relay 1 dry <0-65535> turn on period in second Switch(config)# relay 1 dry 5 <0-65535> turn off period in second Switch(config)# relay 1 dry 5 5
Ping Failure	Switch(config)# relay 1 ping 192.168.250.33 <cr> reset reset a device Switch(config)# relay 1 ping 192.168.250.33 reset <1-65535> reset time Switch(config)# relay 1 ping 192.168.250.33 reset 60 <0-65535> hold time to retry Switch(config)# relay 1 ping 192.168.250.33 reset 60 60
Port Link Failure	Switch(config)# relay 1 port PORTLIST port list Switch(config)# relay 1 port gi1-5
Power Failure	Switch(config)# relay 1 power <1-2> power id any Anyone power failure asserts relay Switch(config)# relay 1 power 1 Switch(config)# relay 1 power 2
Ring Failure	Switch(config)# relay 1 ring

Fault Relay Output (Continued)	
Disable Relay	Switch(config)# no relay 1-2 relay id Switch(config)# no relay 1 <cr>
Display	Switch# show relay 1 Relay Output Type : Port Link Port : 1, 2, 3, 4
Event Selection	Switch(config)# warning-event coldstart Switch cold start event warmstart Switch warm start event linkdown Switch link down event linkup Switch link up event authentication Authentication failure event ring Switch ring event time-sync Switch time synchronize event
Example: Cold Start event	Switch(config)# warning-event coldstart Set cold start event enable ok.
Example: Link Up event	Switch(config)# warning-event linkup [IFNAME] Interface list, ex: Switch(config)# warning-event linkup Set 5 link up event enable ok.
Display	Switch# show warning-event Warning Event: Cold Start: Enabled Warm Start: Disabled Authentication Failure: Disabled Link Down: gi4-5 Link Up: gi4-5 Power Failure: Ring: Disabled Fault Relay: Disabled Time synchronize Failure: Disabled SFP: Enabled DI: Disabled DHCP Snooping: Disabled DAI Statistics Changed: Disabled IPSG Statistics Changed: Disabled Port Security: Disabled

Syslog Configuration	
Local Mode	Switch(config)# log syslog local
Server Mode	Switch(config)# log syslog remote 192.168.250.33
Both	Switch(config)# log syslog local Switch(config)# log syslog remote 192.168.250.33
Disable	Switch(config)# no log syslog local
SMTP Configuration	
SMTP Enable	Switch(config)# smtp-server enable email-alert SMTP Email Alert set enable ok.
Sender mail	Switch(config)# smtp-server server 192.168.250.100 ACCOUNT SMTP server mail account, ex: admin@Pepperl+Fuchs.com Switch(config)# smtp-server server 192.168.250.100 admin@Pepperl+Fuchs.com SMTP Email Alert set Server: 192.168.250.100, Account: admin@Pepperl+Fuchs.com ok.
Receiver mail	Switch(config)# smtp-server receipt 1 abc@Pepperl+Fuchs.com SMTP Email Alert set receipt 1: abc@Pepperl+Fuchs.com ok.
Authentication with user name and password	Switch(config)# smtp-server authentication username admin password admin SMTP Email Alert set authentication Username: admin, Password: admin Note: You can assign string to user name and password.
Disable SMTP	Switch(config)# no smtp-server enable email-alert SMTP Email Alert set disable ok.
Disable Authentication	Switch(config)# no smtp-server authentication SMTP Email Alert set Authentication disable ok.
Display	Switch# sh smtp-server SMTP Email Alert is Enabled Server: 192.168.250.100, Account: admin@Pepperl+Fuchs.com Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: abc@Pepperl+Fuchs.com Receipt 2: Receipt 3: Receipt 4:

5.15. Monitor and Diag (CLI)

The ICRL-M provides several types of features for you to monitor the status of the switch or diagnostic for you to check the problem when encountering problems related to the switch. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log, and Ping.

Optionally, you can use the web user interface for configuration, see *Monitor and Diag* on Page 146.

This table provides detailed information about command lines of the Monitor and Diag configuration.

MAC Address Table	
Aging Time	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! Note: The default aging timeout value is 300.
Add Static Unicast MAC address	Switch(config)# mac-address-table static 00:0D:81:09:FD:E4 vlan 1 interface gigabitethernet5 mac-address-table ucast static set ok! Rule: mac-address-table static MAC_address VLAN VID interface interface_name
Add Multicast MAC address	Switch(config)# mac-address-table multicast 00:0D:81:09:FD:E4 vlan 1 interface gi3-4 Adds an entry in the multicast table ok! Rule: mac-address-table multicast MAC_address VLAN VID interface_list interface_name/range
Show MAC Address Table – All types	Switch# show mac-address-table ***** UNICAST MAC ADDRESS ***** Destination Address Address Type Vlan Destination Port ----- 00:0D:81:09:FD:E4 .ca3b Dynamic 1 gi1 00:0D:81:09:FD:E4 .0386 Dynamic 1 gi2 00:0D:81:09:FD:E4 .0101 Static 1 gi3 00:0D:81:09:FD:E4 .0102 Static 1 gi3 00:0D:81:09:FD:E4 .0100 Management 1 ***** MULTICAST MAC ADDRESS ***** Vlan Mac Address COS Status Ports ----- 1 00:0D:81:09:FD:E4 .0800 0 gi6 1 00:0D:81:09:FD:E4 .ffa 0 gi4,gi6
Show MAC Address Table – Dynamic Learnt MAC addresses	Switch# show mac-address-table dynamic Destination Address Address Type Vlan Destination Port ----- 00:0D:81:09:FD:E4 .ca3b Dynamic 1 gi4 00:0D:81:09:FD:E4 .0386 Dynamic 1 gi6
Show MAC Address Table – Multicast MAC addresses	Switch# show mac-address-table multicast Vlan Mac Address COS Status Ports ----- 1 00:0D:81:09:FD:E4 .0800 0 gi5-6 1 00:0D:81:09:FD:E4 .ffa 0 gi3,gi5-6

4/21/20

MAC Address Table (continued)	
Show MAC Address Table – Static MAC addresses	<pre>Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ----- 00:0D:81:09:FD:E4 Static 1 gi4 000D.8109.FDE5 Static 1 gi5</pre>
Show Aging timeout time	<pre>Switch# show mac-address-table aging-time the mac-address-table aging-time is 300 sec.</pre>
Port Statistics	
Port Statistics	<pre>Switch# show rmon statistics gi4 (select interface) Interface gigabitethernet4 is enable connected, which has Inbound: Good Octets: 178792, Bad Octets: 0 Unicast: 598, Broadcast: 1764, Multicast: 160 Pause: 0, Undersize: 0, Fragments: 0 Oversize: 0, Jabbers: 0, Discards: 0 Filtered: 0, RxError: 0, FCSError: 0 Outbound: Good Octets: 330500 Unicast: 602, Broadcast: 1, Multicast: 2261 Pause: 0, Deferred: 0, Collisions: 0 SingleCollision: 0, MultipleCollision: 0 ExcessiveCollision: 0, LateCollision: 0 Filtered: 0, FCSError: 0 Number of frames received and transmitted with a length of: 64: 2388, 65to127: 142, 128to255: 11 256to511: 64, 512to1023: 10, 1024toMaxSize: 42</pre>
Port Mirroring	
Enable Port Mirror	<pre>Switch(config)# mirror en Mirror set enable ok.</pre>
Disable Port Mirror	<pre>Switch(config)# mirror disable Mirror set disable ok.</pre>
Select Source Port	<pre>Switch(config)# mirror source gi1-2 both Received and transmitted traffic rx Received traffic tx Transmitted traffic Switch(config)# mirror source gi1-2 both Mirror source gi1-2 both set ok. Note: Select source port list and TX/RX/Both mode.</pre>
Select Destination Port	<pre>Switch(config)# mirror destination gi6 Mirror destination gi6 set ok</pre>

Port Mirroring (Continued)	
Display	<pre>Switch# show mirror Mirror Status : Enabled Ingress Monitor Destination Port : gi6 Egress Monitor Destination Port : gi6 Ingress Source Ports :gi1,gi2, Egress Source Ports :gi1,gi2,</pre>
Event Log	
Display	<pre>Switch# show event-log <1>Jan 1 02:50:47 snmpd[101]: Event: Link 4 Down. <2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up. <3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down. <4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.</pre>
Topology Discovery (LLDP)	
Enable LLDP	<pre>Switch(config)# lldp holdtime Specify the holdtime of LLDP in seconds run Enable LLDP timer Set the transmission frequency of LLDP in seconds Switch(config)# lldp run LLDP is enabled!</pre>
Change LLDP timer	<pre>Switch(config)# lldp holdtime <10-255> Valid range is 10~255 Switch(config)# lldp timer <5-254> Valid range is 5~254</pre>
Ping	
Ping IP	<pre>Switch# ping 192.168.11.14 PING 192.168.11.14 (192.168.11.14): 56 data bytes 64 bytes from 192.168.11.14: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=3 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=4 ttl=128 time=0.0 ms --- 192.168.11.14 ping statistics --- packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 1.3/1.3/1.4 ms</pre>

5.16. Saving to Flash (CLI)

Save Configuration allows you to save any configuration you just made to the flash. Powering off the switch without saving the configuration causes loss of the new settings.

Saving to Flash	
Save to Flash	<pre>SWITCH# write Building Configuration... [OK] Switch# copy running-config startup-config Building Configuration... [OK]</pre>

5.17. Logging Out (CLI)

The CLI connection logs out of configure terminal mode, if you do not input any command after 30 seconds.

Logging Out	
Logout	<pre>SWITCH> exit SWITCH# exit</pre>

5.18. Service (CLI)

The service command provides the ability to disable HTTP and Telnet.

Note: *There is not a web user interface page for the service command.*

Service	
Disable HTTP	<pre>Switch(config)# service http disable Switch(config)#</pre>
Enable HTTP	<pre>Switch(config)# service http enable Switch(config)#</pre>
Disable telnet	<pre>Switch(config)# service telnet disable Switch(config)#</pre>
Enable telnet	<pre>Switch(config)# service telnet enable Switch(config)#</pre>

6. Complete CLI List

This section provides the complete listing of RocketLinX ICRL-M commands with the supporting options:

- *User EXEC Mode*
- *Privileged EXEC Mode on Page 219*
- *Global Configuration Mode on Page 226*
- *Port Interface Configuration Mode on Page 234*
- *VLAN Interface Configuration Mode on Page 237*

6.1. User EXEC Mode

For information about accessing *User EXEC* mode, see *User EXEC Mode on Page 218*.

```
ICRL-M> list
enable
exit
list
ping A.B.C.D
ping WORD
ping X:X::X:X
quit
show gvrp statistics [IFNAME]
show ip forwarding
show ip route
show ip route A.B.C.D
show ip route A.B.C.D/M
show ip route supernets-only
show memory
show users
show version
telnet WORD
telnet WORD PORT
traceroute WORD
```

6.2. Privileged EXEC Mode

For information about accessing Privileged EXEC mode, see *Privileged EXEC Mode* on Page 219.

ICRL-M# list

```

archive download-boot /overwrite scp ACCOUNT PASSWORD IMAGE IPADDRESS [PORT]
archive download-boot /overwrite sftp ACCOUNT PASSWORD IMAGE IPADDRESS [PORT]
archive download-boot /overwrite tftp IPADDRESS IMAGE
archive download-sw /overwrite scp ACCOUNT PASSWORD IMAGE IPADDRESS [PORT]
archive download-sw /overwrite sftp ACCOUNT PASSWORD IMAGE IPADDRESS [PORT]
archive download-sw /overwrite tftp IPADDRESS IMAGE
clear erps statistics [0-31]
clear event-log
clear gvrp statistics [IFNAME]
clear ip arp inspection statistics interface [IFNAME]
clear ip arp inspection statistics vlan [VLANID]
clear ip dhcp snooping binding (allldynamicstatic)
clear ip dhcp snooping statistics
clear lacp counters
clear mac-address-table dynamic
clear mac-address-table dynamic address MACADDR
clear mac-address-table dynamic interface IFNAME
clear mac-address-table dynamic vlan VLANID
clear mac-address-table security interface IFNAME
clear redundant-ring statistics [0-31]
clear rmon statistics [IFNAME]
clear spanning-tree counters
clear spanning-tree counters interafce IFNAME
clear spanning-tree detected-protocols
clear spanning-tree detected-protocols interface IFNAME
clock set TIME MONTH DAY YEAR
configure terminal
copy running-config startup-config
copy sftp: URL startup-config ACCOUNT PASSWD
copy startup-config sftp: URL ACCOUNT PASSWD
copy startup-config tftp: URL
copy tftp: URL (ssh-dsslssh-rsa)
copy tftp: URL ssl-cert
copy tftp: URL startup-config
debug cfm (pdultraceldebuglall)
debug dot1x all
debug dot1x errors

```

4/21/20

```

debug dot1x events
debug dot1x packets
debug dot1x registry
debug dot1x state-machine
debug erps (pdultraceldebuglall) <0-31>
debug gmrp
debug gvrp (alllrcvltxlgvrp_eventlvlan_event)
debug ip arp inspection
debug ip dhcp (alllevent)
debug ip dhcp snooping
debug ip dhcp snooping packet
debug ip igmp
debug ip igmp snooping (alllgrouplmanagementlroutertimer)
debug l2 mac (allltraceldebug)
debug lacp (allleventlfsmlmiscpacket)
debug lldp
debug mirror
debug misc [type] [sub]
debug proto pdu
debug qos
debug rate-limit
debug redundant-ring (pdultraceldebuglrapid-dual-hominglrstplmulti-ringlall) <0-31>
debug snmp
debug spanning-tree (alllbpdulconfigleventslgenerallrootlsyncltc)
debug sw-rate-limit get (IFLISTlall) <0-64>
debug sw-rate-limit ioctl_dump
debug sw-rate-limit pkt_dump
debug sw-rate-limit set (IFLISTlall) <0-64> <0-1000>
debug sw-rate-limit set (IFLISTlall) <0-64> off
debug system hardware led mode <0-100>
debug system hardware relay mode <0-100>
debug system info
debug system meminfo
debug trunk
debug vlan (allltraceldebug)
disable
dot1x initialize interface IFNAME
dot1x reauthenticate interface IFNAME
end
exit
list
mac access-group dump <1-1536>

```

```

mac access-group show
no debug cfm
no debug dot1x all
no debug dot1x errors
no debug dot1x events
no debug dot1x packets
no debug dot1x registry
no debug dot1x state-machine
no debug erps <0-31>
no debug gmrp
no debug gvrp (allrcvltxlgvrp_eventlvlan_event)
no debug ip arp inspection
no debug ip dhcp (alllevent)
no debug ip dhcp snooping
no debug ip dhcp snooping packet
no debug ip igmp
no debug ip igmp snooping (allgroupmanagementlroutertimer)
no debug l2 mac (alltraceldebug)
no debug lacp (allleventlfsmlmiscpacket)
no debug lldp
no debug mirror
no debug proto
no debug qos
no debug rate-limit
no debug redundant-ring <0-31>
no debug snmp
no debug spanning-tree (allbpdulconfiglevents|generallrootlsyncltc)
no debug sw-rate-limit ioctl_dump
no debug sw-rate-limit pkt_dump
no debug system hardware led mode
no debug trunk
no debug vlan (alltraceldebug)
no pager
pager
ping A.B.C.D
ping WORD
ping X:X::X:X
quit
read ip dhcp snooping
reboot
reload default-config file
reload default-ssh file

```

4/21/20

```

reload default-ssl file
show acceptable frame type [IFNAME]
show arp access-list [ARP_ACL_NAME]
show auth method list
show auth radius
show auth tacacs+
show cfm database
show cfm domain [NAME]
show clock
show clock summer-time
show clock timezone
show debugging dot1x
show debugging gvrp
show debugging ip dhcp
show debugging ip igmp
show debugging ip igmp snooping
show debugging lacp
show debugging snmp
show debugging spanning-tree
show dot1q-tunnel
show dot1x
show dot1x all
show dot1x authentic-method
show dot1x info
show dot1x interface IFNAME
show dot1x radius
show dot1x statistics interface IFNAME
show dot1x username
show dot1x username mapping
show erps [0-31]
show erps instance
show ethernet-ip
show event-log
show garp timer [IFNAME]
show gmrp
show gvrp configuration [IFNAME]
show gvrp portstate IFNAME VID
show hardware led
show hardware mac
show ingress filtering [IFNAME]
show interface [IFNAME]
show interface vlan [VLANID]

```

4/21/20

```

show ip access-group [INTERFACE]
show ip access-list
show ip access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)
show ip arp inspection interface [IFNAME]
show ip arp inspection statistics interface [IFNAME]
show ip arp inspection statistics vlan [VLANID]
show ip arp inspection statistics-checking
show ip arp inspection vlan [VLANID]
show ip dhcp relay
show ip dhcp server
show ip dhcp server statistics
show ip dhcp snooping
show ip dhcp snooping binding
show ip dhcp snooping database write-delay
show ip forwarding
show ip igmp
show ip igmp group
show ip igmp interface IFNAME
show ip igmp query-interval
show ip igmp query-max-response-time
show ip igmp snooping
show ip igmp snooping multicast (dynamic|user|all) [VLANLIST]
show ip igmp snooping multicast count
show ip igmp snooping vlan (VLANLIST|all)
show ip igmp timers
show ip igmp version
show ip route
show ip route A.B.C.D
show ip route A.B.C.D/M
show ip route supernets-only
show ip verify source checking period
show ip verify source interface [IFNAME]
show ipv6 neighbour
show ipv6 route
show l2_interface [IFNAME]
show lacp counters [GROUPID]
show lacp group [1-8]
show lacp internal [1-8]
show lacp neighbor [1-8]
show lacp port-setting [IFNAME]
show lacp system-id
show lacp system-priority

```

4/21/20

```
show lldp
show lldp neighbors
show lldp statistics
show mac access-group [INTERFACE]
show mac access-list [WORD]
show mac-address-table
show mac-address-table aging-time
show mac-address-table dynamic
show mac-address-table dynamic address MACADDR
show mac-address-table dynamic interface IFNAME
show mac-address-table dynamic vlan VLANID
show mac-address-table multicast
show mac-address-table multicast MACADDR vlan VLANID
show mac-address-table multicast filtering
show mac-address-table security
show mac-address-table static
show mac-address-table static address MACADDR
show mac-address-table static interface IFNAME
show mac-address-table static vlan VLANID
show memory
show mirror
show modbus
show nameserver
show ntp associations
show port-security interface [IFNAME]
show process
show process backup
show ptp
show qos cos-map
show qos dscp-map
show qos port-priority
show qos queue-sched
show qos trust-mode
show rate-limit egress [IFNAME]
show rate-limit ingress [IFNAME]
show redundant-ring [0-31]
show relay 1
show relay 1 status
show rmon statistics [IFNAME]
show running-config
show service
show sfp
```

4/21/20

show sfp ddm
show smtp-server
show smtp-server authentication
show smtp-server email-alert
show smtp-server receipt
show smtp-server server
show snmp-server community
show snmp-server contact
show snmp-server host
show snmp-server info
show snmp-server location
show snmp-server name
show snmp-server trap
show snmp-server user
show spanning-tree active
show spanning-tree interface IFNAME
show spanning-tree mst
show spanning-tree mst <0-15>
show spanning-tree mst <0-15> interface IFNAME
show spanning-tree mst configuration
show spanning-tree mst interface IFNAME
show spanning-tree mst root
show spanning-tree summary
show startup-config
show storm-control [IFNAME]
show tftp
show trunk group [1-8]
show trunk load-balance group [1-8]
show users
show version
show vlan
show vlan (static|dynamic) [VLANID]
show vlan VLANID
show vlan dot1q-tunnel mapping
show vlan management
show vlan name VLANNAME
show vlan private-vlan
show vlan private-vlan port-list
show vlan private-vlan type
show warning-event
telnet WORD
telnet WORD PORT

4/21/20

```
traceroute WORD
write
write file
write ip dhcp snooping
write memory
write terminal
```

6.3. Global Configuration Mode

For information about accessing *Global Configuration* mode, see *Global Configuration Mode* on Page 226.

```
ICRL-M(config)# list
access-list test
arp access-list WORD
auth order <1-3>
auth radius server A.B.C.D key RADIUS_KEY [PORT]
auth tacacs+ (primary|secondary) server A.B.C.D <1-65535>
auth tacacs+ (primary|secondary) server secretkey KEY
auth tacacs+ authen_type (asciilpap|chap)
auth tacacs+ timeout <1-60>)
cfm create domain string NMAE md-level <0-7>
cfm delete domain NMAE
cfm domain NAME add association string NAME vlan <1-4094>
cfm domain NAME association NAME port IFNAME (add|delete) remote-mep <1-8191>
cfm domain NAME association NAME port IFNAME add end-point down <1-8191>
cfm domain NAME association NAME port IFNAME delete end-point down
cfm domain NAME association NAME transmit-interval (1000|10000|60000|600000)
cfm domain NAME delete association NAME
cfm group <0-255> rmep <1-8191>
clock set TIME MONTH DAY YEAR
clock summer-time (enable|disable)
clock summer-time <1-5> <0-6> <1-12> START_TIME <1-5> <0-6> <1-12> END_TIME
clock timezone
(0|1|02|03|04|05|06|07|08|09|10|11|12|13|14|15|16|17|18|19|20|21|22|23|24|25|26|27|28|29|30|31|32|33|34|35|
36|37|38|39|40|41|42|43|44|45|46|47|48|49|50|51|52|53|54|55|56|57|58|59|60|61|62|63|64|65|66|67|68|69|70|
71|72|73|74)
default dot1x system-auth-control
default gvrp configuration
default ip igmp snooping
dot1x authentic-method (radius|local)
dot1x radius secondary-server-ip A.B.C.D key RADIUS_KEY [PORT] [PORT]
dot1x radius server-ip A.B.C.D key RADIUS_KEY [PORT] [PORT]
dot1x system-auth-control
```

4/21/20

```

dot1x username WORD passwd WORD vlan <1-4094>
end
erps <0-31>
erps instance (enable|disable)
erps instance <0-15> vlan VLANMAP
ethernet-ip run
exit
gmrp mode (enable|disable)
gmrp mode (enable|disable) IFNAME
gvrp mode (enable|disable)
gvrp mode (enable|disable) IFNAME
gvrp registration (normal|fixed|forbidden) IFNAME
hostname .DWORD
interface IFNAME
interface vlan VLAN-ID
ip access-list extended (<100-199>|<2000-2699>)
ip access-list extended WORD
ip access-list standard (<1-99>|<1300-1999>)
ip access-list standard WORD
ip arp inspection filter ARP_ACL_NAME vlan VLANID
ip arp inspection gw-ip A.B.C.D vlan VLANID
ip arp inspection gw-ip verify vlan VLANID
ip arp inspection statistics-checking <1-60>
ip arp inspection vlan VLANID
ip dhcp snooping
ip dhcp snooping binding MACADDR vlan VLANID A.B.C.D interface IFNAME
ip dhcp snooping database write-delay <0-86400>
ip dhcp snooping verify mac-address
ip dhcp snooping vlan <1-4094>
ip forwarding
ip igmp snooping
ip igmp snooping immediate-leave
ip igmp snooping immediate-leave vlan (VLANLIST|all)
ip igmp snooping last-member-query-interval TIMEVALUE
ip igmp snooping last-member-query-interval TIMEVALUE vlan (VLANLIST|all)
ip igmp snooping source-only-learning vlan (VLANLIST|all)
ip igmp snooping vlan (VLANLIST|all)
ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE)
ip route A.B.C.D/M (A.B.C.D|INTERFACE)
ip source binding MACADDR vlan VLANID A.B.C.D interface IFNAME
ip verify source checking period <1-60>
ipv6 route X::X::X/M (X::X::X|INTERFACE)

```

```

lACP group <1-8> IFLIST
lACP system-priority <1-65535>
list
lldp holdtime <10-255>
lldp run
lldp timer <5-254>
log stdout
log syslog local
log syslog remote A.B.C.D
mac access-list extended NAME
mac-address-table aging-time TIMEVALUE
mac-address-table multicast MACADDR vlan VLANID interface IFLIST
mac-address-table multicast filtering vlan (VLANLIST|all)
mac-address-table security MACADDR vlan VLANID interface IFNAME
mac-address-table static MACADDR vlan VLANID interface IFNAME
mirror (enable|disable)
mirror destination IFNAME
mirror source IFLIST (rx|tx|both)
modbus (enable|disable)
modbus idle-timeout <500-3000>
modbus master <1-20>
modbus port <1-65535>
nameserver A.B.C.D
no arp access-list WORD
no auth radius server A.B.C.D
no auth tacacs+ (primary|secondary) server
no cfm domain NAME association NAME transmit-interval
no clock set
no clock summer-time
no clock timezone
no dot1x authentic-method
no dot1x radius secondary-server-ip
no dot1x system-auth-control
no dot1x username WORD
no erps instance <0-15>
no ethernet-ip run
no hostname [HOSTNAME]
no interface IFNAME
no interface vlan VLAN-ID
no ip access-list extended (<100-199>|<2000-2699>|WORD)
no ip access-list standard (<1-99>|<1300-1999>|WORD)
no ip arp inspection filter vlan VLANID

```

```

no ip arp inspection gw-ip verify vlan VLANID
no ip arp inspection statistics-checking
no ip arp inspection vlan VLANID
no ip dhcp snooping
no ip dhcp snooping binding MACADDR vlan VLANID A.B.C.D interface IFNAME
no ip dhcp snooping binding table
no ip dhcp snooping verify mac-address
no ip dhcp snooping vlan <1-4094>
no ip forwarding
no ip igmp snooping
no ip igmp snooping immediate-leave
no ip igmp snooping immediate-leave vlan (VLANLIST|all)
no ip igmp snooping last-member-query-interval
no ip igmp snooping last-member-query-interval vlan (VLANLIST|all)
no ip igmp snooping source-only-learning vlan (VLANLIST|all)
no ip igmp snooping vlan (VLANLIST|all)
no ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE)
no ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE) <1-255>
no ip route A.B.C.D/M (A.B.C.D|INTERFACE)
no ip source binding MACADDR vlan VLANID A.B.C.D interface IFNAME
no ipv6 route X:X::X:X/M (X:X::X:X|INTERFACE)
no lacp group <1-8>
no lacp system-priority
no lldp run
no log stdout
no log syslog local
no log syslog remote
no mac access-list extended NAME
no mac-address-table aging-time
no mac-address-table multicast MACADDR vlan VLANID
no mac-address-table multicast MACADDR vlan VLANID interface IFLIST
no mac-address-table multicast filtering vlan (VLANLIST|all)
no mac-address-table security MACADDR vlan VLANID interface IFNAME
no mac-address-table static MACADDR vlan VLANID interface IFNAME
no mirror destination
no mirror source IFLIST (rx|tx|both)
no nameserver A.B.C.D
no ntp peer (primary|secondary)
no ptp run
no qos cos-map
no qos dscp-map
no qos queue-sched

```

no relay 1
 no relay 1 dry
 no relay 1 ping
 no relay 1 ping reset
 no relay 1 port
 no relay 1 power
 no relay 1 ring
 no relay <1-2> di
 no smtp-server authentication
 no smtp-server authentication username password
 no smtp-server enable email-alert
 no smtp-server receipt <1-4>
 no smtp-server server
 no snmp-server community WORD (rolrw)
 no snmp-server community trap
 no snmp-server contact
 no snmp-server enable trap
 no snmp-server host A.B.C.D [VERSION]
 no snmp-server location
 no snmp-server name
 no snmp-server user WORD v3
 no spanning-tree bridge-times
 no spanning-tree forward-time
 no spanning-tree hello-time
 no spanning-tree max-age
 no spanning-tree mst MSTMAP priority
 no spanning-tree mst configuration
 no spanning-tree mst forward-time
 no spanning-tree mst hello-time
 no spanning-tree mst max-age
 no spanning-tree mst max-hops
 no spanning-tree priority
 no spanning-tree transmission-limit
 no trunk group <1-8>
 no trunk load-balance group <1-8>
 no username NAME
 no vlan [VLANID]
 no warning-event (coldstart|warmstart)
 no warning-event (linkdown|linkup) [IFLIST]
 no warning-event authentication
 no warning-event dai-statistics-changed
 no warning-event dhcp-snooping

4/21/20

```

no warning-event di
no warning-event di 1
no warning-event fault-relay
no warning-event fault-relay 1
no warning-event ipsg-statistics-changed
no warning-event port-security [IFLIST]
no warning-event power <1-2>
no warning-event ring
no warning-event sfp
no warning-event time-sync
no write-config (daemonintegrated)
ntp peer (enable|disable)
ntp peer (primary|secondary) IPADDRESS
ptp announce-interval (0|1|2|3|4)
ptp announce-receipt-timeout <2-10>
ptp delay-mechanism (E2E|PTP)
ptp domain-number <0-3>
ptp min-pdelay-req-interval INTERVAL
ptp priority1 <0-255>
ptp priority2 <0-255>
ptp run
ptp run preferred-clock
ptp run slave
ptp sync-interval INTERVAL
qos cos-map PRIORITY QUEUE
qos dscp-map DSCP PRIORITY
qos queue-sched drr <0-2032> <0-2032> <0-2032> <0-2032> <0-2032> <0-2032> <0-2032> <0-2032>
qos queue-sched rr
qos queue-sched sp
qos queue-sched wrr <1-10> <1-10> <1-10> <1-10> <1-10> <1-10> <1-10> <1-10>
qos trust-mode (cos|dscp)
redundant-ring <0-31>
relay 1 di 1 (high|low)
relay 1 dry <0-65535> <0-65535>
relay 1 ping WORD
relay 1 ping WORD reset <1-65535> <0-65535>
relay 1 port PORTLIST
relay 1 power <1-2>
relay 1 power any
relay 1 ring
router dhcp
service http (enable|disable)

```

```

service https (enable|disable)
service netvision (enable|disable)
service telnet (enable|disable)
sfp ddm (enable|disable) all
sfp eject all
sfp scan all
smtp-server authentication
smtp-server authentication username WORD password WORD
smtp-server enable email-alert
smtp-server receipt <1-4> EMAIL
smtp-server server A.B.C.D ACCOUNT
snmp-server community WORD (rolrw)
snmp-server community trap WORD
snmp-server contact .DWORD
snmp-server delay <0-1000000>
snmp-server enable trap
snmp-server host A.B.C.D
snmp-server host A.B.C.D version (1|2) [COMMUNITY]
snmp-server location .DWORD
snmp-server name .DWORD
snmp-server user WORD v3 auth (md5|sha) WORD
snmp-server user WORD v3 noauth
snmp-server user WORD v3 priv (md5|sha) WORD des WORD
spanning-tree (enable|disable)
spanning-tree bridge-times <4-30> <6-40> <1-10>
spanning-tree forward-time <4-30>
spanning-tree hello-time <1-10>
spanning-tree max-age <6-40>
spanning-tree mode (stp|rst)
spanning-tree mode mst
spanning-tree mst MSTMAP priority <0-61440>
spanning-tree mst configuration
spanning-tree mst forward-time <4-30>
spanning-tree mst hello-time <1-10>
spanning-tree mst max-age <6-40>
spanning-tree mst max-hops <1-40>
spanning-tree mst sync vlan <1-4094>
spanning-tree pathcost method (long|short)
spanning-tree priority <0-61440>
spanning-tree transmission-limit <1-10>
tftp disable
tftp enable

```

4/21/20


```
trunk group <1-8> IFLIST
trunk load-balance group <1-8> (src-macldst-maclsrc-dst-maclsrc-ipldst-iplsrc-dst-ip)
username NAME passwd plaintext PASSWD privilege PRIV
vlan <1-4094>
warning-event (coldstart|warmstart)
warning-event (linkdown|linkup) [IFLIST]
warning-event authentication
warning-event dai-statistics-changed
warning-event dhcp-snooping
warning-event di
warning-event di 1
warning-event fault-relay
warning-event fault-relay 1
warning-event ipsg-statistics-changed
warning-event port-security [IFLIST]
warning-event power <1-2>
warning-event ring
warning-event sfp
warning-event time-sync
write-config (daemon|integrated)
```

6.4. Port Interface Configuration Mode

For information about accessing *Port Interface Configuration* mode, see *Port Interface Configuration Mode* on Page 234.

```

ICRL-M(config)# interface gi1
ICRL-M(config-if)# list
  acceptable frame type (all|vlantaggedonly)
  description .LINE
  dot1x admin-control-direction (both|in)
  dot1x default
  dot1x guest-vlan <1-4094>
  dot1x host-mode (single-host|multi-host)
  dot1x mab
  dot1x max-req <1-10>
  dot1x port-control (auto|force-authorized|force-unauthorized)
  dot1x reauthentication
  dot1x timeout (reauth-period|quiet-period|tx-period|supp-timeout|server-timeout) TIMEVALUE
  duplex (half|full)
  end
  ethertype [0x0800-0xFFFF]
  exit
  flowcontrol (off|on)
  garp join-timer <10-10000>
  garp leave-timer <30-30000>
  garp leaveall-timer <150-150000>
  ingress filtering (enable|disable)
  ip access-group (<1-199> |<1300-2699>|WORD) in
  ip arp inspection limit none
  ip arp inspection limit rate <0-65>
  ip arp inspection trust
  ip dhcp snooping trust
  ip verify source port-security (ip|ip-mac)
  lacp port-priority <1-65535>
  lacp timeout (long|short)
  list
  loopback
  mac access-group NAME in
  media-type sfp speed (100|1000)
  mtu <64-9216>
  no description
  no dot1x admin-control-direction
  no dot1x guest-vlan
  
```

4/21/20

```

no dot1x host-mode
no dot1x mab
no dot1x max-req
no dot1x port-control
no dot1x reauthentication
no dot1x timeout (reauth-period|quiet-period|tx-period|supp-timeout|server-timeout)
no duplex
no garp join-timer
no garp leave-timer
no garp leaveall-timer
no ip access-group
no ip arp inspection limit
no ip arp inspection trust
no ip dhcp snooping trust
no ip verify source port-security
no lacp port-priority
no lacp timeout
no loopback
no mac access-group
no mtu
no qos priority
no rate-limit egress bandwidth
no rate-limit ingress bandwidth
no shutdown
no spanning-tree bpduguard
no spanning-tree bpduguard
no spanning-tree cost
no spanning-tree edge-port
no spanning-tree link-type
no spanning-tree mst MSTMAP cost
no spanning-tree mst MSTMAP port-priority
no spanning-tree port-priority
no spanning-tree stp-state
no storm-control (broadcast|dfl|multicast)
no switchport access vlan VLANID
no switchport block
no switchport dot1q-tunnel mode access
no switchport dot1q-tunnel mode uplink
no switchport mode private-vlan host
no switchport mode private-vlan promiscuous
no switchport mode svl
no switchport port-security
    
```

4/21/20

```

no switchport port-security auto-learn
no switchport port-security shutdown-time
no switchport port-security sticky
no switchport private-vlan host-association
no switchport trunk native vlan
no switchport vlan mapping VID dot1q-tunnel OUTERVID
qos priority DEFAULT-PRIORITY
quit
rate-limit egress bandwidth <64-1000000>
rate-limit ingress bandwidth <64-1000000>
sfp ddm (enable|disable)
sfp eject
sfp scan
shutdown
spanning-tree bpdupfilter
spanning-tree bpduguard
spanning-tree cost <1-200000000>
spanning-tree edge-port
spanning-tree link-type (auto|point-to-point|shared)
spanning-tree mst MSTMAP cost <1-200000000>
spanning-tree mst MSTMAP port-priority <0-240>
spanning-tree port-priority <0-240>
spanning-tree stp-state (enable|disable)
speed (10|100|1000|auto)
storm-control (broadcast|dfl|multicast) <2-262142>
switchport access vlan VLANID
switchport access vlan add VLANLIST
switchport access vlan remove VLANLIST
switchport block (multicast|unicast|both)
switchport dot1q-tunnel mode access
switchport dot1q-tunnel mode uplink
switchport mode private-vlan host
switchport mode private-vlan promiscuous
switchport mode svl VLANID
switchport port-security
switchport port-security auto-learn <0-10>
switchport port-security shutdown-time <0-86400>
switchport port-security sticky
switchport private-vlan host-association <2-4094> <2-4094>
switchport private-vlan mapping <2-4094> add VLANLIST
switchport private-vlan mapping <2-4094> remove VLANLIST
switchport trunk allowed vlan add VLANLIST
  
```

4/21/20

```
switchport trunk allowed vlan remove VLANLIST
switchport trunk native vlan VLANID
switchport vlan mapping VID dot1q-tunnel OUTERVID
```

6.5. VLAN Interface Configuration Mode

For information about accessing VLAN Interface Configuration mode, see *VLAN Interface Configuration Mode* on Page 237.

```
ICRL-M(config-if)# interface vlan1
ICRL-M(config-if)# list
description .LINE
end
exit
ip address A.B.C.D/M
ip dhcp client
ip dhcp client renew
ip igmp
ip igmp last-member-query-count CNT
ip igmp last-member-query-interval SECONDS
ip igmp query-interval SECONDS
ip igmp query-max-response-time SECONDS
ip igmp robustness-variable CNT
ip igmp version (1|2)
ipv6 accept-ra
ipv6 address X:X::X:X/M
list
no description
no ip address A.B.C.D/M
no ip dhcp client
no ip igmp
no ipv6 accept-ra
no ipv6 address X:X::X:X/M
no shutdown
quit
shutdown
```

7. Technical Support

7.1. Pepperl+Fuchs SFP Modules

Pepperl+Fuchs provides a variety of SFP transceivers. These certified SFP transceivers can be identified by the RocketLinx ICRL-M and displayed in the web user interface. We recommend using Pepperl+Fuchs SFPs when configuring your RocketLinx ICRL-M.

Note: *Low quality SFP transceivers may result in poor network performance and may not meet claimed distance or temperature ratings.*

7.2. Pepperl+Fuchs Private MIB

Pepperl+Fuchs supports many standard MIBs for users to configure or monitor the switch configuration by SNMP. However, since some commands can't be found in standard MIBs, Pepperl+Fuchs provides a Private MIB file. Compile the private MIB file with your SNMP tool. The private MIB can be downloaded it from <https://www.pepperl-fuchs.com>.

The Private MIB tree is the same as the web tree. This is easier to understand and use. If you are not familiar with a standard MIB, you can directly use the private MIB to manage /monitor the switch, without the need to learn or find where the OIDs of the commands are.

FACTORY AUTOMATION – SENSING YOUR NEEDS



Worldwide Headquarters

Pepperl+Fuchs GmbH
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

USA Headquarters

Pepperl+Fuchs Inc.
Twinsburg, Ohio 44087 · USA
Tel. +1 330 4253555
E-mail: sales@us.pepperl-fuchs.com

Asia Pacific Headquarters

Pepperl+Fuchs Pte Ltd.
Company Registration No. 199003130E
Singapore 139942
Tel. +65 67799091
E-mail: sales@sg.pepperl-fuchs.com

www.pepperl-fuchs.com

 **PEPPERL+FUCHS**
SENSING YOUR NEEDS

Subject to modifications
Copyright PEPPERL+FUCHS • Printed in Germany

TDOCT-B286_ENG

4/21/20