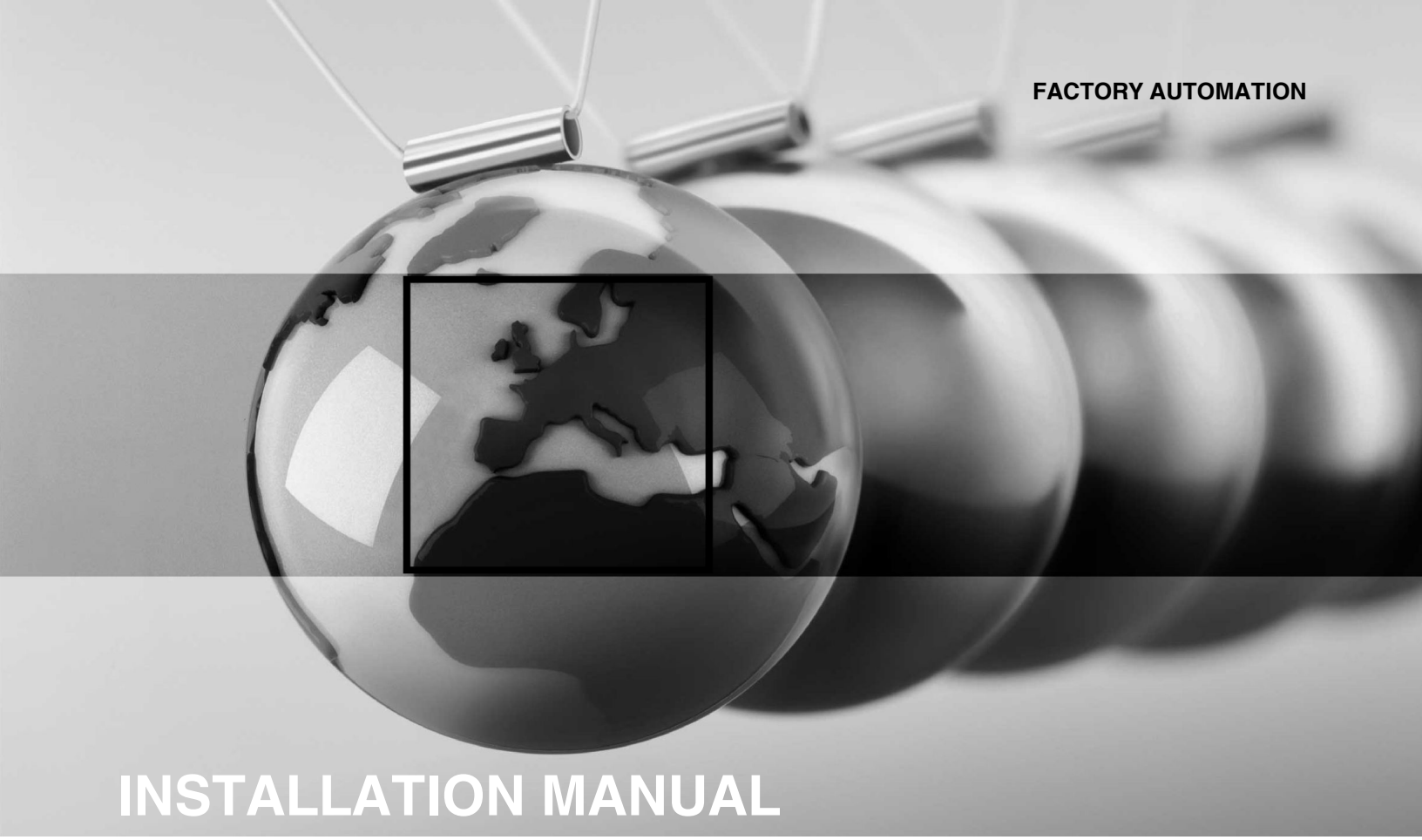
FACTORY AUTOMATION



INSTALLATION MANUAL

ICRL2-M Managed Switches

ICRL2-M-16RJ45/4SFP-10G-DIN

PEPPERL+FUCHS
SENSING YOUR NEEDS

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 10
1.1. Overview 10
1.1.1. ICRL2-M-16RJ45/4SFP-10G-DIN 10
1.2. Notices 11
1.2.1. FCC WARNING 11
1.2.2. CE 11
1.2.3. HOT& COLD WARNING 11
1.2.4. Warnings 11

2. Hardware Installation 13
2.1. Connector Overview 13
2.2. Installation Overview 13
2.3. DIN Rail Installation 14
2.3.1. Mounting the ICRL2-M 14
2.3.2. Dismounting the ICRL2-M 14
2.4. Grounding the ICRL2-M 15
2.5. Wiring the ICRL2-M 15
2.5.1. Wiring Power Input 16
2.5.2. Wiring the Relay Contact (ALM) 17
2.6. Connecting RJ45 Cables 17
2.7. Installing the SFP+ Modules and Fiber Cable 18
2.8. Setting the Alarm DIP Switches 18
2.9. LEDs 19

3. System Status 20
3.1. Console Port 20
3.2. Telnet 21
3.3. Starting the CLI 21
3.3.1. How to Enter Privileged Mode 21
3.4. CLI Commands 22
3.4.1. Command Table Overview 23
3.5. GUI Login 24
3.6. System Information 25
3.6.1. CLI Configuration 25
3.6.2. Web Configuration 25

4. Basic Settings 27
4.1. General Settings 27
4.1.1. System Settings 27
4.1.1.1. CLI Configuration - System Settings / System 27
4.1.1.2. Web Configuration - System Settings / System 29
4.1.2. Jumbo Frame 30
4.1.2.1. CLI Configuration - System Settings / Jumbo Frame 30
4.1.2.2. Web Configuration - System Settings / Jumbo Frame 31
4.1.3. SNTP 32
4.1.3.1. CLI Configuration - System Settings / SNTP 32

4.1.3.2. Web Configuration - System Settings / SNTP 34
4.1.4. Management Host 36
4.1.4.1. CLI Configuration - System Settings / Management Host 36
4.1.4.2. Web Configuration - System Settings / Management Host 37
4.2. MAC Management 38
4.2.1. Static MAC 39
4.2.1.1. CLI Configuration - MAC Management / Static MAC 39
4.2.1.2. Web Configuration - MAC Management / Static MAC 40
4.2.2. MAC Table 41
4.2.2.1. CLI Configuration - MAC Management / MAC Table 41
4.2.2.2. Web Configuration - MAC Management / MAC Table 41
4.2.3. Age Time Settings 42
4.2.3.1. CLI Configuration - MAC Management / Age Time 42
4.2.3.2. Web Configuration - MAC Management / Age Time 42
4.3. Port Mirror 43
4.3.1. CLI Configuration - Port Mirroring 44
4.3.2. Web Configuration - Port Mirror 45
4.4. Port Settings 46
4.4.1. General Settings 47
4.4.1.1. CLI Configuration - Port Settings / General Settings 47
4.4.1.2. Web Configuration - Port Settings / General Settings 48
4.4.2. Port Settings / Information 51
4.4.2.1. CLI Configuration - Port Settings / Information 51
4.4.2.2. Web Configuration - Port Settings / Information 52

5. Advanced Settings 53
5.1. Bandwidth Control 53
5.1.1. QoS 53
5.1.1.1. Bandwidth Control / QoS / Port Priority 55
5.1.1.1.1.CLI Configuration - Bandwidth Control / QoS / Port Priority 55
5.1.1.1.2.Web Configuration - Bandwidth Control / QoS / Port Priority 55
5.1.1.2. Bandwidth Control / QoS / IP DiffServ (DSCP) 56
5.1.1.2.1.CLI Configuration - Bandwidth Control / QoS / IP DiffServ (DSCP) 57
5.1.1.2.2.Web Configuration - Bandwidth Control / QoS / IP DiffServ (DSCP) 58
5.1.1.3. Bandwidth Control / QoS / Priority / Queue Mapping 59
5.1.1.3.1.CLI Configuration - Bandwidth Control / QoS / Priority Queue Mapping 59
5.1.1.3.2.Web Configuration - Bandwidth Control / QoS / Priority Queue Mapping 60
5.1.1.4. Bandwidth Control /QoS / Schedule Mode 60
5.1.1.4.1.CLI Configuration - Bandwidth Control /QoS / Schedule Mode 61
5.1.1.4.2.Web Configuration - Bandwidth Control /QoS / Schedule Mode 61
5.1.2. Bandwidth Control / Rate Limitation 63
5.1.2.1. Bandwidth Control / Rate Limitation / Storm Control 63
5.1.2.1.1.CLI Configuration - Bandwidth Control / Rate Limitation / Storm Control 63
5.1.2.1.2.Web Configuration - Bandwidth Control / Rate Limitation / Storm Control 64
5.1.2.2. Bandwidth Control / Rate Limitation / Bandwidth Limitation 65
5.1.2.2.1.CLI Configuration - Bandwidth Control / Rate Limitation / Bandwidth Limitation 65
5.1.2.2.2.Web Configuration - Bandwidth Control / Rate Limitation / Bandwidth Limitation 66
5.2. IGMP Snooping 67
5.2.1. IGMP Snooping Overview 67
5.2.1.1. IGMP Snooping General Settings 68
5.2.1.1.1.CLI Configuration - IGMP Snooping / General Settings 68
5.2.1.1.2.Web Configuration - IGMP Snooping / General Settings 69
5.2.1.2. IGMP Snooping Port Settings 70
5.2.1.2.1.CLI Configuration - IGMP Snooping / Port Settings 70
5.2.1.2.2.Web Configuration - IGMP Snooping / Port Settings 71

5.2.1.3. IGMP Snooping / Querier Settings 72
5.2.1.3.1.CLI Configuration - IGMP Snooping / Querier Settings 72
5.2.1.3.2.Web Configuration - IGMP Snooping / Querier Settings 73
5.2.2. IGMP Snooping / IGMP Filtering 74
5.2.2.1. General Settings - IGMP Snooping / IGMP Filtering 74
5.2.2.1.1.CLI Configuration - IGMP Snooping / IGMP Filtering / General Settings 74
5.2.2.1.2.Web Configuration - IGMP Snooping / IGMP Filtering / General Settings 74
5.2.2.2. IGMP Snooping / IGMP Filtering / Mulitcast Groups 75
5.2.2.2.1.CLI Configuration - IGMP Snooping / IGMP Filtering / Multicast Groups 75
5.2.2.2.2.Web Configuration - IGMP Snooping / IGMP Filtering / Multicast Groups 76
5.2.2.3. IGMP Snooping / IGMP Filtering / Port Settings 77
5.2.2.3.1.CLI Configuration - IGMP Snooping / IGMP Filtering / Port Settings 77
5.2.2.3.2.Web Configuration - IGMP Snooping / IGMP Filtering / Port Settings 77
5.2.3. Multicast Address Overview 79
5.2.3.1. CLI Configuration - IGMP Snooping / Multicast Address - IGMP Snooping / Multicast Address 81
5.2.3.2. Web Configuration - IGMP Snooping / Multicast Address 81
5.3. VLAN 83
5.3.1. VLAN / Port Isolation 83
5.3.1.1. CLI Configuration - VLAN / Port Isolation 83
5.3.1.2. Web Configuration - VLAN / Port Isolation 84
5.3.2. 802.1Q VLAN 86
5.3.2.1. VLAN / VLAN Settings 87
5.3.2.1.1.CLI Configuration - VLAN / VLAN Settings 87
5.3.2.1.2. Web Configuration - VLAN / VLAN Settings 88
5.3.2.2. VLAN / Tag Settings 89
5.3.2.2.1.CLI Configuration - VLAN / Tag Settings 89
5.3.2.2.2.Web Configuration - VLAN / Tag Settings 90
5.3.2.3. VLAN Port Settings 91
5.3.2.3.1.CLI Configuration - VLAN / Port Settings 91
5.3.2.3.2.Web Configuration - VLAN / Port Settings 92
5.3.3. MAC VLAN 93
5.3.3.1. CLI Configuration - MAC VLAN / MAC VLAN Settings 93
5.3.3.2. Web Configuration - MAC VLAN / MAC VLAN Settings 94
5.3.4. VLAN / Q-in-Q VLAN /VLAN Stacking 95
5.3.4.1. VLAN / Q-in-Q VLAN Stacking 98
5.3.4.1.1.CLI Configuration - VLAN / Q-in-Q / VLAN Stacking 98
5.3.4.1.2.Web Configuration - VLAN / Q-in-Q / VLAN Stacking 99
5.3.4.2. VLAN / Q-in-Q / Port-Based Q-in-Q 100
5.3.4.2.1.CLI Configuration - VLAN / Q-in-Q / Port-Based Q-in-Q 100
5.3.4.2.2.Web Configuration - VLAN / Q-in-Q / Port-Based Q-in-Q 101
5.4. DHCP Options / Option 82 102
5.4.1. CLI Configuration - DHCP Options / Option 82 104
5.4.2. Web Configuration - DHCP Options / Option 82 105
5.5. DHCP Relay 107
5.5.1. CLI Configuration - DHCP Relay 108
5.5.2. Web Configuration - DHCP Relay 109
5.6. Dual Homing 110
5.6.1. CLI Configuration - Dual Homing 110
5.6.2. Web Configuration - Dual Homing 111
5.7. Energy Efficient Ethernet (EEE) 113
5.7.1. CLI Configuration - Energy Efficient Ethernet 113
5.7.2. Web Configuration - Energy Efficient Ethernet 114
5.8. ERPS 115
5.8.1. ERPS / Ring 116

5.8.1.1. CLI Configuration - ERPS Ring 116
5.8.1.2. Web Configuration - ERPS Ring 117
5.8.2. ERPS / Instance 119
5.8.2.1. CLI Configuration ERPS / Instance 119
5.8.2.2. Web Configuration - ERPS Instance 119
5.9. Link Aggregation 121
5.9.1. Link Aggregation / Static Trunk 121
5.9.1.1. CLI Configuration - Link Aggregation / Static Trunk 121
5.9.1.2. Web Configuration - Link Aggregation / Static Trunk 122
5.9.2. Link Aggregation / LACP 123
5.9.2.1. CLI Configuration - Link Aggregation / LACP 123
5.9.2.2. Web Configuration - Link Aggregation / LACP 125
5.9.3. Link Aggregation / LACP Information 127
5.9.3.1. CLI Configuration - Link Aggregation / LACP Information 127
5.9.3.2. Web Configuration - Link Aggregation / LACP Information 127
5.10. Loop Detection 129
5.10.1. CLI Configuration - Loop Detection 129
5.10.2. Web Configuration - Loop Detection 131
5.11. Modbus TCP 133
5.11.1. CLI Configuration - Modbus TCP 139
5.11.2. Web Configuration - Modbus TCP 140
5.12. Spanning Tree Protocols (STP/RSTP) 141
5.12.1. Spanning Tree Protocol General Settings 144
5.12.1.1. CLI Configuration - Spanning Tree Protocol / General Settings 144
5.12.1.2. Web Configuration - Spanning Tree Protocol / General Settings 145
5.12.2. Spanning Tree Protocol / Port Parameters 146
5.12.2.1. CLI Configuration - Spanning Tree Protocol / Port Parameters 146
5.12.2.2. Web Configuration - Spanning Tree Protocol / Port Parameters 148
5.12.3. Spanning Tree Protocol / STP Status 149
5.12.3.1. CLI Configuration - Spanning Tree Protocol / STP Status 149
5.12.3.2. Web Configuration - Spanning Tree Protocol / STP Status 149

6. Security 151
6.1. IP Source Guard 151
6.1.1. DHCP Snooping 151
6.1.1.1. IP Source Guard / DHCP Snooping 154
6.1.1.1.1.CLI Configurations - IP Source Guard / DHCP Snooping 154
6.1.1.1.2.Web Configuration - IP Source Guard / DHCP Snooping 155
6.1.1.2. IP Source Guard / DHCP Snooping / Port Settings 156
6.1.1.2.1.CLI Configurations - IP Source Guard / DHCP Snooping / Port Settings 156
6.1.1.2.2.Web Configuration - IP Source Guard / DHCP Snooping / Port Settings 157
6.1.2. IP Source Guard / Binding Table 158
6.1.2.1. IP Source Guard / DHCP Snooping Binding Table / Static Entry 158
6.1.2.1.1.CLI Configurations - IP Source Guard / DHCP Snooping Binding Table / Static Entry 158
6.1.2.1.2.Web Configuration - IP Source Guard / DHCP Snooping Binding Table / Static Entry 159
6.1.2.2. IP Source Guard / DHCP Snooping Binding Table / Binding Table 160
6.1.2.2.1.CLI Configurations - IP Source Guard / DHCP Snooping Binding Table / Binding Table 160
6.1.2.2.2.Web Configuration - IP Source Guard / DHCP Snooping Binding Table / Binding Table 160
6.1.3. IP Source Guard / ARP Inspection 161
6.1.3.1. IP Source Guard / ARP Inspection 162
6.1.3.1.1.CLI Configurations - IP Source Guard / ARP Inspection 162

6.1.3.1.2.Web Configuration - IP Source Guard / ARP Inspection 163
6.1.3.2. IP Source Guard / ARP Inspection / Filter Table 164
6.1.3.2.1.CLI Configurations - IP Source Guard / ARP Inspection / Filter Table 164
6.1.3.2.2.Web Configuration - IP Source Guard / ARP Inspection / Filter Table 165
6.2. Access Control List (ACL) 166
6.2.1. CLI Configurations- Access Control List 167
6.2.2. Web Configuration - Access Control List 169
6.3. 802.1X 171
6.3.1. Global Settings 173
6.3.1.1. CLI Configurations - 802.1X / Global Settings 173
6.3.1.2. Web Configuration - 802.1X / Global Settings 174
6.3.2. 801.2X / Port Settings 176
6.3.2.1. CLI Configurations - 802.1X / Port Settings 176
6.3.2.2. Web Configuration - 802.1X / Port Settings 177
6.4. Port Security 179
6.4.1. Port Security 179
6.4.1.1. CLI Configurations - Port Security / Port Security Settings 179
6.4.1.2. Web Configuration - Port Security / Port Security Settings 180
6.5. TACACS+ 181
6.5.1. CLI Configurations - TACACS+ 182
6.5.2. Web Configuration - TACACS+ 184

7. Monitor 186
7.1. Alarm 186
7.1.1. CLI Configuration - Alarm 186
7.1.2. Web Configuration - Alarm 187
7.2. Port Statistics 188
7.2.1. CLI Configuration - Port Statistics 188
7.2.2. Web Configuration - Port Statistics 188
7.3. Port Utilization 189
7.3.1. CLI Configuration - Port Utilization 189
7.3.2. Web Configuration - Port Utilization 190
7.4. RMON Statistics 191
7.4.1. CLI Configuration - RMON Statistics 191
7.4.2. Web Configuration - RMON Statistics 191
7.5. Traffic Monitor 193
7.5.1. CLI Configuration - Traffic Monitor 193
7.5.2. Web Configuration - Traffic Monitor 195
7.6. SFP Information 197
7.6.1. CLI Configuration - SFP Information 197
7.6.2. Web Configuration - SFP Information 197
7.7. DI/DO Interface 199
7.7.1. CLI - DI/DO Interface Settings 199
7.7.2. Web Configuration - DI/DO Interface 201

8. Management 203
8.1. SNMP 203
8.1.1. SNMP 204
8.1.1.1. SNMP / SNMP Settings 204
8.1.1.1.1.CLI Configurations - SNMP / SNMP Settings 204
8.1.1.1.2.Web Configuration - SNMP / SNMP Settings 205
8.1.1.2. SNMP / SNMP / Community Name 206
8.1.1.2.1.CLI Configurations - SNMP / SNMP Community Name 206

8.1.1.2.2.Web Configuration - SNMP / SNMP / Community Name 206
8.1.2. SNMP / SNMP Trap / Trap Receiver 207
8.1.2.1. SNMP / SNMP Trap / Trap Receiver 207
8.1.2.1.1.CLI Configurations - SNMP / SNMP Trap / Trap Receiver 207
8.1.2.1.2.Web Configuration - SNMP / SNMP Trap / Trap Receiver 208
8.1.2.2. SNMP / SNMP Trap / Trap Event 209
8.1.2.2.1.CLI Configurations - SNMP / SNMP Trap / Trap Event 209
8.1.2.2.2.Web Configuration - SNMP / SNMP Trap / Trap Event 210
8.1.2.3. SNMP / SNMP Trap / Port Trap Event 211
8.1.2.3.1.CLI Configurations - SNMP / SNMP Trap / Port Trap Event 211
8.1.2.3.2.Web Configuration - SNMP / SNMP Trap / Port Trap Event 212
8.1.3. SNMP / SNMPv3 213
8.1.3.1. SNMP / SNMPv3 / Group Settings 213
8.1.3.1.1.CLI Configurations - SNMP / SNMPv3 / Group Settings 213
8.1.3.1.2.Web Configuration - SNMP / SNMPv3 / Group Settings 213
8.1.3.2. SNMP / SNMPv3 / User Settings 214
8.1.3.2.1.CLI Configurations - SNMP / SNMPv3 / User Settings 214
8.1.3.2.2.Web Configuration - SNMP / SNMPv3 / User Settings 215
8.1.3.3. SNMP / SNMPv3 / View Settings 216
8.1.3.3.1.CLI Configurations - SNMP / SNMPv3 / View Settings 216
8.1.3.3.2.Web Configuration - SNMP / SNMPv3 / View Settings 217
8.2. Auto Provision 218
8.2.1. CLI Configurations - Auto Provision 219
8.2.2. Web Configuration - Auto Provision 219
8.3. Mail Alarm 220
8.3.1. CLI Configurations - Mail Alarm 222
8.3.2. Web Configuration - Mail Alarm 223
8.4. Maintenance 224
8.4.1. Configuration 224
8.4.1.1. CLI Configurations - Maintenance / Configuration 224
8.4.1.2. Web Configuration - Maintenance / Configuration 226
8.4.2. Maintenance / Firmware 227
8.4.2.1. CLI Configurations - Maintenance / Firmware 227
8.4.2.2. Web Configuration - Maintenance / Firmware 228
8.4.3. Maintenance / Reboot 228
8.4.3.1. CLI Configurations - Maintenance / Reboot 228
8.4.3.2. Web Configuration - Maintenance / Reboot 228
8.4.4. Maintenance / Server Control 229
8.4.4.1. CLI Configurations - Maintenance / Server Control 229
8.4.4.2. Web Configuration - Maintenance / Server Control 230
8.5. Syslog 231
8.5.1. CLI Configurations - Syslog 231
8.5.2. Web Configuration - Syslog 232
8.6. USB Functions 233
8.6.1. CLI Configurations - USB Functions 233
8.6.2. Web Configuration - USB Functions 234
8.7. User Account 235
8.7.1. CLI Configurations - User Account 235
8.7.2. Web Configuration - User Account 236
8.8. Device Management 237
8.8.1. LLDP 237
8.8.1.1. CLI Configurations - Device Management / LLDP 237
8.8.1.2. Web Configuration - Device Management / LLDP 238
8.8.2. Manual Registration 240
8.8.2.1. CLI Configuration - Device Management / Manual Registration 240

8.8.2.2. Web Configuration - Device Management / Manual Registration 240
8.8.3. Device Management / ONVIF 242
8.8.3.1. CLI Configurations - Device Management / ONVIF 242
8.8.3.2. Web Configuration - Device Management / ONVIF 242
8.9. Topology Map 244

9. Technical Support 245
9.1. Cable Test 245
9.2. Support Contact Information 245

1. Introduction

This section includes the following subsections:

- *Overview*
- *Notices* on Page 11

1.1. Overview

RocketLinx ICRL2-M Manual refers to the following models in this manual unless a model is specifically mentioned.

- *ICRL2-M-16RJ45/4SFP-10G-DIN* on Page 10

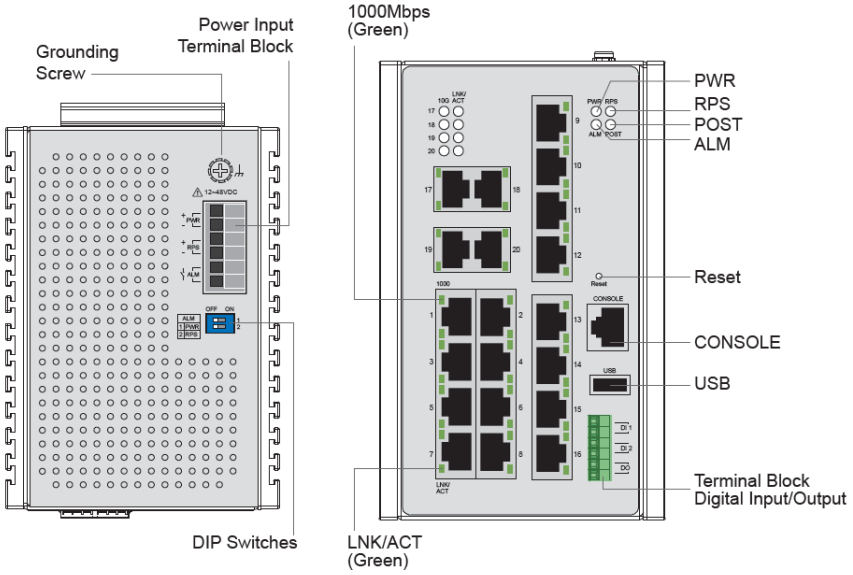
The ICRL2-M series is perfectly suited for industrial network applications, which require managed devices, that offer hassle-free fiber deployment and an ideal solution to deploy in automation as well as surveillance systems.

The ICRL2-M provides a rugged IP30 aluminum case and hardened components that withstand in operating temperatures from -40C to 75C.

1.1.1. ICRL2-M-16RJ45/4SFP-10G-DIN

The ICRL2-M-16RJ45/4SFP-10G-DIN:

- Sixteen standard RJ45 Ethernet ports
- Four 10G SFP ports



Top View **Front View**

8/19/25

1.2. Notices

1.2.1. FCC WARNING

This equipment has been tested and found to comply with the limits for a class A device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

1.2.2. CE

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

1.2.3. HOT& COLD WARNING



The ICRL2-M surface may get very hot or cold depending on the operating environment. Please take special care when touching the ICRL2-M.

1.2.4. Warnings



Take special care to read and understand all the content in the warnings in this manual.



Do not work on the system or connect or disconnect cables during periods of lightning activity!



Before working on the equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.



Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.



An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the terminal block plug.



Ethernet cables must be shielded when used in a central office environment.



If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.



Read the wall-mounting instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system.



Before performing any of the following procedures, ensure that power is removed from the DC circuit.



Read the installation instructions before connecting the system to the power source.



To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

1.This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

2. When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
3. If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.



This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.



Only trained and qualified personnel should be allowed to install, replace, or service this equipment.



When installing or replacing the unit, the ground connection must always be made first and disconnected last.



Voltages that present a shock hazard may exist on Power over Ethernet (PoE) circuits if interconnections are made using uninsulated exposed metal contacts, conductors, or terminals. Avoid using such interconnection methods, unless the exposed metal parts are located within a restricted access location and users and service people who are authorized within the restricted access location are made aware of the hazard. A restricted access area can be accessed only through the use of a special tool, lock and key or other means of security.



No user-serviceable parts inside. Do not open.



This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

2. Hardware Installation

This chapter includes the following information:

- *Connector Overview*
- *Installation Overview* on Page 13
- *DIN Rail Installation* on Page 14
- *Grounding the ICRL2-M* on Page 15
- *Wiring the ICRL2-M* on Page 15
- *Connecting RJ45 Cables* on Page 17
- *Setting the Alarm DIP Switches* on Page 18
- *LEDs* on Page 19

2.1. Connector Overview

The ICRL2-M utilizes ports with copper and SFP fiber port connectors functioning under Ethernet/Fast Ethernet/Gigabit Ethernet standards.

- 10/100/1000Base-T Ports

  The 10/100/1000Base-T ports support network speeds of 10 Mbit/s, 100 Mbit/s or 1000 Mbit/s, and can operate in half- and full-duplex transfer modes.

  These ports also offer automatic MDI/MDI-X crossover detection that gives true “plug-n-play” capability – just plug the network cables into the ports and the ports will adjust according to the end-node devices.

  The following are recommended cabling for the RJ45 connectors: (1) 10Mbit/s – Cat 3 or better; (2) 100/1000 Mbit/s – Cat 5e or better.

- SFP Slots for SFP+ Modules

  The four SFP slots are designed to 1G/10G SFP+ modules that support network speed of 1G/10G.

2.2. Installation Overview

The location chosen for installing the ICRL2-M may greatly affect its performance. When selecting, we recommend considering the following rules:

- Install the ICRL2-M in an appropriate place. See the datasheet at: **https://www.pepperl-fuchs.com** for the acceptable temperature and humidity ranges for your model.
- Install the ICRL2-M in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- Leave at least 10 cm of space at the front and rear of the unit for ventilation.



ATTENTION:

The ICRL2-M-16RJ45/4SFP-10G-DIN is an open type device and ICRL2-M-16RJ45/4SFP-10G-DIN shall be DIN-Rail mounted or wall mounted (optional) in cabinet or enclosure.

2.3. DIN Rail Installation

ATTENTION:

The ICRL2-M is an open type device and shall be DIN-Rail mounted or wall mounted (optional) in the cabinet and the ambient temperature should not exceed the operating temperature.

A corrosion-free mounting rail is advisable. When installing, make sure to allow for enough space between devices to properly install the cabling and provide ample space for air flow.

2.3.1. Mounting the ICRL2-M

Place the ICRL2-M on the DIN rail from above using the slot, push the front of the switch toward the mounting surface until it snaps into place with a click sound.

ATTENTION

A corrosion-free mounting rail is advisable.

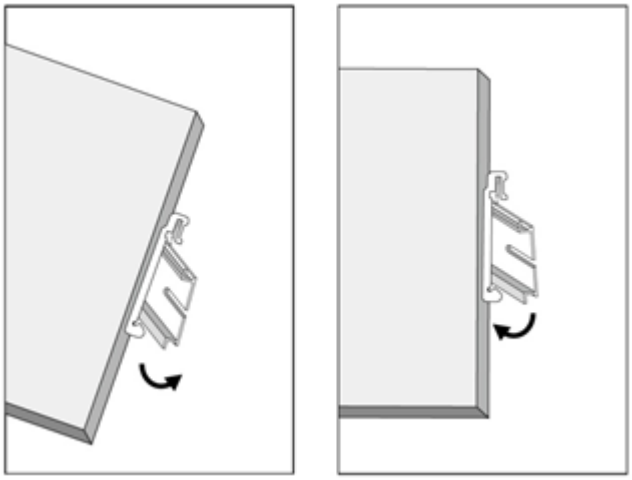
When installing, make sure to allow for enough space to properly install the cabling.

ATTENTION:

This product is intended to be mounted to a well-grounded mounting surface such as a metal panel.

ATTENTION:

The product should be mounted in an Industrial Control Panel and the ambient temperature should not exceed 75°C.



2.3.2. Dismounting the ICRL2-M

1. Pull out the lower edge of the switch and then remove the switch from the DIN rail.
2. Ground the Switch: Before powering on the switch, ground the switch to earth.
3. Ensure the rack on which the switch is to be mounted is properly grounded and incompliance with ETSI ETS 300 253. Verify that there is a good electrical connection to the grounding point on the rack (no paint or isolating surface treatment).



CAUTION:

The earth connection must not be removed unless all power supply connection has been disconnected.

The device is installed in a restricted-access location it has a separate protective earthing terminal on the chassis that must be permanently connected to earth ground to adequately ground the chassis and protect the operator from electrical hazards.



ATTENTION:

The product should be mounted in an Industrial Control Panel and the ambient temperature should not exceed 75°C.

2.4. Grounding the ICRL2-M

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.



ATTENTION

This product is intended to be mounted to a well-grounded mounting surface such as a metal panel.

2.5. Wiring the ICRL2-M



WARNING

Safety measures should be taken before connecting the power cable. Turn off the power before connecting modules or wires. The correct power supply voltage is listed on the product label. Check the voltage of your power source to make sure that you are using the correct voltage. DO NOT use a voltage greater than what is specified on the product label. Calculate the maximum possible current in each power wire and common wire.

Observe all electrical codes dictating the maximum current allowable for each wire size. If current exceeds the maximum rating, the wiring can overheat causing serious damage to your equipment.

Read and follow these guidelines:

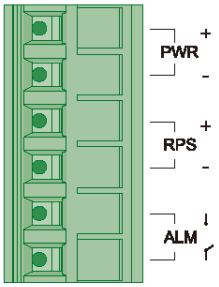
- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross make sure the wires are perpendicular at the intersection point.

  Note: *Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.*

- You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- You should separate input wiring from output wiring.
- We advise that you label the wiring to all devices in the system.

2.5.1. Wiring Power Input

The top view of Terminal Block is displayed.



- PWR for Primary Power input

Model	Power
ICRL2-M-16RJ45/4SFP-10G-DIN	12 - 48 V DC @ 1.8A

- RPS for Redundant Power Input.

Redundant Power Input: You can use Terminal Block (PWR) as primary power and Terminal Block (RPS) for redundant power.

Note: *Check the polarity while connecting.*

WARNING

Safety measures should be taken before connecting the power cable.Turn off the power before connecting modules or wires. The correct power supply voltage is listed on the product label. Check the voltage of your power source to make sure that you are using the correct voltage. DO NOT use a voltage greater than what is specified on the product label. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current exceeds the maximum rating, the wiring can overheat causing serious damage to your equipment.

CAUTION

Use copper conductors only. Wiring cable temperature should support at least 60/75°C.

Tighten the wire to a torque value 5lb. The wire gauge for the terminal block should range between 12~24 AWG.

MISE EN GARDE

Utilisez uniquement des conducteurs en cuivre. La température maximale du câble ne doit pas dépasser 60/75°C.

Serrer le fil à une valeur de couple de 5lb. Le calibre de fil du bornier doit être compris entre 12 et 24 AWG.

ATTENTION

The ICRL2-M power shall be supplied by SELV circuit.

Please read and follow these guidelines:

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.

  Note: *Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.*

- You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together
- You should separate input wiring from output wiring
- We advise that you label the wiring to all devices in the system.

To insert power wire and connect the specified voltage range at the power terminal block, follow the steps below:

1. Use a flat-head screwdriver to loosen the wire-clamp screws.
2. Insert the negative/positive DC wires into the PWR-/PWR+ and RPS-/RPS+ terminals, respectively.
3. Tighten the wire-clamp screws to prevent the wires from loosening.

Note: *We strongly request that each Industrial PoE switch to connect to individual power supply. Please do not use one power supply to two or more PoE switches at a time.*

2.5.2. Wiring the Relay Contact (ALM)

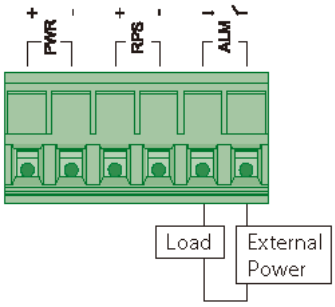
The ICRL2-M has one set of relay alarm output. This relay contact uses two contacts of the terminal block on the ICRL2-M top panel. The two contacts of the terminal block connector are used to detect user-configured events. The two wires attached to the fault contacts form an open circuit when a user-configured event is triggered.

- The ICRL2-M has lost power from one of the DC power inputs.

OR

- One of the ports for which the corresponding PORT ALARM DIP Switch is set to ON is not properly connected.

If a user-configured event does not occur, the fault circuit remains closed..



Note: *Relay rating: 24 V @ 1 A.*

CAUTION

Use copper conductors only. Wiring cable temperature should support at least 60/75°C.

Tighten the wire to a torque value 5lb. The wire gauge for the terminal block should range between 12~24 AWG.

MISE EN GARDE

Utilisez uniquement des conducteurs en cuivre. La température maximale du câble ne doit pas dépasser 60/75°C.

Serrer le fil à une valeur de couple de 5lb. Le calibre de fil du bornier doit être compris entre 12 et 24 AWG.

2.6. Connecting RJ45 Cables

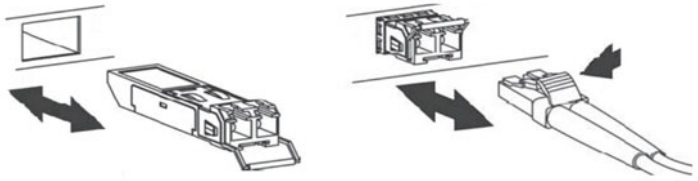
Connect one end of an Ethernet cable into the Ethernet port of the ICRL2-M and the other end to the attached networking device.

- ICRL2-M-16RJ45/4SFP-10G-DIN
  - Ports 1-16 supports 10/100/1000Mbit/s speed
  - Ports 17-20 SFP+ port support 10 Gigabit speed
- All the RJ45 ports on the ICRL2-M support auto-negotiation and auto MDI/MDI-X to eliminate the need for crossover cabling.

Note: *Category 5e cable or above should be used.*

2.7. Installing the SFP+ Modules and Fiber Cable

1. Slide the selected SFP module into the selected SFP slot (Make sure the SFP module is aligned correctly with the inside of the slot).
2. Insert and slide the module into the SFP slot until it clicks into place.
3. Remove any rubber plugs that may be present in the SFP.
4. Align the fiber cable's connector with the SFP and insert the connector.
5. Slide the connector in until a click is heard.
6. If you want to pull the connector out, first push down the release clip on top of the connector to release the connector from the SFP module.

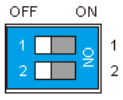


To properly connect fiber cabling: Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

Note: *When inserting the cable, be sure the tab on the plug clicks into position to ensure that it is properly seated.*

Check the corresponding port LED on the ICRL2-M to be sure that the connection is valid. Refer to *LEDs* on Page 19.

2.8. Setting the Alarm DIP Switches

DIP Switch Settings		
	1 PWR	• ON: Primary power alarm reporting is enabled • OFF: Primary power alarm reporting is disabled
	2 RPS	• ON: Redundant power alarm reporting is enabled • OFF: Redundant power alarm reporting is disabled

2.9. LEDs

LED Name	LED Status	Description
PWR (Green)	Lit	Primary power on
	Off	Primary power off or failure
RPS (Green)	Lit	Redundant power on
	Off	Redundant power off or failure
ALM (Red)	Lit	Alarm triggered for abnormal power status and anomalous features.
	Off	Normal operation or DIP switch OFF
POST (Green)	Lit	The ICRL2-M is ready or running
	Blinking	Self-testing the ICRL2-M during power on
	Off	The ICRL2-M is not ready
SFP (Green) Fiber Ports	Lit	Port link up
	Blinking	Activity - receiving or transmitting data
	Off	Port disconnected or link failed
1000 (Green)	Lit	Link speed at 1000 Mbit/s
	Off	Link speed at 10/100 Mbit/s
LNK/ACT (Green)	Lit	Port link up
	Blinking	Activity - receiving or transmitting data
	Off	Port disconnected or link failed

3. System Status

Note: *Use the console port or Telnet to program the initial IP address.*

3.1. Console Port

Use the following steps to connect the console port for initial IP address configuration or to access the command line interface.

1. Connect your computer to the console port on the ICRL2-M using the appropriate cable.
2. Use terminal emulation software with the following default settings:

Console Port Settings	
Setting	**Default Value**
Terminal Emulation	VT100
Baud Rate	38400
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

If the console cable shipped with the ICRL2-M has been misplaced, you can build a cable using this information.

Signal	DB9 Pins	RJ45 Pins
Rx	2	3
Tx	9	2
Gnd	5	5

3. Press **Enter** to open the login screen.
   - Default Username is **admin**
   - Default Password is **admin**

3.2. Telnet

Use the following steps to connect using Telnet for initial IP address configuration or to access the command line interface.

1. Connect your computer to one of the Ethernet ports.
2. Open a Telnet session to the ICRL2-M IP address. If this is your first login, use the default management values in the following table.

Telnet	
Setting	**Default Value**
IP Address	192.168.250.250
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Management VLAN	1
Default Username	admin
Default Password	admin

3. Make sure your computer IP address is in the same subnet, unless you are accessing the ICRL2-M through one or more routers.

3.3. Starting the CLI

Use the following steps to start the CLI (command line interface).

1. Press **Enter** key to enter the login command prompt when below message is displayed on the screen.

   Please press Enter to activate this console

2. Type **admin** to enter the CLI mode when the following message displays.

   L2SWITCH login:

   You can execute a few limited commands when CLI prompt displays.

3.3.1. How to Enter Privileged Mode

If you want to execute more powerful commands, you must enter privileged mode using the **enable** command.

1. Enter enable at the command prompt.

   L2SWITCH>
   L2SWITCH>enable

2. Enter the valid username and password when below prompt displays.

   Note: *Following displays the default user and password.*

   user:admin
   password:admin
   L2SWITCH#

3.4. CLI Commands

The following provides detailed information about the CLI commands.

CLI Command Modes		
Mode	**Command**	**Description**
enable	show hostname	Displays the system's network name.
configure	reboot	Reboots the system.
eth0	ip addressA.B.C.D/M	Configures a static IP and subnet mask for the system.
interface	show	Displays the current port configurations.
acl	show	Displays the current access control profile.
vlan	show	Displays the current VLAN configurations.

Modetype:

- **enable**

  Command prompt **L2SWITCH#**. Commands can be executed in this command prompt.

- **configure**

  Command prompt **L2SWITCH(config)#**. Commands can be executed in this command prompt. In **Enable** code, executing command **configure terminal** and pressing **Enter** to access the configure mode.

  L2SWITCH#configure terminal

- **eth0**

  Command prompt **L2SWITCH(config-if)#**". Commands can be executed in this command prompt. In **Configure** code, executing command **interface eth0** and pressing **Enter** to access the eth0 interface mode.

  L2SWITCH(config)#interface eth0 L2SWITCH(config-if)#

- **interface**

  Command prompt **L2SWITCH(config-if)#**". Commands can be executed in this command prompt.

  In **Configure** code, executing command **interface gigaethernet1/0/5** enter the interface port 5 mode. Or optionally enter command **interface fastethernet1/0/5** enter the interface port 5 mode.

  Note: *Depending on your port speed, gigaethernet1/0/5 for gigabit Ethernet ports and fastethernet1/0/5 for fast Ethernet ports.*

  L2SWITCH(config)#interface gigaethernet1/0/5 L2SWITCH(config-if)#

- **vlan**

  Command prompt **L2SWITCH(config-vlan)#**. Commands can be executed in this command prompt.

  In **Configure** mode, executing command **vlan 2** enter the vlan 2 mode.

  Note: *Where **2** is the vlan ID.*

  L2SWITCH(config)#vlan 2 L2SWITCH(config-vlan)#

- **acl**

  Command prompt **L2SWITCH(config-acl)#**. Commands can be executed in this command prompt. In Configure mode, executing command **access-list test** enter the access-list test mode.

  Note: *Where **test** is the profile name.*

  L2SWITCH(config)#access-list test L2SWITCH(config-acl)#

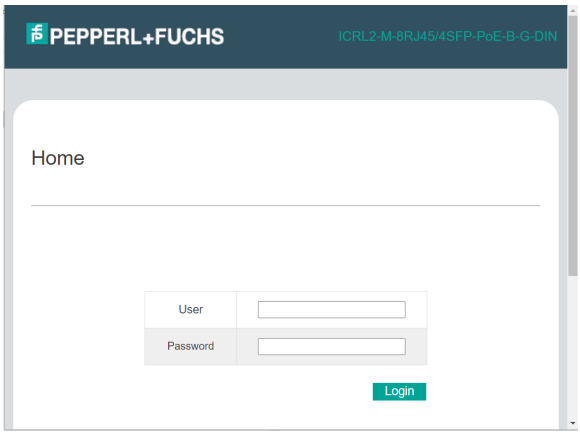
3.4.1. Command Table Overview

Command Table Overview			
Mode	**Prompt**	**Enter Command**	**Parent Mode**
enable	L2SWITCH#		
config	L2SWITCH(config)#	configure terminal	enable
acl	L2SWITCH(config-acl)#	access-list name NAME ip-type ipv4	config
acl	L2SWITCH(config-acl-ipv6)#	access-list name NAME ip-type ipv6	config
auto provision	L2SWITCH(auto-provision)#	auto-provision	config
eth0	L2SWITCH(config-if)#	interface eth0	config
dhcp server	L2SWITCH(config-erps-inst)#	dhcp-server pool POOL_ID	config
dhcp ipv6 server	L2SWITCH(config-erps-inst)#	dhcpv6-server pool POOL_ID	config
dhcp ipv6 server vendor	L2SWITCH(config-erps-inst)#	vendor-specific VENDOR_ID	dhcp ipv6 server
erps	L2SWITCH(config-erps-ring)#	erps ring-id RING_ID	config
erps instance	L2SWITCH(config-erps-inst)#	erps instance	config
interface range	L2SWITCH(config-if-range)#	interface range gigabitethernet1/0/ PORTLIST	config
vlan debug	L2SWITCH(if-vlan-debug)#	interface vlan-debug VLAN_ID	config
pppoe vlan	L2SWITCH(if-pppoe-vlan)#	pppoe intermediate-agent vlan VLAN_ID	config
inter vlan route	L2SWITCH(config-if-vlan-l3)#	interface vlan 2	config
igmp filter	L2SWITCH(config-igmp)#	igmp-snooping filtering profile NAME	config
interface	L2SWITCH(config-if)#	interface gigabitethernet1/0/2	config
mlds	L2SWITCH(config-mlds)#	mld-snooping vlan VLAN_ID	config
mrp	L2SWITCH(config-mrp)#	mrp ring-id RING_ID	config
mstp	L2SWITCH(config-mst)#	spanning-tree mst configuration	config
mvr	L2SWITCH(config-mvr)#	mvr VLAN_ID	config
ptp	L2SWITCH(config-ptp)#	ptp domain DOMAIN_ID	config
ptp-port	L2SWITCH(config-ptp-port)#	port PORT_ID	ptp
qinq	L2SWITCH(config-qinq)#	vlan-stacking selective-qinq NAME	config
vlan	L2SWITCH(config-vlan)#	vlan VLAN_ID	config
vlan-range	L2SWITCH(config-vlan-range)#	vlan range VLAN_ID_LIST	config

3.5. GUI Login

Use this procedure to log into the ICRL2-M web interface.

Note: *The default User name is admin and the default Password is admin.*



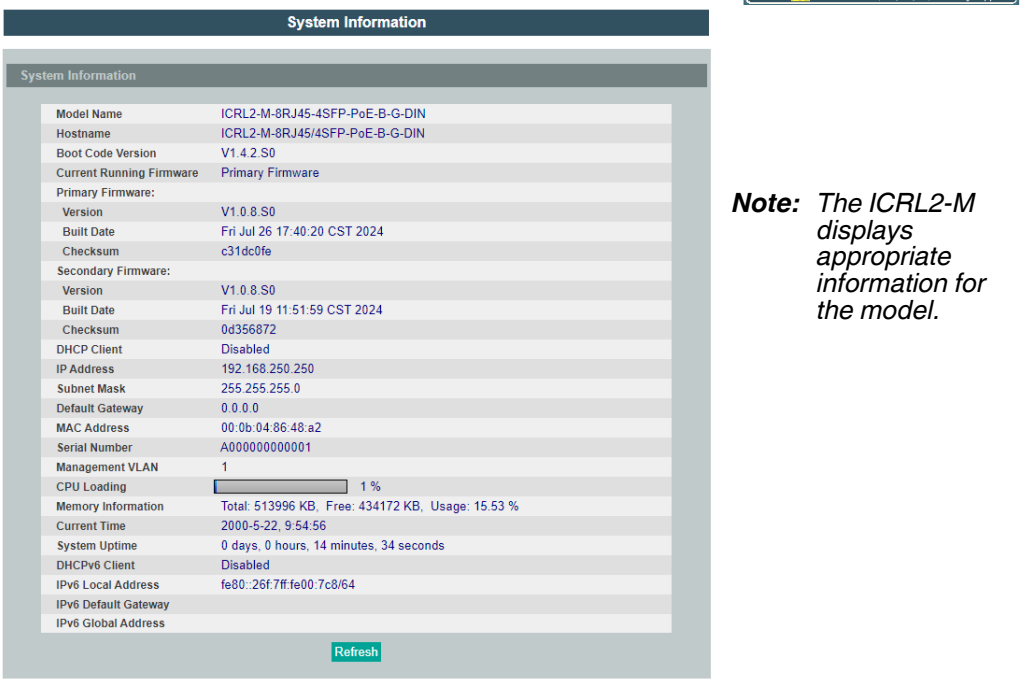
3.6. System Information

3.6.1. CLI Configuration

CLI System Information		
Mode	**Command**	**Description**
enable	show hostname	Displays the system's network name.
enable	show interface eth0	Displays the current Eth0 configurations.
enable	show model	Displays the system information.
enable	show running-config	Displays the current operating configurations.
enable	show system-info	Displays the system's CPU loading and memory information.
enable	show uptime	Displays the system up time.

3.6.2. Web Configuration

The System Information window appears each time you log into the program. Alternatively, this window can be accessed by clicking **System Status > System Information.**



Note: *The ICRL2-M displays appropriate information for the model.*

8/19/25

System Settings	
Parameter	**Description**
System Information	
Model Name	Displays the model name of the ICRL2-M.
Host name	Displays the name of the ICRL2-M.
Boot Code Version	Displays the boot code version.
Current Running Firmware	Displays the current running firmware, primary or secondary.
Primary Firmware	
Version	Displays the version of primary firmware.
Built Date	Displays the built date of primary firmware.
Checksum	Displays the checksum of primary firmware.
Secondary Firmware	
Version	Displays the version of secondary firmware.
Built Date	Displays the built date of econdary firmware.
Checksum	Displays the checksum of secondary firmware.
DHCP Client	Displays whether the DHCP client is enabled on the ICRL2-M.
IP Address	Indicates the IP address of the ICRL2-M.
Subnet Mask	Indicates the subnet mask of the ICRL2-M.
Default Gateway	Indicates the default gateway of the ICRL2-M.
MAC Address	Displays the MAC (Media Access Control) address of the ICRL2-M.
Serial Number	Serial number assigned by manufacture for identification of the unit.
Management VLAN	Displays the VLAN ID that is used for the ICRL2-M management purposes.
CPU Loading	Displays the percentage of your ICRL2-M's system load.
Memory Information	Displays the total memory the ICRL2-M has and the memory which is currently available (Free) and occupied (Usage).
Current Time	Displays current date (yyyy-mm-dd) and time (hh:mm:ss).
DHCPv6 Client	Displays whether the DHCPv6 client is enabled on the ICRL2-M.
IPv6 Local Address	Displays the ICRL2-M's local IP address for IPv6.
IPv6 Default Gateway	Displays the default gateway for IPv6.
IPv6 Global Address	Displays the ICRL2-M's global IP address for IPv6.
Refresh	Click **Refresh** to reload the running configuration values.

4. Basic Settings

4.1. General Settings

- *System Settings*
- *Jumbo Frame* on Page 30
- *SNTP* on Page 32
- *Management Host* on Page 36

4.1.1. System Settings

The following information is applicable to System Settings.

- Management VLAN
  - To specify a VLAN group which can access the ICRL2-M. Valid VLAN range is from 1 to 4094.
  - To configure a management VLAN, create the management VLAN first, the management VLAN must have one member port.
- Host Name

  The **hostname** is same as the SNMP system name with a maximum of 64 characters.

  The first 16 characters of the **hostname** is configured as the CLI prompt.

  Note the following default values:
  - Hostname: L2SWITCH
  - Default DHCP client: disabled.
  - Default Static IP: 192.168.250.250
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 0.0.0.0
  - Management VLAN:1

4.1.1.1. CLI Configuration - System Settings / System

CLI System Settings / System		
Mode	**Command**	**Description**
enable	show interface eth0	Displays the eth0 configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	hostname STRINGS	Sets the system's network name.
configure	interface eth0	Enters the eth0 interface mode to configure the system IP.
eth0	show	Displays the eth0 configurations.
eth0	ip address A.B.C.D/M	Configures a static IP and subnet mask for the system.

CLI System Settings / System (Continued)		
Mode	**Command**	**Description**
eth0	ip address default-gateway A.B.C.D	Configures the system default gateway.
eth0	ip dhcp client (disable | enable | renew | next_restart)	Configures a DHCP client function for the system. • **disable**: Use a static IP address on the ICRL2-M. • **enable & renew**: Use DHCP client to get an IP address from DHCP server. • **next_restart**: The settings take effect on next system restart.
eth0	management vlan <1-4094>	Configures the management VLAN.
eth0	ip ipv6-address AAAA:BBBB:CCCC:DDDD:EEEE :FFFF:GGGG:HHHH/M	Configures a global scope of IPv6 address and subnet mask for the system.
eth0	ip ipv6-addressdefault-gateway AAAA:BBBB:CCCC:DDDD:EEEE :FFFF:GGGG:HHHH	Configures a default gateway for the system.
eth0	ip ipv6-dhcp client (disable | enable | renew | next_restart)	Configures a DHCPv6 client function for the system. • **disable**: Use a static IP address on the ICRL2-M. • **enable & renew**: Use DHCPv6 client to get an IP address from DHCPv6 server. • **next_restart**: The settings will take effect on next system restart.

Examples: How to Configure an IP Address

- Enter configure mode.

  L2SWITCH#configure terminal
  L2SWITCH(config)#

- To enter the ETH0 interface mode.

  L2SWITCH(config)#interface eth0
  L2SWITCH(config-if)#

- To get an IP address from a DHCP server.

  L2SWITCH(config-if)#ip dhcp client enable

- To configure a static IP address and a gateway for the ICRL2-M.

  L2SWITCH(config-if)#ip address 192.168.202.111/24
  L2SWITCH(config-if)#ip address default-gateway 192.168.202.1

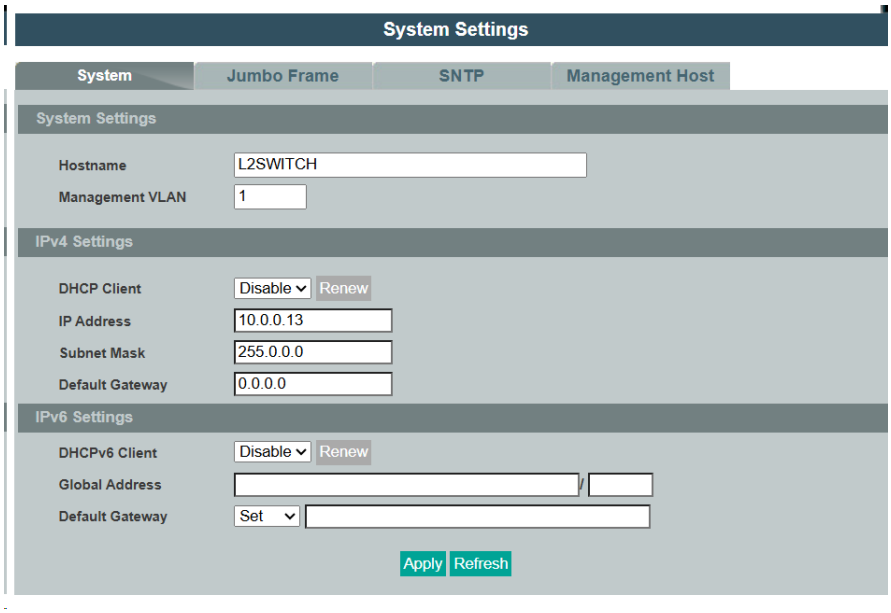
- To configure a static global IPv6 address and a gateway for the ICRL2-M.
  - Set the static global IPv6 address first.

    L2SWITCH(config-if)#ip ipv6-address 3ffe::1235/64
  - Set the IPv6 default gateway address.

    L2SWITCH(config-if)#ip ipv6-address default-gateway3ffe::1234

4.1.1.2. Web Configuration - System Settings / System

The following provides supporting information for web configuration on the Systems Settings page.



System Settings / System	
Parameter	**Description**
System Settings	
Hostname	Enter up to 64 alphanumeric characters for the name of your ICRL2-M. The hostname should be the combination of the digit or the alphabet or hyphens (-) or underscores (_).
Management VLAN	Enter a VLAN ID used for ICRL2-M management purposes.
IPv4 Settings	
DHCP Client	Select Enable to enable a DHCP client. Select Renew to renew the DHCP lease.
IP Address	Configures a IPv4 address for your ICRL2-M in dotted decimal notation. For example, 192.168.250.250.
Subnet Mask	Enter the IP subnet mask of your ICRL2-M in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.1.
IPv6 Settings	
DHCPv6 Client	• Select **Enable** to allow the ICRL2-M to automatically get an IP address from a DHCPv6 server. • Click **Renew** to have the ICRL2-M re-get an IP address from the DHCP server. • Select **Disable** if you want to configure the ICRL2-M's IP address manually.
Global Address	Configure a global IPv6 address for the ICRL2-M.

System Settings / System (Continued)	
Parameter	**Description**
Default Gateway	• **Set** – Set an IPv6 default gateway for the ICRL2-M. • **Unset** – Unset the IPv6 default gateway for the ICRL2-M.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the existing configuration values.

4.1.2. Jumbo Frame

Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumbo frames can enhance data transmission efficiency in a network. The bigger the frame size, the better the performance.

Notes:

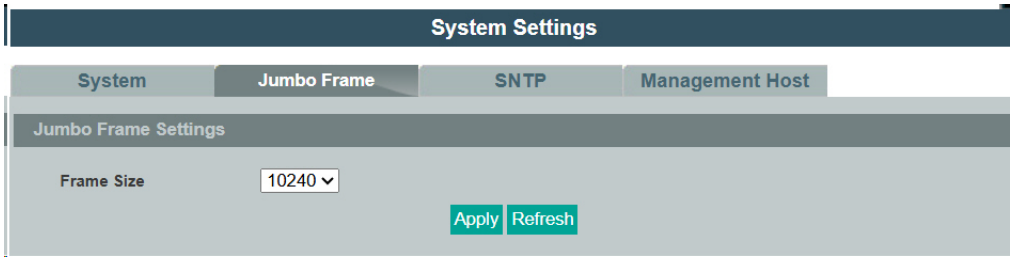
- The default jumbo frame is 10240 bytes.
- The jumbo frame settings will apply to all ports.
- If the size of a packet exceeds the jumbo frame size, the packet will be dropped.
- The available values are 1522, 1536, 1552, 9216,10240.

4.1.2.1. CLI Configuration - System Settings / Jumbo Frame

CLI System Settings / Jumbo Frame		
Mode	**Command**	**Description**
enable	show jumboframe	Displays the current jumbo frame settings.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	jumboframe(1522 | 1536 | | 9216 | 10240)	Configures the maximum number of bytes of frame size.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	jumboframe(1522 | 1536 | 9216 | 10240)	Configures the maximum number of bytes of frame size.

4.1.2.2. Web Configuration - System Settings / Jumbo Frame

System Settings / Jumbo Frame	
Parameter	**Description**
Frame Size	Configures the maximum number of bytes of frame size for specified port(s). Available sizes:1522/1536/1552/9216/10240.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.



4.1.3. SNTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. A less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time is known as the Simple Network Time Protocol (SNTP). NTP provides Coordinated Universal Time (UTC). No information about time zones or daylight saving time is transmitted; this information is outside its scope and must be obtained separately.

UDP Port: 123.

Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

Notes:

- The SNTP server always replies the UTC current time.
- When the ICRL2-M receives the SNTP reply time, the ICRL2-M adjusts the time with the time zone configuration and then configures the time to the ICRL2-M.
- If the time server's IP address is not configured, the ICRL2-M does not send any SNTP request packets.
- If there are no SNTP reply packets, the ICRL2-M retries every 10 seconds forever.
- If the ICRL2-M has received an SNTP reply, the ICRL2-M retrieves the time from the NTP server every 24 hours.
- If the time zone and time NTP server have been changed, the ICRL2-M repeats the query process.
- No default SNTP server.

4.1.3.1. CLI Configuration - System Settings / SNTP

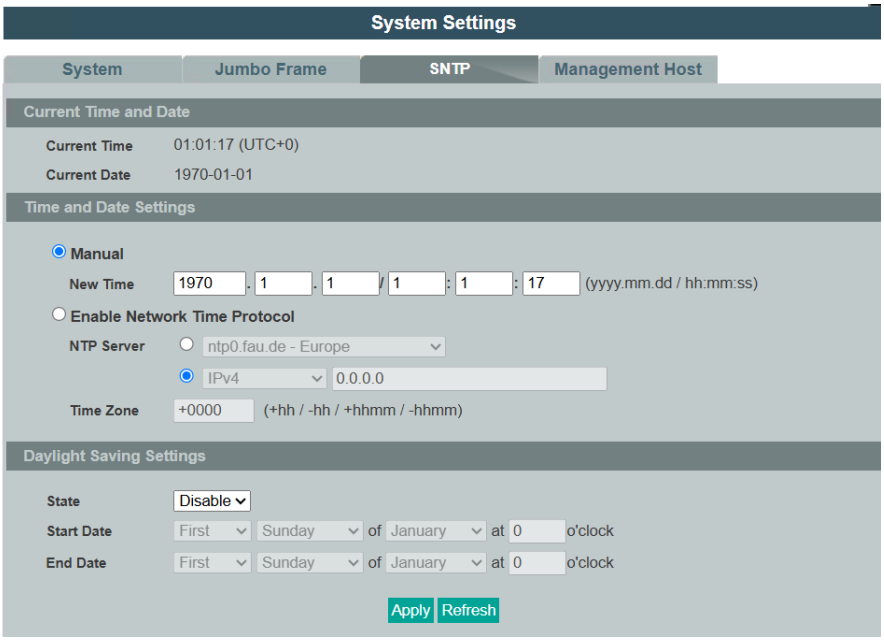
CLI System Settings / SNTP		
Mode	**Command**	**Description**
enable	show time	Displays current time and time configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	time HOUR:MINUTE:SECOND	Sets the current time on the ICRL2-M. • hour: 0-23 • min: 0-59 • sec: 0-59 ***Note:*** *If you configure Daylight Saving Time after you configure the time, the ICRL2-M will apply Daylight Saving Time.*
configure	time date YEAR/MONTH/DAY	Sets the current date on the ICRL2-M. • year: 1970- • month: 1-12 • day: 1-31
configure	time daylight-saving-time	Enables the daylight saving time.
configure	no time daylight-saving-time	Disables daylight saving on the ICRL2-M.
configure	time daylight-saving-time start-date (first | second | third | fourth | last)(Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH HOUR	Sets the start time of the Daylight Saving Time.

CLI System Settings / SNTP (Continued)		
Mode	**Command**	**Description**
configure	time daylight-saving-time end-date (first | second | third | fourth | last)(Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH HOUR	Sets the end time of the Daylight Saving Time.
configure	time ntp-server (disable | enable)	Disables / enables the NTP server state.
configure	time ntp-server IP_ADDRESS	Sets the IP address of your time server.
configure	time ntp-server domain-name STRING	Sets a domain name of your time server.
configure	time timezone STRING	Configures the time difference between UTC (formerly known as GMT) and your time zone. Valid Range: -1200 ~ +1200.

Example with default IP address:

L2SWITCH(config)#time ntp-server 192.168.250.250
L2SWITCH(config)#time timezone +0800
L2SWITCH(config)#time ntp-server enable
L2SWITCH(config)#time daylight-saving-time start-date first Monday6 0
L2SWITCH(config)#time daylight-saving-time end-date last Saturday 10 0

4.1.3.2. Web Configuration - System Settings / SNTP



System Settings / SNTP	
Parameter	**Description**
Current Time and Date	
Current Time	Displays the time you open / refresh this menu.
Current Date	Displays the date you open / refresh this menu.
Time and Date Setting	
Manual	Select this option if you want to enter the system date and time manually.
New Time	Enter the new date in year, month and day format and time in hour, minute and second format. The new date and time then appear in the Current Date and Current Time fields after you click **Apply**.
Enable Network Time Protocol	Select this option to use Network Time Protocol (NTP) for the time service.
NTP Server	Select a pre-designated time server or type the IP address or type the domain name of your timeserver. The ICRL2-M searches for the timeserver for up to 60 seconds.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.

System Settings / SNTP (Continued)	
Parameter	**Description**
Daylight Saving Settings	
State	Select **Enable** if you want to use Daylight Saving Time. Otherwise, select Disable to turn it off.
Start Date	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving Time. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and 2:00. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving Time. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and 2:00. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

4.1.4. Management Host

This feature limits the hosts that can manage the ICRL2-M.

Any hosts can manage the ICRL2-M via telnet or web browser. If the user has configured one or more management host, the ICRL2-M can be managed by these hosts only. The feature allows the user to configure management IP based on particular IP or whole subnet.

Note: *The feature allows the user to configure management host up to10 entries. The default is none, any host can manage the ICRL2-M via telnet or web browser.*

4.1.4.1. CLI Configuration - System Settings / Management Host

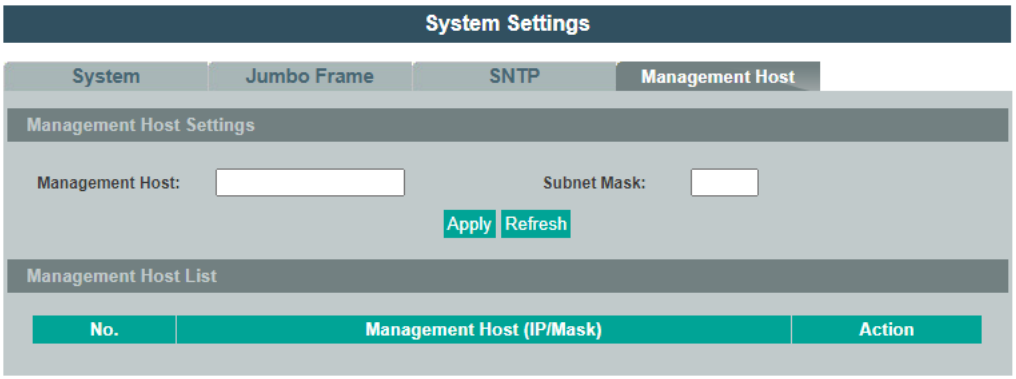
CLI System Settings / Management Host		
Mode	**Command**	**Description**
enable	show interface eth0	Displays the eth0 configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface eth0	Enters the eth0 interface mode to configure the system configurations.
eth0	management host	Configures a static IP and subnet mask for the system.
eth0	show	Displays the all of the interface eth0 configurations.
eth0	management host A.B.C.D	Adds a management host address.
eth0	management subnet-host A.B.C.D/M	Adds a management host address with a subnet mask.
eth0	no management host A.B.C.D	Deletes a management host address.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#management subnet-host 192.168.202.1/24
Success!
L2SWITCH(config-if)#management host 192.168.203.12
Success!
L2SWITCH(config-if)#management host 192.168.203.13
Success!
L2SWITCH(config-if)#show
    DHCPServerport(s):1-6
Eth0
    DHCPclient:Enable
    DHCPv6 client:Disable
    Management vlan:1
    Management Host:192.168.202.1/24,192.168.203.12/32,192.168.203.13/32
    Default gateway:192.168.202.1
    Link encap:Ethernet HWaddr00:0B:04:90:60:21
    inet addr:192.168.202.74 Bcast:192.168.202.255 Mask:255.255.255.0
    inet6 addr:fe80::20b:4ff:fe90:6021/64 Scope:Link
    UPBROADCASTRUNNINGALLMULTIMULTICAST MTU:1500
Metric:1
    ASYMMTU:0
    RXpackets:17931 errors:0dropped:6680overruns:0 frame:0
```

TX packets:6500 errors:0 dropped:0overruns:0 carrier:0
collisions:0 txqueuelen:500
RXbytes:3565872(3.4Mb) TX bytes:1173040(1.1 Mb)

4.1.4.2. Web Configuration - System Settings / Management Host



System Settings / Management Host	
Parameter	**Description**
Management Host Settings	
Management Host	Configures the management host.
Subnet Mask	Configures the subnet, so that any host in that subnet can control the ICRL2-M.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Management Host List	
No.	Displays a sequential number for each management host.
Management Host (IP/ Mask)	Displays the management host and the number of mask bit.
Action	Click **Delete** to remove the specified entry.

4.2. MAC Management

Dynamic Address

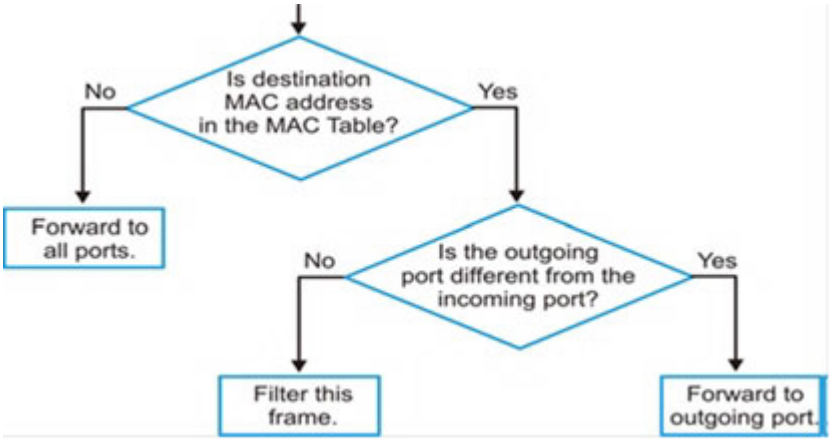
The MAC addresses are learnt by the ICRL2-M. When the ICRL2-M receives frames, it will record the source MAC, the received port and the VLAN in the address table with an age time. When the age time is expired, the address entry will be removed from the address table.

Static Address

The MAC addresses are configured by users. The static addresses will not be aged out by the ICRL2-M; it can be removed by user only. The maximum static address entry is up to 256.

MAC Table (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the ICRL2-M's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the ICRL2-M, the MAC address of the device is shown on the ICRL2-M's MAC Table. It also shows whether the MAC address is dynamic (learned by the ICRL2-M) or static (manually entered). The ICRL2-M uses the MAC Table to determine how to forward frames. See the following figure.

1. The ICRL2-M examines the received frame and learns the port from which this source MAC address came.
2. The ICRL2-M checks to see if the frame's destination MAC address matches a source MAC address already learnt in the MAC Table.
   - If the ICRL2-M has already learnt the port for this MAC address, then it forwards the frame to that port.
   - If the ICRL2-M has not already learnt the port for this MAC address, then the frame is flooded to all ports. If too much port flooding, it may lead to network congestion.
   - If the ICRL2-M has already learnt the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.



MAC Table Flowchart

Notes:

- The default MAC address table age time is 300 seconds.
- The Maximum static address entry is 256.

4.2.1. Static MAC

4.2.1.1. CLI Configuration - MAC Management / Static MAC

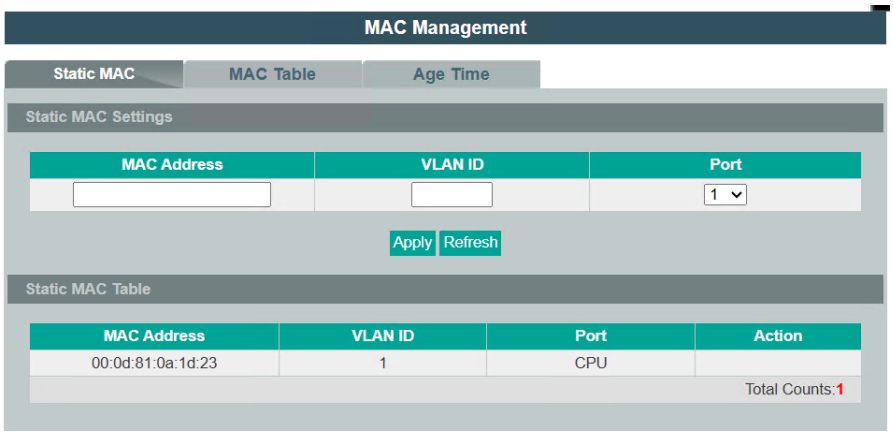
CLI MAC Management / Static MAC		
Mode	**Command**	**Description**
enable	show mac-address-table (static | dynamic)	Displays the current static/dynamic unicast address entries.
enable	configure terminal	Changes the mode to configure mode.
configure	mac-address-table static MACADDR vlan <1-4094> port PORT_ID	Configures a static unicast entry.
configure	no mac-address-table static MACADDR vlan <1-4094>	Removes a static unicast entry from the address table.

Example:

L2SWITCH(config)#mac-address-table static 00:11:22:33:44:55 vlan 1 port 1

4.2.1.2. Web Configuration - MAC Management / Static MAC

A static Media Access Control (MAC) address is an address that has been manually entered in the MAC address table, and do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port, so this may reduce the need for broadcasting.



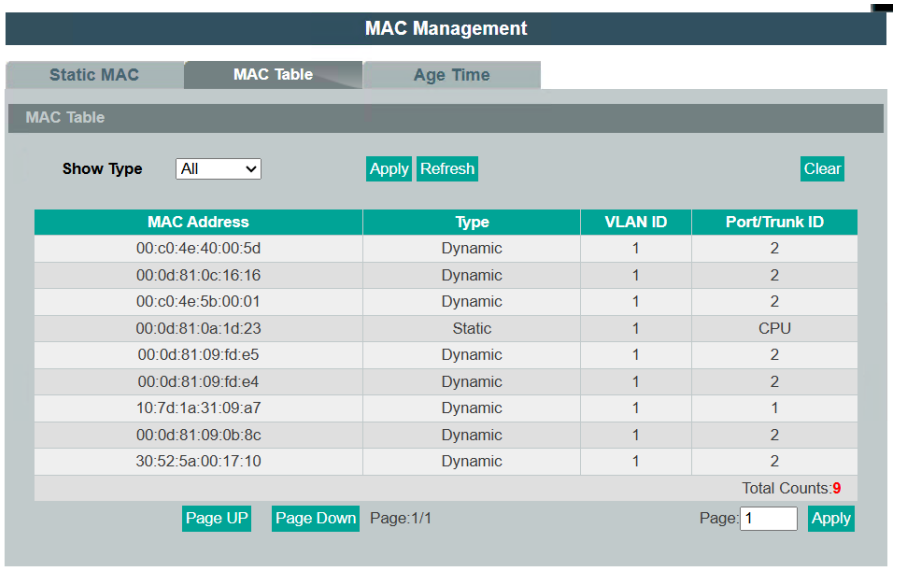
MAC Management / MAC Management / Static MAC	
Parameter	**Description**
Static MAC Settings	
MAC Address	Enter the MAC address of a computer or device that you want to add to the MAC address table. Valid format is hh:hh:hh:hh:hh:hh.
VLAN ID	Enter the VLAN ID to apply to the computer or device.
Port	Enter the port number to which the computer or device is connected.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Static MAC Table	
MAC Address	Displays the MAC address of a manually entered MAC address entry.
VLAN ID	Displays the VID of a manually entered MAC address entry.
Port	Displays the port number of a manually entered MAC address entry. The MAC address with port CPU means the ICRL2-M's MAC addresses itself.
Action	Click **Delete** to remove this manually entered MAC address entry from the MAC address table. You cannot delete the ICRL2-M's MAC address from the static MAC address table.

4.2.2. MAC Table

4.2.2.1. CLI Configuration - MAC Management / MAC Table

CLI MAC Management / MAC Table		
Mode	**Command**	**Description**
enable	show mac-address-table (static | dynamic)	Displays the current static/dynamic unicast address entries.
enable	show mac-address-table mac MACADDR	Displays information of a specific MAC.
enable	show mac-address-table port PORT_ID	Displays the current unicast address entries learnt by the specific port.
enable	configure terminal	Changes the mode to configure mode.
configure	clear mac address-table dynamic	Clears the dynamic address entries.

4.2.2.2. Web Configuration - MAC Management / MAC Table



MAC Management / MAC Table	
Parameter	**Description**
Show Type Apply	**Select All**, **Static**, **Dynamic** or **Port** and then click **Apply** to display the corresponding MAC address entries on this screen.
Refresh	Click **Refresh** to reload the running configuration values.
MAC Address	Displays a MAC address.
Type	Displays whether this entry was entered manually (Static) or whether it was learned by the ICRL2-M (Dynamic).

MAC Management / MAC Table (Continued)	
Parameter	**Description**
VLAN ID	Displays the VLAN ID of the MAC address entry.
Port / Trunk ID	Displays the port number / Trunk ID the MAC address entry is associated. It displays CPU if it is the entry for the ICRL2-M itself. The CPU means that it is the ICRL2-M's MAC.
Total Counts	Displays the total entries in the MAC table.

4.2.3. Age Time Settings

4.2.3.1. CLI Configuration - MAC Management / Age Time

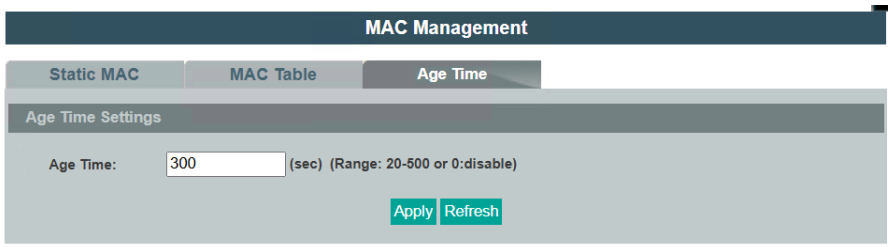
CLI MAC Management / Age Time Settings		
Mode	**Command**	**Description**
enable	show mac-address-table aging-time	Displays the current MAC address table age time.
enable	configure terminal	Changes the mode to configure mode.
configure	mac-address-table aging-time VALUE	Configures the mac table aging time. The range is 20 to 400 or 0: disable.

Examples:

L2SWITCH(config)#mac-address-table aging-time 200
Success!

L2SWITCH#show mac-address-table aging-time
The mac-address-table aging-time is 200 sec.

4.2.3.2. Web Configuration - MAC Management / Age Time



MAC Management / Age Time	
Parameter	**Description**
Age Time	Configure the age time; the valid range is from 20 to 400 seconds. The default value is 300 seconds. 0 means that the system will not age out any entries.

MAC Management / Age Time (Continued)	
Parameter	**Description**
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

4.3. Port Mirror

The Port-Based Mirroring is used on a network switch to send a copy of network packets sent/received on one or a range of switch ports to a network monitoring connection on another switch port (Monitor to Port). This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

Port Mirroring, together with a network traffic analyzer, helps to monitor network traffic. Users can monitor the selected ports (Source Ports) for egress and/or ingress packets.

Source Mode:

- Ingress: The received packets will be copied to the monitor port.
- Egress: The transmitted packets will be copied to the monitor port.
- Both: The received and transmitted packets are copied to the monitor port.

Notes:

1. The monitor port cannot be a trunk member port.
2. The monitor port cannot be ingress or egress port.
3. If the Port Mirror function is enabled, the Monitor-to Port can receive mirrored packets only.
4. If a port has been configured as a source port and then user configures the port as a destination port, the port is removed from the source ports automatically.

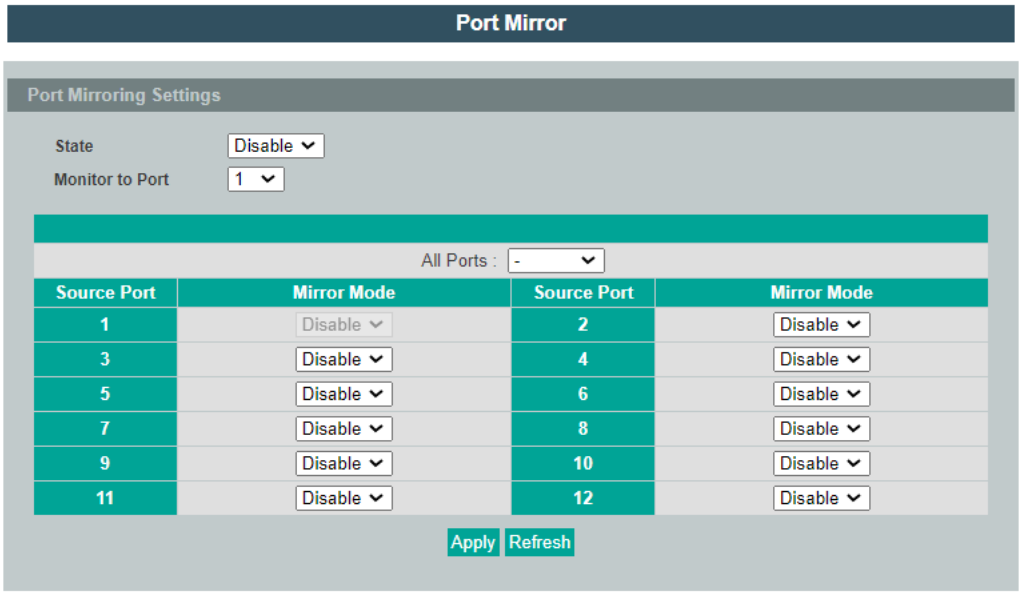
4.3.1. CLI Configuration - Port Mirroring

CLI Port Mirroring		
Mode	**Command**	**Description**
enable	show mirror	Displays the current port mirroring configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	mirror (disable | enable)	Disables / enables the port mirroring on the ICRL2-M.
configure	mirror destination port PORT_ID	Specifies the monitor port for the port mirroring.
configure	mirror source ports PORT_LIST mode (both | ingress | egress)	Adds a port or a range of ports as the source ports of the port mirroring.
configure	no mirror source ports PORT_LIST	Removes a port or a range of ports from the source ports of the port mirroring.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#mirror destination port9
Success!
L2SWITCH(config)#mirror source ports 1-8 mode ingress
Success!
L2SWITCH(config)#exit
L2SWITCH#show mirror
Mirror Configurations:
State: Disabled.
Monitor port: 9.
Ingress port(s): 1-8.
Egress port(s): None.

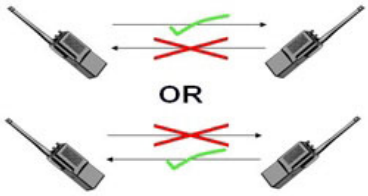
4.3.2. Web Configuration - Port Mirror



Port Mirror	
Parameter	**Description**
State	Select **Enable** to turn on port mirroring or select Disable to turn it off.
Monitor to Port	Select the port which connects to a network traffic analyzer.
All Ports	Settings in this field apply to all ports. • Use this field only if you want to make some settings the same for all ports. • Use this field first to set the common settings and then make adjustments on a port-by-port basis.
Source Port	Displays the number of a port.
Mirror Mode	Select **Ingress**, **Egress** or **Both** to only copy the ingress (incoming), egress (outgoing) or both (incoming and outgoing) traffic from the specified source ports to the monitor port. Select **Disable** to not copy any traffic from the specified source ports to the monitor port.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

4.4. Port Settings

- Duplex mode: A duplex communication system is a system composed of two connected parties or devices that can communicate with one another in both directions.
- Half Duplex: A half-duplex system provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.



- Full Duplex: A full-duplex, or sometimes double-duplex system, allows communication in both directions, and, unlike half-duplex, allows this to happen simultaneously. Land-line telephone networks are full-duplex, since they allow both callers to speak and be heard at the same time.



- Auto MDI-MDIX: Auto-MDIX (automatic medium-dependent interface crossover) is a computer networking technology that automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately, thereby removing the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. When it is enabled, either type of cable can be used or the interface automatically corrects any incorrect cabling. For Auto-MDIX to operate correctly, the speed on the interface and duplex setting must be set to "auto".
- Auto Negotiation: Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the ICRL2-M negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the ICRL2-M determines the connection speed by detecting the signal on the cable and using half-duplex mode. When the ICRL2-M's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
- Flow Control: A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses.IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill and resend later. The ICRL2-M uses IEEE802.3x flow control in full duplex mode and back pressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Notes:

- 1000 Base-T does not support force mode.
- The default port Speed & Duplex is auto for all ports.
- The default port Flow Control is Off for all ports.

4.4.1. General Settings

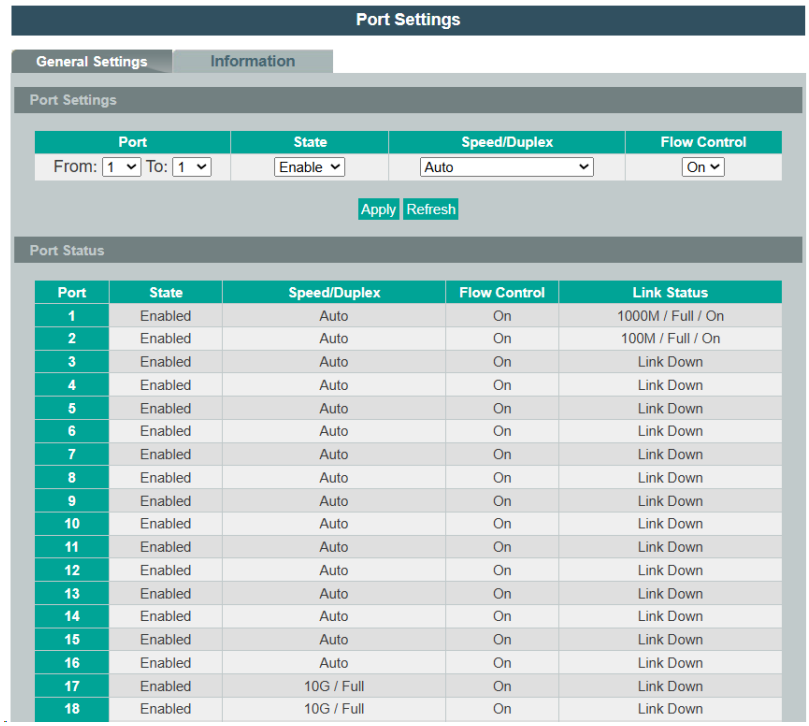
4.4.1.1. CLI Configuration - Port Settings / General Settings

CLI Port Settings / General Settings		
Mode	**Command**	**Description**
enable	show interface IFNAME	Displays the current port configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	show	Displays the current port configurations.
interface	loopback (none | mac)	Tests the loopback mode of operation for the specific port.
interface	flowcontrol (off | on)	Disables / enables the flow control for the port.
interface	speed (auto | 10-full | 10-half |100-full | 100-half | 1000-full)	Configures the speed and duplex for the port.
interface	shutdown	Disables the specific port.
interface	no shutdown	Enables the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	shutdown	Disables the specific ports.
if-range	no shutdown	Enables the specific ports.
if-range	speed (auto | 10-full | | 10-half | 100-full | 100-half | 1000-full)	Configures the speed and duplex for the port.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#interface gi1/0/1
L2SWITCH(config-if)#speed auto

4.4.1.2. Web Configuration - Port Settings / General Settings



Port Settings / General Settings	
Parameter	**Description**
Port Settings	
Port	Select a port or a range ports you want to configure on this screen.
State	Select **Enable** to activate the port or **Disable** to deactivate the port.
Speed/Duplex	Select the speed and duplex mode of the port. The choices are: • Auto • 10 Mbps / Full • 10 Mbps / Full / Nway • 10 Mbps / Half • 10 Mbps / Half / Nway • 100 Mbps / Full • 100 Mbps / Full / Nway • 100 Mbps / Half • 100 Mbps / Half / Nway • 1000 Mbps / Full • 1000 Mbps / Full / Nway • 10 Gbps / Full

Port Settings / General Settings (Continued)	
Parameter	**Description**
Flow Control	Select **On** to enable access to buffering resources for the port thus ensuring lossless operation across network switches. Otherwise, select **Off** to disable it.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

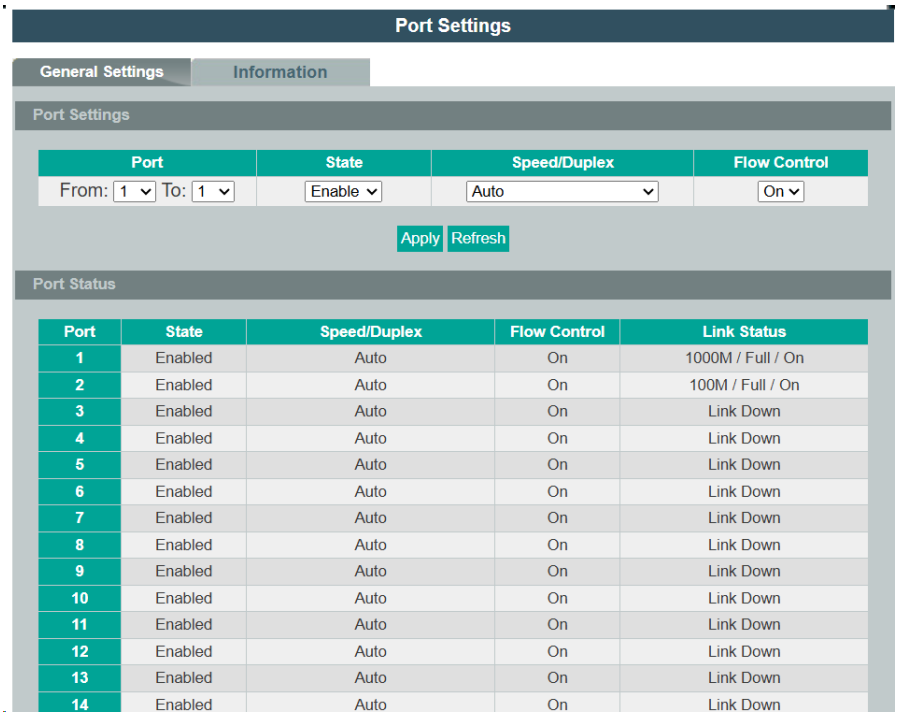
Port Settings / General Settings (Continued)	
Parameter	**Description**
Port Status	
Port	Displays the port number.
State	Displays whether the port is enabled or disabled.
Speed/Duplex	Displays the speed either 10M, 100M, 1000M or 10G and the mode.
Flow Control	Displays whether the port's flow control is On or Off.
Link Status	Displays the link status of the port. If the port is up, it displays the port's speed, duplex and flow control setting. Otherwise, it displays Link Down if the port is disabled or not connected to any device.

4.4.2. Port Settings / Information

4.4.2.1. CLI Configuration - Port Settings / Information

CLI Port Settings / Information		
Mode	**Command**	**Description**
enable	show interface IFNAME	Displays the current port configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	show	Displays the current port configurations.
interface	description STRING	Configures a description for the specific port. The length of description is up to 240 characters.
interface	no description	Configures the default port description.
interface	alias STRING	Configures an alias for the specific port. The length of alias is up to 64 characters.
interface	no alias	Resets the alias to default.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	description STRINGs	Configures a description for the specific ports.
if-range	no description	Configures the default port description for the specific ports.
if-range	alias STRING	Configures an alias for the specific ports. The length of alias is up to 64 characters.
if-range	no alias	Resets the alias to default.

4.4.2.2. Web Configuration - Port Settings / Information



Port Settings / Information	
Parameter	**Description**
Port Settings	
Port	Select a port or a range ports you want to configure on this screen.
State	Default is **Enable**. Select **Disable** to disable a specific port.
Speed/Duplex	Select the appropriate speed/duplex for the attached device.
Flow Control	Default is **On** and select **Off** to disable.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Port Status	
Port	Displays the port number.
State	Displays whether the port is enabled or disabled.
Speed/Duplex	Displays the speed and duplex.
Flow Control	Displays whether flow control is enabled or disabled.
Link Status	Displays the speed and duplex or port is down.

5. Advanced Settings

5.1. Bandwidth Control

5.1.1. QoS

Each egress port can support up to 8 transmit queues. Each egress transmit queue contains a list specifying the packet transmission order. Every incoming frame is forwarded to one of the 8 egress transmit queues of the assigned egress port, based on its priority. The egress port transmits packets from each of the 8 transmit queues according to a configurable scheduling algorithm, which can be a combination of Strict Priority (SP) and/or Weighted Round Robin (WRR).

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

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to give preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The ICRL2-M supports 802.1p priority queuing. The ICRL2-M has 8 priority queues. These priority queues are numbered from 7 (Class 7) — the highest priority queue — to 0 (Class 0) — the lowest priority queue.

The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the ICRL2-M's priority queues as follows:

Priority: 0 1 2 3 4 5 6 7

Queue: 2 0 1 3 4 5 6 7

Priority scheduling is implemented by the priority queues stated above. The ICRL2-M will empty the four hardware priority queues in order, beginning with the highest priority queue, 7, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

QoS Enhancement

You can configure the ICRL2-M to prioritize traffic even if the incoming packets are not marked with IEEE 802.1p priority tags or change the existing priority tags based on the criteria you select. The ICRL2-M allows you to choose one of the following methods for assigning priority to incoming packets on the ICRL2-M:

- 802.1p Tag Priority- Assign priority to packets based on the packet's 802.1p tagged priority.
- Port Based QoS - Assign priority to packets based on the incoming port on the ICRL2-M.
- DSCP Based QoS- Assign priority to packets based on their Differentiated Services Code Points (DSCPs).

Note: *Advanced QoS methods only affect the internal priority queue mapping for the ICRL2-M. The ICRL2-M does not modify the IEEE 802.1p value for the egress frames. You can choose one of these ways to alter the way incoming packets are prioritized or you can choose not to use any QoS enhancement setting on the ICRL2-M.*

802.1p Priority

When using 802.1p priority mechanism, the packet is examined for the presence of a valid 802.1p priority tag. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

Ethernet Packet:

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

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

802.1Q Tag:

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

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

Priority Levels

PCP: Priority Code Point.

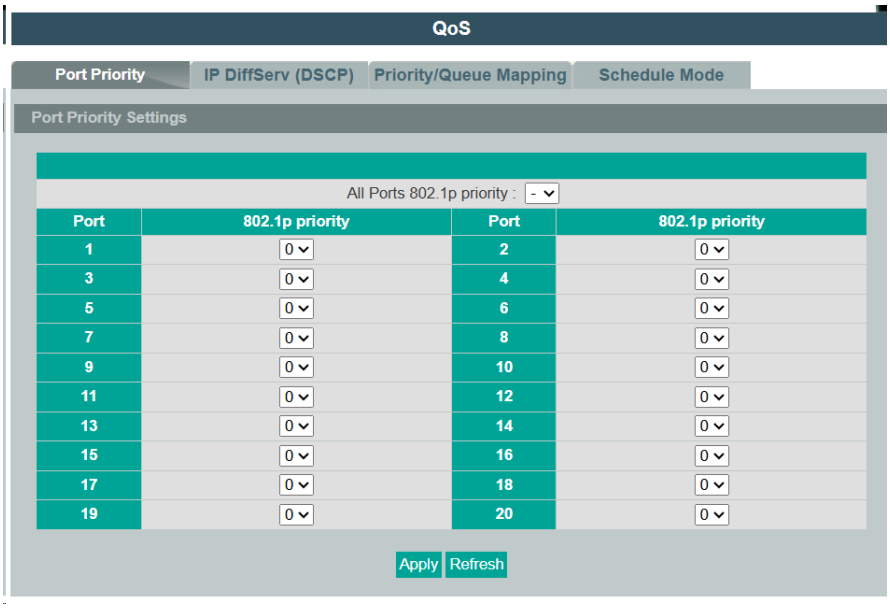
PCP	Network Priority	Traffic Characteristics
1	0 (lowest)	Background
0	1	Best Effort
2	2	Excellent Effort
3	3	Critical Applications
4	4	Video, <100ms latency
5	5	Video, < 10ms latency
6	6	Internetwork Control
7	7 (highest)	Network Control

5.1.1.1. Bandwidth Control / QoS / Port Priority

5.1.1.1.1. CLI Configuration - Bandwidth Control / QoS / Port Priority

CLI Bandwidth Control / QoS / Port Priority		
Mode	**Command**	**Description**
enable	show interface IFNAME	Displays the current port configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	default-priority <0-7>	Allows the user to specify a default priority handling of untagged packets received by the ICRL2-M. The priority value entered with this command will be used to determine which of the hardware priority queues the packet is forwarded to. Default: 0.
interface	no default-priority	Configures the default priority (0) for the specific port.

5.1.1.1.2. Web Configuration - Bandwidth Control / QoS / Port Priority



Bandwidth Control / QoS / Port Priority	
Parameter	**Description**
All Ports 802.1p priority	Use this field to set a priority for all ports. The value indicates packet priority and is added to the priority tag field of incoming packets. The values range from 0 (lowest priority) to 7 (highest priority).
Port	Displays the number of a port.

Bandwidth Control / QoS / Port Priority (Continued)	
Parameter	**Description**
802.1p Priority	Select a priority for packets received by the port. Only packets without 802.1p priority tagged will be applied the priority you set here.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.1.1.2. Bandwidth Control / QoS / IP DiffServ (DSCP)

DiffServ (DSCP)

Differentiated Services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing Quality of Service (QoS) guarantees on modern IP networks. DiffServ can, for example, be used to provide low-latency, guaranteed service (GS) to critical network traffic such as voice or video while providing simple best-effort traffic guarantees to non-critical services such as web traffic or file transfers.

Differentiated Services Code Point (DSCP) is a 6-bit field in the header of IP packets for packet classification purposes. DSCP replaces the outdated IP precedence, a 3-bit field in the Type of Service byte of the IP header originally used to classify and prioritize types of traffic.

When using the DiffServ priority mechanism, the packet is classified based on the DSCP field in the IP header. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

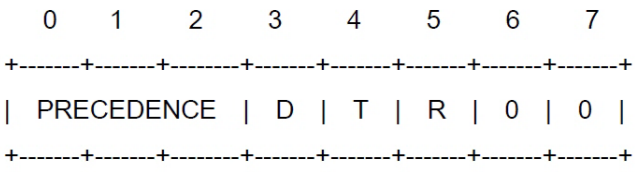
Version	IHL	**Type of Service**	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				Padding

Example Internet Datagram Header

IP Header Type of Service: 8 bits

The Type of Service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Several networks offer service precedence, which somehow treats high precedence traffic as more important than other traffic (generally by accepting only traffic above certain precedence at time of high load). The major choice is a three way trade off between low-delay, high-reliability, and high-throughput.

Bits 0-2	Precedence	
Bit 3	0 = Normal Delay	1 = Low Delay.
Bit 4	0 = Normal Throughput	1 = High Throughput.
Bit 5	0 = Normal Reliability	1 = High Reliability.
Bits 6-7	Reserved for Future Use	



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

The use of the Delay, Throughput, and Reliability indications may increase the cost (in some sense) of the service. In many networks better performance for one of these parameters is coupled with worse performance on another. Except for very unusual cases at most two of these three indications should be set.

The type of service is used to specify the treatment of the datagram during its transmission through the Internet system. Example mappings of the Internet type of service to the actual service provided on networks such as AUTODIN II, ARPANET, SATNET, and PRNET is given in "Service Mappings".

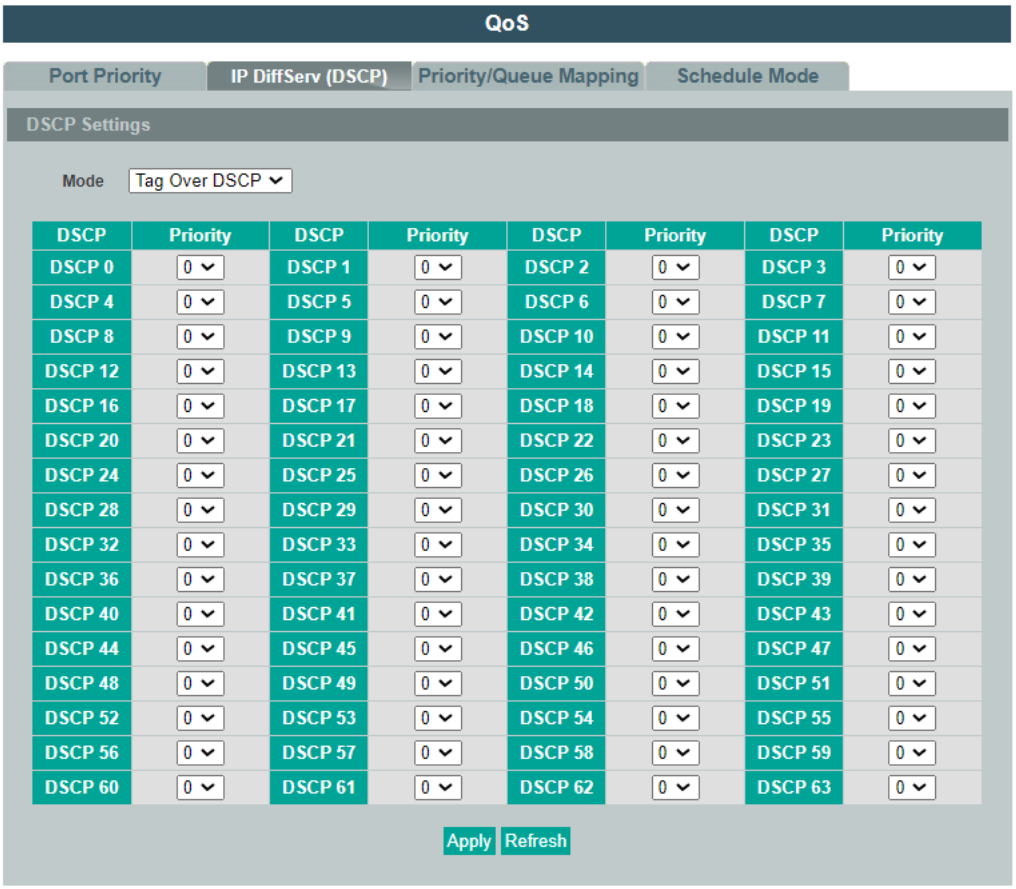
The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway control originators only.

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

5.1.1.2.1. CLI Configuration - Bandwidth Control / QoS / IP DiffServ (DSCP)

CLI Bandwidth Control / QoS / IP DiffServ (DSCP)		
Mode	**Command**	**Description**
enable	show diffserv	Displays DiffServ configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	diffserv (disable | enable)	Disables / enables the DiffServ function.
configure	diffserv dscp <0-63> priority <0-7>	Sets the DSCP-to-IEEE 802.1q mappings.

5.1.1.2.2. Web Configuration - Bandwidth Control / QoS / IP DiffServ (DSCP)



Bandwidth Control / QoS / IP DiffServ (DSCP)	
Parameter	**Description**
DSCP Settings	
Mode	**Tag Over DSCP** or **DSCP Over Tag**. **Tag Over DSCP** means the 802.1p tag has higher priority than DSCP.
Priority	Displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.1.1.3. Bandwidth Control / QoS / Priority / Queue Mapping

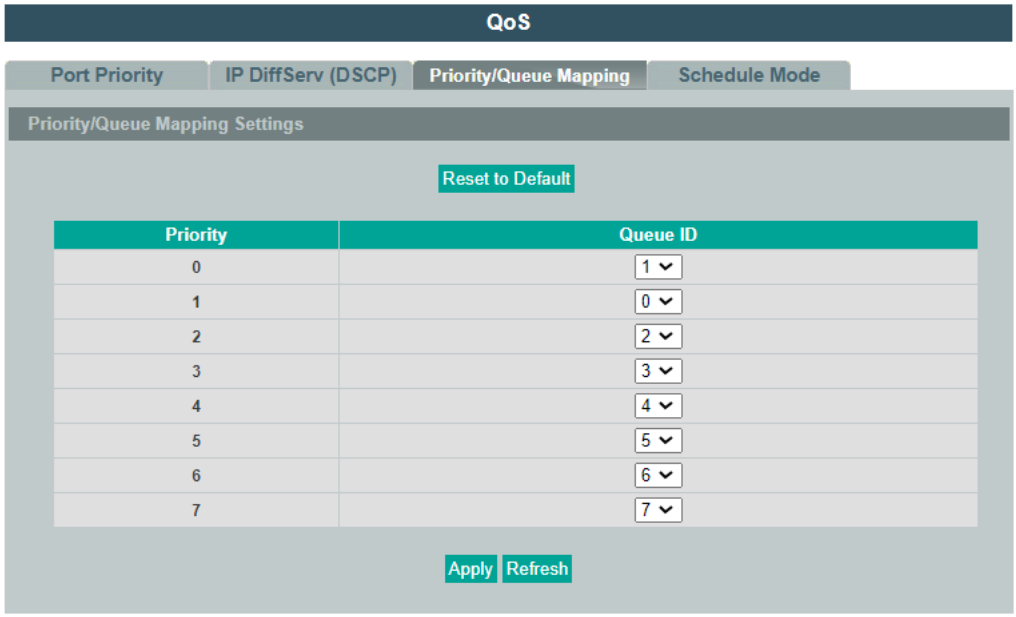
5.1.1.3.1. CLI Configuration - Bandwidth Control / QoS / Priority Queue Mapping

CLI Bandwidth Control / QoS / Priority / Queue Mapping		
Mode	**Command**	**Description**
enable	show queue cos-map	Displays the current 802.1p priority mapping to the service queue.
enable	configure terminal	Changes the mode to configure mode.
configure	queue cos-map <0-7> <0-7>	Configures the 802.1p priority mapping to the service queue.
configure	no queue cos-map	Configures the 802.1p priority mapping to the service queue to default.

Example:

```
L2SWITCH(config)#queue cos-map 0 1
Success!
L2SWITCH(config)#queue cos-map 1 2
Success!
L2SWITCH(config)#queue cos-map 2 3
Success!
L2SWITCH(config)#queue cos-map 3 4
Success!
L2SWITCH(config)#queue cos-map 4 5
Success!
L2SWITCH(config)#queue cos-map 5 6
Success!
L2SWITCH(config)#queue cos-map 6 7
Success!
L2SWITCH(config)#queue cos-map 7 0
Success!
L2SWITCH(config)#exit
L2SWITCH#show queue cos-map
The mapping of the Priority to Queue are:
    PRIO 0 ==> COSQ 1
    PRIO 1 ==> COSQ 2
    PRIO 2 ==> COSQ 3
    PRIO 3 ==> COSQ 4
    PRIO 4 ==> COSQ 5
    PRIO 5 ==> COSQ 6
    PRIO 6 ==> COSQ 7
    PRIO 7 ==> COSQ 0
```

5.1.1.3.2. Web Configuration - Bandwidth Control / QoS / Priority Queue Mapping



Bandwidth Control / QoS / Priority / Queue Mapping	
Parameter	**Description**
Reset to Default	Click this button to reset the priority to queue mappings to the defaults.
Priority	Displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Queue ID	Select the number of a queue for packets with the priority level.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.1.1.4. Bandwidth Control /QoS / Schedule Mode

Queuing Algorithms

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

- Strict-Priority (SPQ)

  The packets on the high priority queue are always service firstly.

- Weighted round robin (WRR)

  Round Robin scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of

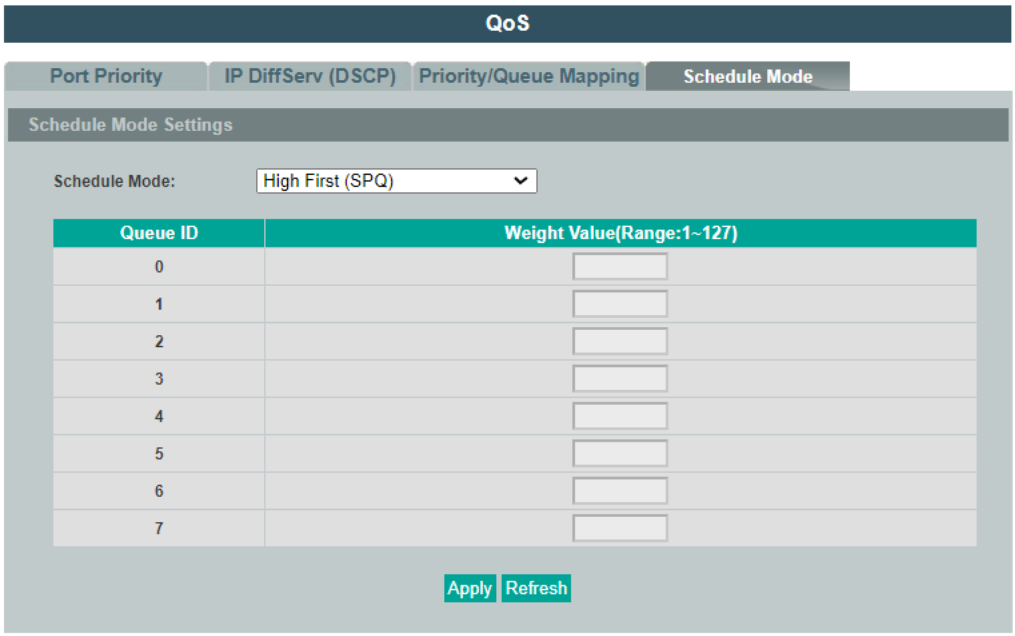
bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

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

5.1.1.4.1. CLI Configuration - Bandwidth Control /QoS / Schedule Mode

CLI Bandwidth Control / QoS / Schedule Mode		
Mode	**Command**	**Description**
enable	show qos mode	Displays the current QoS scheduling mode of IEEE 802.1p.
enable	configure terminal	Changes the mode to configure mode.
configure	qos mode high-first	Configures the QoS scheduling mode to high-first, each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets.
configure	qos mode wrr-queue weights <1-127> <1-127> <1-127> <1-127> <1-127> <1-127> <1-127> <1-127>	Configures the QoS scheduling mode to Weighted Round Robin.

5.1.1.4.2. Web Configuration - Bandwidth Control /QoS / Schedule Mode



8/19/25

Bandwidth Control / QoS / Schedule Mode	
Parameter	**Description**
Schedule Mode	Select High First (SPQ), Weighted Round Robin (WRR) or Weighted Fair Queuing (WFQ). ***Note:*** *Queue weights can only be changed when Weighted Round Robin is selected.* Weighted Round Robin scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights.
Queue ID	Indicates which Queue (0 to 7) you are configuring. Queue 0 has the lowest priority and Queue 7 the highest priority.
Weight Value	You can only configure the queue weights when Weighted Round Robin is selected. Bandwidth is divided across the different traffic queues according to their weights.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.1.2. Bandwidth Control / Rate Limitation

5.1.2.1. Bandwidth Control / Rate Limitation / Storm Control

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

Storm Control protects the ICRL2-M bandwidth from flooding packets, including broadcast packets, multicast packets, and destination lookup failure (DLF). The Rate is a threshold that limits the total number of the selected type of packets. For example, if the broadcast and multicast options are selected, the total amount of packets per second for those two types will not exceed the limit value.

Broadcast storm control limits the number of broadcast, multicast and unknown unicast (also referred to as Destination Lookup Failure or DLF) packets the ICRL2-M receives per second on the ports. When the maximum number of allowable broadcast, multicast and unknown unicast packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and unknown unicast packets in your network.

Storm Control unit: 652 pps.

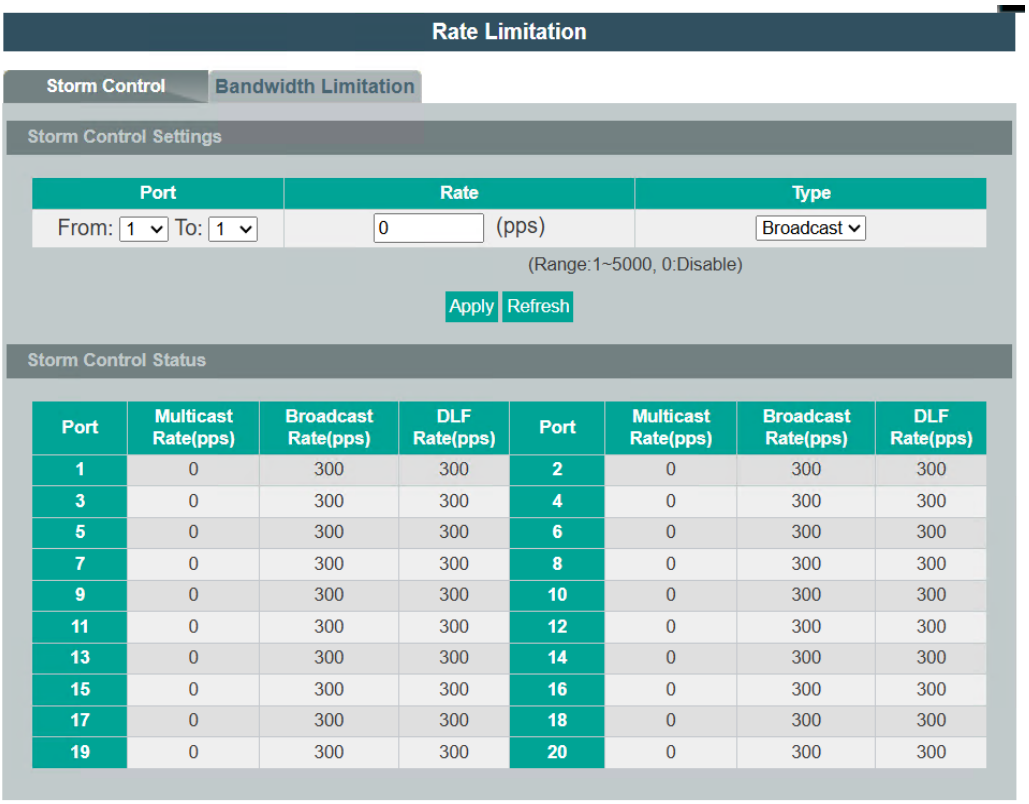
5.1.2.1.1. CLI Configuration - Bandwidth Control / Rate Limitation / Storm Control

CLI Bandwidth Control / Rate Limitation / Storm Control		
Mode	**Command**	**Description**
enable	show storm-control	Displays the current storm control configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	Enables the bandwidth limit for broadcast or multicast or DLF packets and set the limitation.
configure	no storm-controltype (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	Disables the bandwidth limit for broadcast or multicast or DLF packets.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#storm-control rate 1 type broadcast ports 1-6
L2SWITCH(config)#storm-control rate 1 type multicast ports 1-6
L2SWITCH(config)#storm-control rate 1 type DLF ports 1-6

5.1.2.1.2. Web Configuration - Bandwidth Control / Rate Limitation / Storm Control



Bandwidth Control / Rate Limitation / Storm Control	
Parameter	**Description**
Port	Select the port number for which you want to configure storm control settings.
Rate	Select the number of packets (of the type specified in the Type field) per second the ICRL2-M can receive per second.
Type	Select: • **Broadcast** - to specify a limit for the amount of broadcast packets received per second. • **Multicast** - to specify a limit for the amount of multicast packets received per second. • **DLF** - to specify a limit for the amount of DLF packets received per second. Or other combinations such as **Bcast+Mcast**, **Bcast_DLF**, **Mcast+DLF**, **Bcast+Mcast+DLF**.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.1.2.2. Bandwidth Control / Rate Limitation / Bandwidth Limitation

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

- **Rate Limitation unit**: Mbit/s (Mbps).
- Default Settings: All ports' Ingress and Egress rate limitation are disabled.

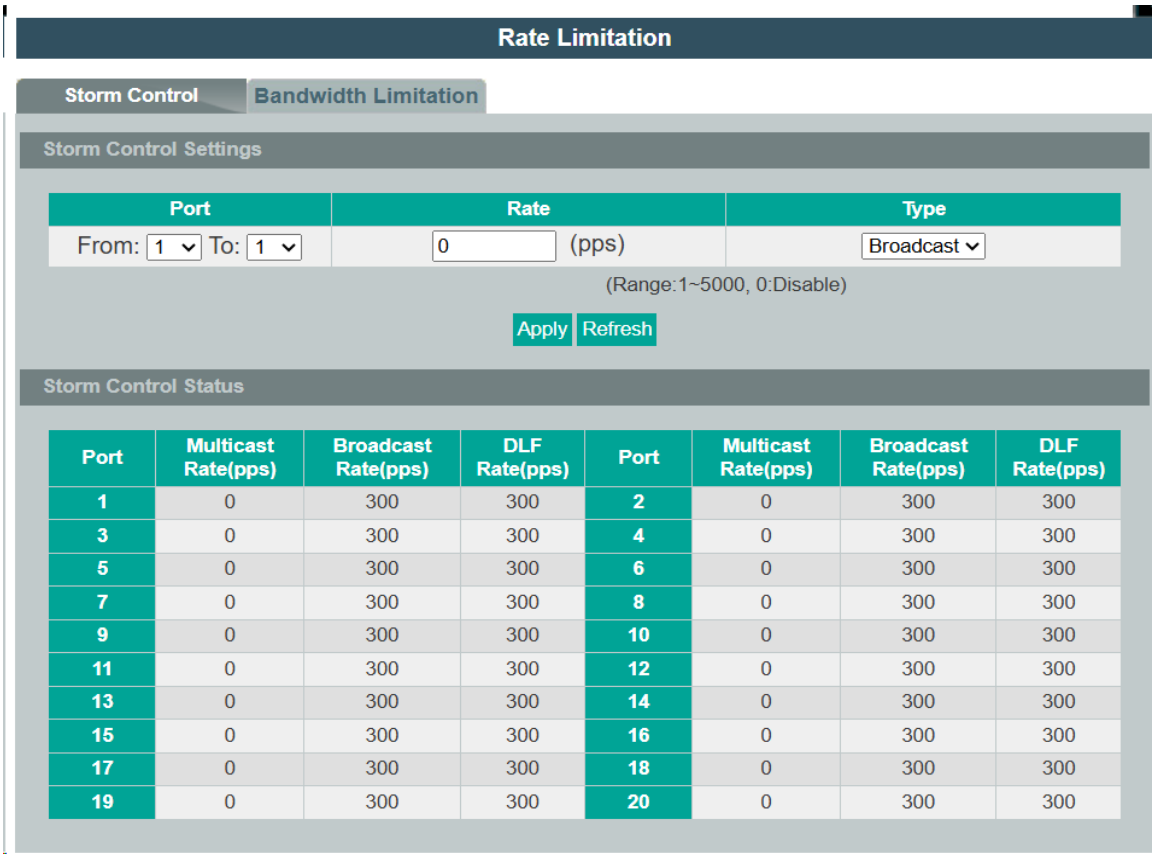
5.1.2.2.1. CLI Configuration - Bandwidth Control / Rate Limitation / Bandwidth Limitation

CLI Bandwidth Control / Rate Limitation / Bandwidth Limitation		
Mode	**Command**	**Description**
enable	show bandwidth-limit	Displays the current rate control configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	Enables the bandwidth limit for outgoing packets and set the limitation.
configure	no bandwidth-limit egress ports PORTLISTS	Disables the bandwidth limit for outgoing packets.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	Enables the bandwidth limit for incoming packets and set the limitation.
configure	no bandwidth-limit ingress ports PORTLISTS	Disables the bandwidth limit for incoming packets.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#bandwidth-limit ingress 1 ports 1-3
Success!
```

5.1.2.2.2. Web Configuration - Bandwidth Control / Rate Limitation / Bandwidth Limitation



Bandwidth Control / Rate Limitation / Bandwidth Limitation	
Parameter	**Description**
Storm Control Settings	
Port	Select the port that you want to configure.
Rate (pps)	Range is 1 - 5000 0 to disable
Type	Choices are: • Broadcast • Multicast • DLF
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.2. IGMP Snooping

5.2.1. IGMP Snooping Overview

The IGMP snooping is for multicast traffic. The ICRL2-M can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the ICRL2-M to learn multicast groups without you having to manually configure them.

The ICRL2-M can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the ICRL2-M to learn multicast groups without you having to manually configure them.

The ICRL2-M forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your ICRL2-M.

The ICRL2-M can perform IGMP snooping on up to 4094 VLANs. You can configure the ICRL2-M to automatically learn multicast group membership of any VLANs. The ICRL2-M then performs IGMP snooping on the first VLANs that send IGMP packets. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the ICRL2-M does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

IGMP snooping report suppression:

This feature enables the Layer 2 device to forward only the first IGMP report for a multicast group to its directly connected Layer 3 device. Other reports for the same group in the same query interval are discarded. Use this feature to reduce multicast traffic.

Configurations:

Users can enable/disable the IGMP Snooping on the ICRL2-M. Users also can enable/disable the IGMP Snooping on a specific VLAN. If the IGMP Snooping on the ICRL2-M is disabled, the IGMP Snooping is disabled on all VLANs even some of the VLAN IGMP Snooping are enabled.

Default Settings

- If received packets are not received after 400 seconds, all multicast entries will be deleted.
- The default global IGMP snooping state is disabled.
- The default VLAN IGMP snooping state is disabled for all VLANs.
- The unknown multicast packets will be dropped.
- The default port Immediate Leave state is disabled for all ports.
- The default port Querier Mode state is auto for all ports.
- The IGMP snooping Report Suppression is disabled.

Note: *There are a global state and per VLAN states. When the global state is disabled, the IGMP snooping on the ICRL2-M is disabled even per VLAN states are enabled. When the global state is enabled, user must enable per VLAN states to enable the IGMP Snooping on the specific VLAN.*

5.2.1.1. IGMP Snooping General Settings

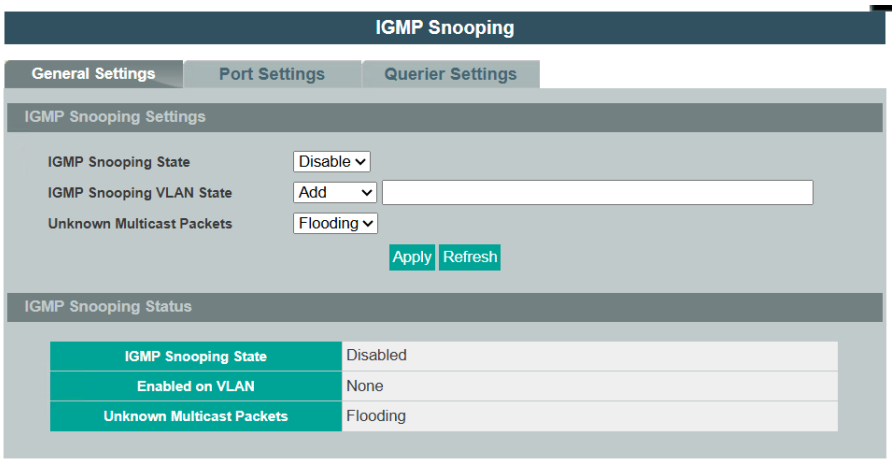
5.2.1.1.1. CLI Configuration - IGMP Snooping / General Settings

CLI IGMP Snooping / General Settings		
Mode	**Command**	**Description**
enable	show igmp-snooping	Displays the current IGMP snooping configurations.
enable	show igmp-snooping counters	Displays the current IGMP snooping counters.
enable	configure terminal	Changes the mode to configure mode.
configure	clear igmp-snooping counters	Clears all of the IGMP snooping counters.
configure	igmp-snooping (disable | enable)	Disables / enables the IGMP snooping on the ICRL2-M.
configure	igmp-snooping report-suppression (disable | enable)	Disables / enables the IGMP snooping report suppression function on the ICRL2-M.
configure	igmp-snooping vlan VLANID	Enables the IGMP snooping function on a VLAN or range of VLANs.
configure	no igmp-snooping vlan VLANID	Disables the IGMP snooping function on a VLAN or range of VLANs.
configure	igmp-snooping unknown-multicast (drop | flooding)	Configures the process for unknown multicast packets when the IGMP snooping function is enabled. drop: Drop all of the unknown multicast packets. flooding: Flooding the unknown multicast packets to all ports.

Example:

L2SWITCH(config)#igmp-snooping enable
L2SWITCH(config)#igmp-snooping vlan 1

5.2.1.1.2. Web Configuration - IGMP Snooping / General Settings



IGMP Snooping / General Settings	
Parameter	**Description**
IGMP Snooping Settings	
IGMP Snooping State	Select **Enable** to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select Disable to deactivate the feature.
IGMP Snooping VLAN State	Select **Add** and enter VLANs upon which the ICRL2-M is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLANs. Select Delete and enter VLANs on which to have the ICRL2-M not perform IGMP snooping.
Unknown Multicast Packets	Specify the action to perform when the ICRL2-M receives an unknown multicast frame. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
IGMP Snooping Status	
IGMP Snooping State	Displays whether IGMP snooping is globally enabled or disabled.
Enable on VLAN	Displays VLANs on which the ICRL2-M is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any VLAN yet.
Unknown Multicast Packets	Displays whether the ICRL2-M is set to drop or flooding unknown multicast packets.

5.2.1.2. IGMP Snooping Port Settings

Immediate Leave

When you enable IGMP Immediate-Leave processing, the ICRL2-M immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN. (Immediate Leave is only supported on IGMP Version 2 hosts).

The ICRL2-M uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the ICRL2-M sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Without Immediate Leave, when the ICRL2-M receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP specific query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership.

Port IGMP Querier Mode

- Auto: The ICRL2-M uses the port as an IGMP query port if the port receives IGMP query packets.
- Fixed: The ICRL2-M always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). The ICRL2-M always forwards the client's report/leave packets to the port. Normally, the port is connected to an IGMP server.
- Edge: The ICRL2-M does not use the port as an IGMP query port. The IGMP query packets received by this port will be dropped. Normally, the port is connected to an IGMP client.

Note: *The ICRL2-M will forward the IGMP join and leave packets to the query port.*

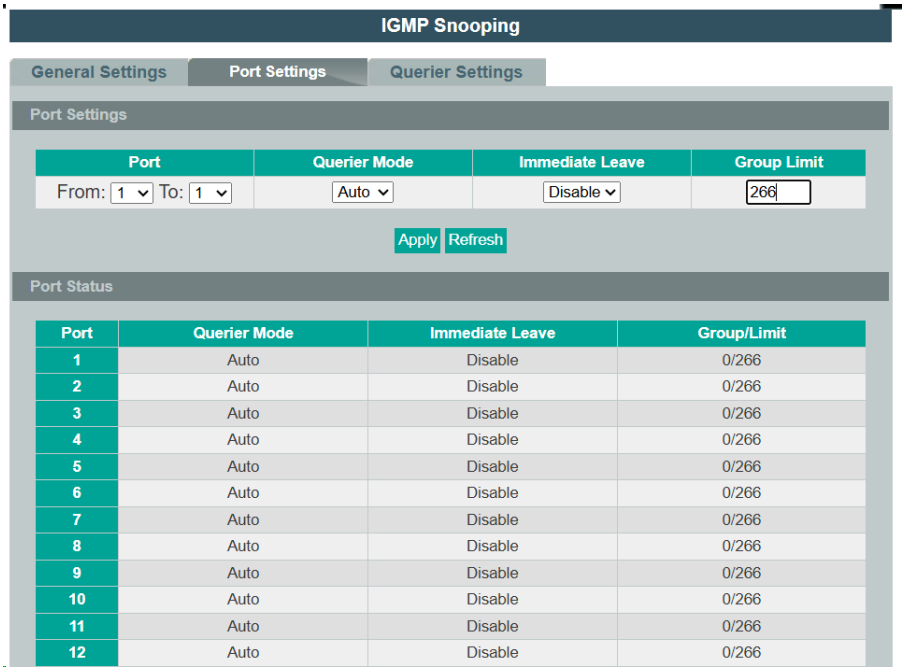
5.2.1.2.1. CLI Configuration - IGMP Snooping / Port Settings

,

CLI IGMP Snooping / Port Settings		
Mode	**Command**	**Description**
enable	show igmp-snooping	Displays the current IGMP snooping configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	igmp-immediate-leave	Enables the IGMP Snooping immediate leave function for the specific port.
interface	no igmp-immediate-leave	Disables the IGMP Snooping immediate leave function for the specific port.
interface	igmp-group-limit VALUE	Configures the maximum groups for the specific port.
interface	no igmp-group-limit	Configures the default value for the limitation of the maximum groups for the specific port.
interface	igmp-querier-mode (auto | fixed | edge)	Specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The ICRL2-M forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default: auto)

CLI IGMP Snooping / Port Settings (Continued)		
Mode	**Command**	**Description**
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	igmp-immediate-leave	Enables the IGMP Snooping immediate leave function for the specific ports.
if-range	no igmp-immediate-leave	Disables the IGMP Snooping immediate leave function for the specific ports.
if-range	igmp-group-limit VALUE	Configures the maximum groups for the specific port.
if-range	no igmp-group-limit	Configures the default value for the limitation of the maximum groups for the specific port.
if-range	igmp-querier-mode (auto | fixed | edge)	Specifies whether or not and under what conditions the ports is (are) IGMP query port(s). The ICRL2-M forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default: auto)

5.2.1.2.2. Web Configuration - IGMP Snooping / Port Settings



IGMP Snooping / Port Settings	
Parameter	**Description**
Port Settings	
Querier Mode	Select the desired setting, **Auto**, **Fixed**, or **Edge. Auto** means the ICRL2-M uses the port as an IGMP query port if the port receives IGMP query packets. Fixed means the ICRL2-M always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). Edge means the ICRL2-M does not use the port as an IGMP query port. In this case, the ICRL2-M does not keep a record of an IGMP router being connected to this port and the ICRL2-M does not forward IGMP join or leave packets to this port.
Immediate Leave	Select individual ports on which to enable immediate leave.
Group Limit	Configures the maximum group for the port or a range of ports.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.2.1.3. IGMP Snooping / Querier Settings

IGMP Querier

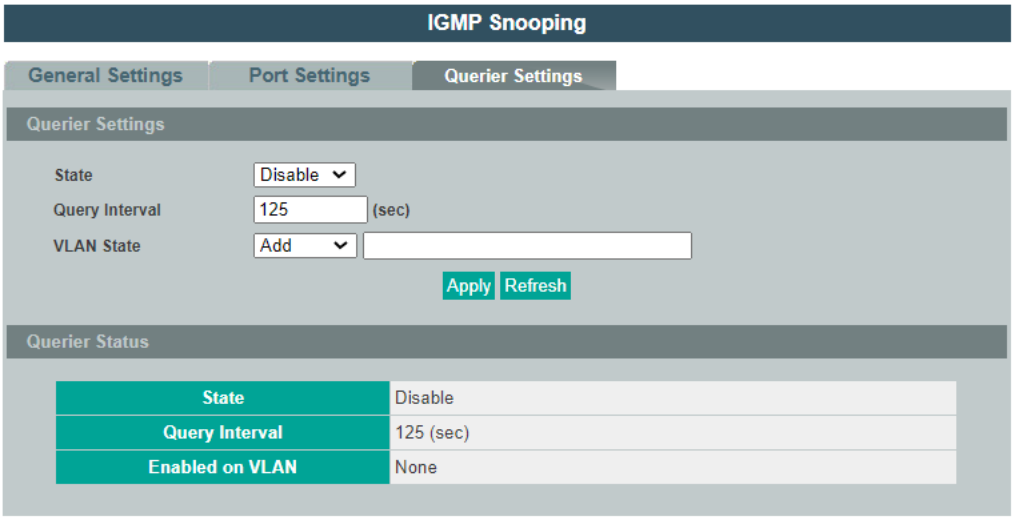
There is normally only one Querier per physical network. All multicast routers start up as a Querier on each attached network. If a multicast router hears a Query message from a router with a lower IP address, it MUST become a Non-Querier on that network. If a router has not heard a Query message from another router for [Other Querier Present Interval], it resumes the role of Querier. Routers periodically [Query Interval]send a General Query on each attached network for which this router is the Querier, to solicit membership information. On startup, a router SHOULD send [Startup Query Count] General Queries spaced closely together [Startup Query Interval] in order to quickly and reliably determine membership information. A General Query is addressed to the all-systems multicast group (224.0.0.1), has a Group Address field of 0, and has a Max Response Time of [Query Response Interval].

5.2.1.3.1. CLI Configuration - IGMP Snooping / Querier Settings

CLI IGMP Snooping / Querier Settings		
Mode	**Command**	**Description**
enable	show igmp-snooping querier	Displays the current IGMP Queriers.
enable	configure terminal	Changes the mode to configure mode.
configure	igmp-snooping querier (disable | enable)	Disables / enables the IGMP snooping querier on the ICRL2-M.
configure	igmp-snooping querier vlan VLANIDs	Enables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	no igmp-snooping querier vlan VLANIDs	Disables the IGMP snooping querier function on a VLAN or range of VLANs.

CLI IGMP Snooping / Querier Settings (Continued)		
Mode	**Command**	**Description**
configure	igmp-snooping query interval <2-300>	Configures the query interval for the Querier. Unit: second.

5.2.1.3.2. Web Configuration - IGMP Snooping / Querier Settings



IGMP Snooping / Querier Settings	
Parameter	**Description**
Querier Settings	
State	Configures the global Querier state.
Query Interval	Configures the interval which Querier send query packet periodically.
VLAN State	Enables the Querier state in a VLAN or a range of VLAN.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Querier Status	
State	This filed indicates the current global Querier status.
Query Interval	Indicates the interval which Querier send query packet periodically.
Enable on VLAN	Displays VLANs on which the ICRL2-M is to perform IGMP querier. None displays if you have not enabled IGMP querier on any VLAN yet.

5.2.2. IGMP Snooping / IGMP Filtering

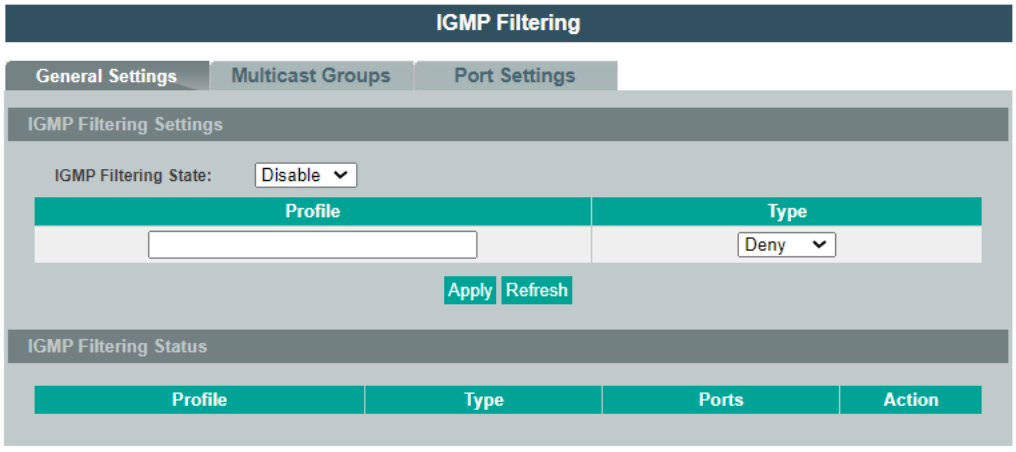
The IGMP Snooping Filter allows users to configure one or some of range or multicast address to drop or to forward them.

5.2.2.1. General Settings - IGMP Snooping / IGMP Filtering

5.2.2.1.1. CLI Configuration - IGMP Snooping / IGMP Filtering / General Settings

CLI IGMP Snooping / IGMP Filtering / General Settings		
Mode	**Command**	**Description**
enable	show igmp-snooping filtering	Displays the IGMP snooping filtering configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	igmp-snooping filtering (enable | disable)	Enables/disables the IGMP snooping filtering profiles on the ICRL2-M.
configure	igmp-snooping filtering profile STRING	Creates a filtering profile and enters the IGMP snooping filtering profiles configuration mode.
configure	no igmp-snooping filtering all	Removes all of the IGMP snooping filtering profiles from the ICRL2-M.
configure	no igmp-snooping filtering STRINGS	Removes the IGMP snooping filtering profiles by name from the ICRL2-M.
config-igmp	type (deny | permit)	Configures the type of deny or permit for the group.

5.2.2.1.2. Web Configuration - IGMP Snooping / IGMP Filtering / General Settings



8/19/25

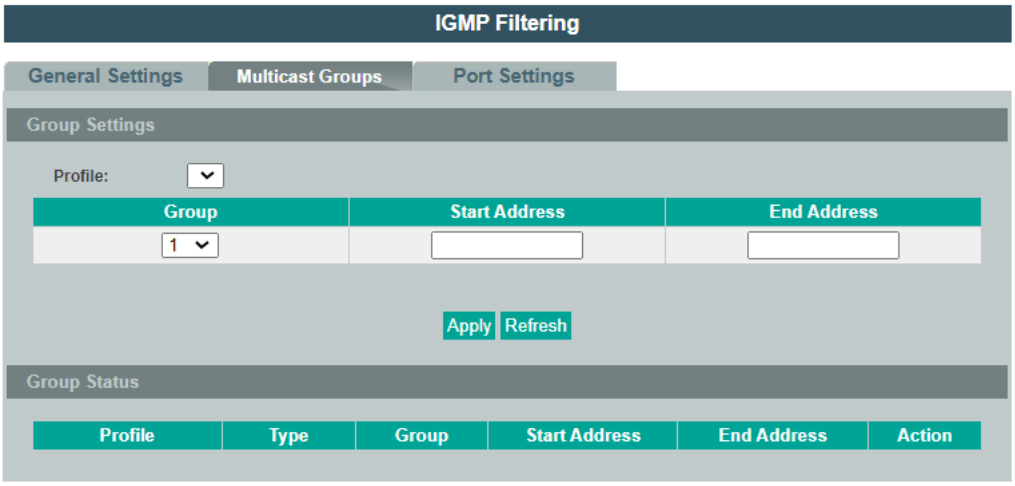
IGMP Snooping / IGMP Filtering / General Settings	
Parameter	**Description**
IGMP Filtering Settings	
IGMP Filtering State	Configures the global IGMP Filtering state.
Profile	Creates the IGMP Filtering profile.
Type	Configures the type of action for the profile.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
IGMP Filtering Status	
Profile	The profile name.
Type	The type of action.
Ports	Indicates the ports that the IGMP Filtering profile is activated.
Action	Click Delete to delete the profile.

5.2.2.2. IGMP Snooping / IGMP Filtering / Mulitcast Groups

5.2.2.2.1. CLI Configuration - IGMP Snooping / IGMP Filtering / Multicast Groups

CLI IGMP Snooping / IGMP Filtering / Multicast Groups		
Mode	**Command**	**Description**
enable	show igmp-snooping filtering	Displays the IGMP snooping filtering configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	igmp-snooping filtering profile STRING	Creates a filtering profile and enters the IGMP snooping filtering profiles configuration mode.
config-igmp	Group GROUP_ID start-address START-ADDR end-address END-ADDR	Configures the group configurations, including group index and start multicast address and end multicast address.
config-igmp	no group GROUP-ID	Removes the group configurations.
config-igmp	no group all	Removes all of the group configurations.

5.2.2.2.2. Web Configuration - IGMP Snooping / IGMP Filtering / Multicast Groups



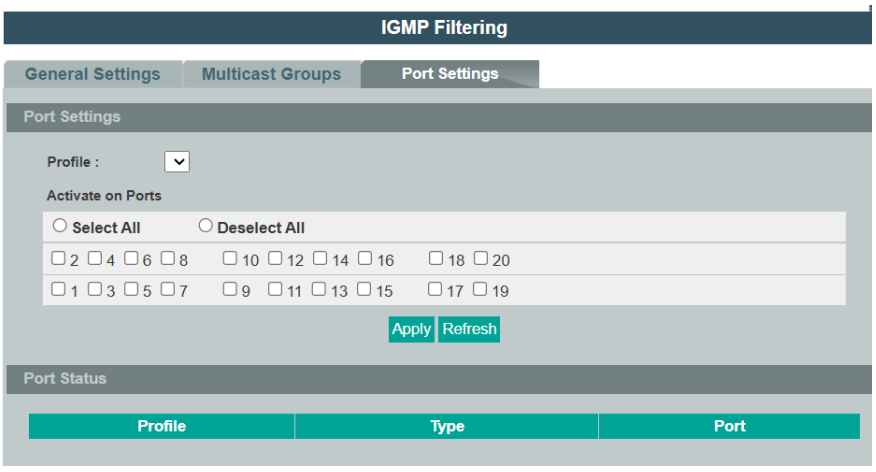
IGMP Snooping / IGMP Filtering / Multicast Groups	
Parameter	**Description**
Group Settings	
Profile	Selects the profile which you want to configure the group.
Group	Selects the group index.
Start Address	Configures the first multicast address of the group.
End Address	Configures the last multicast address of the group.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.2.2.3. IGMP Snooping / IGMP Filtering / Port Settings

5.2.2.3.1. CLI Configuration - IGMP Snooping / IGMP Filtering / Port Settings

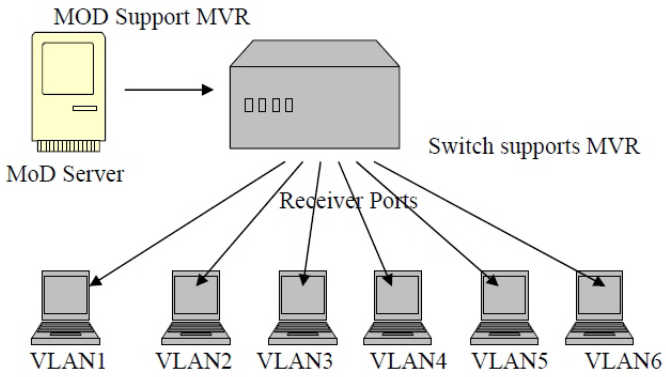
CLI IGMP Snooping / IGMP Filtering / Port Settings		
Mode	**Command**	**Description**
enable	show igmp-snooping filtering	Displays the IGMP snooping filtering configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	igmp-snooping filtering profile STRING	Enables the IGMP snooping filtering profiles on the range of ports.
interface	no igmp-snooping filtering profile STRINGS	Disables the IGMP snooping filtering profiles on the range of ports.
configure	interface range gigabitethernet1/0/PORTLISTS	Enters the if-range configure mode.
if-config	igmp-snooping filtering profile STRING	Enables the IGMP snooping filtering profiles on the range of ports.
if-config	no igmp-snooping filtering profile STRINGS	Disables the IGMP snooping filtering profiles on the range of ports.

5.2.2.3.2. Web Configuration - IGMP Snooping / IGMP Filtering / Port Settings



IGMP Snooping / IGMP Filtering / Port Settings	
Parameter	**Description**
Profile	Selects the profile which you want to activate on the ports.
Activate on Ports	Selects the ports which you want to activate the IGMP Filtering profile.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.2.3. Multicast Address Overview



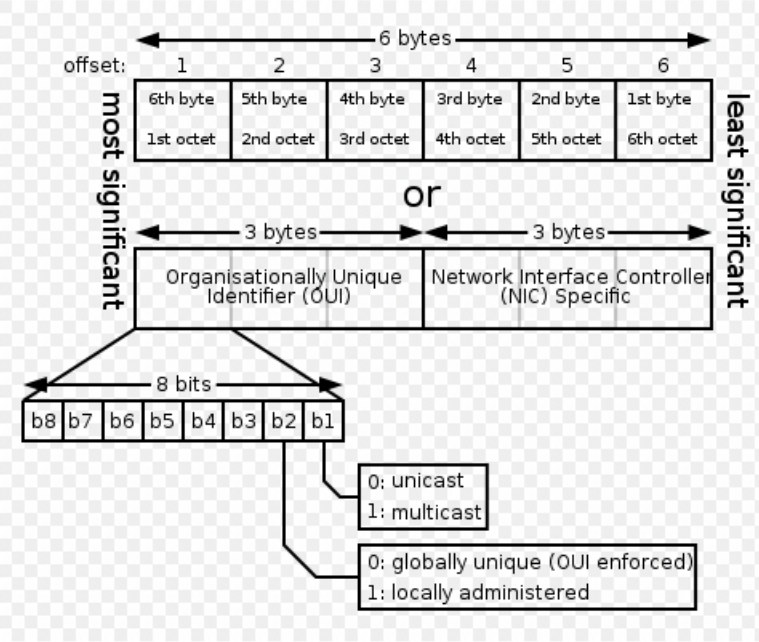
MOD Support MVR

A multicast address is associated with a group of interested receivers. According to RFC 3171, addresses 224.0.0.0 to 239.255.255.255, the former Class D addresses, are designated as multicast addresses in IPv4.

The IANA owns the OUI MAC address 01:00:5e, therefore multicast packets are delivered by using the Ethernet MAC address range 01:00:5e:00:00:00 - 01:00:5e:7f:ff:ff. This is 23 bits of available address space.

The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. This means that there is ambiguity in delivering packets. If two hosts on the same subnet each subscribe to a different multicast group whose address differs only in the first 5 bits, Ethernet packets for both multicast groups will be delivered to both hosts, requiring the network software in the hosts to discard the un-required packets.

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



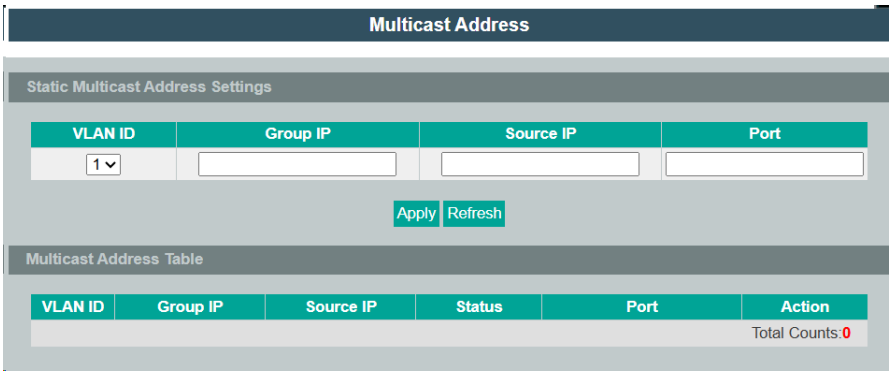
IP Multicast Address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	The All Hosts multicast group that contains all systems on the same network segment
224.0.0.2	The All Routers multicast group that contains all routers on the same network segment
224.0.0.5	The Open Shortest Path First (OSPF) All SPF Routers address. Used to send Hello packets to all OSPF routers on a network segment
224.0.0.6	The OSPF All D Routers address. Used to send OSPF routing information to OSPF designated routers on a network segment
224.0.0.9	The RIP version 2 group address, used to send routing information using the RIP protocol to all RIP v2-aware routers on a network segment
224.0.0.10	EIGRP group address. Used to send EIGRP routing information to all EIGRP routers on a network segment
224.0.0.13	PIM Version 2 (Protocol Independent Multicast)
224.0.0.18	Virtual Router Redundancy Protocol
224.0.0.19 - 21	IS-IS over IP
224.0.0.22	IGMP Version 3 (Internet Group Management Protocol)
224.0.0.102	Hot Standby Router Protocol Version 2
224.0.0.251	Multicast DNS address

IP Multicast Address	Description
224.0.0.252	Link-local Multicast Name Resolution address
224.0.1.1	Network Time Protocol address
224.0.1.39	Cisco Auto-RP-Announce address
224.0.1.40	Cisco Auto-RP-Discovery address
224.0.1.41	H.323 Gatekeeper discovery address

5.2.3.1. CLI Configuration - IGMP Snooping / Multicast Address - IGMP Snooping / Multicast Address

CLI IGMP Snooping / Multicast Address		
Mode	**Command**	**Description**
enable	show mac-address-table multicast	Displays the current static/dynamic multicast address entries.
enable	show mac-address-table multicast vlan <1-4094>	Displays the current static/dynamic multicast address entries with a specific VLAN.
enable	configure terminal	Changes the mode to configure mode.
configure	mac-address-table multicast MACADDR vlan <1-4094> ports PORTLIST	Configures a static multicast entry.
configure	no mac-address-table multicast MACADDR	Removes a static multicast entry from the address table.

5.2.3.2. Web Configuration - IGMP Snooping / Multicast Address



IGMP Snooping / Multicast Address	
Parameter	**Description**
Static Multicast Address Settings	
VLAN ID	Configures the VLAN that you want to configure.
Group IP	Configures the multicast group IP address.
Source IP	Configures the host's IP address that sends out the multicast stream.
Port	Configures the member port for the multicast address.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.3. VLAN

5.3.1. VLAN / Port Isolation

The port isolation is a port-based virtual LAN feature. It partitions the ICRL2-M ports into virtual private domains designated on a per port basis. Data switching outside of the port's private domain is not allowed. It will ignore the packets' tag VLAN information.

This feature is a per port setting to configure the egress port(s) for the specific port to forward its received packets. If the CPU port (Port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the ICRL2-M.

If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports.CPU refers to the ICRL2-M management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the ICRL2-M cannot be managed from that port.

Example: If you want to allow port-1 and port-3 to talk to each other, you must configure as below:

```
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#port-isolation ports 3
L2SWITCH(config-if)#exit
    ; Allow the port-1 to send its ingress packets to port-3.

L2SWITCH(config)#interface 1/0/3
L2SWITCH(config-if)#port-isolation ports 1
L2SWITCH(config-if)#exit
    ; Allow the port-3to send its ingress packets to port-1
```

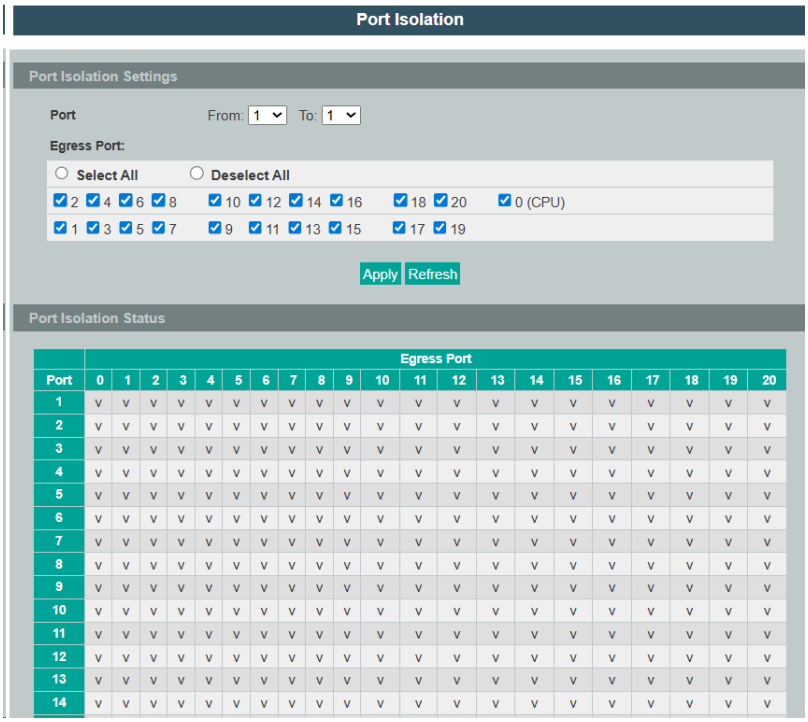
5.3.1.1. CLI Configuration - VLAN / Port Isolation

CLI VLAN / Port Isolation		
Mode	**Command**	**Description**
enable	show port-isolation	Displays the current port isolation configurations. "V" indicates the port's packets can be sent to that port. "-" indicates the port's packets cannot be sent to that port.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	port-isolation ports PORTLISTS	Configures a port or a range of ports to egress traffic from the specific port.
interface	no port-isolation	Configures all ports to egress traffic from the specific port.

Example:

```
L2SWITCH(config)#interface 1/0/2
L2SWITCH(config-if)#port-isolation ports 3-10
```

5.3.1.2. Web Configuration - VLAN / Port Isolation



Note: *Number of ports displayed varies depending on the ICRL2-M.*

VLAN / Port Isolation	
Parameter	**Description**
Port Isolation Settings	
Port	Select a port number to configure its port isolation settings. **Select All** Ports to configure the port isolation settings for all ports on the ICRL2-M.
Egress Port	An egress port is an outgoing port, that is, a port through which a data packet leaves. Selecting a port as an outgoing port means it will communicate with the port currently being configured.
Select All/Deselect All	Click **Select All** to mark all ports as egress ports and permit traffic. Click **Deselect All** to un-check all ports and isolate them. Deselecting all ports means the port being configured cannot communicate with any other port.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Port Isolation Status	
	“V” indicates the port’s packets can be sent to that port. “-” indicates the port’s packets cannot be sent to that port.

5.3.2. 802.1Q VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network ICRL2-M. Network reconfiguration can be done through software instead of physically relocating devices.

VID- VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q. It has 12 bits and allow the identification of 4096 (2^12) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the ICRL2-M on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

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

- Forwarding Tagged and Untagged Frames

  Each port on the ICRL2-M is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware ICRL2-M to an 802.1Q VLAN-unaware ICRL2-M, the ICRL2-M first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware ICRL2-M to an 802.1QVLAN-aware ICRL2-M, the ICRL2-M first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

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

- 802.1QPort base VLAN

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

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

  The device that is attached to the port likely has no understanding that a VLAN exists. The device simply knows that it is a member of a subnet and that the device should be able to talk to all other members of the subnet by simply sending information to the cable segment. The ICRL2-M is responsible for identifying that the information came from a specific VLAN and for ensuring that the information gets to all other members of the VLAN. The ICRL2-M is further responsible for ensuring that ports in a different VLAN do not receive the information.

  This approach is quite simple, fast, and easy to manage in that there are no complex lookup tables required for VLAN segmentation. If port-to-VLAN association is done with an application-specific integrated circuit (ASIC), which allows the port-to-VLAN mapping to be done at the hardware level.

Default Settings

- The default PVID is 1 for all ports.
- The default Acceptable Frame is All for all ports.
- All ports join in the VLAN 1.

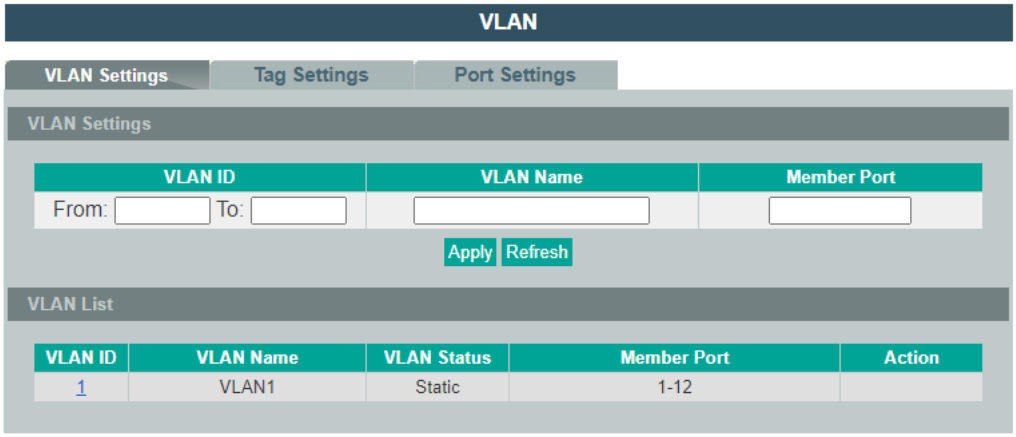
Note: *The maximum VLAN group is 4094.*

5.3.2.1. VLAN / VLAN Settings

5.3.2.1.1. CLI Configuration - VLAN / VLAN Settings

CLI VLAN / VLAN Settings		
Mode	**Command**	**Description**
enable	show vlan	Displays all of the VLAN configurations.
enable	show vlan <1-4094>	Displays the VLAN configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	vlan <1~4094>	Enables a VLAN and enters the VLAN mode.
configure	no vlan <1~4094>	Deletes a VLAN.
vlan	show	Displays the current VLAN configurations.
vlan	name STRING	Assigns a name for the specific VLAN. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters
vlan	no name	Configures the VLAN name to default. ***Note:*** *The default VLAN name is "VLAN"+VLAN-ID, VLAN1, VLAN2,…*
vlan	add PORTLISTS	Adds a port or a range of ports to the VLAN.
vlan	fixed PORTLISTS	Assigns ports for permanent member of the VLAN.
vlan	no fixed PORTLISTS	Removes all fixed member from the VLAN.
configure	vlan range VLANLIST	Configures a range of VLANs.
configure	no vlan range VLANLIST	Removes a range of VLANs.
vlan-range	add PORTLISTS	Adds a port or a range of ports to the VLANs.
vlan-range	fixed PORTLISTS	Assigns ports for permanent member of the VLAN group.
vlan-range	no fixed PORTLISTS	Removes all fixed member from the VLANs.

5.3.2.1.2. Web Configuration - VLAN / VLAN Settings



VLAN / VLAN Settings	
Parameter	**Description**
VLAN Settings	
VLAN ID	Enter the VLAN ID for this entry; the valid range is between 1 and 4094.
VLAN Name	Enter a descriptive name for the VLAN for identification purposes. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
Member Port	Enter the port numbers you want the ICRL2-M to assign to the VLAN as members. You can designate multiple port numbers individually by using a comma (,) and by range with a hyphen (-).
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
VLAN List	
VLAN ID	Displays the index number of the VLAN entry. Click the number to modify the VLAN.
VLAN Name	Displays the name of the VLAN.
VLAN Status	Displays the status of the VLAN. Static or Dynamic (802.1QVLAN).
Member Port	Displays which ports have been assigned as members of the VLAN. This will display None if no ports have been assigned.
Action	Click Delete to remove the VLAN. The VLAN 1 cannot be deleted.

5.3.2.2. VLAN / Tag Settings

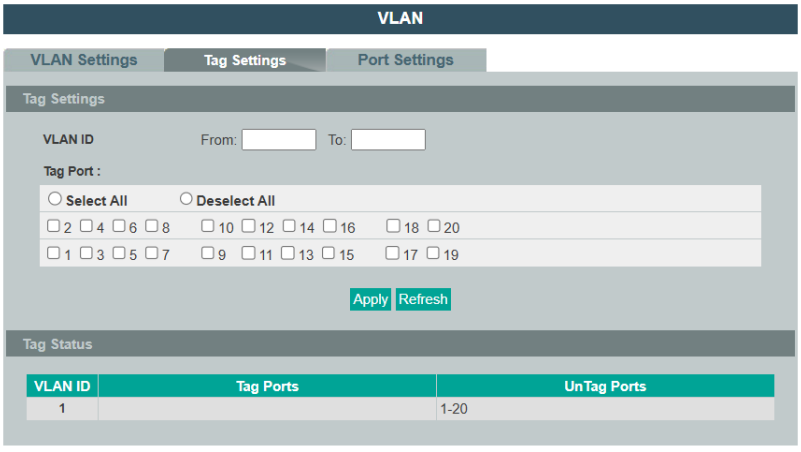
5.3.2.2.1. CLI Configuration - VLAN / Tag Settings

CLI VLAN / Tag Settings		
Mode	**Command**	**Description**
enable	show vlan	Displays all of the VLAN configurations.
enable	show vlan <1-4094>	Displays the VLAN configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	vlan <1~4094>	Enables a VLAN and enters the VLAN mode.
vlan	show	Displays the current VLAN configurations.
vlan	add PORTLISTS	Adds a port or a range of ports to the VLAN.
vlan	tagged PORTLISTS	Assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the VLAN.
vlan	no tagged PORTLISTS	Removes all tagged member from the VLAN.
vlan	Untagged PORTLISTS	Assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the VLAN.
vlan	no untagged PORTLISTS	Removes all untagged member from the VLAN.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#vlan 2
L2SWITCH(config-vlan)#fixed 1-6
L2SWITCH(config-vlan)#tagged 1-3

5.3.2.2.2. Web Configuration - VLAN / Tag Settings



Note: *Number of ports displayed varies depending on the ICRL2-M.*

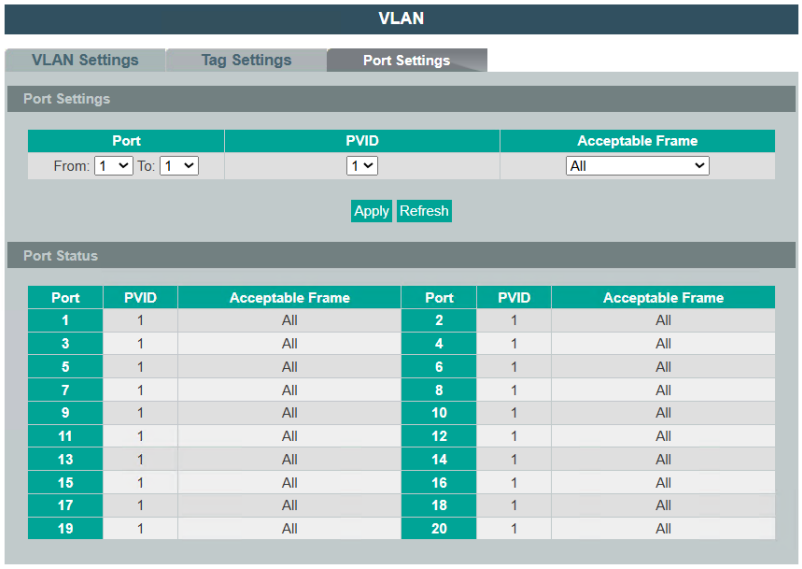
VLAN / Tag Settings	
Parameter	**Description**
VLAN ID	Enter the VLAN ID range for port tagging settings; the valid range is between 1 and 4094.
Tag Port	Selecting a port which is a member of the selected VLAN ID will make it a tag port. This means the port will tag all outgoing frames transmitted with the VLAN ID.
Select All	Click **Select All** to mark all member ports as tag ports.
Deselect All	Click **Deselect All** to mark all member ports as untag ports.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.3.2.3. VLAN Port Settings

5.3.2.3.1. CLI Configuration - VLAN / Port Settings

CLI VLAN / Port Settings		
Mode	**Command**	**Description**
enable	show vlan	Displays all of the VLAN configurations.
enable	show vlan <1-4094>	Displays the VLAN configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	acceptable frame type (all | tagged | untagged)	Configures the acceptable frame type. **all** - acceptable all frame types. **tagged** - acceptable tagged frame only. **untagged** – acceptable untagged frame only.
interface	pvid <1-4094>	Configures a VLAN ID for the port default VLAN ID.
interface	no pvid	Configures 1 for the port default VLAN ID.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	acceptable frame type (all | tagged | untagged)	Configures the acceptable frame type. **all** - acceptable all frame types. **tagged** - acceptable tagged frame only. **untagged** – acceptable untagged frame only.
if-range	pvid <1-4094>	Configures a VLAN ID for the port default VLAN ID.
if-range	no pvid	Configures 1 for the port default VLAN ID.

5.3.2.3.2. Web Configuration - VLAN / Port Settings



Note: *Number of ports displayed varies depending on the ICRL2-M.*

VLAN / Port Settings	
Parameter	**Description**
Port	Select a port number to configure from the drop-down box. Select All to configure all ports at the same time.
PVID	Select a PVID (Port VLAN ID number) from the drop-down box.
Acceptable Frame	Specify the type of frames allowed on a port. Choices are All, VLAN Untagged Only or VLAN Tagged Only. • Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. • Select **VLAN Tagged Only** to accept only tagged frames on this port. All untagged frames will be dropped. • Select **VLAN Untagged Only** to accept only untagged frames on this port. All tagged frames will be dropped.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.3.3. MAC VLAN

The MAC base VLAN allows users to create VLAN with MAC address. The MAC address can be the leading three or more bytes of the MAC address.

For example, 00:01:02 or 00:03:04:05 or 00:01:02:03:04:05.

When the ICRL2-M receives packets, it will compare MAC-based VLAN configures. If the SA is matched the MAC-based VLAN configures, the ICRL2-M replace the VLAN with user configured and them forward them.

For example:

Configurations: 00:01:02, VLAN=23, Priority=2.

The packets with SA=00:01:02:xx:xx:xx will be forwarded to VLAN 22 member ports.

Note: *The 802.1Q port base VLAN should be created first.*

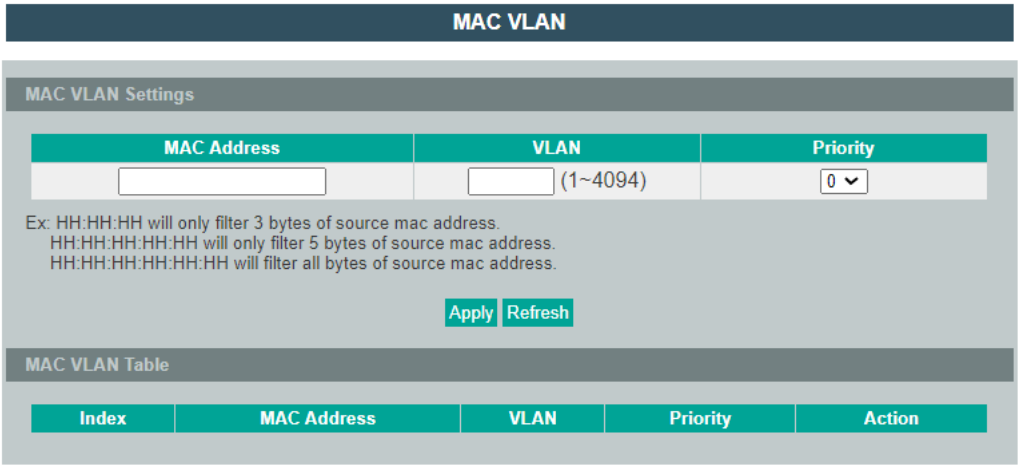
5.3.3.1. CLI Configuration - MAC VLAN / MAC VLAN Settings

CLI VLAN MAC-based VLAN		
Mode	**Command**	**Description**
enable	show mac-vlan	Displays the all of the mac-vlan configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	mac-vlan STRINGS vlan <1-4094> priority <0-7>	Creates a mac-vlan entry with the leading three or more bytes of mac address and the VLAN and the priority.
configure	no mac-vlan entry STRINGS	Deletes a mac-vlan entry.
configure	no mac-vlan all	Deletes all of the mac-vlan entries.

Example:

L2SWITCH(config)#mac-vlan 00:01:02:03 vlan 111 priority 1
L2SWITCH(config)#mac-vlan 00:01:02:22:04 vlan 121 priority 1
L2SWITCH(config)#mac-vlan 00:01:22:22:04:05 vlan 221 priority 1

5.3.3.2. Web Configuration - MAC VLAN / MAC VLAN Settings



VLAN / MAC VLAN Settings	
Parameter	**Description**
MAC VLAN Settings	
MAC Address	Configures the leading three or more bytes of the MAC address.
VLAN	Configures the VLAN.
Priority	Configures the 802.1Q priority.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
MAC VLAN Table	
Action	Click **Delete** to delete the MAC VLAN profile.

5.3.4. VLAN / Q-in-Q VLAN /VLAN Stacking

Q-in-Q tunneling is also known as VLAN stacking. Both of them use 802.1q double tagging technology. Q-in-Q is required by ISPs (Internet Service Provider) that need Transparent LAN services (TLS), and the service provider has their own set of VLAN, independent of customer VLANs. Typically, each service provider VLAN interconnects a group of sites belonging to a customer. However, a service provider VLAN could also be shared by a set of customers sharing the same end points and quality of service requirements of the VLAN. Double tagging is considered to be a relatively simpler way of implementing transparent LAN. This is accomplished by encapsulating Ethernet Frame. A second or outer VLAN tag is inserted in Ethernet frames sent over the ingress PE (Provider Edge). This VLAN tag corresponds to the VLAN of the Service Provider (SP). When the frame reaches the destination PE, the SP VLAN is stripped off. The DA of the encapsulated frame and the VLAN ID are used to take further L2 decisions, similar to an Ethernet frame arriving from a physical Ethernet port. The SP VLAN tag determines the VPLS (Virtual Private LAN Service) membership. Double tagging aggregates multiple VLANs within another VLAN and provides a private, dedicated Ethernet connection between customers to reach their subnet transparently across multiple networks. Thus service providers can create their own VLANs without interfering with customer VLANs by using double tagging. This allows them to connect customers to ISPs and ASPs (Application Service Provider).

The ports that are connected to the service provider VLANs are called tunnel ports, and the ports that are connected to the customer VLANs are called access (subscriber/customer) ports. When a port is configured as tunnel port, all the outgoing packets on this port will be sent out with SPVLAN (SPVID and 1p priority) tag. The incoming packet can have two tags (SPVLAN + CVLAN), one tag (SPVLAN or CVLAN), or no tag. In all cases, the packet is sent out with a SPVLAN tag. When a port is configured as an access port, the incoming traffic can have only a CVLAN (CVID and 1p priority) tag or no tag. Hence, all the packets that are being sent out of access ports will be untagged or single tagged (CVLAN). When a port is configured as a normal port, it will ignore the frames with double tagging.

Double Tagging Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

TPID	Priority	VID

- TPID (Tag Protocol Identifier) is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. The value of this field is 0x8100 as defined in IEEE 802.1Q. Other vendors may use a different value, such as 0x9100.
- Tunnel TPID is the VLAN stacking tag type the ICRL2-M adds to the outgoing frames sent through a Tunnel Port of the service provider's edge devices
- Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for. "0" is the lowest priority level and "7" is the highest.
- VID is the VLAN ID. SP VID is the VID for the second or outer (service provider's) VLAN tag. CVID is the VID for the first or inner (Customer's) VLAN tag.

The frame formats for an untagged Ethernet frame; a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) are shown as following.

untagged frame	DA	SA	Len or Etype	Data	FCS						
single-tagged frame	DA	SA	TPID	P	VID	Len or Etype	Data	FCS			
double-tagged frame	DA	SA	Tunnel TPID	P	VID	TPID	P	VID	Len or Etype	Data	FCS

DA	Destination Address
SA	Source Address

8/19/25

Tunnel TPID	Tag Protocol Identifier added on a tunnel port
P	802.1p priority
VID	VLAN ID
Len or Etype	Length or Ethernet frame type
Data	Frame data
FCS	Frame Check Sequence

VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, Normal, Access Port and Tunnel Port.

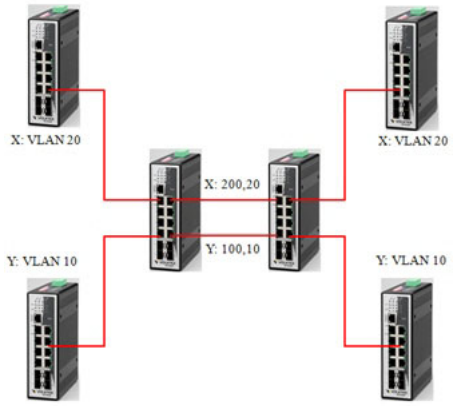
- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices. The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.
- Select **Tunnel Port** for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).

Note: *In order to have the double tagged frames switching correctly, user has to configure a service provider’s VLAN (SPVLAN) on the Q-in-Q ICRL2-M. Then, the double tagged frames can be switched according to the SP VID. The SPVLAN should include all the related Tunnel and Access ports. Also, user has to configure the Tunnel posts as tagged ports and the Access ports as untagged ports.*

Port-based Q-in-Q

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

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



This example shows how to configure ICRL2-M A with ports 1 on the ICRL2-M to tag incoming frames with the service provider's VID of 200 (ports are connected to customer X network) and configure port 7 to service provider's VID of 100 (ports are connected to customer Y network).This example also shows how to set the priority for port 1 to 3 and port 7 to 4.

```
L2SWITCH(config)# vlan-stacking port-based
L2SWITCH(config)# vlan-stacking tpid-table index 2 value 88a8
L2SWITCH(config)# vlan 10
L2SWITCH(config-vlan)# fixed 5,6
L2SWITCH(config-vlan)# tagged 5
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 100
L2SWITCH(config-vlan)# fixed 5,6
L2SWITCH(config-vlan)# tagged 6
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 20
L2SWITCH(config-vlan)# fixed 1,2
L2SWITCH(config-vlan)# tagged 1
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 200
L2SWITCH(config-vlan)# fixed 1,2
L2SWITCH(config-vlan)# tagged 2
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# interface gigaethernet1/0/1
L2SWITCH(config-if)# vlan-stacking port-based role access
L2SWITCH(config-if)# vlan-stacking spvid 200
L2SWITCH(config-if)# vlan-stacking priority 3
L2SWITCH(config)# interface gigaethernet1/0/2
L2SWITCH(config-if)# vlan-stacking port-based role tunnel
L2SWITCH(config-if)# vlan-stacking tunnel-tpid index 2
L2SWITCH(config)# interface gigaethernet1/0/5
L2SWITCH(config-if)# vlan-stacking port-based role access
L2SWITCH(config-if)# vlan-stacking spvid 100
L2SWITCH(config-if)# vlan-stacking priority 4
L2SWITCH(config)# interface gigaethernet1/0/6
L2SWITCH(config-if)# vlan-stacking port-based role tunnel
L2SWITCH(config-if)# vlan-stacking tunnel-tpid index 2
L2SWITCH(config-if)# exit
L2SWITCH(config)# exit
L2SWITCH# show vlan-stacking
L2SWITCH# show vlan-stacking tpid-table
L2SWITCH# show vlan-stacking port-based-qinq
```

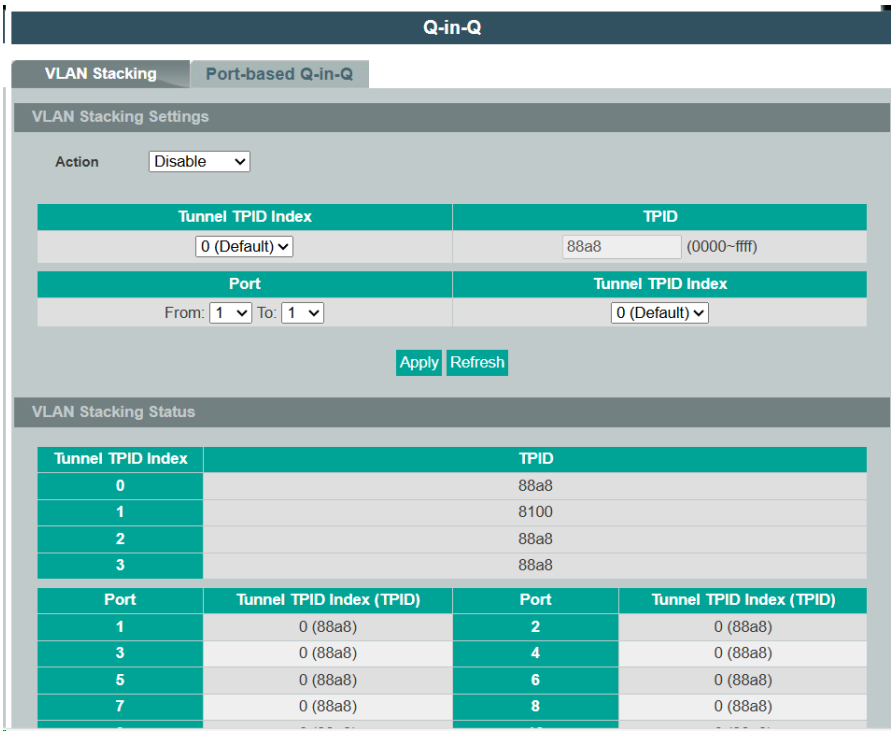
Default Setting: VLAN Stacking is disabled.

5.3.4.1. VLAN / Q-in-Q VLAN Stacking

5.3.4.1.1. CLI Configuration - VLAN / Q-in-Q / VLAN Stacking

CLI / VLAN / Q-in Q / VLAN Stacking		
Mode	**Command**	**Description**
enable	show vlan-stacking	Displays the current vlan-stacking type.
enable	show vlan-stacking tpid-inform	Displays the TPID configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	vlan-stacking (disable | port-based | selective)	Disable the VLAN stacking or enable the vlan-stacking with port-based or selective on the ICRL2-M.
configure	vlan-stacking tpid-table index <2-6> value STRINGS	Configures TPID table.
configure	interface IFNAME	Enters the interface configure mode.
interface	vlan-stacking tunnel-tpid index <1-6>	Sets TPID for a Q-in-Q tunnel port.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	vlan-stacking tunnel-tpid index <1-6>	Sets TPID for a Q-in-Q tunnel port.

5.3.4.1.2. Web Configuration - VLAN / Q-in-Q / VLAN Stacking



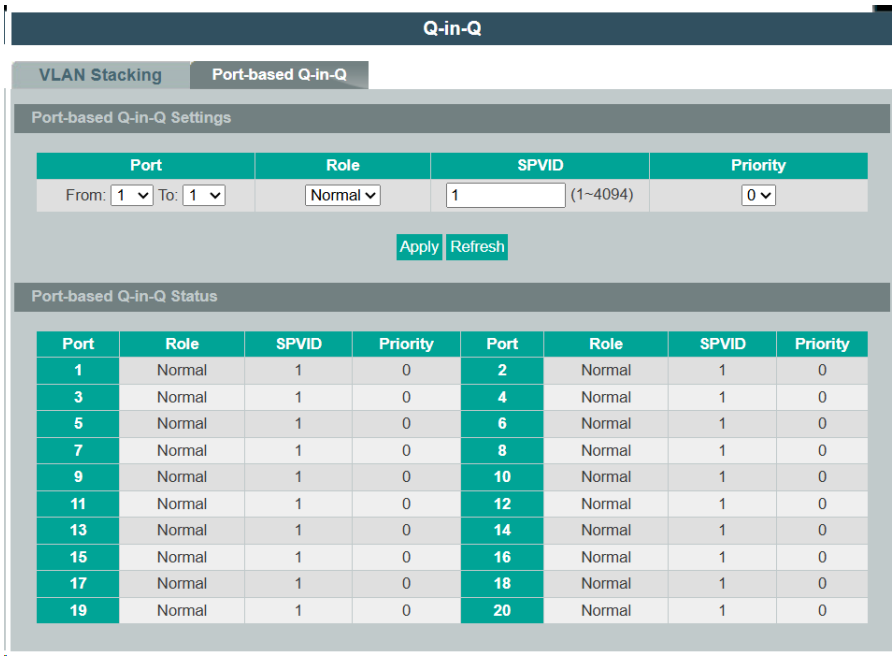
VLAN / Q-in-Q / VLAN Stacking	
Parameter	**Description**
VLAN Stacking Settings	
Action	Select one of the three modes, **Disable** or **Port-Based** or **Selective** for the VLAN stacking. Configures the TPID Table: The TPID table has 6 entries.
Tunnel TPID Index	Selects the table index.
Configures the Port TPID	
Port	Selects a port or a range of ports which you want to configure.
Tunnel TPID Index	Configures the index of the TPID Table for the specific ports.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Action	Click **Delete** to delete the MAC VLAN profile.

5.3.4.2. VLAN / Q-in-Q / Port-Based Q-in-Q

5.3.4.2.1. CLI Configuration - VLAN / Q-in-Q / Port-Based Q-in-Q

CLI / VLAN / Q-in Q / Port-based		
Mode	**Command**	**Description**
enable	show vlan-stacking portbased-qinq	Displays the port-based q-in-Q configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	vlan-stacking port-based priority <0~7>	Sets the priority in port based Q-in-Q.
interface	vlan-stacking port-based role (tunnel | access | normal)	Sets VLAN stacking port role.
interface	vlan-stacking port-based spvid <1~4096>	Sets the service provider's VID of the specified port.
interface	vlan-stacking tunnel-tpid index <1-6>	Sets TPID for a Q-in-Q tunnel port.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	vlan-stacking port-based priority <0~7>	Sets the priority in port based Q-in-Q.
if-range	vlan-stacking port-based role (tunnel | access | normal)	Sets VLAN stacking port role.
if-range	vlan-stacking port-based spvid <1~4096>	Sets the service provider's VID of the specified port.
if-range	vlan-stacking tunnel-tpid index <1-6>	Sets TPID for a Q-in-Q tunnel port.

5.3.4.2.2. Web Configuration - VLAN / Q-in-Q / Port-Based Q-in-Q



VLAN / Q-in-Q / Port-based Q-in-Q	
Parameter	**Description**
Port	Selects a port or a range of ports which you want to configure.
Role	Selects one of the three roles, **Normal** and **Access** and **Tunnel**, for the specific ports.
SPVID	Configures the service provider's VLAN.
Priority	Configures the priority for the specific ports.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.4. DHCP Options / Option 82

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

The DHCP option 82 is working on the DHCP snooping or/and DHCP relay.

The ICRL2-M will monitor the DHCP packets and append some information as below to the DHCPDISCOVER and DHCPREQUEST packets. The ICRL2-M will remove the DHCP Option 82 from the DHCPOFFER and DHCPACK packets. The DHCP server will assign IP domain to the client dependent on these information.

The maximum length of the information is 32 characters.

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the ICRL2-M, a subscriber device is identified by the ICRL2-M port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access ICRL2-M and are uniquely identified.

When you enable the DHCP snooping information option 82 on the ICRL2-M, this sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the ICRL2-M receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the ICRL2-M MAC address (the remote-ID sub-option) and the port identifier, vlan-mod-port, from which the packet is received (the circuit-ID sub-option).
- If the IP address of the relay agent is configured, the ICRL2-M adds the IP address in the DHCP packet.
- The ICRL2-M forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82 capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.
- The DHCP server unicast’s the reply to the ICRL2-M if the request was relayed to the server by the ICRL2-M. When the client and server are on the same subnet, the server broadcasts the reply. The ICRL2-M verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The ICRL2-M removes the option-82 field and forwards the packet to the ICRL2-M port that connects to the DHCP client that sent the DHCP request.

Option Frame Format:

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

The Agent Information field consists of a sequence of Sub-Opt/Length value for each sub-option, encoded in the following manner:

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

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

8/19/25

Circuit ID Sub-option Format:

Sub-option Type	Length	Information
0x01		Circuit Form

Remote ID Sub-option Frame Format:

Sub-option Type	Length	Type	Length	MAC Address
0x02	8	0	6	6

Circuit Form:

The circuit form is a flexible architecture. It allows user to combine any information or the system configurations into the circuit sub-option.

The Circuit Form is a string format. And its maximum length is 100 characters.

The keyword, %SPACE, will be replaced with a space character.

The other keywords get system configurations from the system and then replace the keyword and its leading code in the Circuit form. Eventually, the content of the circuit form is part of the payload on the DHCP option 82 packet.

Rules:

- The keyword must have a leading code '%'. For example: %HOSTNAME.
- If there are any characters following the keywords, you must add '+' between the keyword and character. For example: %HOSTNAME+/.
- If there are any characters before the keyword, you must add '+' between the character and the keyword. For example: Test+%HOSTNAME.

Keyword	Description
HOSTNAME	Add the system name into the Circuit sub-option.
SPACE	Add a space character.
SVLAN	Add the service provider VLAN ID into the Circuit sub-option. If the service provider VLAN is not defined, the system will return PVLAN.
CVLAN	Add the customer VLAN ID into the Circuit sub-option If the CVLAN is not defined, the system returns 0.
PORT	Add the transmit port ID into the Circuit sub-option.
FRAME	Add the frame ID into the Circuit sub-option. The frame ID is configured with the CLI command, "dhcp-options option82 circuit_frame VALUE". Or GUI Circuit Frame.
SHELF	Add the shelf ID into the Circuit sub-option. The shelf ID is configured with the CLI command, "dhcp-options option82 circuit_shelf VALUE". Or GUI Circuit Shelf.
SLOT	Add the slot ID into the Circuit sub-option. The slot ID is configured with the CLI command, "dhcp-options option82 circuit_slot VALUE". Or GUI Circuit Slot.

For Example:

HOSTNAME=L2SWITCH.
SVLAN=44.
CVLAN=32.

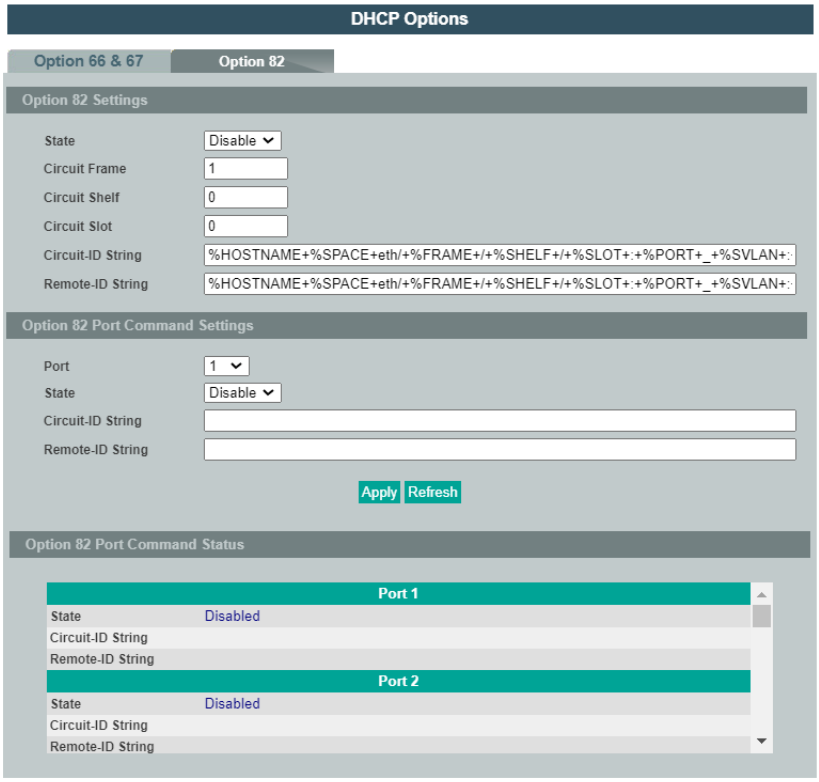
Circuit Form=RD+%SPACE+Department+%SPACE+%HOSTNAME+%SPACE+%PORT+_+%SVLAN+.+%CVLAN

The circuit sub-option result is: RD Department L2SWITCH 1_44.32

5.4.1. CLI Configuration - DHCP Options / Option 82

CLI DHCP Options / Option 82		
Mode	**Command**	**Description**
enable	show dhcp-options	Displays the DHCP options configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	dhcp-options option82 (disable | enable)	Disables / enables the DHCP option 82 on the ICRL2-M.
configure	dhcp-options option82 circuit_id STRING	Configures the information of the circuit ID sub-option.
configure	no dhcp-options option82 circuit_id	Removes the information of the circuit ID sub-option.
configure	dhcp-options option82 remote_id STRING	Configures the information of the remote ID sub-option.
configure	no dhcp-options option82 remote_id	Removes the information of the remote ID sub-option.
configure	dhcp-options option82 circuit_frame VALUE	Configures the frame ID for the circuit sub-option.
configure	dhcp-options option82 circuit_shelf VALUE	Configures the shelf ID for the circuit sub-option.
configure	dhcp-options option82 circuit_slot VALUE	Configures the slot ID for the circuit sub-option.

5.4.2. Web Configuration - DHCP Options / Option 82



DHCP Options / Option 82	
Parameter	**Description**
Option 82 Settings	
State	Select this option to enable / disable the DHCP option 82 on the ICRL2-M.
Circuit Frame	The frame ID for the circuit sub-option.
Circuit Shelf	The shelf ID for the circuit sub-option.
Circuit Slot	The slot ID for the circuit sub-option.
Circuit-ID String	The String of the circuit ID sub-option information.
Remote-ID String	The String of the remote ID sub-option information.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

DHCP Options / Option 82 (Continued)	
Parameter	**Description**
Option 82 Port Settings	
Port	The port ID.
Circuit-ID String	The String of the circuit ID sub-option information for the specific port.
Remote-ID String	The String of the remote ID sub-option information for the specific port.

5.5. DHCP Relay

Because the DHCPDISCOVER message is a broadcast message, and broadcasts only cross other segments when they are explicitly routed, you might have to configure a DHCP Relay Agent on the router interface so that all DHCPDISCOVER messages can be forwarded to your DHCP server. Alternatively, you can configure the router to forward DHCP messages and BOOTP message. In a routed network, you would need DHCP Relay Agents if you plan to implement only one DHCP server.

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

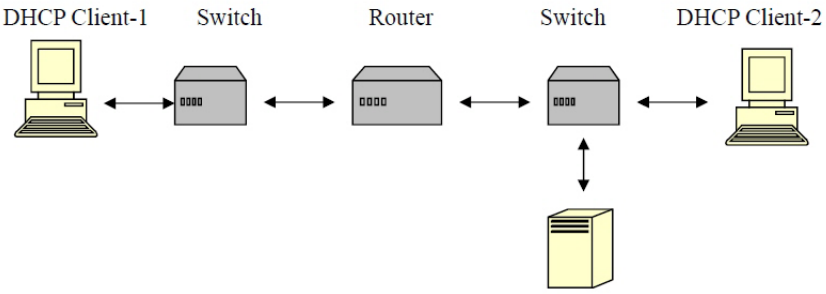
Most of the time in small networks DHCP uses broadcasts however there are some circumstances where unicast addresses will be used. A router for such a subnet receives the DHCP broadcasts, converts them to unicast (with a destination MAC/IP address of the configured DHCP server, source MAC/IP of the router itself). The field identified as the GIADDR in the main DHCP page is populated with the IP address of the interface on the router it received the DHCP request on. The DHCP server uses the GIADDR field to identify the subnet the device and select an IP address from the correct pool. The DHCP server then sends the DHCP OFFER back to the router via unicast which then converts it back to a broadcast and out to the correct subnet containing the device requesting an address.

Configurations:

Users can enable/disable the DHCP Relay on the ICRL2-M. Users also can enable/disable the DHCP Relay on a specific VLAN. If the DHCP Relay on the ICRL2-M is disabled, the DHCP Relay is disabled on all VLANs even some of the VLAN DHCP Relay are enabled.

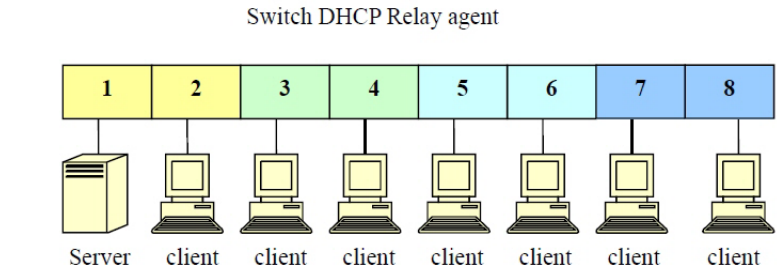
Applications

- Application-1 (Over a Router)



- Application-2 (Local in different VLANs)

The DHCP cleint-1 and DHCP client-2 are located in different VLANs, but they allocate IP address from the same DHCP server.



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

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

Result: Hosts connected to port 2,3,4,5,6,7,8 can get IP from DHCP server.

Note: *The DHCP Server must connect to the management VLAN member ports. The DHCP Relay in management VLAN should be enabled.*

Default Settings

- The default global DHCP relay state is disabled.
- The default VLAN DHCP relay state is disabled for all VLANs.
- The default DHCP server is 0.0.0.0

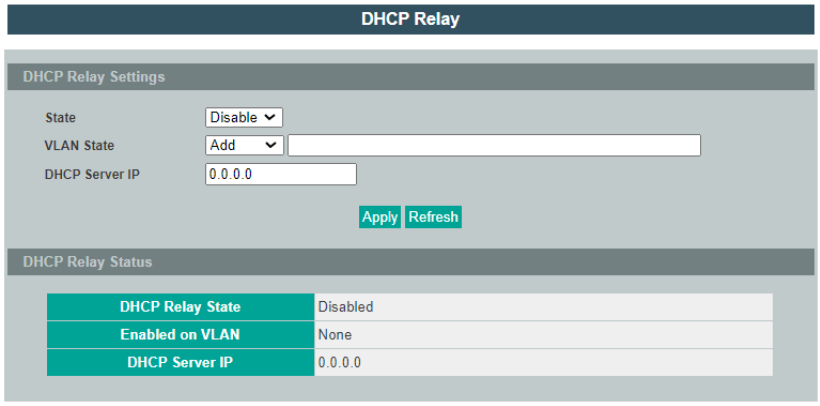
5.5.1. CLI Configuration - DHCP Relay

CLI DHCP Relay		
Mode	**Command**	**Description**
enable	show dhcp relay	Displays the current configurations for the DHCP relay.
enable	configure terminal	Changes the mode to configure mode.
configure	dhcp relay (disable | enable)	Disables/enables the DHCP relay on the ICRL2-M.
configure	dhcp relay vlan VLAN_RANGE	Enables the DHCP relay function on a VLAN or a range of VLANs.
configure	no dhcp relay vlan VLAN_RANGE	Disables the DHCP relay function on a VLAN or a range of VLANs.
configure	dhcp helper-address IP_ADDRESS	Configures the DHCP server's IP address.
configure	no dhcp helper-address	Removes the DHCP server's IP address.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#ip address 172.20.1.101/24
L2SWITCH(config-if)#ip address default-gateway 172.20.1.1
L2SWITCH(config)#dhcp relay enable
L2SWITCH(config)# dhcp relay vlan 1
L2SWITCH(config)# dhcp helper-address 172.20.1.1
```

5.5.2. Web Configuration - DHCP Relay



DHCP Relay / DHCP Relay Settings	
Parameter	**Description**
State	Enables/ disables the DHCP relay for the ICRL2-M.
VLAN State	Enables / disables the DHCP relay on the specific VLAN(s).
DHCP Server IP	Configures the DHCP server's IP address.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.6. Dual Homing

Dual Homing is a network topology in which a device is connected to the network by way of two independent access points (points of attachment). One access point is the primary connection, and the other is a standby connection that is activated in the event of a failure of the primary connection.

How Dual-Homing Works?

Assume the primary connection and secondary connections are connected to Internet by different way. For example, primary connection is connected to a physical network but secondary connection is connected to a wireless network. When enable dual homing feature, device will default connect to Internet by primary connection and secondary connection will be shutdown. If the port or all ports of primary connection are link-down, the device will replace primary connection by secondary connection to connect to Internet. At this situation, if secondary connection is also link-down, device will do nothing. Secondary connection only works as primary connection disconnecting.

Note: *If the channel is a single port, then the port cannot add into any trunk group.*

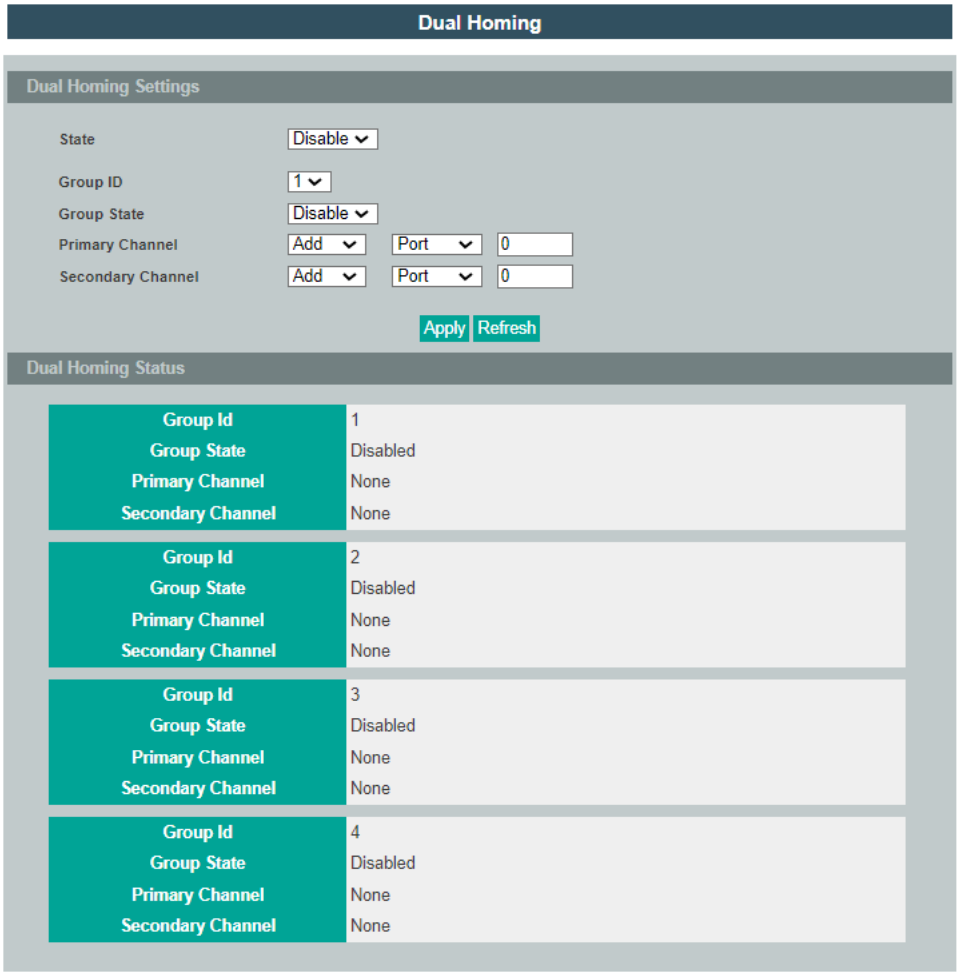
5.6.1. CLI Configuration - Dual Homing

CLI Dual Homing		
Mode	**Command**	**Description**
enable	show dual-homing	Displays the dual-homing information.
enable	configure terminal	Changes the mode to configure mode.
configure	dual-homing (disable | enable)	Disables / enables the dual-homing function for the system.
configure	dual-homing primary-channel (port | trunk) VALUE	Sets the dual-homing primary channel for the system. The channel can be a single port or a trunk group.
configure	no dual-homing primary-channel	Removes the dual-homing primary channel for the system.
configure	dual-homing secondary-channel (port | trunk) VALUE	Sets the dual-homing secondary channel for the system. The channel can be a single port or a trunk group.
configure	no dual-homing secondary-channel	Removes the dual-homing secondary channel for the system.

Example:

L2SWITCH(config)#link-aggregation 1 ports 5-6
L2SWITCH(config)#link-aggregation 1 enable
L2SWITCH(config)#dual-homing primary-channel port 2
L2SWITCH(config)#dual-homing secondary –channel trunk 1
L2SWITCH(config)#dual-homing enable

5.6.2. Web Configuration - Dual Homing



Dual Homing Settings	
Parameter	**Description**
State	Enables/ disables the Dual-Homing for the ICRL2-M.
Group ID	Selects a group which you want to configure.
Group State	Enables/ disables the Dual-Homing for a group.
Primary channel	Configures / Resets the primary channel for a group. The channel can be single port or a trunk group.
Secondary channel	Configures / Resets the secondary channel for a group. The channel can be single port or a trunk group.
Apply	Click **Apply** to change the settings.

Dual Homing Settings (Continued)	
Parameter	**Description**
Refresh	Click **Refresh** to reload the running configuration values.

5.7. Energy Efficient Ethernet (EEE)

The Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods.

EEE can be enabled on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

Note: *This feature is for Ethernet copper ports only.*

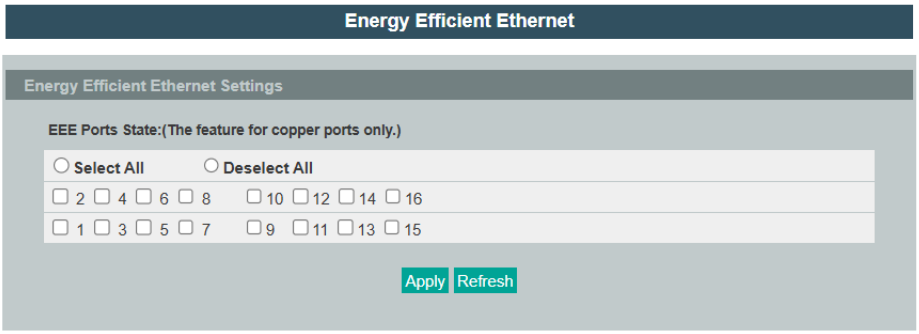
5.7.1. CLI Configuration - Energy Efficient Ethernet

CLI Energy Efficient Ethernet		
Mode	**Command**	**Description**
enable	show interface IFNAME	Displays the current port configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	eee (disable | enable)	Enables / disables the EEE function on this port.

Example:

- **L2SWITCH#configure terminal**
- **L2SWITCH(config)#interface gigabitethernet1/0/1**
- **L2SWITCH(config-if)#eee enable**
  Success!
- **L2SWITCH(config-if)#eee disable**
  Success!

5.7.2. Web Configuration - Energy Efficient Ethernet



Note: *Number of ports displayed varies depending on the ICRL2-M.*

Energy Efficient Ethernet Settings	
Parameter	**Description**
EEE Port State	Click a port to enable IEEE 802.3az Energy Efficient Ethernet on that port.
Select All	Click this to enable IEEE 802.3az Energy Efficient Ethernet across all ports.
Deselect All	Click this to disable IEEE 802.3az Energy Efficient Ethernet across all ports.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.8. ERPS

The ITU-T G.8032 Ethernet Ring Protection switching feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

The Ethernet ring protection functionality includes the following:

- Loop avoidance
- The use of learning, forwarding, and Filtering Database (FDB) mechanisms

Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL) and under normal conditions this ring link is blocked, i.e., not used for service traffic. One designated Ethernet ring node, the RPL owner node, is responsible to block traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL owner node is responsible for unblocking its end of the RPL, unless the RPL has failed, allowing the RPL to be used for traffic. The other Ethernet ring node adjacent to the RPL, the RPL neighbor node, may also participate in blocking or unblocking its end of the RPL.

The Ethernet rings could support a multi-ring/ladder network that consists of conjoined Ethernet rings by one or more interconnection points. The protection switching mechanisms and protocol defined in this Recommendation shall be applicable for a multi-ring/ladder network, if the following principles are adhered to:

- R-APS channels are not shared across Ethernet ring interconnections;
- On each ring port, each traffic channel and each R-APS channel are controlled (e.g., for blocking or flushing) by the Ethernet ring protection control process (ERP control process) of only one Ethernet ring;
- Each major ring or sub-ring must have its own RPL.

In an Ethernet ring, without congestion, with all Ethernet ring nodes in the idle state (i.e., no detected failure, no active automatic or external command and receiving only "NR, RB" R-APS messages), with less than 1200 km of ring fiber circumference and fewer than 16 Ethernet ring nodes, the ICRL2-M completion time (transfer time as defined in [ITU-T G.808.1]) for a failure on a ring link shall be less than 50ms.

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

The ICRL2-M supports up to six rings.

Guard timer -- All ERNs use a guard timer. The guard timer prevents the possibility of forming a closed loop and prevents ERNs from applying outdated R-APS messages. The guard timer activates when an ERN receives information about a local switching request, such as after a ICRL2-M fail (SF), manual ICRL2-M (MS), or forced ICRL2-M (FS). When this timer expires, the ERN begins to apply actions from the R-APS it receives. This timer cannot be manually stopped.

Wait to restore (WTR) timer -- The RPL owner uses the WTR timer. The WTR timer applies to the revertive mode to prevent frequent triggering of the protection switching due to port flapping or intermittent signal failure defects. When this timer expires, the RPL owner sends a R-APS (NR, RB) through the ring.

Wait to Block (WTB) timers -- This wait-to-block timer is activated on the RPL owner. The RPL owner uses WTB timers before initiating an RPL block and then reverting to the idle state after operator-initiated commands, such as for FS or MS conditions, are entered. Because multiple FS commands are allowed to co-exist in a ring, the WTB timer ensures that the clearing of a single FS command does not trigger the re-blocking of the RPL. The WTB timer is defined to be 5 seconds longer than the guard timer, which is enough time to allow a reporting ERN to transmit two R-APS messages and allow the ring to identify the latent condition. When clearing a MS command, the WTB timer prevents the formation of a closed loop due to the RPL owner node applying an outdated remote MS request during the recovery process.

Hold-off timer -- Each ERN uses a hold-off timer to delay reporting a port failure. When the timer expires, the ERN checks the port status. If the issue still exists, the failure is reported. If the issue does not exist, nothing is reported.

ERPS revertive and non-revertive switching

ERPS considers revertive and non-revertive operation. In revertive operation, after the condition (s) causing a ICRL2-M has cleared, the traffic channel is restored to the working transport entity, i.e. blocked on the RPL. In the case of clearing of a defect, the traffic channel reverts after the expiry of a WTR timer, which is used to avoid toggling protection states in case of intermittent defects. In non-revertive operation, the traffic channel continues to use the RPL, if it is not failed, after a ICRL2-M condition has cleared.

Control VLAN:

The pure ERPS control packets domain only, no other packets are transmitted in this VLAN to guarantee no delay for the ERPS. So when you configure a Control VLAN for a ring, the VLAN should be a new one. The ERPS will create this control VLAN and its member ports automatically. The member port should have the Left and Right ports only.

In ERPS, the control packets and data packets are separated in different VLANs. The control packets are transmitted in a VLAN which is called the Control VLAN.

Notice:

Control VLAN and Instance:

In CLI or Web configurations, there are the Control VLAN and the Instance settings.

If the Control VLAN is configured for a ring and you want to configure an instance for the ring. The control VLAN of the instance must be same as the Control VLAN; otherwise, you will get an error. If you still want to use this instance, you can change the Control VLAN to same as the control VLAN of the instance first. And then configures the instance.

Notes:

- The valid instance ID is from 1 to 30
- The maximum active instance is 6

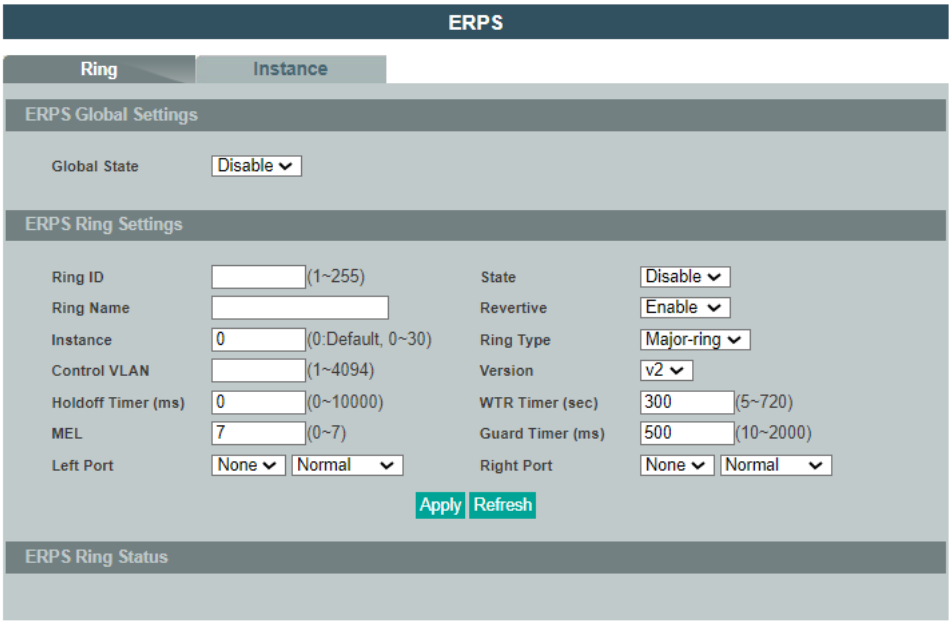
5.8.1. ERPS / Ring

5.8.1.1. CLI Configuration - ERPS Ring

CLI ERPS Ring		
Mode	**Command**	**Description**
enable	show erps	Displays the ERPS configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	erps enable	Enables the global ERPS on the ICRL2-M.
configure	no erps enable	Disables the global ERPS on the ICRL2-M.
configure	erps ring-id <1-255>	Creates an ERPS ring and its ID and enter ERPS mode.
configure	no erps ring-id <1-255>	Creates an ERPS ring and enter ERPS mode to configure detail ring configurations.
erps-ring	show	Displays the configurations of the ring.
erps-ring	control-vlan <1-4094>	Configures a control-vlan for the ERPS ring.
erps-ring	guard-timer <10-2000>	Configures the Guard Timer for the ERPS ring. (default:500ms)

CLI ERPS Ring (Continued)		
Mode	**Command**	**Description**
erps-ring	holdoff-timer <0-10000>	Configures the Hold-off Timer for the ERPS ring. (default:0 ms)
erps-ring	left-port PORTID type [owner | neighbor | normal]	Configures the left port and type for the ERPS ring.
erps-ring	mel <0-7>	Configures a Control MEL for the ERPS ring.
erps-ring	name STRING	Configures a name for the ERPS ring.
erps-ring	revertive	Configures the revertive mode for the ERPS ring.
erps-ring	no revertive	Configures then on-revertive mode for the ERPS ring.
erps-ring	right-port PORTID type [owner | neighbor | normal]	Configures the right port and type for the ERPS ring.
erps-ring	ring enable	Enables the ring.
erps-ring	no ring enable	Disables the ring.
erps-ring	version (v1 | v2)	Configures a version for the ERPS ring.
erps-ring	wtr-timer <5-720>	Configures the WTR Timer for the ERPS ring. (default: 5 minutes)

5.8.1.2. Web Configuration - ERPS Ring



8/19/25

ERPS / Ring	
Parameter	**Description**
Global State	Enables / disables the global ERPS state.
Ring ID	Configures the ring ID. The Valid value is from 1 to 255.
State	Enables/ disables the ring state.
Ring Name	Configures the ring name.(Up to 32 characters)
Revertive	Enables / disables the revertive mode.
Instance	Configures the instance for the ring. The Valid value is from 0 to 30. 0-Disable means the ERPS is running in version 1. The control VLAN of the instance should be same as below Control VLAN.
Control VLAN	Configures the Control VLAN which is the ERPS control packets domain for the ring.
Version	Configures the version for the ring.
Hold-off Timer	Configures the Hold-off time for the ring. The Valid value is from 0 to 10000 (ms).
WTR Timer	Configures the WTR time for the ring. The Valid value is from 5 to 12 (min).
MEL	Configures the Control MEL for the ring. The Valid value is from 0 to 7. The default is 7.
Guard Timer	Configures the Guard time for the ring. The Valid value is from 10 to 2000 (ms).
Left Port	Configures the left port and its type for the ring. The valid port type is one of Owner, Neighbor or Normal.
Right Port	Configures the right port and its type for the ring. The valid port type is one of Owner, Neighbor or Normal.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.8.2. ERPS / Instance

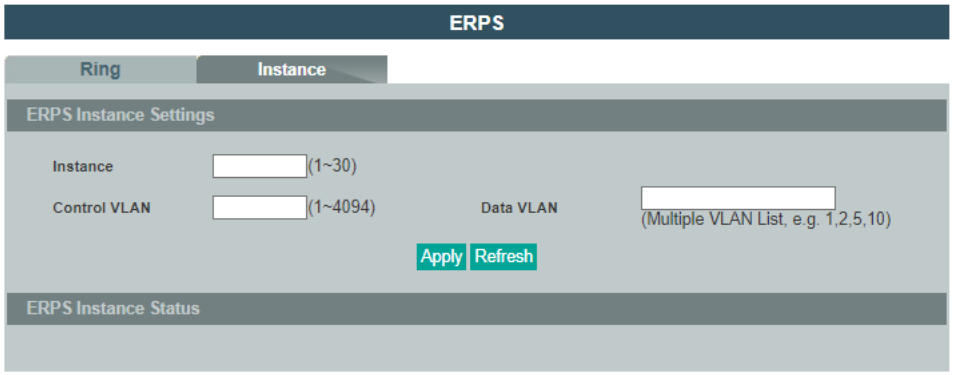
For ERPS version 2, the instance is a profile specifies a control VLAN and a data VLAN or multiple data VLANs for the ERPS. In ERPS, it can separate the control packets and data packets in different VLANs. The control packets is in the Control VLAN and the data packets can be in one or multiple data VLAN. And then user can assign an instance to an ERPS ring easily.

- In ERPS version 1, if a port is blocked by ERPS, all packets are blocked.
- In ERPS version 2, if a port is blocked by a ring of ERPS, only the packets belong to the VLANs in the instance are blocked.

5.8.2.1. CLI Configuration ERPS / Instance

CLI / ERPS / Instance		
Mode	**Command**	**Description**
enable	show erps instance	Displays all of the ERPS instance configurations.
enable	show erps instance <1-30>	Displays the specific ERPS instance configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	erps instance	Enters the instance configure mode.
config-erps-inst	instance <1-30> control-vlan <1-4094> data-vlan VLANLISTS	Configures a new instance and specifies its control VLAN and data VLAN.
config-erps-inst	no instance <1-30>	Removes an instance.
config-erps-inst	show	Displays all of the instance configurations.

5.8.2.2. Web Configuration - ERPS Instance



ERPS / Instance	
Parameter	**Description**
Instance	Configures the instance ID. The valid value is from 1 to 31.
Control VLAN	Configures the control VLAN for the instance. The valid value is from 1 to 4094.
Data VLAN	Configures the data VLAN for the instance. The valid value is from 1 to 4094. It can be one or multiple VLANs.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.9. Link Aggregation

5.9.1. Link Aggregation / Static Trunk

Link Aggregation (Trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports. The ICRL2-M supports both static and dynamic link aggregation.

Note: *In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your ICRL2-M.*

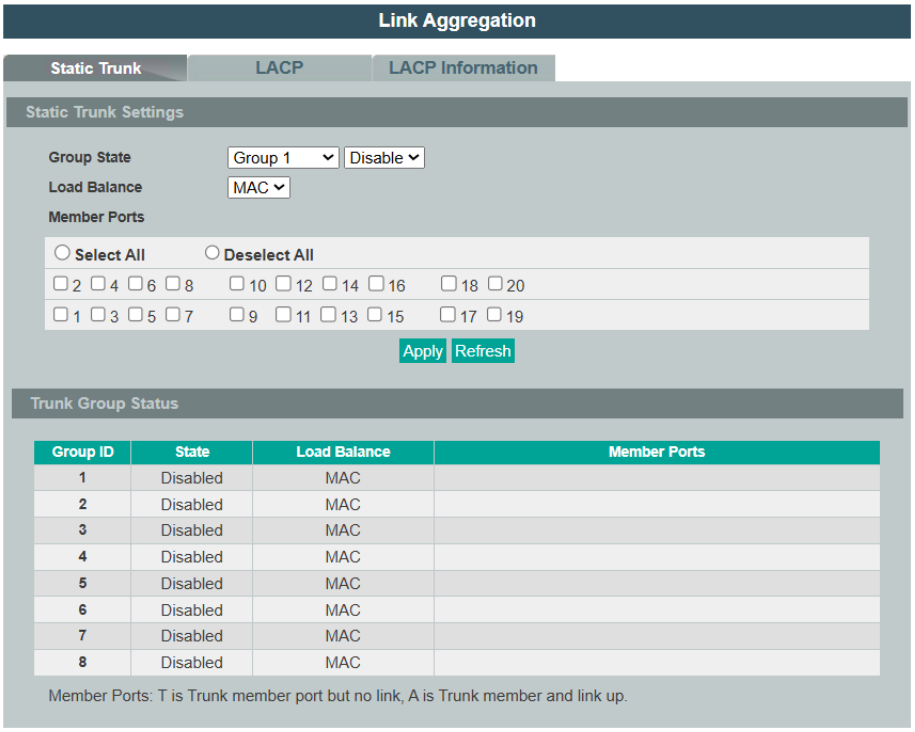
5.9.1.1. CLI Configuration - Link Aggregation / Static Trunk

CLI / Link Aggregation / Static Trunk		
Mode	**Command**	**Description**
enable	show link-aggregation	Displays the current trunk configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	link-aggregation [GROUP_ID] (disable | enable)	Disables / enables the trunk on the specific trunk group.
configure	link-aggregation [GROUP_ID] load-balance (mac | ip)	Configures the load balance algorithm for the trunk group.
configure	link-aggregation [GROUP_ID] interface PORTLISTS	Adds ports to a specific trunk group.
configure	no link-aggregation [GROUP_ID] interface PORTLISTS	Delete ports from a specific trunk group.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#link-aggregation 1 enable
L2SWITCH(config)#link-aggregation 1 ports 1-4

5.9.1.2. Web Configuration - Link Aggregation / Static Trunk



Note: *Number of ports displayed varies depending on the ICRL2-M.*

Link Aggregation / Static Trunk	
Parameter	**Description**
Group State	Select the group ID to use for this trunk group, that is, one logical link containing multiple ports. Select Enable to use this static trunk group.
Load Balance	Configures the load balance algorithm (MAC/IP) for the specific trunk group.
Member Ports	Select the ports to be added to the static trunk group.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

5.9.2. Link Aggregation / LACP

The ICRL2-M adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking. The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention.

Notes:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, and duplex mode and flow control settings.
- Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

System Priority:

The ICRL2-M with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP), the smaller the number, the higher the priority level.

System ID:

The LACP system ID is the combination of the LACP system priority value and the MAC address of the router.

Administrative Key:

The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:

- Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium.
- Configuration restrictions that you establish.

Port Priority:

The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Default Settings

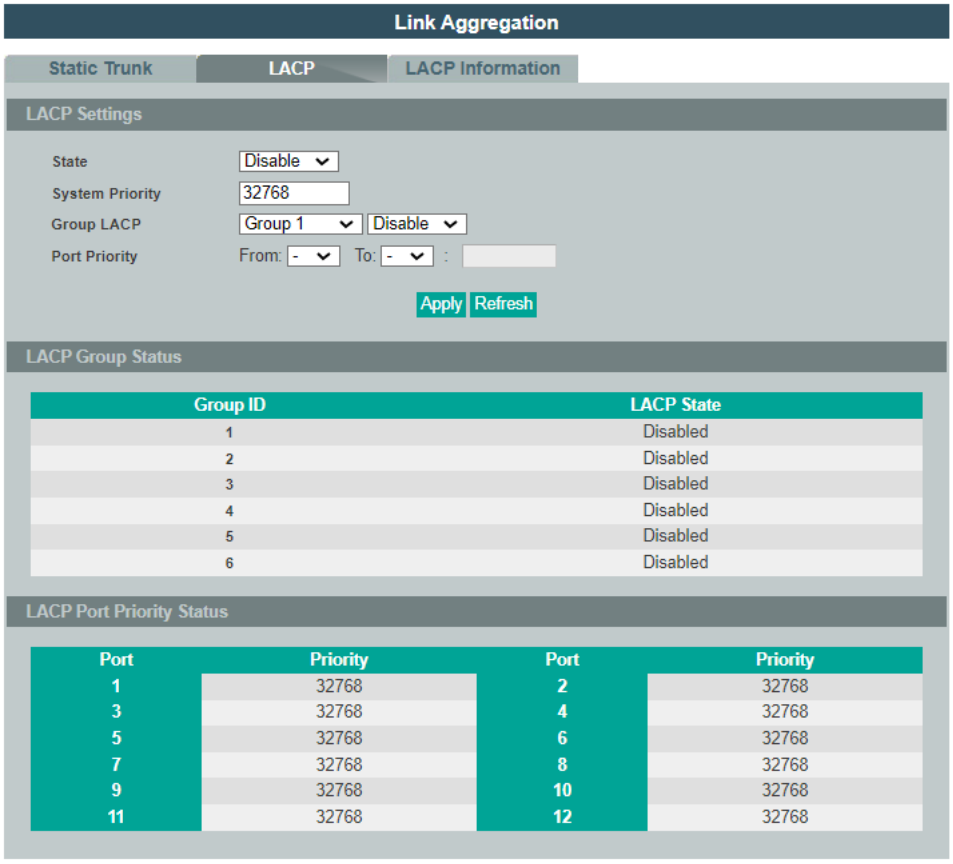
- The default System Priority is 32768.
- The default group LACP state is disabled for all groups.

5.9.2.1. CLI Configuration - Link Aggregation / LACP

CLI Link Aggregation / LACP		
Mode	**Command**	**Description**
enable	show lacp counters [GROUP_ID]	Displays the LACP counters for the specific group or all groups.
enable	show lacp port_priority	Displays the port priority for the LACP.
enable	show lacp sys_id	Displays the actor’s and partner’s system ID.

CLI Link Aggregation / LACP (Continued)		
Mode	**Command**	**Description**
enable	configure terminal	Changes the mode to configure mode.
configure	lacp (disable | enable)	Disables / enables the LACP on the ICRL2-M.
configure	lacp GROUP_ID (disable | enable)	Disables / enables the LACP on the specific trunk group.
configure	clear lacp counters [PORT_ID]	Clears the LACP statistics for the specific port or all ports.
configure	lacp system-priority <1-65535>	Configures the system priority for the LACP. Note: The default value is 32768.
configure	no lacp system-priority	Configures the default for the system priority for the LACP.
configure	interface IFNAME	Enters the interface configure mode.
interface	lacp port_priority <1-65535>	Configures the priority for the specific port. ***Note:*** *The default value is 32768.*
interface	no lacp port_priority	Configures the default for the priority for the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	lacp port_priority <1-65535>	Configures the priority for the specific ports. ***Note:*** *The default value is 32768.*
if-range	no lacp port_priority	Configures the default for the priority for the specific ports.

5.9.2.2. Web Configuration - Link Aggregation / LACP



Link Aggregation / LACP	
Parameter	**Description**
State	Select **Enable** from the drop down box to enable Link Aggregation Control Protocol (LACP). Select **Disable** to not use LACP.
System Priority	LACP system priority is a number between 1 and 65,535. The ICRL2-M with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group LACP	Select a trunk group ID and then select whether to Enable or Disable Group Link Aggregation Control Protocol for that trunk group.
Port Priority	Select a port or a range of ports to configure its (their) LACP priority.
Apply	Click **Apply** to change the settings.

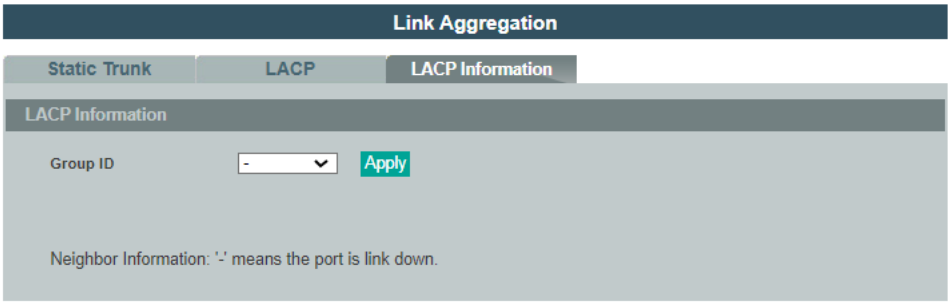
Link Aggregation / LACP (Continued)	
Parameter	**Description**
Refresh	Click **Refresh** to reload the running configuration values.

5.9.3. Link Aggregation / LACP Information

5.9.3.1. CLI Configuration - Link Aggregation / LACP Information

CLI Link Aggregation / LACP Information		
Mode	**Command**	**Description**
enable	show lacp internal [GROUP_ID]	Displays the LACP internal information for the specific group or all groups.
enable	show lacp neighbor [GROUP_ID]	Displays the LACP neighbor's information for the specific group or all groups.

5.9.3.2. Web Configuration - Link Aggregation / LACP Information



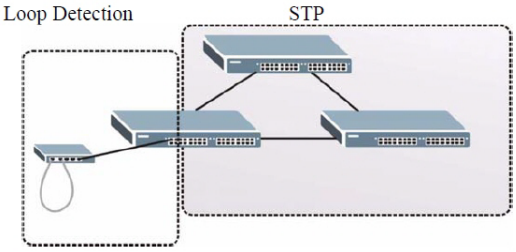
Link Aggregation / LACP Information	
Parameter	**Description**
LACP Information	
Group ID	Select a LACP group that you want to view.
Apply	Click **Apply** to change the settings.
Neighbors Information	
Port	The LACP member port ID.
System Priority	LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)
System ID	The neighbor ICRL2-M's system ID.
Port	The direct connected port Id of the neighbor ICRL2-M.
Age	The available time period of the neighbor ICRL2-M LACP information.

Link Aggregation / LACP Information (Continued)	
Parameter	**Description**
Port State	The direct connected port's state of the neighbor ICRL2-M.
Port Priority	The direct connected port's priority of the neighbor ICRL2-M.
Oper Key	The Oper key of the neighbor ICRL2-M.
Internal Information	
Port	The LACP member port ID.
Port Priority	The port priority of the LACP member port.
Admin Key	The Admin key of the LACP member port.
Oper Key	The Oper key of the LACP member port.
Port State	The port state of the LACP member port.

5.10. Loop Detection

Loop detection is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a ICRL2-M that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a ICRL2-M are connected with the same cable. When a ICRL2-M in loop state sends out broadcast messages the messages loop back to the ICRL2-M and are re-broadcast again and again causing a broadcast storm.

The difference between the Loop Detection and STP:



The loop detection function sends probe packets periodically to detect the loop in the network by checking the port loop state. The ICRL2-M shuts down that particular port if it detects the probe packets spiral back to the same port of ICRL2-M.

Furthermore, the ICRL2-M generates Syslog, internal log messages, SNMP traps, and turns on the Alarm (ALM) LED when it shuts down the port via the loop detection feature.

Loop Recovery:

When the loop detection is enabled, the ICRL2-M will send one probe packet every two seconds periodically and listen to this packet. If it receives the same packet at the same port, the ICRL2-M will disable it. After a period (recovery time) the ICRL2-M will enable this port and continue to perform the loop detection again.

5.10.1.CLI Configuration - Loop Detection

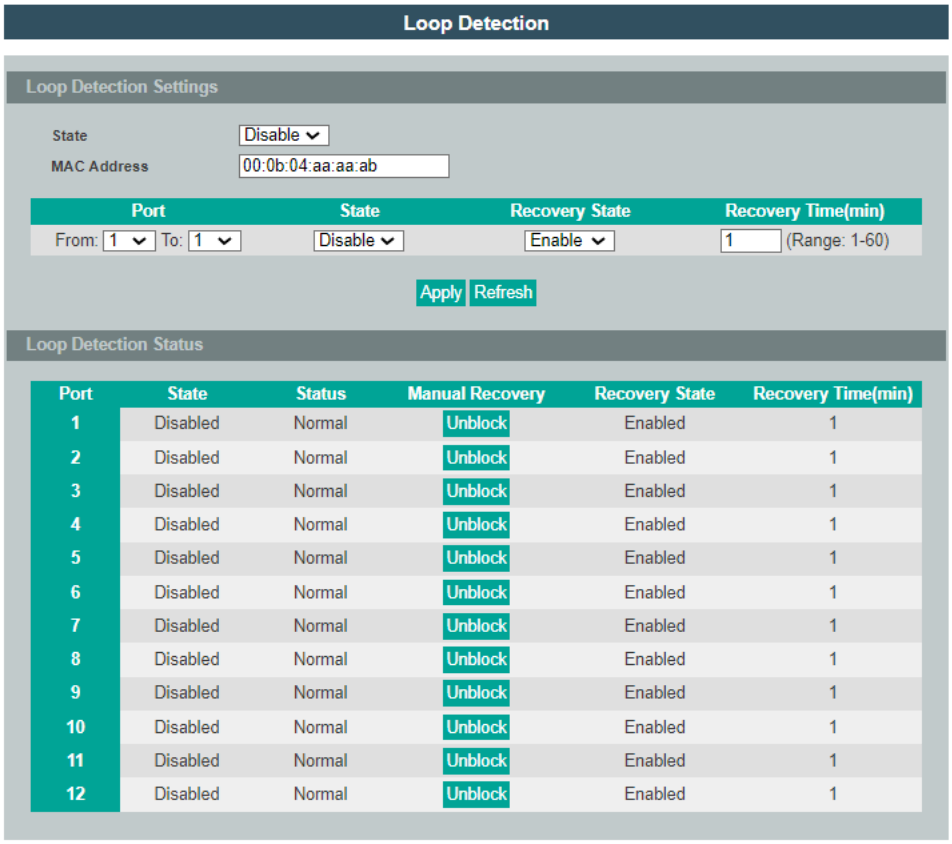
CLI Loop Detection		
Mode	**Command**	**Description**
enable	show loop-detection	Displays the current loop detection configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	loop-detection (disable | enable)	Disables / enables the loop detection on the ICRL2-M.
configure	loop-detection address MACADDR	Configures the destination MAC for the loop detection special packets.
configure	no loop-detection address	Configures the destination MAC to default (00:0b:04:AA:AA:AB).
configure	interface IFNAME	Enters the interface configure mode.
interface	loop-detection (disable | enable)	Disables / enables the loop detection on the port.
interface	no shutdown	Enables the port. It can unblock port blocked by loop detection.

CLI Loop Detection (Continued)		
Mode	**Command**	**Description**
interface	loop-detection recovery (disable | enable)	Enables / disables the recovery function on the port.
interface	loop-detection recovery time <1-60>	Configures the recovery period time.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	loop-detection (disable | enable)	Disables / enables the loop detection on the ports.
if-range	loop-detection recovery (disable | enable)	Enables / disables the recovery function on the port.
if-range	loop-detection recovery time <1-60>	Configures the recovery period time.

Example:

L2SWITCH(config)#loop-detection enable
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#loop-detection enable

5.10.2.Web Configuration - Loop Detection



Loop Detection	
Parameter	**Description**
Loop Detection Settings	
State	Select this option to enable loop guard on the ICRL2-M.
MAC Address	Enter the destination MAC address the probe packets will be sent to. If the port receives these same packets the port will be shut down.
Port	Select a port on which to configure loop guard protection.
State	Select **Enable** to use the loop guard feature on the ICRL2-M.
Recovery State	Select **Enable** to reactivate the port automatically after the designated recovery time has passed.
Recovery Time	Specify the recovery time in minutes that the ICRL2-M waits before reactivating the port. This can be between 1 to 60 minutes.
Apply	Click **Apply** to change the settings.

Loop Detection (Continued)	
Parameter	**Description**
Refresh	Click **Refresh** to reload the running configuration values.
Loop Detection Status	
Port	Displays a port number.
State	Displays if the loop guard feature is enabled.
Status	Displays if the port is blocked.
Manual Recovery	Click **Unblock** to reactivate the port manually.
Recovery State	Displays if the loop recovery feature is enabled.
Recovery Time (min)	Displays the recovery time for the loop recovery feature.

5.11. Modbus TCP

Modbus TCP supports different types of data format for reading. The primary four types are:

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

Modbus Data Map and Information Interpretation of the ICRL2-M Series

The Modbus base address of ICRL2-M switches is 1001(decimal) for Function Code 4.

Modbus Data Map and Information Interpretation of the ICRL2-M Series			
Address Offset	**Data Type**	**Interpretation**	**Description**
System Information			
0x0000	1 word	HEX	Vendor ID = 0x0b04
0x0001	16 words	ASCII	Vendor Name = Pepperl+Fuchs Word 0 Hi byte = 'V' Word 0 Lo byte = 'o' Word 1 Hi byte = 'l' Word 1 Lo byte = 'k' Word 2 Hi byte = 't' Word 2 Lo byte = 'e' Word 3 Hi byte = 'k' Word 3 Lo byte = '' Word 4 Hi byte = 'C' Word 4 Lo byte = 'o' Word 5 Hi byte = 'r' Word 5 Lo byte = 'p' Word 6 Hi byte = '.' Word 6 Lo byte = '\0'

Modbus Data Map and Information Interpretation of the ICRL2-M Series (Continued)			
Address Offset	**Data Type**	**Interpretation**	**Description**
0x0020	16 words	ASCII	Product Name = ICRL2-M-16RJ45/4SFP-10G-DIN Word 0 Hi byte = 'I' Word 0 Lo byte = 'E' Word 1 Hi byte = 'N' Word 1 Lo byte = '-' Word 2 Hi byte = '8' Word 2 Lo byte = '6' Word 3 Hi byte = '4' Word 3 Lo byte = '8' Word 4 Hi byte = 'A' Word 5 Lo byte = '\0'
0x0040	7 words		Product Serial Number Example: Serial No=2249-000001
0x0050	12 words	ASCII	Firmware Version=V1.0.1.S0 Word 0 Hi byte = '8' Word 0 Lo byte = '6' Word 1 Hi byte = '4' Word 1 Lo byte = '8' Word 2 Hi byte = '-' Word 2 Lo byte = '0' Word 3 Hi byte = '0' Word 3 Lo byte = '0' Word 4 Hi byte = '-' Word 4 Lo byte = '1' Word 5 Hi byte = '.' Word 5 Lo byte = '4' Word 6 Hi byte = '.' Word 6 Lo byte = '1' Word 7 Hi byte = '.' Word 7 Lo byte = 'S' Word 8 Hi byte = '0' Word 8 Lo byte = '\0'
0x0060	16 words	ASCII	Firmware Release Date= See System Information

Modbus Data Map and Information Interpretation of the ICRL2-M Series (Continued)			
Address Offset	**Data Type**	**Interpretation**	**Description**
0x0070	3 words	HEX	Ethernet MAC Address Example: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 04 Word 2 Lo byte = 0 x 05
0x0080	1 word	HEX	Power 1(PWR) Alarm, DIP switch 1 need ON 0x0000: no alarm 0x0001: input voltage <44V 0x0002: input voltage > 57V 0x0003: No PWR input
0x0081	1 word	HEX	Power 2(RPS) Alarm, DIP switch 1 need ON 0x0000: no alarm 0x0001: input voltage <44V 0x0002: input voltage > 57V 0x0003: No RPS input
0x0090	1 word	HEX	Fault LED Status 0x0000: No 0x0001: Yes Port Information

Modbus Data Map and Information Interpretation of the ICRL2-M Series (Continued)			
Address Offset	**Data Type**	**Interpretation**	**Description**
Port Information			
0x0100 to 0x0109	1 word	HEX	Port 1 to 10 Link Status 0x0000: Link down 0x0001: 10M-Full-FC_ON (FC: Flow Control) 0x0002: 10M-Full-FC_OFF 0x0003: 10M-Half-FC_ON 0x0004: 10M-Half-FC_OFF 0x0005: 100M-Full-FC_ON 0x0006: 100M-Full-FC_OFF 0x0007: 100M-Half-FC_ON 0x0008: 100M-Half-FC_OFF 0x0009: 1000M-Full-FC_ON 0x000A: 1000M-Full-FC_OFF 0x000B: 1000M-Half-FC_ON 0x000C: 1000M-Half-FC_OFF 0xFFFF: No port
0x0200 to 0x0213 (port 1) 0x0220 to 0x0233 (port 2) … 0x0320 to 0x0333 (port 6)	20 words	ASCII	Port 1 to 6 Description Port Description = “100TX,RJ45.” Or “1000TX,SFP.” Word 0 Hi byte = ‘1’ Word 0 Lo byte = ‘0’ Word 1 Hi byte = ‘0’ Word 1 Lo byte = ‘T’ … Word 4 Hi byte = ‘4’ Word 4 Lo byte = ‘5’ Word 5 Hi byte = ‘.’ Word 5 Lo byte = ‘\0’
0x0400 to 0x0413 (port 1 to 6)	2 words	HEX	Port 1 to 6 Tx Packets Example: port 1 Tx Packet Amount = 0x87654321 Word 0 =8765 Word 1 = 4321
0x0440 to 0x0453 (port 1 to 6)	2 words	HEX	Port 1 to 6 Rx Packets Example: port 1 Rx Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456

Modbus Data Map and Information Interpretation of the ICRL2-M Series (Continued)			
Address Offset	**Data Type**	**Interpretation**	**Description**
0x0480 to 0x0493 (port 1 to 6)	2 words	HEX	Port 1 to 6 Tx Error Packets Example: port 1 Tx Error Packet Amount = 0x87654321 Word 0 =8765 Word 1 = 4321
0x04C0 to 0x04D3 (port 1 to 6)	2 words	HEX	Port 1 to 6 Rx Error Packets Example: port 1 Rx Error Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456 STP Information
STP Information			
0x0500	1 word	HEX	STP Status: 0x0000 : STP is disabled. 0x0001 : STP 0x0002 : RSTP 0x0003 : MSTP
Xpress Ring Information			
0x0501	1 word	HEX	Xpress Ring Status on the ICRL2-M: 0x0000 : Disabled. 0x0001 : Enabled
0x0510	1 word	HEX	Status of Xpress-ring1 of the ICRL2-M 0x0000 : Disabled 0x0001 : Enabled
0x0511	1 word	HEX	Status of Xpress-ring2 of the ICRL2-M 0x0000 : Disabled 0x0001 : Enabled
0x0512	3 word	HEX	Destination MAC of the Xpress-ring1 Word 0 Lo byte = MAC0 Word 0 Hi byte = MAC1 Word 1Lo byte = MAC2 Word 1 Hi byte = MAC3 Word 2Lo byte = MAC4 Word 2 Hi byte = MAC5

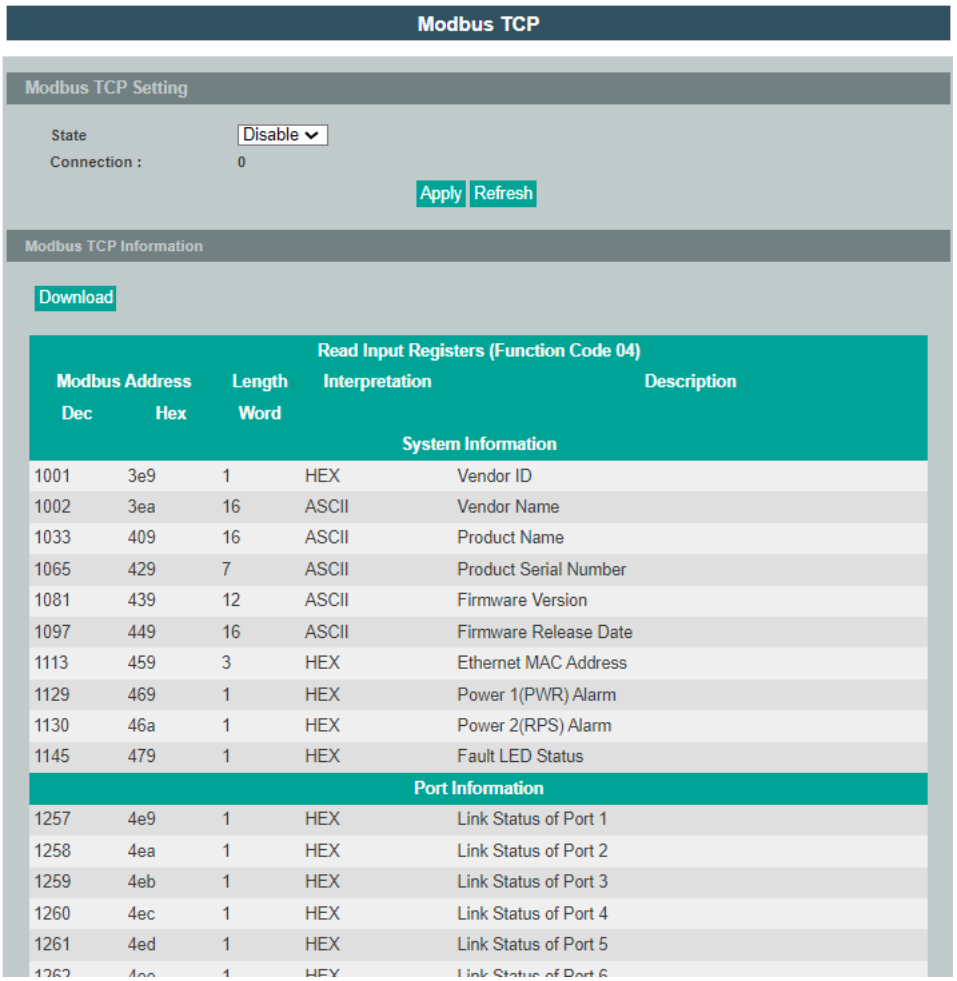
Modbus Data Map and Information Interpretation of the ICRL2-M Series (Continued)			
Address Offset	**Data Type**	**Interpretation**	**Description**
0x0515	3 word	HEX	Destination MAC of the Xpress-ring2 Word 0 Lo byte = MAC0 Word 0 Hi byte = MAC1 Word 1Lo byte = MAC2 Word 1 Hi byte = MAC3 Word 2Lo byte = MAC4 Word 2 Hi byte = MAC5
0x0518	1 word	HEX	Primary Port of the Xpress-ring1 Word 0 Hi byte = Port ID.
0x0519	1 word	HEX	Secondary Port of the Xpress-ring1 Word 0 Hi byte = Port ID.
0x051a	1 word	HEX	Primary Port of the Xpress-ring2 Word 0 Hi byte = Port ID.
0x051b	1 word	HEX	Secondary Port of the Xpress-ring2 Word 0 Hi byte = Port ID.
0x051c	1 word	HEX	Role of Xpress-ring1 0x0000 : Forwarder 0x0001 : Arbiter
0x051d	1 word	HEX	Role of Xpress-ring2 0x0000 : Forwarder 0x0001 : Arbiter
0x051e	1 word	HEX	Primary Port Status of Xpress-ring1 0x0000 : link down 0x0001 : forwarding 0x0002 : blocking
0x051f	1 word	HEX	Secondary Port Status of Xpress-ring1 0x0000 : link down 0x0001 : forwarding 0x0002 : blocking
0x0520	1 word	HEX	Primary Port Status of Xpress-ring2 0x0000 : link down 0x0001 : forwarding 0x0002 : blocking

Modbus Data Map and Information Interpretation of the ICRL2-M Series (Continued)			
Address Offset	**Data Type**	**Interpretation**	**Description**
0x0521	1 word	HEX	Secondary Port Status of Xpress-ring2 0x0000 : link down 0x0001 : forwarding 0x0002 : blocking

5.11.1.CLI Configuration - Modbus TCP

CLI Modbus TCP		
Mode	**Command**	**Description**
enable	show modbus-tcp state	Displays the current Modbus TCP configurations.
enable	show modbus-tcp register-addr range NUMRANGE	Displays the range of the Modbus TCP registrations.
enable	configure terminal	Changes the mode to configure mode.
configure	modbus-tcp (disable | enable)	Disables / enables the Modbus TCP on the ICRL2-M.

5.11.2.Web Configuration - Modbus TCP



Modbus TCP	
Parameter	**Description**
Modbus TCP Settings	
State	Select this option to enable / disable the Modbus on the ICRL2-M.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Modbus TCP Information	
Download	Click the Download button to download all of the registers information to load host.

5.12. Spanning Tree Protocols (STP/RSTP)

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a ICRL2-M to interact with other (R)STP compliant switches in your network to ensure that only one path exists between any two stations on the network.

The ICRL2-M supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

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

The ICRL2-M uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database.

In STP, the port states are Blocking, Listening, Learning, Forwarding.

In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: *In this document, "STP" refers to both STP and RSTP.*

STP Terminology

- The root bridge is the base of the spanning tree.
- Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

	Link Speed	Recommended Value	Recommended Range	Allowed Range
Path Cost	4 Mbps	250	100 to 1000	1 to 65535
	10 Mbps	100	50 to 600	
	16 Mbps	62	40 to 400	
	100 Mbps	19	10 to 60	
	1 Gbps	4	3 to 10	
	10 Gbps	2	1 to 5	

- On each bridge, the bridge communicates with the root through the root port. The root port is the port on this ICRL2-M with the lowest path cost to the root (the root-path cost). If there is no root port, then this ICRL2-M has been accepted as the root-bridge of the spanning tree network.
- For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

Forward Time (Forward Delay):

This is the maximum time (in seconds) the ICRL2-M will wait before changing states. This delay is required because every ICRL2-M must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30seconds.

Max Age:

This is the maximum time (in seconds) the ICRL2-M can wait without receiving a BPDU before attempting to reconfigure. All ICRL2-M ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, anew root port is selected from among the ICRL2-M ports attached to the network. The allowed range is 6 to 40 seconds.

Hello Time:

This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root ICRL2-M. The allowed range is 1 to 10 seconds.

Path Cost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge, the slower the media, the higher the cost.

How STP Works?

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

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed. Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

802.1D STP

The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. It is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation. In the OSI model for computer networking, STP falls under the OSI layer-2. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

The Spanning Tree Protocol (STP) is defined in the IEEEStandard802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the tree, leaving a single active path between any two network nodes.

STP switch port states

- Blocking - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.
- Listening - The ICRL2-M processes BPDUs and awaits possible new information that would cause it to return to the blocking state.
- Learning - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)
- Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

802.1w RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

RSTP bridge port roles:

- Root - A forwarding port that is the best port from Non-root-bridge to Root-bridge
- Designated - A forwarding port for every LAN segment

- Alternate - An alternate path to the root bridge. This path is different than using the root port.
- Backup - A backup/redundant path to a segment where another bridge port already connects.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

Edge Port:

They are attached to a LAN that has no other bridges attached. These edge ports transition directly to the forwarding state. RSTP still continues to monitor the port for BPDUs in case a bridge is connected. RSTP can also be configured to automatically detect edge ports. As soon as the bridge detects a BPDU coming to an edge port, the port becomes a non-edge port.

Forward Delay:

The range is from 4 to 30 seconds. This is the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).

Transmission Limit:

This is used to configure the minimum interval between the transmissions of consecutive RSTP BPDUs. This function can only be enabled in RSTP mode. The range is from 1 to 10 seconds.

Hello Time:

Set the time at which the root ICRL2-M transmits a configuration message. The range is from 1 to 10 seconds.

Bridge priority:

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will become the root device.

Port Priority:

Set the port priority in the ICRL2-M. Low numeric value indicates a high priority. A port with lower priority is more likely to be blocked by STP if a network loop is detected. The valid value is from 0 to 240.

Path Cost:

The valid value is from 1 to 200000000. Higher cost paths are more likely to be blocked by STP if a network loop is detected.

BPDU Guard

This is a per port setting. If the port is enabled in BPDU guard and receive any BPDU, the port will be set to disable to avoid the error environments. User must enable the port by manual.

BPDU Filter

It is a feature to filter sending or receiving BPDUs on a ICRL2-M port. If the port receives any BPDUs, the BPDUs will be dropped.

Note: *If both of the BPDU filter and BPDU guard are enabled, the BPDU filter has the high priority.*

Root Guard

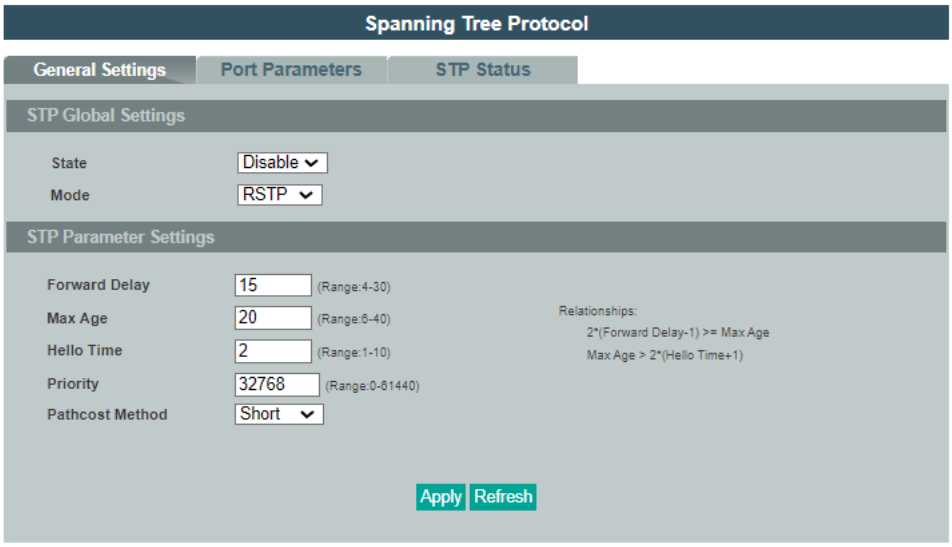
The Root Guard feature forces an interface to become a designated port to prevent surrounding switches from becoming a root ICRL2-M. In other words, Root Guard provides a way to enforce the root bridge placement in the network. The Root Guard feature prevents a Designated Port from becoming a Root Port. If a port on which the Root Guard feature receives a superior BPDU, it moves the port into a root-inconsistent state (effectively equal to a listening state), thus maintaining the current Root Bridge status. The port can be moved to forwarding state if no superior BPDU received by this port for three hello times.

5.12.1.Spanning Tree Protocol General Settings

5.12.1.1. CLI Configuration - Spanning Tree Protocol / General Settings

CLI / Spanning Tree Protocol / General Settings		
Mode	**Command**	**Description**
enable	show spanning-tree active	Displays the spanning tree information for only active port(s)
enable	show spanning-tree blocked ports	Displays the spanning tree information for only blocked port(s)
enable	show spanning-tree summary	Displays the summary of port states and configurations
enable	clear spanning-tree counters	Clears spanning-tree statistics for all ports.
enable	clear spanning-tree counters PORT_ID	Clears spanning-tree statistics for a specific port.
enable	configure terminal	Changes the mode to configure mode.
configure	spanning-tree (disable | enable)	Disables / enables the spanning tree function for the system.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	Configures the bridge times(forward-delay, max-age, hello-time).
configure	no spanning-tree algorithm-timer	Configures the default values for forward-time &max-age &hello-time.
configure	spanning-tree forward-time <4-30>	Configures the bridge forward delay time (sec).
configure	no spanning-tree forward-time	Configures the default values for forward-time.
configure	spanning-tree hello-time <1-10>	Configures the bridge hello time (sec).
configure	no spanning-tree hello-time	Configures the default values for hello-time.
configure	spanning-tree max-age <6-40>	Configures the bridge message max-age time (sec).
configure	no spanning-tree max-age	Configures the default values for max-age time.
configure	spanning-tree mode (rstp | stp | mst)	Configures the spanning mode.
configure	spanning-tree path-cost method (short | long)	Configures the path-cost method.
configure	spanning-tree priority <0-61440>	Configures the priority for the system.
configure	no spanning-tree priority	Configures the default values for the system priority.

5.12.1.2. Web Configuration - Spanning Tree Protocol / General Settings



Spanning Tree Protocol / General Settings	
Parameter	**Description**
State	Select **Enable** to use Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP).
Mode	Select to use either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP).
Forward Time	This is the maximum time (in seconds) the ICRL2-M will wait before changing states. This delay is required because every ICRL2-M must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30seconds.
Max Age	This is the maximum time (in seconds) the ICRL2-M can wait without receiving a BPDU before attempting to reconfigure. All ICRL2-M ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, anew root port is selected from among the ICRL2-M ports attached to the network. The allowed range is 6 to 40 seconds.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root ICRL2-M. The allowed range is 1 to 10 seconds.

Spanning Tree Protocol / General Settings (Continued)	
Parameter	**Description**
Priority	Priority is used in determining the root ICRL2-M, root port and designated port. The ICRL2-M with the highest priority (lowest numeric value) becomes the STP root ICRL2-M. If all switches have the same priority, the ICRL2-M with the lowest MAC address will then become the root ICRL2-M. Enter a value from 0~61440. The lower the numeric value you assign, the higher the priority for this bridge. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.
Path cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

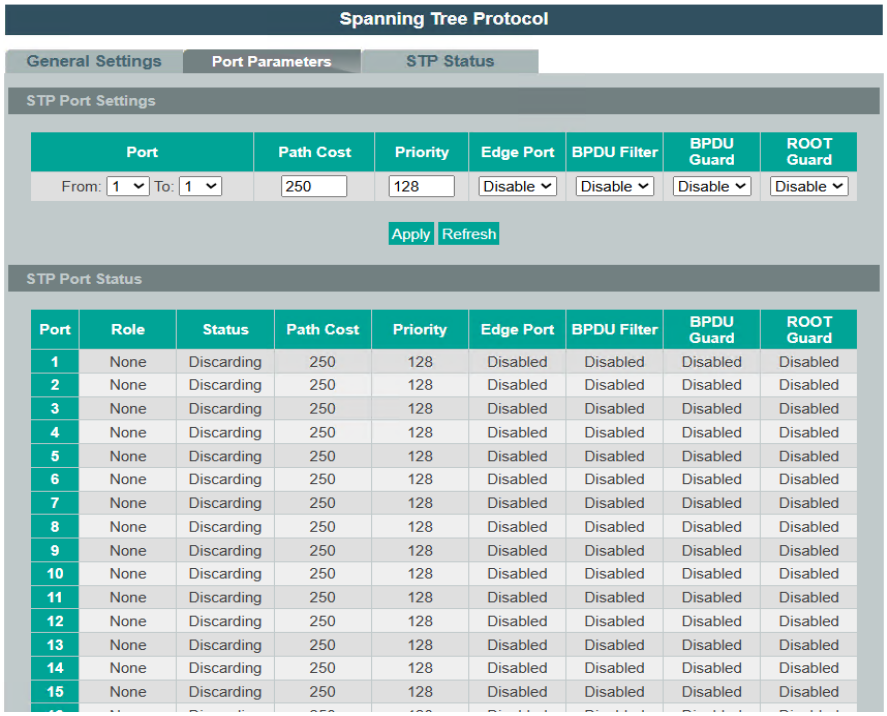
5.12.2.Spanning Tree Protocol / Port Parameters

5.12.2.1. CLI Configuration - Spanning Tree Protocol / Port Parameters

CLI / Spanning Tree Protocol / Port Parameters		
Mode	**Command**	**Description**
enable	show spanning-tree blocked ports	Displays the spanning tree information for only blocked port(s)
enable	show spanning-tree port detail PORT_ID	Displays the spanning tree information for the interface port.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	spanning-tree (disable | enable)	Configures enables/disables the STP function for the specific port.
interface	spanning-tree bpdufilter (disable | enable)	Configures enables/disables the BPDU filter function for the specific port.
interface	spanning-tree bpduguard (disable | enable)	Configures enables/disables the BPDU guard function for the specific port.
interface	spanning-tree rootguard (disable | enable)	Enables/disables the BPDU Root guard port setting for the specific port.
interface	spanning-tree edge-port (disable | enable)	Enables/disables the edge port setting for the specific port.

CLI / Spanning Tree Protocol / Port Parameters (Continued)		
Mode	**Command**	**Description**
interface	spanning-tree cost VALUE	Configures the cost for the specific port. Cost range: • 16-bit based value range 1-65535, • 32-bit based value range 1-200000000.
interface	no spanning-tree cost	Configures the path cost to default for the specific port.
interface	spanning-tree port-priority <0-240>	Configures the port priority for the specific port. Default: 128.
interface	no spanning-tree port-priority	Configures the port priority to default for the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	spanning-tree(disable | enable)	Configures enables/disables the STP function for the specific port.
if-range	spanning-tree bpdufilter (disable | enable)	Configures enables/disables the BPDU filter function for the specific port.
if-range	spanning-tree bpduguard (disable | enable)	Configures enables/disables the BPDU guard function for the specific port.
if-range	spanning-tree rootguard (disable | enable)	Enables/disables the BPDU Root guard port setting for the specific port.
if-range	spanning-tree edge-port (disable | enable)	Enables/disables the edge port setting for the specific port.
if-range	spanning-tree cost VALUE	Configures the cost for the specific port. Cost range: • 16-bit based value range 1-65535, • 32-bit based value range 1-200000000.
if-range	no spanning-tree cost	Configures the path cost to default for the specific port.
if-range	spanning-tree port-priority <0-240>	Configures the port priority for the specific port. Default: 128.
if-range	no spanning-tree port-priority	Configures the port priority to default for the specific port.

5.12.2.2. Web Configuration - Spanning Tree Protocol / Port Parameters



Spanning Tree Protocol / Port Parameters	
Parameter	**Description**
STP Port Settings	
Port	Selects a port that you want to configure.
Path Cost	Configures the path cost for the specific port.
Priority	Configures the priority for the specific port.
Edge Port	Configures the port type for the specific port. Edge or Non-Edge.
BPDU Filter	Enables/Disables the BPDU filter function for the specific port.
BPDU Guard	Enables/Disables the BPDU guard function for the specific port.
ROOT Guard	Enables/Disables the BPDU root guard function for the specific port.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
STP Port Status	
Role	The port role. Should be one of the Alternated / Designated / Root / Backup / None.

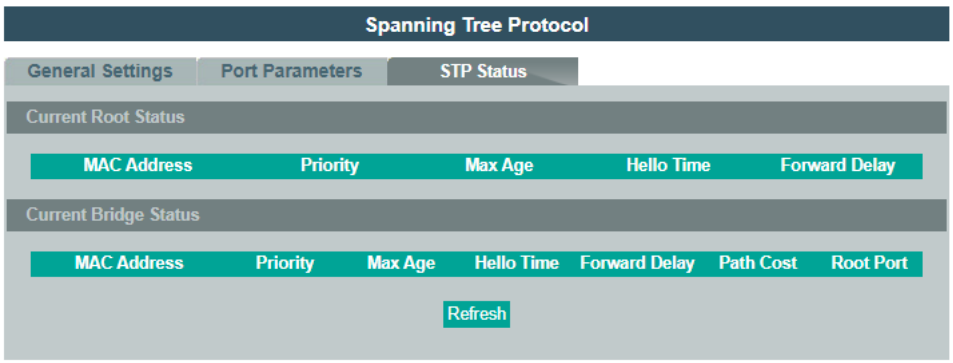
Spanning Tree Protocol / Port Parameters (Continued)	
Parameter	**Description**
Status	The port's status. Should be one of the Discarding / Blocking / Listening / Learning / Forwarding / Disabled.
Path Cost	The port's path cost.
Priority	The port's priority.
Edge Port	The state of the edge function.
BPDU Filter	The state of the BPDU filter function.
BPDU Guard	The state of the BPDU guard function.
ROOT Guard	The state of the BPDU Root guard function.

5.12.3.Spanning Tree Protocol / STP Status

5.12.3.1. CLI Configuration - Spanning Tree Protocol / STP Status

CLI / Spanning Tree Protocol / STP Status		
Mode	**Command**	**Description**
enable	show-spanning-tree active	This command displays the spanning tree information and active port information.

5.12.3.2. Web Configuration - Spanning Tree Protocol / STP Status



Spanning Tree Protocol / STP Status	
Parameter	**Description**
Current Root Status	
MAC address	This is the MAC address of the root bridge.
Priority	Root refers to the base of the spanning tree (the root bridge). Displays the root bridge's priority. This ICRL2-M may also be the root bridge.
MAX Age	Maximum time (in seconds) the ICRL2-M can wait without receiving a configuration message before attempting to reconfigure.
Hello Time	Time interval (in seconds) at which the root ICRL2-M transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Forward Delay	Time (in seconds) the root ICRL2-M will wait before changing states.
Refresh	Click **Refresh** to reload the running configuration values.
Current Bridge Status	
MAC address	This is the MAC address of the current bridge.
Priority	Priority is used in determining the root ICRL2-M, root port and designated port. The ICRL2-M with the highest priority (lowest numeric value) becomes the STP root ICRL2-M. If all switches have the same priority, the ICRL2-M with the lowest MAC address will then become the root ICRL2-M. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.
MAX Age	Maximum time (in seconds) the ICRL2-M can wait without receiving a BPDU before attempting to reconfigure. All ICRL2-M ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the ICRL2-M ports attached to the network.
Hello Time	Time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root ICRL2-M.
Forward Delay	Maximum time (in seconds) the ICRL2-M will wait before changing states. This delay is required because every ICRL2-M must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.
Root Cost	Number of the port on the ICRL2-M through which this ICRL2-M must communicate with the root of the Spanning Tree.

6. Security

6.1. IP Source Guard

IP Source Guard is a security feature that restricts IP traffic on un-trusted Layer 2 ports 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. Any IP traffic coming into the interface with a source IP address other than that assigned (via DHCP or static configuration) will be filtered out on the un-trusted Layer 2 ports.

The IP Source Guard feature is enabled in combination with the DHCP snooping feature on un-trusted Layer 2 interfaces. It builds and maintains an IP source binding table that is learned by DHCP snooping or manually configured (static IP source bindings). An entry in the IP source binding table contains the IP address and the associated MAC and VLAN numbers. The IP Source Guard is supported on Layer 2 ports only, including access and trunk ports.

The IP Source Guard features include below functions:

1. DHCP Snooping.
2. DHCP Binding table.
3. ARP Inspection.
4. Blacklist Filter. (arp-inspection mac-filter table)

6.1.1. DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering un-trusted DHCP messages and by building and maintaining a DHCP snooping binding database, which is also referred to as a DHCP snooping binding table.

DHCP snooping acts like a firewall between un-trusted hosts and DHCP servers. You can use DHCP snooping to differentiate between un-trusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

The DHCP snooping binding database contains the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local un-trusted interfaces of a switch.

When a ICRL2-M receives a packet on an un-trusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the ICRL2-M compares the source MAC address and the DHCP client hardware address. If addresses match (the default), the ICRL2-M forwards the packet. If the addresses do not match, the ICRL2-M drops the packet.

The ICRL2-M drops a DHCP packet when one of these situations occurs:

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

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

Trusted vs. Un-trusted Ports

Every port is either a trusted port or an un-trusted port for DHCP snooping. This setting is independent of the trusted/un-trusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or un-trusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The ICRL2-M discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The ICRL2-M learns dynamic bindings from trusted ports.

Note: *The ICRL2-M drops all DHCP requests if you enable DHCP snooping and there are no trusted ports.*

Un-trusted ports are connected to subscribers. The ICRL2-M discards DHCP packets from un-trusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

DHCP Snooping Database

The ICRL2-M stores the binding table in volatile memory. If the ICRL2-M restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again.

Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the ICRL2-M.

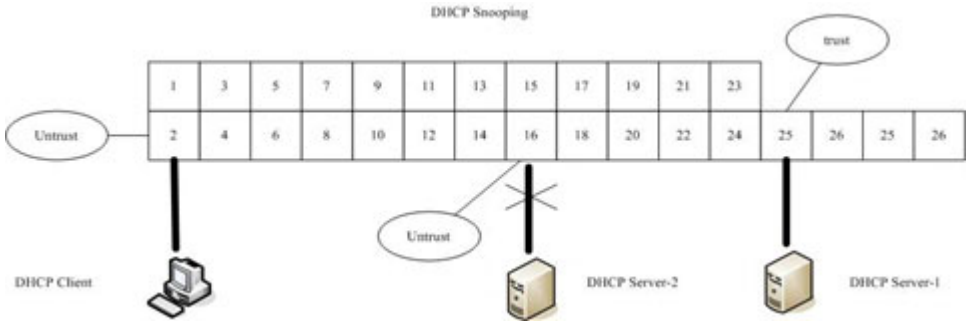
1. Enable DHCP snooping on the ICRL2-M.
2. Enable DHCP snooping on each VLAN.
3. Configure trusted and un-trusted ports.
4. Configure static bindings.

Notes:

- The ICRL2-M will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
- If the port link down, the entries learned by this port in the DHCP snooping binding table will be deleted.
- You must enable the global DHCP snooping and DHCP Snooping for VLAN first.

The main purposes of the DHCP Snooping are:

1. Create and maintain binding table for ARP Inspection function.
2. Filter the DHCP server's packets that the DHCP server connects to an un-trusted port.



Note:*The DHCP server connected to an un-trusted port will be filtered.*

Notes:

- There are a global state and per VLAN states.

- When the global state is disabled, the DHCP Snooping on the ICRL2-M is disabled even per VLAN states are enabled.
- When the global state is enabled, user must enable per VLAN states to enable the DHCP Snooping on the specific VLAN.

VLAN 1	Ports 1-4
DHCP Client-1	Connect to Port 3
DHCP Server	Connect to Port 1

Procedures:

1. Default environments:
   a. DHCP Client-1: ipconfig /release
   b. DHCP Client-1: ipconfig /renew
   DHCP Client-1 can get an IP address.
2. Enable the global DHCP Snooping.
   a. L2SWITCH(config)#dhcp-snooping
   b. DHCP Client-1: ipconfig /release
   c. DHCP Client-1: ipconfig /renew
   DHCP Client-1 can get an IP address.
3. Enable the global DHCP Snooping and VLAN 1 DHCP Snooping.
   a. L2SWITCH(config)#dhcp-snooping
   b. L2SWITCH(config)#dhcp-snooping vlan 1
   c. DHCP Client-1: ipconfig /release
   d. DHCP Client-1: ipconfig /renew
   DHCP Client-1 cannot get an IP address because the DHCP server connects to a un-trusted port.
4. Enable the global DHCP Snooping and VLAN 1 DHCP Snooping.
   a. L2SWITCH(config)#dhcp-snooping
   b. L2SWITCH(config)#dhcp-snooping vlan 1
   c. L2SWITCH(config)#interface gi1/0/1
   d. L2SWITCH(config-if)#dhcp-snooping trust
   e. DHCP Client-1: ipconfig /release
   f. DHCP Client-1: ipconfig /renew
   DHCP Client-1 can get an IP address.
5. If you configure a static host entry in the DHCP snooping binding table, and then you want to change the host to DHCP client, the host will not get a new IP from DHCP server, and then you must delete the static host entry first.

6.1.1.1. IP Source Guard / DHCP Snooping

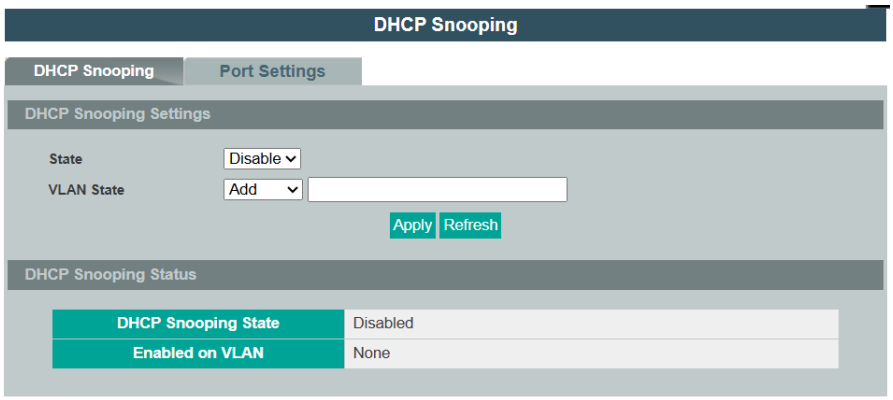
6.1.1.1.1. CLI Configurations - IP Source Guard / DHCP Snooping

CLI DHCP Snooping / DHCP Snooping		
Mode	**Command**	**Description**
enable	show dhcp-snooping	Displays the current DHCP snooping configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	dhcp-snooping (disable l enable)	Disables/enables the DHCP snooping on the ICRL2-M.
configure	dhcp-snooping vlan VLANLISTS	Enables the DHCP snooping function on a VLAN or range of VLANs.
configure	no dhcp-snooping vlan VLANLISTS	disables the DHCP snooping function on a VLAN or range of VLANs.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#dhcp-snooping enable
L2SWITCH(config)#dhcp-snooping vlan 1

6.1.1.1.2. Web Configuration - IP Source Guard / DHCP Snooping



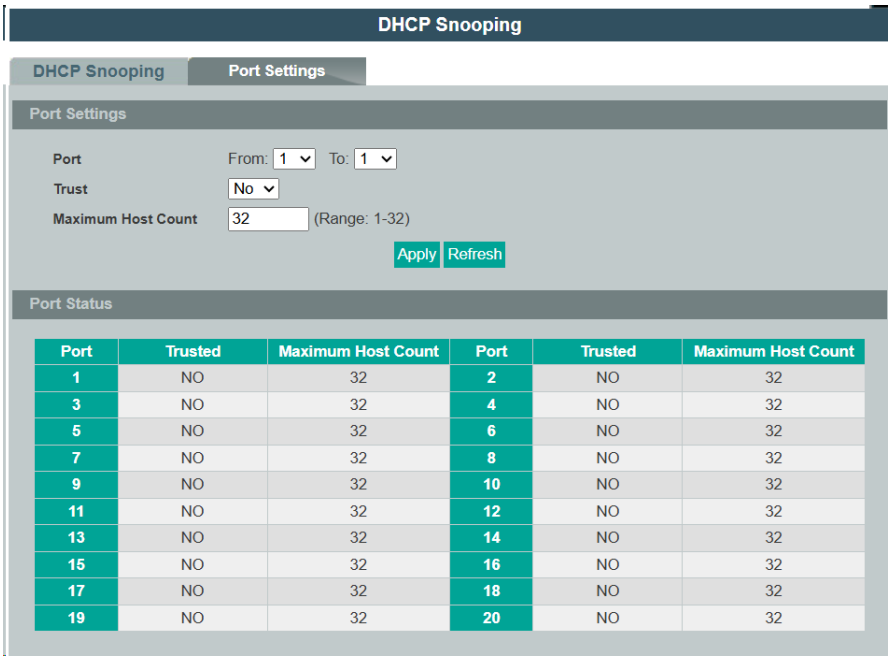
IP Source Guard / DHCP Snooping / DHCP Snooping	
Parameter	**Description**
DHCP Snooping Settings	
State	Select **Enable** to use DHCP snooping on the ICRL2-M. You must enable DHCP snooping on specific VLANs and specify trusted ports. ***Note:*** *The ICRL2-M drops all DHCP requests if you enable DHCP snooping and there are no trusted ports.* Select Disable to not use DHCP snooping.
VLAN State	Select **Add** and enter the VLAN IDs to enable DHCP snooping. Designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-). Select **Delete** and enter the VLAN IDs you no longer want the ICRL2-M to use DHCP snooping.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
DHCP Snooping Status	
DHCP Snooping State	Displays the current status of the DHCP Snooping feature, **Enabled** or **Disabled**.
Enabled on VLAN	Displays the VLAN IDs that have DHCP snooping enabled. Displays **None** if no VLANs are set.

6.1.1.2. IP Source Guard / DHCP Snooping / Port Settings

6.1.1.2.1. CLI Configurations - IP Source Guard / DHCP Snooping / Port Settings

IP Source Guard / CLI DHCP Snooping / Port Settings		
Mode	**Command**	**Description**
enable	show dhcp-snooping	Displays the current DHCP snooping configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	dhcp-snooping host count <1-32>	Configures the maximum host count for the specific port.
interface	no dhcp-snooping host count	Configures the maximum host count to default for the specific port. The default host count is 32.
interface	dhcp-snooping trust	Configures the trust port for the specific port.
interface	no dhcp-snooping trust	Configures the un-trust port for the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	dhcp-snooping host count <1-32>	Configures the maximum host count for the specific ports.
if-range	no dhcp-snooping host count	Configures the maximum host count to default for the specific ports. The default host count is 32.
if-range	dhcp-snooping trust	Configures the trust port for the specific ports.
if-range	no dhcp-snooping trust	Configures the un-trust port for the specific ports.

6.1.1.2.2. Web Configuration - IP Source Guard / DHCP Snooping / Port Settings



Port	Trusted	Maximum Host Count	Port	Trusted	Maximum Host Count
1	NO	32	2	NO	32
3	NO	32	4	NO	32
5	NO	32	6	NO	32
7	NO	32	8	NO	32
9	NO	32	10	NO	32
11	NO	32	12	NO	32
13	NO	32	14	NO	32
15	NO	32	16	NO	32
17	NO	32	18	NO	32
19	NO	32	20	NO	32

IP Source Guard / DHCP Snooping / Port Settings	
Parameter	**Description**
Port	Select a port number to modify its configurations..
Trust	Configures the specific port if it is a trust port.
Maximum Host Count	Enter the maximum number of hosts (1-32) that are permitted to simultaneously connect to a port.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

6.1.2. IP Source Guard / Binding Table

The DHCP Snooping binding table records the host information learned by DHCP snooping function (dynamic) or set by user (static). The ARP inspection will use this table to forward or drop the ARP packets. If the ARP packets sent by invalid host, they will be dropped. If the Lease time is expired, the entry will be removed from the table.

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

6.1.2.1. IP Source Guard / DHCP Snooping Binding Table / Static Entry

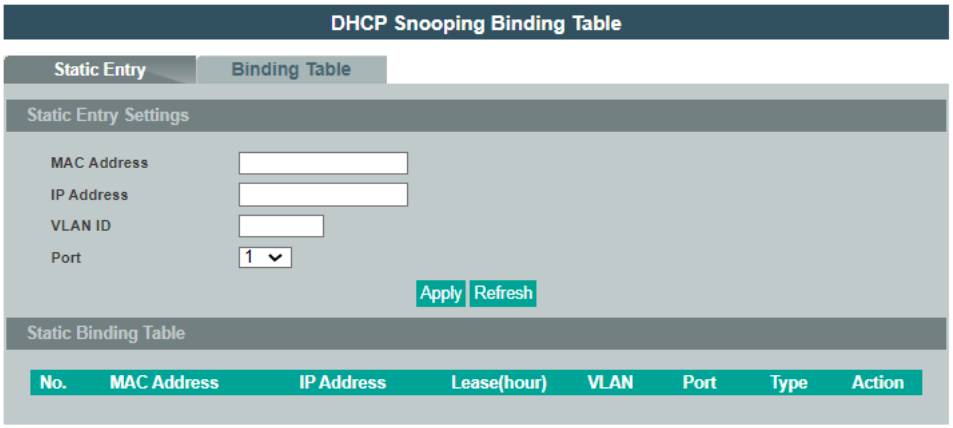
6.1.2.1.1. CLI Configurations - IP Source Guard / DHCP Snooping Binding Table / Static Entry

CLI IP Source Guard / DHCP Snooping Binding Table / Static Entry		
Mode	**Command**	**Description**
enable	show dhcp-snooping binding	Displays the current DHCP snooping binding table.
enable	configure terminal	Changes the mode to configure mode.
configure	dhcp-snooping binding mac MAC_ADDR ip IP_ADDR vlan <1-4094> port PORT_NO	Configures a static host into the DHCP snooping binding table.
configure	no dhcp-snooping binding mac MACADDR	Removes a static host from the DHCP snooping binding table.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#dhcp-snooping binding mac 00:11:22:33:44:55 ip 1.1.1.1 vlan 1 port2
L2SWITCH(config)#no dhcp-snooping binding mac 00:11:22:33:44:55
L2SWITCH#show dhcp-snooping binding

6.1.2.1.2. Web Configuration - IP Source Guard / DHCP Snooping Binding Table / Static Entry



IP Source Guard / DHCP Snooping Binding Table / Static Entry	
Parameter	**Description**
Static Entry Settings	
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN ID	Enter the source VLAN ID in the binding.
Port	Specify the port in the binding.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Static Binding Table	
No.	Displays a sequential number for each binding. Click it to update an existing entry.
MAC Address	Displays the source MAC address in the binding.
IP Address	Displays the IP address assigned to the MAC address in the binding.
Lease (Hour)	Displays how long the binding is valid.
VLAN	Displays the source VLAN ID in the binding.
Port	Displays the port number in the binding.
Type	Displays how the ICRL2-M learned the binding. **Static**: This binding was learned from information provided manually by an administrator. **Dynamic**: This binding was learned by snooping DHCP packets.

IP Source Guard / DHCP Snooping Binding Table / Static Entry (Continued)	
Parameter	**Description**
Action	Click **Delete** to remove the specified entry.

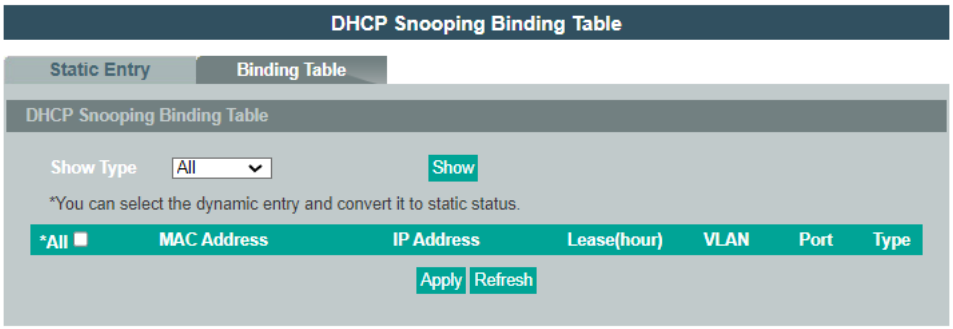
6.1.2.2. IP Source Guard / DHCP Snooping Binding Table / Binding Table

Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The ICRL2-M learns the dynamic bindings by snooping DHCP packets and from information provided manually in the Static Entry Settings screen.

6.1.2.2.1. CLI Configurations - IP Source Guard / DHCP Snooping Binding Table / Binding Table

CLI IP Source Guard / DHCP Snooping Binding Table / Binding Table		
Mode	**Command**	**Description**
enable	show dhcp-snooping binding	Displays the current DHCP snooping binding table.

6.1.2.2.2. Web Configuration - IP Source Guard / DHCP Snooping Binding Table / Binding Table



IP Source Guard / DHCP Snooping Binding Table / Binding Table	
Parameter	**Description**
MAC Address	Displays the source MAC address in the binding.
IP Address	Displays the IP address assigned to the MAC address in the binding.
Lease	Displays how long the binding is valid.
VLAN	Displays the source VLAN ID in the binding.
Port	Displays the port number in the binding. If this field is blank, the binding applies to all ports.

IP Source Guard / DHCP Snooping Binding Table / Binding Table (Continued)	
Parameter	**Description**
Type	Displays how the ICRL2-M learned the binding. Static: This binding was learned from information provided manually by an administrator. Dynamic: This binding was learned by snooping DHCP packets.
Apply	Click Apply to configure the settings.
Refresh	Click **Refresh** to reload the running configuration values.

6.1.3. IP Source Guard / ARP Inspection

Dynamic ARP inspection is a security feature which validates ARP packet in a network by performing IP to MAC address binding inspection. Those will be stored in a trusted database (the DHCP snooping database) before forwarding. Dynamic ARP intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed.The ICRL2-M performs these activities:

- Intercepts all ARP requests and responses on untrusted ports.
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before it updates the local ARP cache or before it forwards the packet to the appropriate destination.

Trusted and untrusted port

- This setting is independent of the trusted and untrusted setting of the DHCP Snooping.
- The ICRL2-M does not discard ARP packets on trusted ports for any reasons.
- The ICRL2-M discards ARP packets on un-trusted ports if the sender's information in the ARP packets does not match any of the current bindings.
- Normally, the trusted ports are the uplink port and the untrusted ports are connected to subscribers.

Configurations:

Users can enable/disable the ARP Inspection on the ICRL2-M. Users also can enable/disable the ARP Inspection on a specific VLAN. If the ARP Inspection on the ICRL2-M is disabled, the ARP Inspection is disabled on all VLANs even some of the VLAN ARP Inspection are enabled.

Notes: *There are a global state and per VLAN states.*

- When the global state is disabled, the ARP Inspection on the ICRL2-M is disabled even per VLAN states are enabled.
- When the global state is enabled, user must enable per VLAN states to enable the ARP Inspection on the specific VLAN.

6.1.3.1. IP Source Guard / ARP Inspection

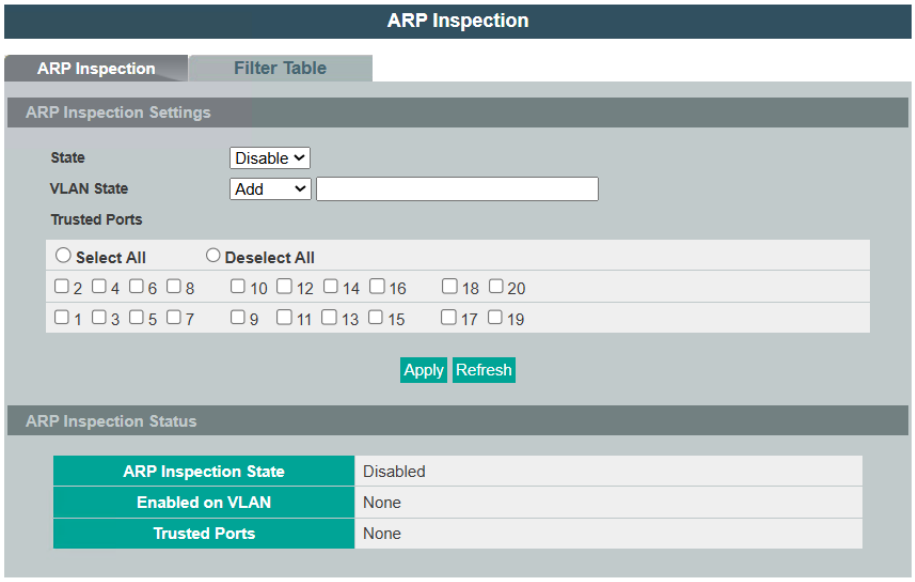
6.1.3.1.1. CLI Configurations - IP Source Guard / ARP Inspection

CLI IP Source Guard / ARP Inspection		
Mode	**Command**	**Description**
enable	show arp-inspection	Displays the current ARP Inspection configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	arp-inspection (disable | enable)	Disables/enables the ARP Inspection function on the ICRL2-M.
configure	arp-inspection vlan VLANLISTS	Enables the ARP Inspection function on a VLAN or range of VLANs.
configure	no arp-inspection vlan VLANLISTS	Disables the ARP Inspection function on a VLAN or range of VLANs.
configure	interface IFNAME	Enters the interface configure mode.
interface	arp-inspection trust	Configures the trust port for the specific port.
interface	no arp-inspection trust	Configures the un-trust port for the specific port.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#arp-inspection enable
L2SWITCH(config)#arp-inspection vlan 1
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#arp-inspection trust

6.1.3.1.2. Web Configuration - IP Source Guard / ARP Inspection



Note: *Number of ports displayed varies depending on the ICRL2-M.*

IP Source Guard / ARP Inspection	
Parameter	**Description**
ARP Inspection Settings	
State	Use this to Enable or Disable ARP inspection on the ICRL2-M.
VLAN State	Enter the VLAN IDs you want the ICRL2-M to enable ARP Inspection for. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-).
Trusted Ports	Select the ports which are trusted and deselect the ports which are un-trusted. The ICRL2-M does not discard ARP packets on trusted ports for any reason. The ICRL2-M discards ARP packets on un-trusted ports in the following situations: • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on un-trusted ports.
Select All	Click this to set all ports to trusted.
Deselect All	Click this to set all ports to un-trusted.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

IP Source Guard / ARP Inspection (Continued)	
Parameter	**Description**
ARP Inspection Status	
ARP Inspection State	Displays the current status of the ARP Inspection feature, **Enabled** or **Disabled**.
Enabled on VLAN	Displays the VLAN IDs that have ARP Inspection enabled on them. This will display None if no VLANs have been set.
Trusted Ports	Displays the ports which are trusted. This will display None if no ports are trusted.

6.1.3.2. IP Source Guard / ARP Inspection / Filter Table

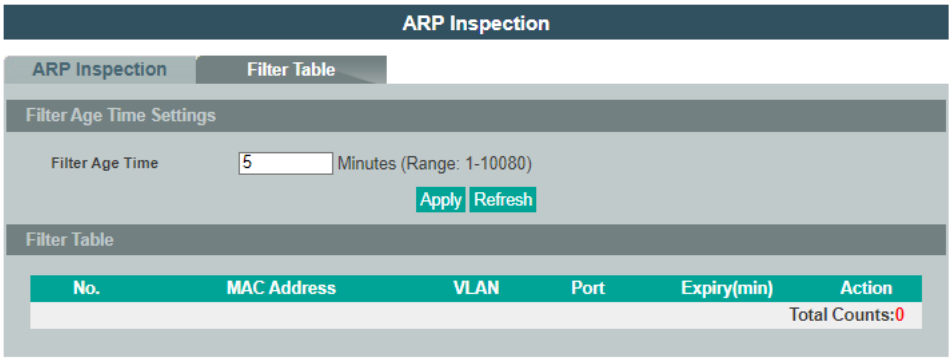
Dynamic ARP inspections validates the packet by performing IP to MAC address binding inspection stored in a trusted database (the DHCP snooping database) before forwarding the packet. When the ICRL2-M identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. The ICRL2-M also periodically deletes entries if the age-time for the entry is expired.

- If the ARP Inspection is enabled and the system detects invalid hosts, the system creates a filtered entry in the MAC address table.
- When the Port link down and ARP Inspection is disabled, ICRL2-M removes the MAC-filter entries learned by this port.
- When the Port link down and ARP Inspection is enabled, ICRL2-M removes the MAC-filter entries learned by this port.
- The maximum entry of the MAC address filter table is 256.
- When MAC address filter table of ARP Inspection is full, the ICRL2-M receives unauthorized ARP packet, and it automatically creates a SYSLOG and drop this ARP packet. The SYSLOG event happens on the first time.

6.1.3.2.1. CLI Configurations - IP Source Guard / ARP Inspection / Filter Table

CLI IP Source Guard / ARP Inspection / Filter Table		
Mode	**Command**	**Description**
enable	show arp-inspection mac-filter	Displays the current ARP Inspection filtered MAC.
enable	configure terminal	Changes the mode to configure mode.
configure	arp-inspection mac-filter age <1-10080>	Configures the age time for the ARP inspection MAC filter entry.
configure	clear arp-inspection mac-filter	Clears all of entries in the filter table.
configure	no arp-inspection mac-filter mac MACADDR vlan <1-4094>	Removes an entry from the ARP inspection MAC filter table.

6.1.3.2.2. Web Configuration - IP Source Guard / ARP Inspection / Filter Table



IP Source Guard / ARP Inspection / Filter Table	
Parameter	**Description**
Filter Age Time Settings	
Filter Age Time	This setting has no effect on existing MAC address filters. Enter how long (1-10080 minutes) the MAC address filter remains in the ICRL2-M after the ICRL2-M identifies an unauthorized ARP packet. The ICRL2-M automatically deletes the MAC address filter afterwards.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Filter Table	
No.	Displays a sequential number for each MAC address filter.
MAC Address	Displays the source MAC address in the MAC address filter.
VLAN	Displays the source VLAN ID in the MAC address filter.
Port	Displays the source port of the discarded ARP packet.
Expiry (min)	Displays how long (in minutes) the MAC address filter remains in the ICRL2-M.
Action	Click Delete to remove the record manually.
Total	Displays the current number of MAC address filters that were created because the ICRL2-M identified unauthorized ARP packets.

6.2. Access Control List (ACL)

Access control list (ACL) is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

L2 ACL function allows user to configure a few rules to reject packets from the specific ingress ports or all ports. These rules will check the packets' source MAC address and destination MAC address. If packets match these rules, the system will do the actions "deny". "deny" means rejecting these packets.

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

L2 ACL Support:

1. Filter a specific source MAC address.
   Command: *sourcemac host MACADDR*
2. Filter a specific destination MAC address.
   Command: *destination mac host MACADDR*
3. Filter a range of source MAC address.
   Command: *sourcemac MACADDR MACADDR*
   The second MACADDR is a mask, for example: ffff.ffff.0000
4. Filter a range of destination MAC address.
   Command: *destination mac MACADDR MACADDR*
   The second MACADDR is a mask, for example: ffff.ffff.0000

L3 ACL Support:

1. Filter a specific source IP address.
   Command: *source ip host IPADDR*
2. Filter a specific destination IP address.
   Command: *destination iphost IPADDR*
3. Filter a range of source IP address.
   Command: *source ip IPADDRIPADDR*
   The second IPADDR is a mask, for example: 255.255.0.0
4. Filter a range of destination IP address.
   Command: destinationip IPADDRIPADDR

L4 ACL Support:

1. Filter a UDP/TCP source port.
2. Filter a UDP/TCP destination port.

Notes:

- Maximum profile: 64.
- Maximum profile name length: 16.
- The ACL name should be the combination of the digit or the alphabet.

6.2.1. CLI Configurations- Access Control List

CLI Access Control List		
Mode	**Command**	**Description**
enable	show access-list	Displays all of the access control profiles.
enable	configure terminal	Changes the mode to configure mode.
configure	access-list STRING ip-type (ipv4 | ipv6)	Creates a new access control profile. Where the STRING is the profile name. And you can specify the type, ipv4 or ipv6.
configure	no access-list STRING	Deletes an access control profile.
acl	show	Displays the current access control profile.
acl	action (disable | drop | permit | dscp | 802.1p)	Actives this profile. • disable – disable the profile. • drop – If packets match the profile, the packets will be dropped. • permit – If packets match the profile, the packets will be forwarded. • dscp – dscp remark. • 802.1p – 802.1p remark.
acl	action dscp remarking <0-63>	Actives this profile and specify that it is for DSCP remark. And configures the new DSCP value which will be override to all packets matched this profile.
acl	action 802.1p remarking <0-7>	Actives this profile and specify that it is for 802.1p remark. And configures the new 802.1p value which will be override to all packets matched this profile.
acl	802.1p VALUE	Configures the 802.1p value for the profile.
acl	dscp VALUE	Configures the DSCP value for the profile.
acl	destination mac hostMACADDR	Configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	Configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	Configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile.
acl	no destination mac	Removes the destination MAC from the profile.
acl	ethertype STRING	Configures the ether type for the profile. Where the STRING is a hex-decimal value. e.g.: 08AA.

CLI Access Control List (Continued)		
Mode	**Command**	**Description**
acl	no ethertype	Removes the limitation of the ether type from the profile.
acl	source mac host MACADDR	Configures the source MAC and mask for the profile.
acl	source mac MACADDR MACADDR	Configures the source AMC and mask for the profile.
acl	no source mac	Removes the source MAC and mask from the profile.
acl	source ip host IPADDR	Configures the source IP address for the profile.
acl	source ip IPADDR IPMASK	Configures the source IP address and mask for the profile.
acl	no source ip	Removes the source IP address from the profile.
acl	destination ip host IPADDR	Configures a specific destination IP address for the profile.
acl	destination ip IPADDR IPMASK	Configures the destination IP address and mask for the profile.
acl	no destination ip	Removes the destination IP address from the profile.
acl	l4-source-port IPADDR	Configures UDP/TCP source port for the profile.
acl	no l4-source-port IPADDR	Removes the UDP/TCP source port from the profile.
acl	L4-destination-port PORT	Configures the UDP/TCP destination port for the profile.
acl	no l4-destination-port	Removes the UDP/TCP destination port from the profile.
acl	vlan <1-4094>	Configures the VLAN for the profile.
acl	no vlan	Removes the limitation of the VLAN from the profile.
acl	source interface PORT_ID	Configures the source interface for the profile.
acl	no source interface PORT_ID	Removes the source interface from the profile.

Where the MAC mask allows users to filter a range of MAC in the packets' source MAC or destination MAC.

For example:

source mac 00:01:02:03:04:05 ff:ff:ff:ff:00

Filters source MAC range from 00:01:02:03:00:00 to 00:01:02:03:ff:ff

Where the IPMASK mask allows users to filter a range of IP in the packets' source IP or destination IP.

For example:

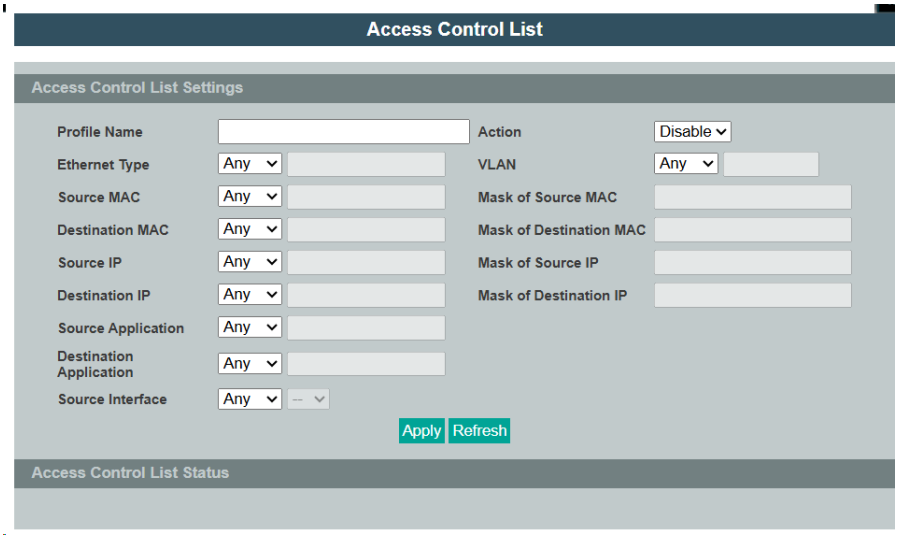
source ip 172.20.1.1 255.255.0.0

Filters source IP range from 172.20.0.0 to 172.20.255.255

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#access-list 111
L2SWITCH(config-acl)#vlan 2
L2SWITCH(config-acl)#source interface 1
L2SWITCH(config-acl)#show
Profile Name: 111
Activate: disabled
VLAN: 2
Source Interface: 1
Destination MAC Address: any
Source MAC Address: any
Ethernet Type: any
Source IP Address: any
Destination IP Address: any
Source Application: any
Destination Application: any

6.2.2. Web Configuration - Access Control List



Access Control List	
Parameter	**Description**
Profile Name	The access control profile name.
Action	Selects **Disables**/**Drop**/**Permits**/**DSCP**/**802.1P** action for the profile.

8/19/25

Access Control List (Continued)	
Parameter	**Description**
Ethernet Type	Configures the Ethernet type of the packets for the profile.
VLAN	Configures the VLAN of the packets for the profile.
Source MAC	Configures the source MAC of the packets for the profile.
Mask of Source MAC	Configures the bitmap mask of the source MAC of the packets for the profile. If the Source MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Source MAC field.
Destination MAC	Configures the destination MAC of the packets that you want to filter.
Mask of Destination MAC	Configures the bitmap mask of the destination MAC of the packets that you want to filter. If the Destination MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Destination MAC field.
Source IP	Configures the source IP of the packets for the profile.
Mask of Source IP	Configures the bitmap mask of the source IP of the packets for the profile. If the Source IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Source IP field.
Destination IP	Configures the destination IP of the packets for the profile.
Mask of Destination IP	Configures the bitmap mask of the destination IP of the packets for the profile. If the Destination IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Destination IP field.
Source Application	Configures the source UDP/TCP ports of the packets for the profile.
Destination Application	Configures the destination UDP/TCP ports of the packets for the profile.
Source Interface(s)	Configures one or a rage of the source interfaces of the packets for the profile.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

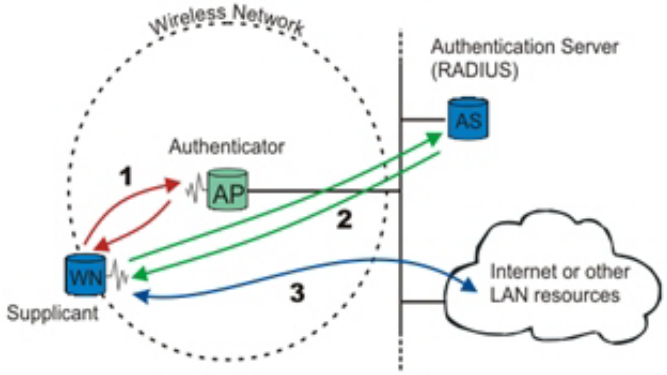
6.3. 802.1X

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

802.1X provides port-based authentication, which involves communications between a supplicant, authenticator, and authentication server. The supplicant is often software on a client device, such as a laptop, the authenticator is a wired Ethernet switch or wireless access point, and an authentication server is generally a RADIUS database. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity is authorized. An analogy to this is providing a valid passport at an airport before being allowed to pass through security to the terminal. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the credentials are valid (in the authentication server database), the supplicant (client device) is allowed to access resources located on the protected side of the network.

Upon detection of the new client (supplicant), the port on the ICRL2-M (authenticator) is enabled and set to the "unauthorized" state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is blocked at the network layer (Layer 3). The authenticator sends out the EAP-Request identity to the supplicant, the supplicant responds with the EAP-response packet that the authenticator forwards to the authenticating server. If the authenticating server accepts the request, the authenticator sets the port to the "authorized" mode and normal traffic is allowed. When the supplicant logs off, it sends an EAP-logoff message to the authenticator. The authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.

The following figure illustrates how a client connecting to an IEEE 802.1xauthentication enabled port goes through a validation process. The ICRL2-M prompts the client for login information in the form of a user name and password.



When the client provides the login credentials, the ICRL2-M sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Local User Accounts

By storing user profiles locally on the ICRL2-M, your ICRL2-M is able to authenticate users without interacting with a network authentication server. However, there is a limit on the number of users you may authenticate in this way.

Guest VLAN:

The Guest VLAN in IEEE 802.1x port authentication on the ICRL2-M to provide limited services to clients, such as downloading the IEEE 802.1x client. These clients might be upgrading their system for IEEE 802.1x authentication.

When you enable a guest VLAN on an IEEE 802.1x port, the ICRL2-M assigns clients to a guest VLAN when the ICRL2-M does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

Port Parameters:

- **Admin Control Direction**:
  - both: drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication.
  - in: drop only incoming packets on the port when a user has not passed 802.1x port authentication.
- **Re-authentication**: Specify if a subscriber has to periodically re-enter his or her user name and password to stay connected to the port.
- **Reauth-period:** Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.
- **Port Control Mode**:
  - auto: Users can access network after authenticating.
  - force-authorized: Users can access network without authentication.
  - force-unauthorized: Users cannot access network.
- **Quiet Period**: Specify a period of the time the client has to wait before the next re-authentication attempt. This will prevent the ICRL2-M from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.
- **Server Timeout**: The server-timeout value is used for timing out the Authentication Server.
- **Supp-Timeout**: The supp-timeout value is the initialization value used for timing out a Supplicant.
- **Max-req Time**: Specify the amount of times the ICRL2-M will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.

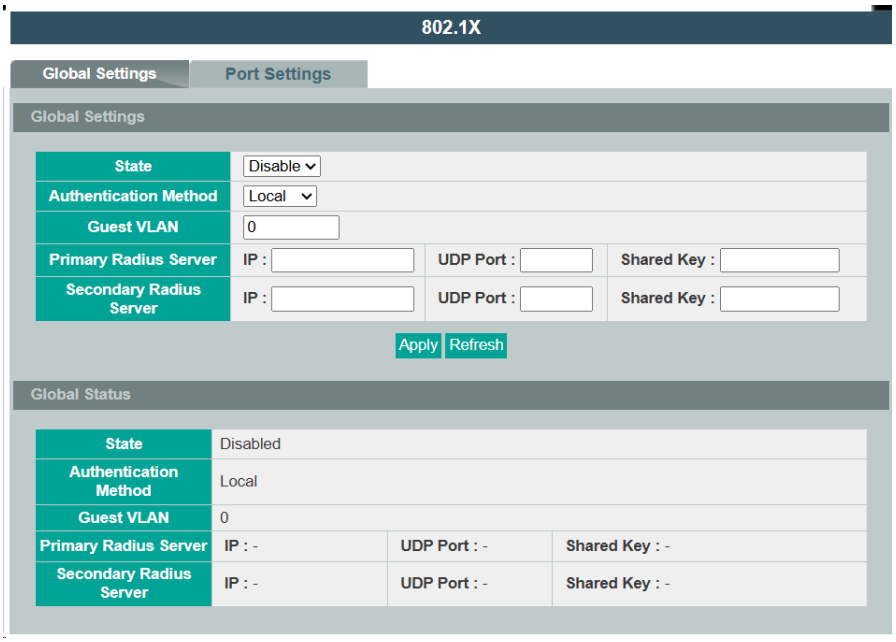
Default Settings	
global 802.1x state	disabled.
802.1x Authentication Method	local.
port 802.1x state	disabled for all ports.
port Admin Control Direction	both for all ports.
port Re-authentication	disabled for all ports.
port Control Mode	auto for all ports.
port Guest VLAN	0 for all ports. (Guest VLAN is disabled).
port Max-req Time	2 times for all ports.
port Reauth period	3600 seconds for all ports.
port Quiet period	60 seconds for all ports.
port Supp timeout	30 seconds for all ports.
port Server timeout	30 seconds for all ports.

6.3.1. Global Settings

6.3.1.1. CLI Configurations - 802.1X / Global Settings

CLI 802.1X / Global Settings		
Mode	**Command**	**Description**
enable	show dot1x	Displays the current 802.1x configurations.
enable	show dot1x username	Displays the current user accounts for the local authentication.
enable	show dot1x accounting-record	Displays the local accounting records.
enable	configure terminal	Changes the mode to configure mode.
configure	dot1x authentication (disable | enable)	Enables/disables the 802.1x authentication on the ICRL2-M.
configure	dot1x authentic-method (local | radius)	Configures the authentic method of802.1x.
configure	no dot1xauthentic-method	Configures the authentic method of 802.1x to default.
configure	dot1x accounting (disable | enable)	Enables/disables the dot1x local accounting records.
configure	dot1x accounting-clean	Cleans all of the accounting records.
configure	dot1x default	Sets all of the configuration to default settings.
configure	dot1x guest-vlan <1-4094>	Configures the guest VLAN.
configure	no dot1x guest-vlan	Removes the guest VLAN.
configure	dot1x radius primary-server-ip <IP> port PORTID	Configures the primary radius server.
configure	dot1x radius primary-server-ip <IP> port PORTID key KEY	Configures the primary radius server.
configure	no dot1x radius primary-server-ip	Removes the secondary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID	Configures the secondary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID key KEY	Configures the secondary radius server.
configure	no dot1x radius secondary-server-ip	Removes the secondary radius server.
configure	dot1x username <USERNAME> <PASSWORD>	Configures the user account for local authentication.
configure	no dot1x username <STRING>	Deletes the user account for local authentication.

6.3.1.2. Web Configuration - 802.1X / Global Settings



802.1X / Global Settings	
Parameter	**Description**
Global Settings	
State	Select Enable to permit 802.1x authentication on the ICRL2-M. ***Note:*** *You must first enable 802.1x authentication on the ICRL2-M before configuring it on each port.*
Authentication Method	Select whether to use Local or RADIUS as the authentication method. The Local method of authentication uses the “guest” and “user” user groups of the user account database on the ICRL2-M itself to authenticate. However, only a certain number of accounts can exist at one time. RADIUS is a security protocol used to authenticate users by means of an external server instead of an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS allows you to validate an unlimited number of users from a central location.
Guest VLAN	Configure the guest VLAN.

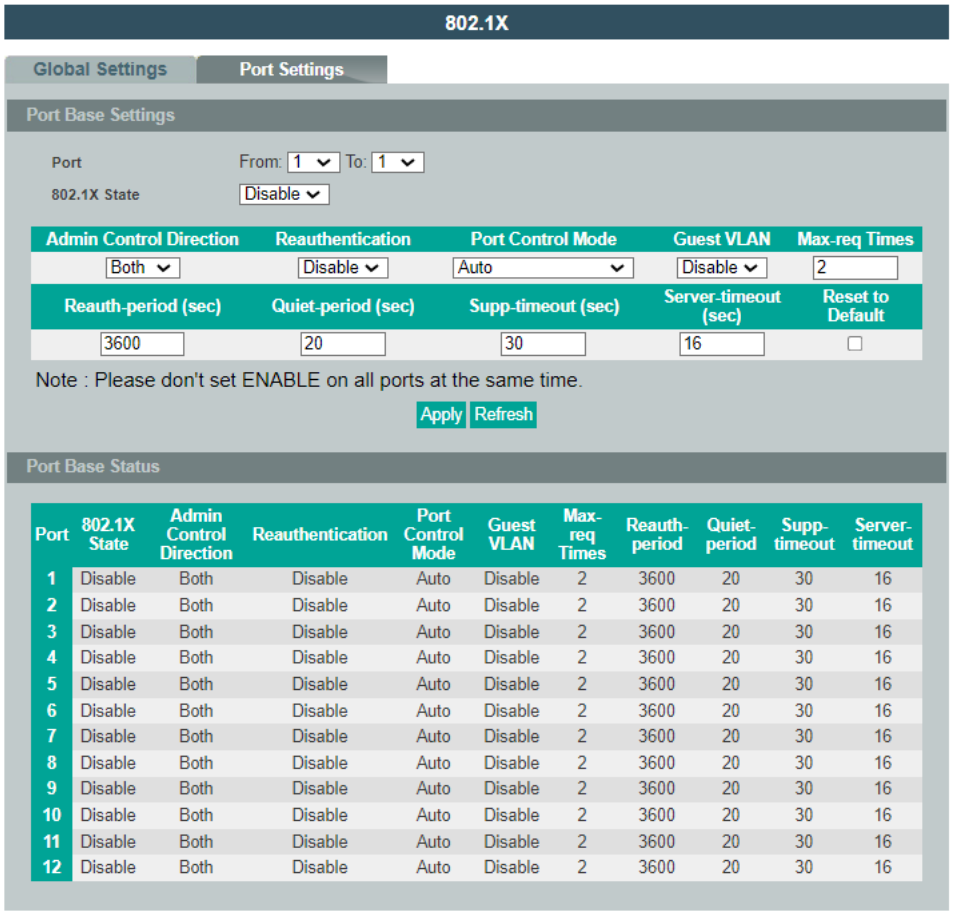
802.1X / Global Settings (Continued)	
Parameter	**Description**
Primary Radius Server	When RADIUS is selected as the 802.1x authentication method, the Primary Radius Server will be used for all authentication attempts. • **IP Address**: Enter the IP address of an external RADIUS server in dotted decimal notation. • **UDP Port**: The default port of a RADIUS server for authentication is 1812. • **Share Key**: Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the ICRL2-M. This key is not sent over the network. This key must be the same on the external RADIUS server and the ICRL2-M.
Secondary Radius Server	Backup server used only when the Primary Radius Server is down. • **IP Address**: Enter the IP address of an external RADIUS server in dotted decimal notation. • **UDP Port**: The default port of a RADIUS server for authentication is 1812. • **Share Key**: Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the ICRL2-M. This key is not sent over the network. This key must be the same on the external RADIUS server and the ICRL2-M.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

6.3.2. 801.2X / Port Settings

6.3.2.1. CLI Configurations - 802.1X / Port Settings

CLI 802.1X / Port Settings		
Mode	**Command**	**Description**
enable	show dot1x	Displays the current 802.1x configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	dot1x admin-control-direction (both | in)	Configures the control direction for blocking packets.
interface	dot1x default	Sets the port configuration to default settings.
interface	dot1x max-req <1-10>	Sets the max-req times for the port.
interface	dot1x port-control (auto | force-authorized | force-unauthorized)	Configures the port control mode on the port.
interface	dot1x authentication (disable | enable)	Enables/disables the 802.1x authentication on the port.
interface	dot1x reauthentication (disable | enable)	Enables/disables re-authentication on the port.
interface	dot1x timeout quiet-period	Configures the quiet-period value on the port.
interface	dot1x timeout server-timeout	Configures the server-timeout value on the port.
interface	dot1x timeout reauth-period	Configures the reauth-period value on the port.
interface	dot1x timeout supp-timeout	Configures the supp-timeout value on the port.
interface	dot1x guest-vlan (disable | enable)	Disables / enables guest VLAN on the port.

6.3.2.2. Web Configuration - 802.1X / Port Settings



802.1X / Port Settings	
Parameter	**Description**
Port	Select a port number to configure.
802.1x State	Select **Enable** to permit 802.1x authentication on the port. You must first enable 802.1x authentication on the ICRL2-M before configuring it on each port.
Admin Control Direction	Select **Both** to drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. Select **In** to drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Re-authentication	Specify if a subscriber has to periodically re-enter his or her user name and password to stay connected to the port.

802.1X / Port Settings (Continued)	
Parameter	**Description**
Port Control Mode	Select **Auto** to require authentication on the port. Select **Force Authorized** to always force this port to be authorized. Select **Force Unauthorized** to always force this port to be unauthorized. No packets can pass through this port.
Guest VLAN	Select **Disable** to disable Guest VLAN on the port. Select **Enable** to enable Guest VLAN on the port.
Max-req Time	Specify the amount of times the ICRL2-M will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.
Reauth period	Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.
Quiet period	Specify a period of the time the client has to wait before the next re-authentication attempt. This will prevent the ICRL2-M from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.
Supp timeout	Specify how long the ICRL2-M will wait before communicating with the server. The acceptable range for this field is 0 to 65535 seconds.
Server timeout	Specify how long the ICRL2-M to time out the Authentication Server. The acceptable range for this field is 0 to 65535 seconds.
Reset to Default	Select this and click **Apply** to reset the custom 802.1x port authentication settings back to default.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

6.4. Port Security

The ICRL2-M will learn the MAC address of the device directly connected to a particular port and allow traffic through. The ICRL2-M controls which devices can connect to a ICRL2-M port or how many of them can connect to it (such as when a hub or another ICRL2-M is connected to the port).

For example: one ICRL2-M port left free and we need to connect five hosts to it. Connect a hub or switch to the free port. Connecting a switch or a hub to a port has implications. It means that the network will have more traffic. If a switch or a hub is connected by a user instead of an administrator, then there are chances that loops will be created. So, it is best that number of hosts allowed to connect is restricted at the switch level. This can be done using the “port-security limit” command. This command configures the maximum number of MAC addresses that can source traffic through a port.

Port security can sets maximum number of MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses are dropped. It can be use MAC table to check it. The static MAC addresses are included for the limit.

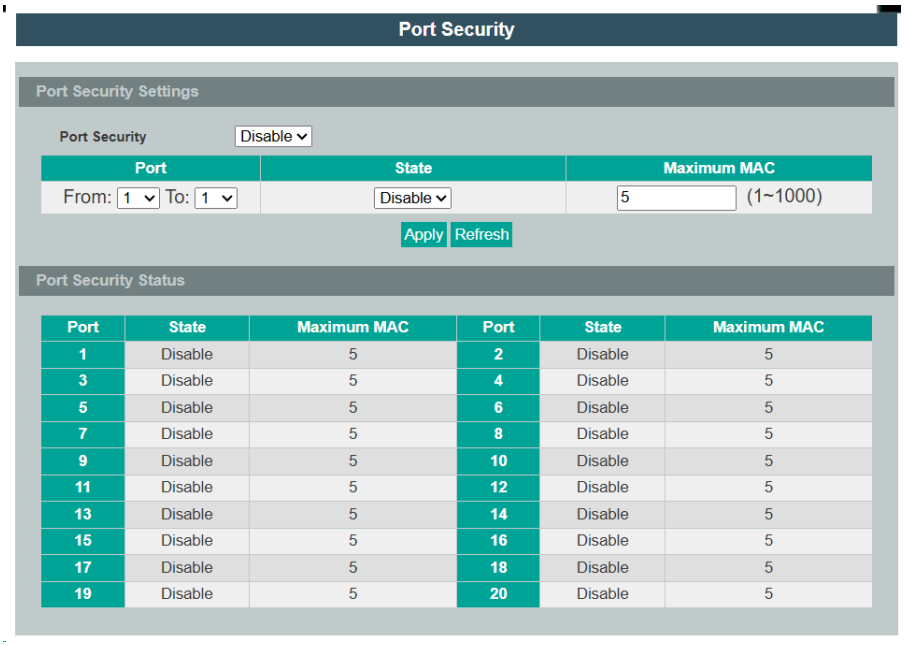
Note: *If you configure a ICRL2-M port from disabled to enabled, all of the MAC learned by this port are cleared.*

6.4.1. Port Security

6.4.1.1. CLI Configurations - Port Security / Port Security Settings

CLI Port Security / Port Security Settings		
Mode	**Command**	**Description**
enable	show port-security	Displays the current port security configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	port-security (disable | enable)	Enables / disables the global port security function.
configure	interface IFNAME	Enters the interface configure mode.
interface	port-security (disable | enable)	Enables / disables the port security function on the specific port.
interface	port-security limit <1-1000>	Configures the maximum MAC entries on the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	port-security (disable | enable)	Enables / disables the port security function for the specified ports
if-range	port-security limit <1-1000>	Configures the maximum MAC entries for the specified ports.

6.4.1.2. Web Configuration - Port Security / Port Security Settings



Port Security / Port Security Settings	
Parameter	**Description**
Port Security	Select Enable/Disable to permit Port Security on the ICRL2-M.
Port	Select a port number to configure.
State	Select **Enable**/**Disable** to permit Port Security on the port.
Maximum MAC	The maximum number of MAC addresses allowed per interface. The acceptable range is 1 to 1000.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

6.5. TACACS+

The purpose of this enhancement is to support TACACS+ on the ICRL2-M platforms. Terminal Access Controller Access Control System Plus is a security application that provides centralized validation of users attempting to gain access to a router, network access server etc. In order for the TACACS+ feature on the ICRL2-M products to work it would need a TACACS+ server, which would typically be a daemon running on a centralized UNIX or Windows authentication, authorization and accounting facilities for managing network access points from a single management service.

Product Features

The TACACS+ implementation will support the following features:

- The implementation will conform to version 1.78 of the TACACS+ draft RFC.
- Authentication, Authorization and Accounting can be run as well as disabled independently of each other.
- In case TACACS+ authentication fails on account of the server being unreachable the box can be made to default to a local authentication policy.
- TACACS+ packet body encryption will be supported.
- Single TACACS+ server will be support.
- Multiple connect mode will be support.
- Syslog messages will be support.

Functional Description

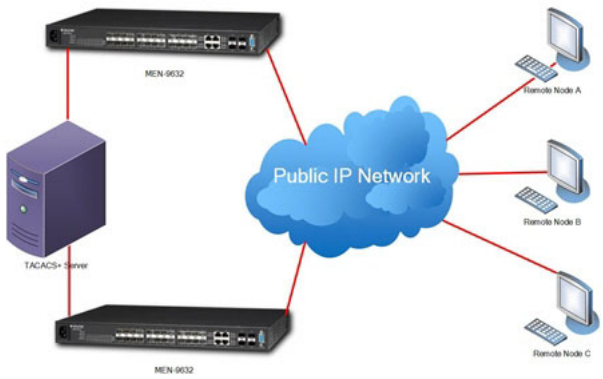
The TACACS+ implementation will provide the following services:

- Authentication: Complete control of authentication through login and password dialog, challenge and response, messaging support etc.
- Authorization: Control over user capabilities for the duration of the user session, like setting auto commands, enforcing restrictions on what configuration commands a user may execute, session duration etc.
- Accounting: Collecting and sending information used for billing, auditing, and reporting to the TACACS+ daemon.

Each of the above mentioned services can be configured and run independent of the others. The TACACS+ implementation will provide authentication and confidentiality between the router and the TACACS+ daemon. It runs on TCP port 49.

Application:

Remote network access is witnessing a major paradigm shift that from terminal access to LAN access. Single users want to connect to the corporate network in the same way that they connect at work i.e. as a LAN user. This places increased emphasis on network access security. As a result of this network managers are concerned with 3 parameters: authentication, authorization and accounting. This is where TACACS+ enters into the picture. A typical deployment using TACACS+ could be as follow:



Notes:

- TACACS+ service must be enabled before configuring the authentication, authorization and accounting parameters, otherwise it will return error as TACACS+ service is not enabled.
- Not allowed to disable the Authentication login mode when both enabled login-mode and login local.
- Not allowed to disable the Authentication enable mode when both enabled enable-mode and enable local.
- Not allowed to enable the login-mode local when login-mode is in disable.

8/19/25

- Not allowed to enable the enable-mode local when enable-mode is in disable.
- For input CLI, user must supply full command or partial command with TAB (command must be completed). The reason is only the command after user HIT the ENTER is only send to TACACS+ server for authorization or accounting. So if this command is partial then subsequently authorization or accounting fails.

6.5.1. CLI Configurations - TACACS+

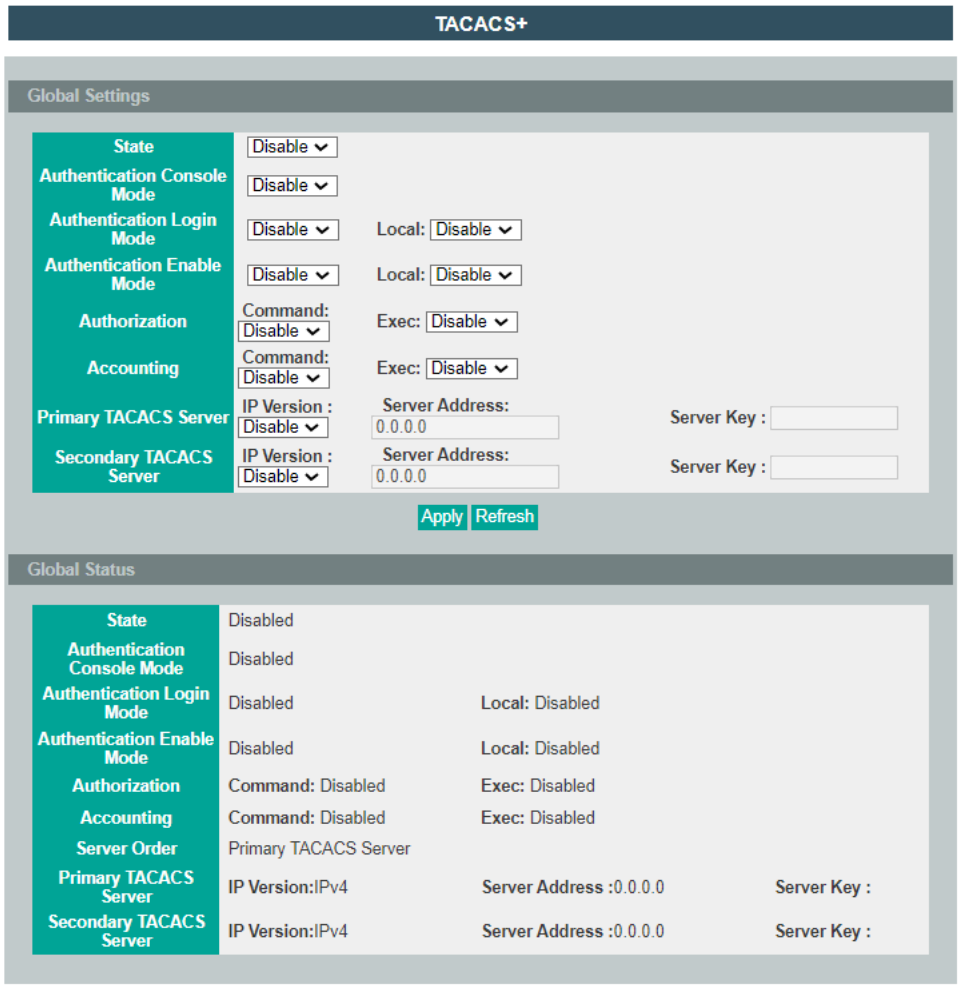
CLI TACACS+		
Mode	**Command**	**Description**
enable	show tacacs-plus	To show the TACACS+ Statistics.
enable	configure terminal	Changes the mode to configure mode.
configure	tacacs-plus server-host <ipaddr>	Sets the TACACS+ Server ip address
configure	no tacacs-plus server-host	Resets the TACACS+ Server ip address as 0.0.0.0
configure	tacacs-plus server-key <key>	Sets the TACACS+ server key
configure	no tacacs-plus server-key	Resets the TACACS+ server key as default key(NULL means no key)
configure	tacacs-plus enable	Enables the TACACS+ service
configure	no tacacs-plus enable	Disables the TACACS+ service
configure	tacacs-plus authentication login-mode enable	Enables the authentication login mode
configure	no tacacs-plus authentication login-mode enable	Disables the authentication login mode
configure	tacacs-plus authentication login-mode local enable	Enables the authentication login local mode
configure	no tacacs-plus authentication login-mode local enable	Disables the authentication login local mode
configure	tacacs-plus authentication enable-mode enable	Enables the authentication in enable mode.
configure	no tacacs-plus authentication enable-mode enable	Disables the authentication in enable mode.
configure	tacacs-plus authentication enable-mode local enable	Enables the authentication enable local mode
configure	no tacacs-plus authentication enable-mode local enable	Disables the authentication enable local mode
configure	tacacs-plus authorization commands enable	Enables the authorization show commands.

CLI TACACS+ (Continued)		
Mode	**Command**	**Description**
configure	no tacacs-plus authorization commands enable	Disables the authorization show commands.
configure	tacacs-plus authorization exec enable	Enables the authorization configuration commands.
configure	no tacacs-plus authorization exec enable	Disables the authorization configuration commands.
configure	tacacs-plus accounting commands enable	Enables the level 1 commands for accounting.
configure	no tacacs-plus accounting commands enable	Disables the level 1 commands for accounting.
configure	tacacs-plus accounting exec enable	Enables the level 15 commands for accounting.
configure	no tacacs-plus accounting exec enable	Disables the level15 commands for accounting
configure	tacacs-plus line-console enable	Enables TACACSP on the console port.
configure	no tacacs-plus line-console enable	Disables TACACSP on the console port.

Example:

```
L2SWITCH#show tacacs-plus
TACACS+ Server Host              :0.0.0.0
TACACS+ State                    :disabled
TACACS+ line-console mode        :disabled
Authentication Login mode        :disabled          Local: disabled
Authentication Enable mode       :disabled          Local: disabled
Authorization                    :Command: disabled Exec : disabled
Accounting                       :Command: disabled Exec : disabled
Authentication Sessions          :0
Authorization Sessions           :0
Accounting Sessions              :0
```

6.5.2. Web Configuration - TACACS+



TACACS+	
Parameter	**Description**
Global Settings	
State	Enables / Disables the TACACS+ service.
Authentication Console Mode	Enables / Disables the authentication in console mode.
Authentication Login Mode (TACACS+ server)	Enables / Disables the authentication in login mode. (this authentication is done by TACACS+ server).
Authentication Login Mode (Local)	Enables / Disables the authentication in login mode. (this authentication is done by ICRL2-M when it cannot find TACACS+ server).

TACACS+ (Continued)	
Parameter	**Description**
Authentication Enable Mode (TACACS+ server)	Enables / Disables the authentication in Enable mode. (this authentication is done by TACACS+ server).
Authentication Enable Mode (Local)	Enables / Disables the authentication in Enable mode. (this authentication is done by ICRL2-M when it cannot find TACACS+ server).
Authorization Command	Enables / Disables the authorization with show commands.
Authorization Exec	Enables / Disables the authorization with configuration commands.
Accounting Command	Enables / Disables the level 1 command for the Accounting.
Accounting Exec	Enables / Disables the level 15 command for the Accounting.
TACACS Server IP Version	Select whether IPv4 or IPv6.
TACACS Server IP	Configures the TACACS server's IP.
TACACS Server. Server Key	Configures the server key for the TACACS server.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

7. Monitor

7.1. Alarm

The feature displays if there are any abnormal situation need process immediately.

Note: *The Alarm DIP allows users to configure if send alarm message when the corresponding event occurs.*

For Example:

P1: ON, The ICRL2-M sends alarm message when port 1 is link down.

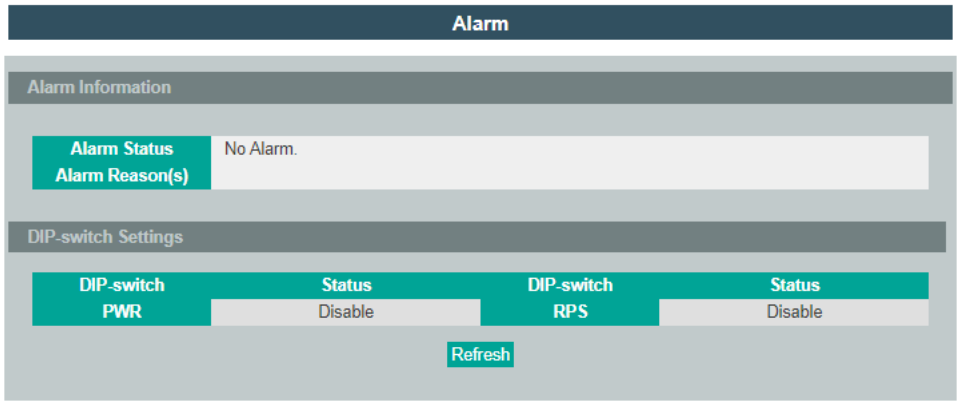
PWR: ON, The ICRL2-M sends alarm message when the main power supply disconnected.

RPS: ON, The ICRL2-M sends alarm message when the redundant power supply disconnected.

7.1.1. CLI Configuration - Alarm

CLI Alarm		
Mode	**Command**	**Description**
enable	show alarm-info	Displays alarm information.

7.1.2. Web Configuration - Alarm



Alarm	
Alarm Information	
Alarm Status	Indicates if there is any alarm events.
Alarm Reason(s)	Displays all of the detail alarm events.
DIP ICRL2-M Settings	
DIP ICRL2-M	Displays the DIP ICRL2-M name.
Status	Indicates the DIP swich setting for the ICRL2-M current status.
Refresh	Click **Refresh** to reload the running configuration values.

7.2. Port Statistics

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

7.2.1. CLI Configuration - Port Statistics

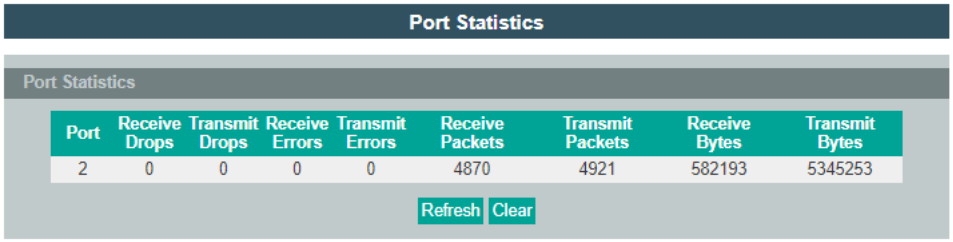
CLI Port Statistics		
Mode	**Command**	**Description**
enable	show port-statistics	Displays the link up ports' statistics.

Example:

L2SWITCH#show port-statistics

	Packets		Bytes		Errors		Drops	
Port	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
7	1154	2	108519	1188	0	0	0	0

7.2.2. Web Configuration - Port Statistics



Port Statistics	
Parameter	**Description**
Port	Select a port or a range of ports to display their statistics.
Receive Drops	Displays the received drop count.
Transmit Drops	Displays the transmitted drop count.
Receive Errors	Displays the received error count.
Transmit Errors	Displays the transmitted error count.
Receive Packets	Displays the received packet count.

Port Statistics (Continued)	
Parameter	**Description**
Transmit Packets	Displays the transmitted packet count.
Receive Bytes	Displays the received byte count.
Transmit Bytes	Displays the transmitted byte count.
Refresh	Click **Refresh** to reload the running configuration values.
Clear	Click **Clear** to clear all of statistics.

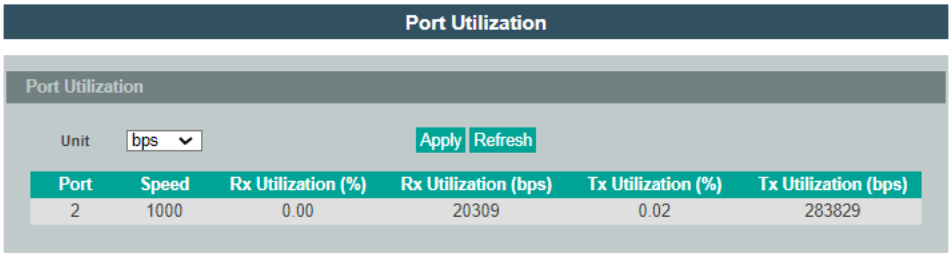
7.3. Port Utilization

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

7.3.1. CLI Configuration - Port Utilization

CLI Port Utilization		
Mode	**Command**	**Description**
enable	show port-utilization (bps | Kbps | Mbps)	Displays the link up ports' traffic utilization.

7.3.2. Web Configuration - Port Utilization



Port Utilization	
Parameter	**Description**
Unit	Select a unit for displaying the port utilization.
Port	Select a port or a range of ports to display their RMON statistics.
Speed	Current port speed.
Rx Utilization (%)	Port receiving traffic utilization in percentage
Rx Utilization (bps)	Port receiving traffic utilization in bits per second
Tx Utilization (%)	Port transmitting traffic utilization in percentage
Tx Utilization (bps)	Port transmitting traffic utilization in bits per second
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

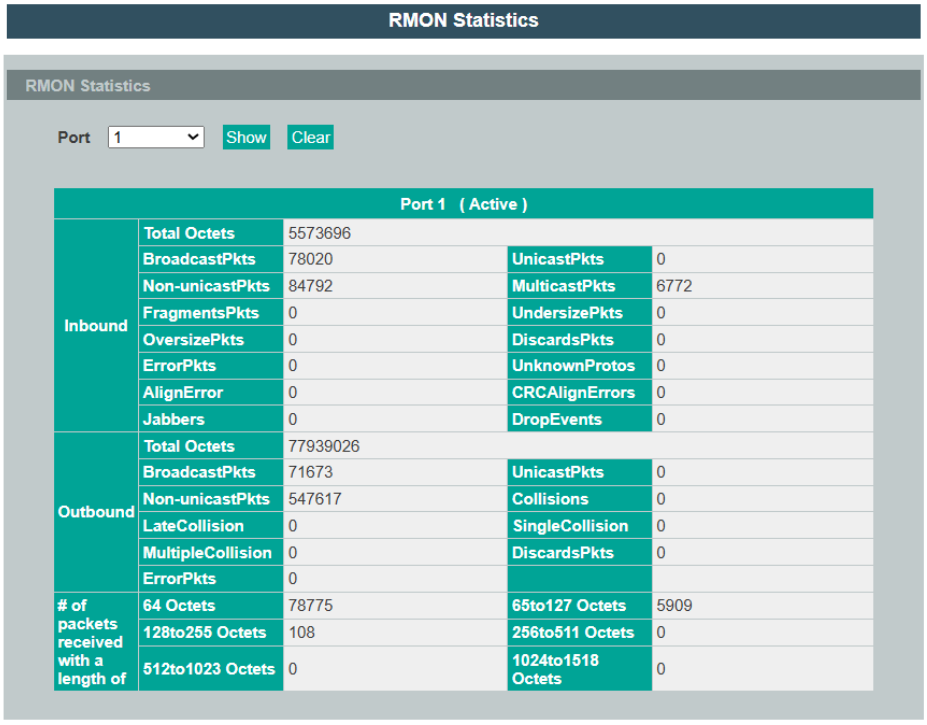
7.4. RMON Statistics

This feature helps users to monitor or clear the port's RMON statistics.

7.4.1. CLI Configuration - RMON Statistics

CLI RMON Statistics		
Mode	**Command**	**Description**
enable	show rmon statistics	Displays the RMON statistics.
enable	configure terminal	Changes the mode to configure mode.
configure	clear rmon statistics [IFNAME]	Clears one port's or all ports' RMON statistics.

7.4.2. Web Configuration - RMON Statistics



RMON Statistics	
Parameter	**Description**
Port	Select a port or a range of ports to display their RMON statistics.
Show	Shows RMON statistics.
Clear	Clear the RMON statistics for the port or a range of ports.

7.5. Traffic Monitor

The function can be enabled / disabled on a specific port or globally be enabled disabled on the ICRL2-M. The function will monitor the broadcast / multicast / broadcast and multicast packets rate. If the packet rate is over the user's specification, the port will be blocked. And if the recovery function is enabled, the port will be enabled after recovery time.

You can configure the recovery time and quarantine times. If a port is blocked by this function, after the time period recovery time, the port isolated first and continue monitored X times (X=quarantine times). If storm traffic is under packet rate all times monitored, the port will be enabled and be monitored again.

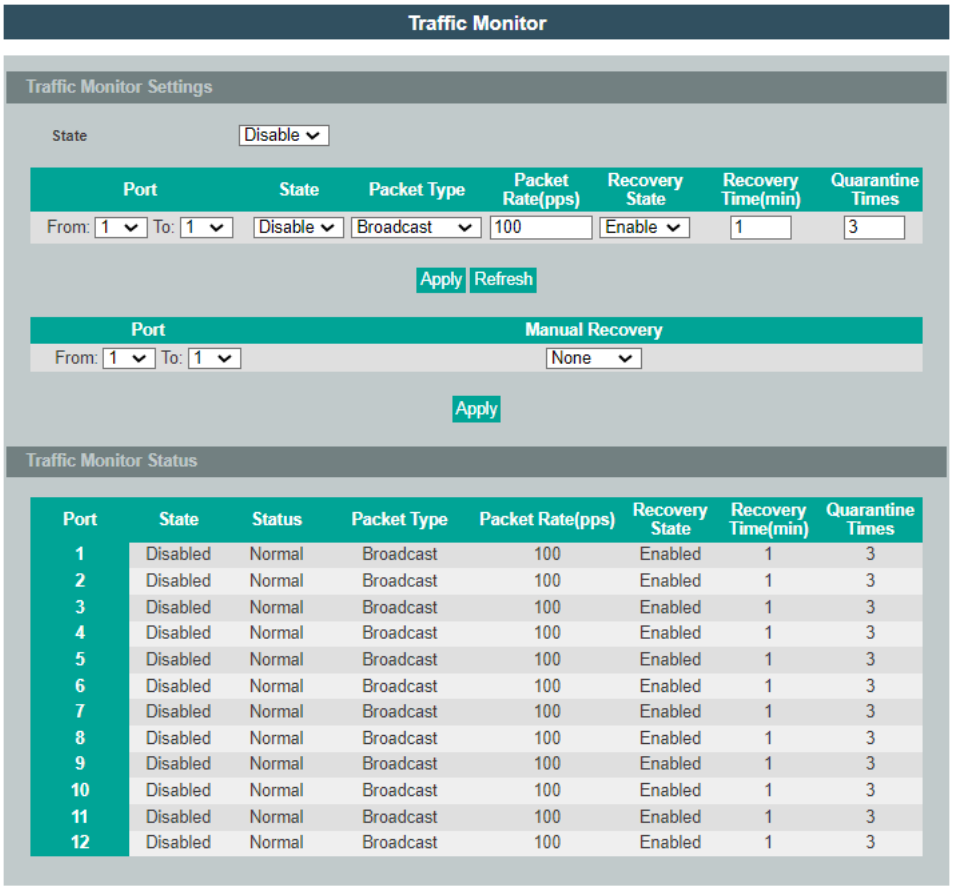
When a port is blocked by this function, the ICRL2-M records a log message in local database or syslog server and send a trap to trap receiver and turn on the ALM LED..

7.5.1. CLI Configuration - Traffic Monitor

CLI / Traffic Monitor		
Mode	**Command**	**Description**
enable	show traffic-monitor	Displays the traffic monitor configurations and current status.
enable	configure terminal	Changes the mode to configure mode.
configure	traffic-monitor (disable | enable)	Enables / disables the traffic monitor on the ICRL2-M.
configure	interface IFNAME	Enters the interface configure mode.
interface	traffic-monitor (disable | enable)	Enables / disables the traffic monitor on the port.
interface	traffic-monitor rate RATE_LIMIT type (bcast | mcast | bcast+mcast)	Configures the packet rate and packet type for the traffic monitor on the port. • **bcast** – Broadcast packets. • **mcast** – Multicast packets. • **bcast+ mcast** - Broadcast packets and Multicast packets.
interface	traffic-monitor recovery (disable | enable)	Enables / disables the recovery function for the traffic monitor on the port.
interface	traffic-monitor recovery time <1-60>	Configures the recovery time for the traffic monitor on the port.
interface	traffic-monitor quarantine times <1-20>	Configures the quarantine times for the traffic monitor on the port.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	traffic-monitor (disable | enable)	Enables / disables the traffic monitor on the port.

CLI / Traffic Monitor (Continued)		
Mode	**Command**	**Description**
if-range	traffic-monitor rateRATE_LIMIT type (bcast | mcast | bcast+mcast)	Configures the packet rate and packet type for the traffic monitor on the port. • **bcast** – Broadcast packets. • **mcast** – Multicast packets. • **bcast+ mcast** - Broadcast packets and Multicast packets.
if-range	traffic-monitor recovery (disable | enable)	Enables / disables the recovery function for the traffic monitor on the port.
if-range	traffic-monitor recovery time <1-60>	Configures the recovery time for the traffic monitor on the port.
if-range	traffic-monitor quarantine times <1-20>	Configures the quarantine times for the traffic monitor on the port.

7.5.2. Web Configuration - Traffic Monitor



Traffic Monitor	
Parameter	**Description**
State	Globally enables / disables the traffic monitor function.
Port	The port range which you want to configure.
State	Enables / disables the traffic monitor function on these ports.
Packet Type	Specify the packet type which you want to monitor.
Packet Rate	Specify the packet rate which you want to monitor.
Recover State	Enables / disables the recovery function for the traffic monitor function on these ports.
Recovery Time	Configures the recovery time for the traffic monitor function on these ports.(Range: 1 – 60 minutes)

Traffic Monitor (Continued)	
Parameter	**Description**
Quarantine Times	Configures the quarantine times for the traffic monitor on these ports. (Range: 1 – 20 times)
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Manual Recovery	Select **Unblock** to enable these ports blocked by traffic monitor.
Apply	Click **Apply** to change the settings.

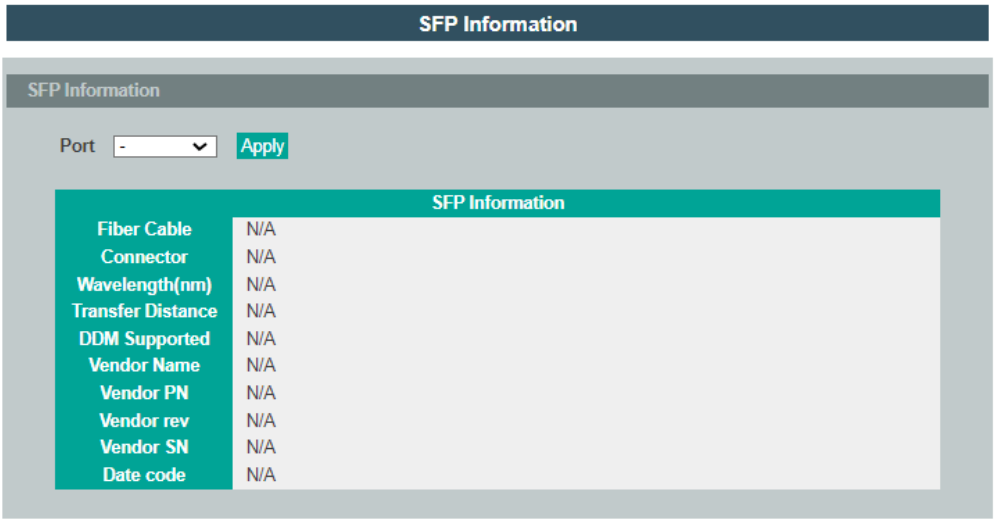
7.6. SFP Information

The SFP information allows user to know the SFP module's information, such as vendor name, connector type, revision, serial number, manufacture date, and to know the DDMI information if the SFP modules have supported the DDMI function.

7.6.1. CLI Configuration - SFP Information

CLI SFP Information		
Mode	**Command**	**Description**
enable	show sfp info port PORT_ID	Displays the SFP information.
enable	show sfp ddmi port PORT_ID	Displays the SFP DDMI status.

7.6.2. Web Configuration - SFP Information



SFP Information	
Parameter	**Description**
SFP Information	
Port	Select a port number to configure.
Apply	Click **Apply** to display the SFP information.
SFP Information	
Fiber Cable	To indicate if the fiber cable is connected.
Connector	Code of optical connector type.
Vendor Name	SFP vendor name.
Vendor PN	Part Number.
Vendor rev	Revision level for part number.
Vendor SN	Serial number (ASCII).
Date Code	Manufacturing date code.

Note: *If the fiber cable is not connected, the Rx Power fields are not available.*

7.7. DI/DO Interface

7.7.1. CLI - DI/DO Interface Settings

DI/DO Interface Settings		
Mode	**Command**	**Description**
enable	show di_interface	Displays the DI/DO interface configurations and current status.
configure	di_interface state (disable | enable)	Disables / enables the global DI/DO interface.
configure	di_interface id <1-2> enable-state (disable | enable)	Disables / enables functionalities of the specific DI interface ID on the ICRL2-M.
configure	di_interface id <1-2> normal-status (open | close)	Configures the default state as the open circuit (Normally Open, NO) or as the close circuit (Normally Closed, NC) for the specific DI interface ID. open – The normal default state is “open” circuit and the abnormal state is “close” (short) circuit. close – The normal default state is “close”.
configure	di_interface id <1-2> alarm-relay (yes | no)	Configures the alarm relay function for the specific DI interface ID. yes – The system will trigger the alarm relay and put the DO interface into “close” state when the specific DI interface is not at normal state.
configure	di_interface id <1-2> alarm-trap (yes | no)	Configures the alarm trap function for the specific DI interface ID. yes – The system will send a SNMP trap to trap receiver and put the DO interface into “close” state when the specific DI interface is not at normal state.
configure	di_interface id <1-2> alarm-syslog-email (yes | no)	Configures the alarm syslog and e-Mail functions for the specific DI interface ID. yes – The system will send a log message to syslog server and mail server and put the DO interface into “close” state when the specific DI interface is not at normal state.

Example:

```
L2SWITCH#show di_interface

The Global Digital State: Disabled

Digital Input(DI)-1
  Current Status       : Open
  ==============================
  The State            : Disabled
  Set Normal Status    : Open
  Enable Alarm Relay   : Yes
  Enable Trap          : Yes
```

```
  Enable Syslog, E-Mail : Yes

Digital Input(DI)-2
  Current Status       : Open
  ==============================
  The State            : Disabled
  Set Normal Status    : Open
  Enable Alarm Relay   : Yes
  Enable Trap          : Yes
  Enable Syslog, E-Mail : Yes

Digital Output(DO)
  Current Status       : Open
  ==============================

L2SWITCH#configure terminal
L2SWITCH(config)#di_interface state enable
Success!

L2SWITCH(config)#di_interface id 1 enable-state enable
Success!

L2SWITCH(config)#di_interface id 1 normal-status close
Success!

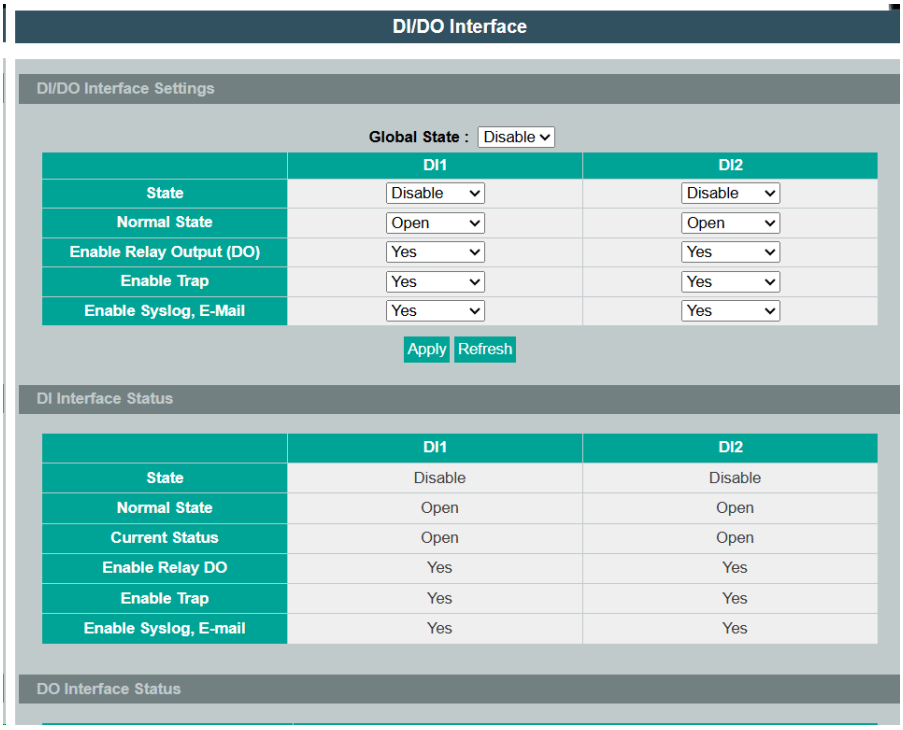
L2SWITCH(config)#di_interface id 1 alarm-relay yes
Success!

L2SWITCH(config)#di_interface id 1 alarm-trap no
Success!

L2SWITCH(config)#di_interface id 1 alarm-syslog-email no
Success!

L2SWITCH(config)#
```

7.7.2. Web Configuration - DI/DO Interface



DI/DO Interface	
Parameter	**Description**
DI/DO Interface Settings	
State	Select **Disable** to disable the global DI/DO Interface. (default). Select **Enable** to enable the global DI/DO Interface.
Normal State	Select **Open** to configure the default state as the open circuit (Normally Open, NO) on the specific DI interface. (default). Select **Close** to configure the default state as the close circuit (Normally Closed, NC) on the specific DI interface.
Enable Relay Output (DO)	Select **Yes** to enable the alarm relay functionality on the specific DI interface. (default). Select **No** to disable the alarm relay functionality on the specific DI interface.
Enable Trap	Select **Yes** to enable the alarm trap functionality on the specific DI interface. (default). Select **No** to disable the alarm trap functionality on the specific DI interface.
Enable Syslog, E-Mail	Selecs **Yes** to enable the alarm syslog/e-Mail functionality on the specific DI interface. (default). Select **No** to disable the alarm syslog/e-Mail functionality on the specific DI interface.

DI/DO Interface (Continued)	
Parameter	**Description**
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

8. Management

8.1. SNMP

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

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

Support below MIBs:

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

SNMP community act like passwords and are used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default SNMP community is “public” for both SNMP v1 and SNMP v2c before SNMP v3 is enabled. Once SNMP v3 is enabled, the communities of SNMP v1 and v2c have to be unique and cannot be shared.

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

- Network ID = (Host IP & Mask).
- User need only input the network ID and leave the host ID to 0. If user has input the host ID, such as 192.168.1.102, the system will reset the host ID, such as 192.168.1.0

Note: *Allow user to configure the community string and rights only.*

User configures the Community String and the Rights and the Network ID of Trusted Host=0.0.0.0, Subnet Mask=0.0.0.0. It means that all hosts with the community string can access the ICRL2-M.

SNMP Default Settings	
SNMP	disabled.
System Location	L2SWITCH. (Maximum length 64 characters)
System Contact	None. (Maximum length 64 characters)
System Name	None. (Maximum length 64characters)
Trap Receiver	None
Community Name	None
Maximum entry for community	3
Maximum entry for trap receiver	5

8.1.1. SNMP

8.1.1.1. SNMP / SNMP Settings

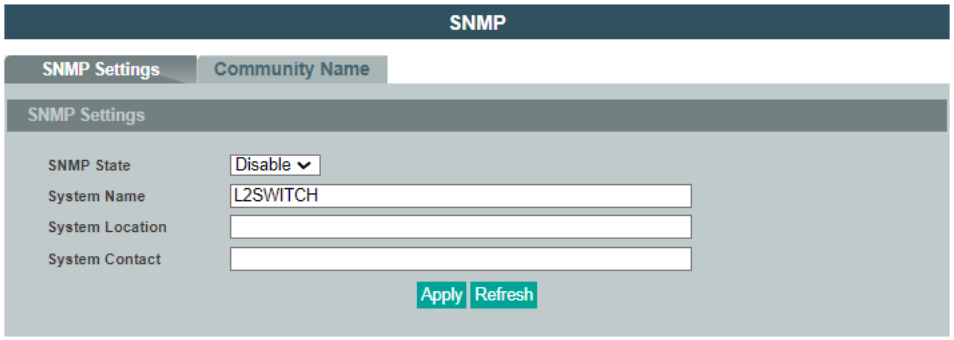
8.1.1.1.1. CLI Configurations - SNMP / SNMP Settings

CLI Management / SNMP / SNMP Settings		
Mode	**Command**	**Description**
enable	show snmp	Displays the SNMP configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	snmp (disable | enable)	Disables/enables the SNMP on the ICRL2-M.
configure	snmp system-contact STRING	Configures contact information for the system.
configure	snmp system-location STRING	Configures the location information for the system.
configure	snmp system-name STRING	Configures a name for the system. (The System Name is same as the host name)
configure	no snmp system-contact STRING	Resets the contact information for the system.
configure	no snmp system-location STRING	Resets the location information for the system.
configure	no snmp system-name STRING	Resets the system name for the system.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#snmp enable
L2SWITCH(config)#snmp community public rw trusted-host 192.168.200.106/24
L2SWITCH(config)#snmp trap-receiver 192.168.200.106 v2c public
L2SWITCH(config)#snmp system-contact IT engineer
L2SWITCH(config)#snmp system-location Branch-Office

8.1.1.1.2. Web Configuration - SNMP / SNMP Settings



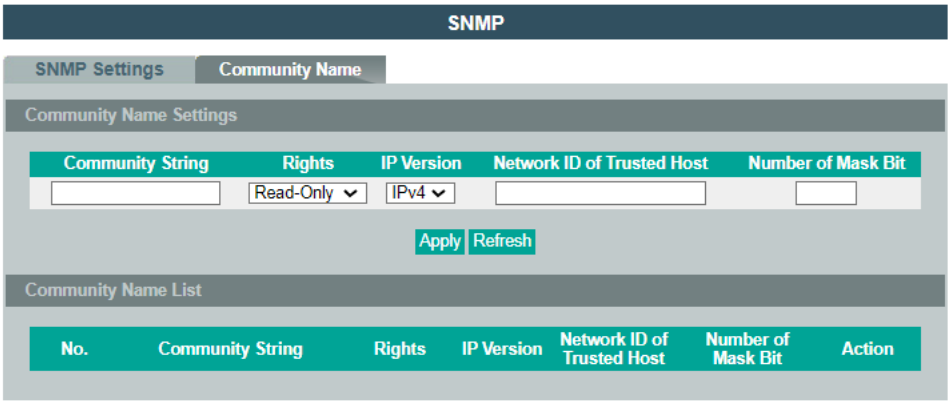
SNMP / SNMP Settings	
Parameter	**Description**
SNMP State	Select Enable to activate SNMP on the ICRL2-M. Select Disable to not use SNMP on the ICRL2-M.
System Name	Type a System Name for the ICRL2-M. (The System Name is same as the host name.)
System Location	Type a System Location for the ICRL2-M.
System Contact	Type a System Contact for the ICRL2-M.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

8.1.1.2. SNMP / SNMP / Community Name

8.1.1.2.1. CLI Configurations - SNMP / SNMP Community Name

CLI SNMP / SNMP / Community Name		
Mode	**Command**	**Description**
enable	show snmp	Displays the SNMP configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	snmp community STRING (ro | rw) trusted-host IPADDR	Configures the SNMP community name.

8.1.1.2.2. Web Configuration - SNMP / SNMP / Community Name



SNMP / SNMP / Community Name	
Parameter	**Description**
Community Name Settings	
Community String	Enter a Community string, this will act as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Rights	Select Read-Only to allow the SNMP manager using this string to collect information from the ICRL2-M. Select Read-Write to allow the SNMP manager using this string to create or edit MIBs (configure settings on the ICRL2-M).

SNMP / SNMP / Community Name (Continued)	
Parameter	**Description**
Network ID of Trusted Host	Type the IP address of the remote SNMP management station in dotted decimal notation, for example 192.168.1.0.
Mask	Type the subnet mask for the IP address of the remote SNMP management station in dotted decimal notation, for example: 255.255.255.0.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Community Name List	
Action	Click Delete to remove a specific Community String.

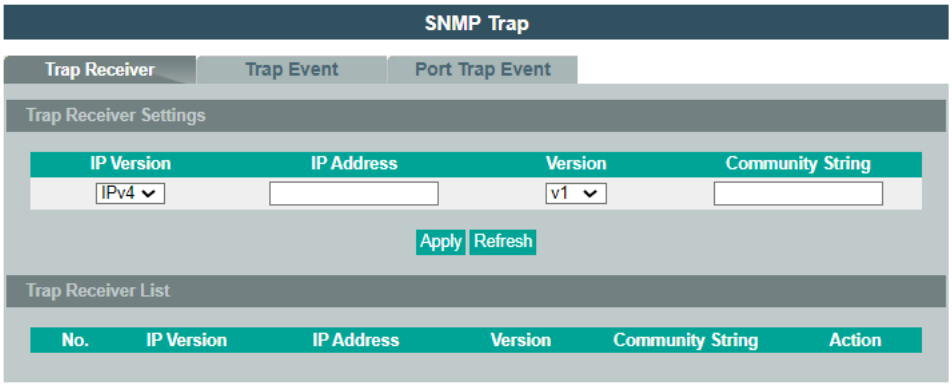
8.1.2. SNMP / SNMP Trap / Trap Receiver

8.1.2.1. SNMP / SNMP Trap / Trap Receiver

8.1.2.1.1. CLI Configurations - SNMP / SNMP Trap / Trap Receiver

CLI Management SNMP / SNMP Trap / Trap Receiver		
Mode	**Command**	**Description**
enable	show snmp	Displays the SNMP configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	snmp trap-receiver IPADDR (v1 | v2c) COMMUNITY	Configures the trap receiver's configurations, including the IP address, version (v1 or v2c) and community.
configure	snmp trap-ipv6-receiver IPADDR (v1 | v2c) COMMUNITY	Configures the trap IPv6 receiver's configurations, including the IP address, version (v1 or v2c) and community.

8.1.2.1.2. Web Configuration - SNMP / SNMP Trap / Trap Receiver



SNMP / SNMP Trap / Trap Receiver	
Parameter	**Description**
IP Address	Enter the IP address of the remote trap station in dotted decimal notation.
Version	Select the version of the Simple Network Management Protocol to use. v1 or v2c.
Community String	Specify the community string used with this remote trap station.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Trap Receiver List	
Action	Click **Delete** to remove a configured trap receiver station.

8.1.2.2. SNMP / SNMP Trap / Trap Event

The features allow users to enable/disables individual trap notification.

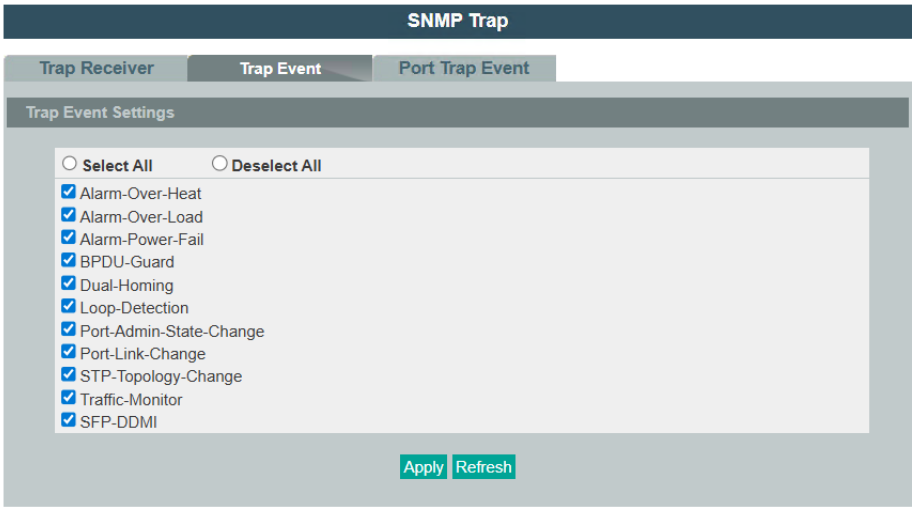
SNMP / SNMP Trap / Trap Event	
Trap Event	**Description**
alarm-over-heat	Trap when system's temperature is too high.
alarm-over-load	Trap when system is over load.
alarm-power-fail	Trap when system power is over voltage/under voltage. RPS over voltage/RPS under voltage.
bpdu	Trap when port is blocked by BPDU Guard/BDPU Root Guard/BPDU port state changed.
dual-homing	Trap when port is blocked by Dual Homing.
dying-gasy	Trap when system is power off.
loop-detection	Trap when port is blocked by Loop Detection.
pd-alive	Trap when PD device has no responses.
port-admin-state-change	Trap when port is enabled/disable by administrator.
port-link-change	Trap when port is link up/down change.
power-source-change	Trap when the power source has been changed. (AC to DC or DC to AC)
stp-topology-change	Trap when the STP topology change.
traffic-monitor	Trap when port is blocked by Traffic Monitor.
xpress-ring	Trap when port is blocked by Xpress Ring.

8.1.2.2.1. CLI Configurations - SNMP / SNMP Trap / Trap Event

CLI SNMP Trap / Trap Event		
Mode	**Command**	**Description**
enable	show snmp trap-event	Displays the SNMP configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	snmp trap-event alarm-over-heat (disable/enable)	Enables/disables the alarm-over-heat trap.
configure	snmp trap-event alarm-over-load (disable/enable)	Enables/disables the alarm-over-load trap.
configure	snmp trap-event alarm-power-fail (enable/enable)	Enables/disables the alarm-power-fail trap.

CLI SNMP Trap / Trap Event (Continued)		
Mode	**Command**	**Description**
configure	snmp trap-event bpdu (disable/enable)	Enables/disables the BPDU port state change/BPDU Root Guard/BPDU Guard trap.
configure	snmp trap-event dual-homing (disable/enable)	Enables/disables the dual-homing trap.
configure	snmp trap-event dying-gasp (disable/enable)	Enables/disables the dying-gasp trap.
configure	snmp trap-event loop-detection (disable/enable)	Enables/disables the loop-detection trap.
configure	snmp trap-event pd-alive (disable/enable)	Enables/disables the PD alive trap.
configure	snmp trap-event port-admin-state-change (disable/enable)	Enables/disables the port-admin-state-change trap.
configure	snmp trap-event port-link-change (disable/enable)	Enables/disables the port-link-change trap.
configure	snmp trap-event power-source-change (disable/enable)	Enables/disables the power-source-change trap.
configure	snmp trap-event stp-topology-change (disable/enable)	Enables/disables the stp-topology-change trap.
configure	snmp trap-event traffic-monitor (disable/enable)	Enables/disables the traffic-monitor trap.
configure	snmp trap-event xpress-ring (disable/enable)	Enables/disables the xpress-ring trap.

8.1.2.2.2. Web Configuration - SNMP / SNMP Trap / Trap Event



SNMP / SNMP Trap / Trap Event	
Parameter	**Description**
Select all	Enables all of trap events.
Deselect All	Disables all os trap events.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

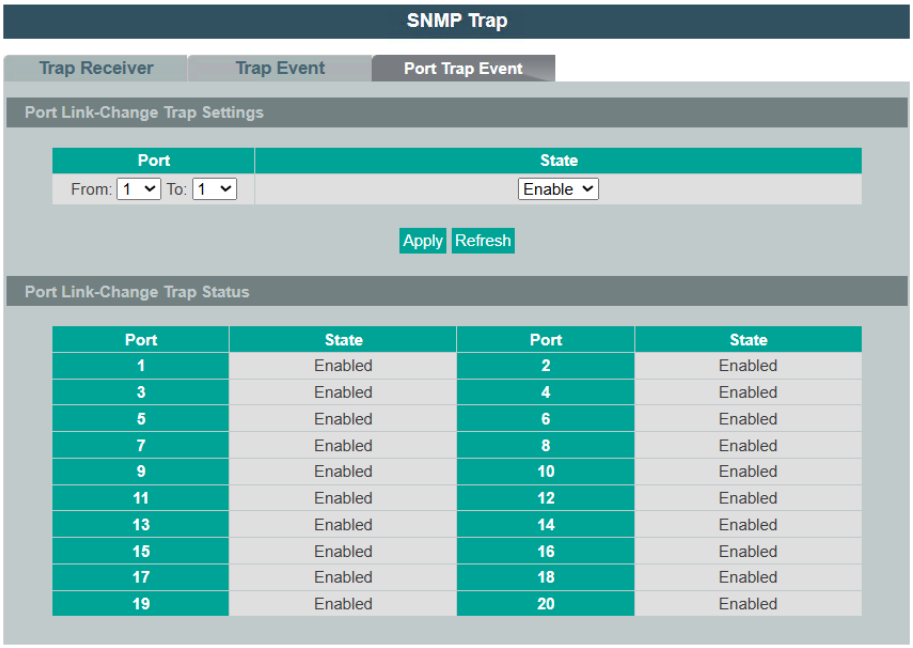
8.1.2.3. SNMP / SNMP Trap / Port Trap Event

The features allow users to enable/disables port-link-change trap notification by individual port.

8.1.2.3.1. CLI Configurations - SNMP / SNMP Trap / Port Trap Event

CLI SMNP / SNMP Trap / Port Trap Event		
Mode	**Command**	**Description**
enable	show snmp port-link-change-trap	Displays the SNMP port link-change trap configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	interface IFNAME	Enters the interface configure mode.
interface	snmp port-link-change-trap	Enables the link change trap on the specific port.
interface	no snmp port-link-change-trap	Disables the link change trap on the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	Enters the if-range configure mode.
if-range	snmp port-link-change-trap	Enables the link change trap on the specific ports.
if-range	no snmp port-link-change-trap	Disables the link change trap on the specific ports.

8.1.2.3.2. Web Configuration - SNMP / SNMP Trap / Port Trap Event



SNMP / SNMP Trap / Port Trap Event	
Parameter	**Description**
Port	Selects the range of ports.
State	Selects the state for the ports.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

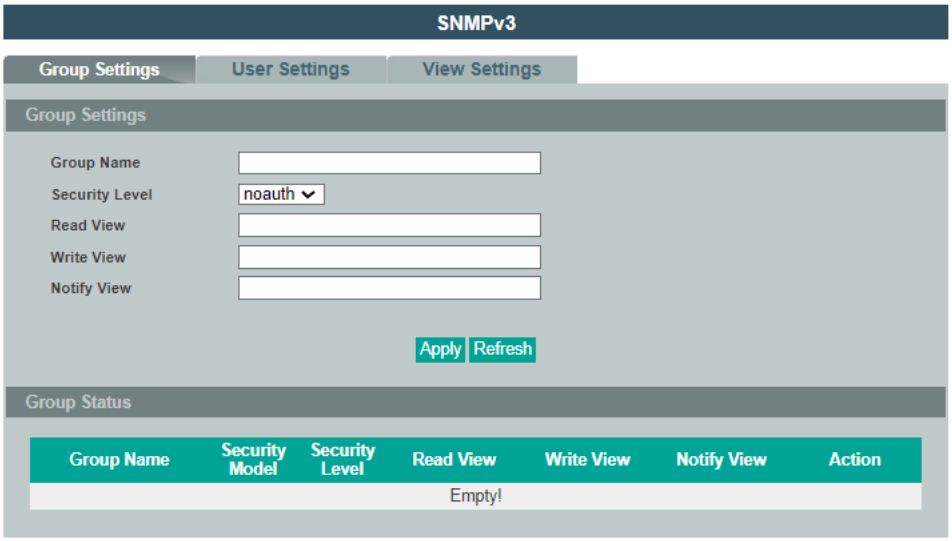
8.1.3. SNMP / SNMPv3

8.1.3.1. SNMP / SNMPv3 / Group Settings

8.1.3.1.1. CLI Configurations - SNMP / SNMPv3 / Group Settings

CLI SNMP / SNMPv3 / Group Settings		
Mode	**Command**	**Description**
enable	show snmp group	Displays all snmp v3 groups.
enable	configure terminal	Changes the mode to configure mode.
configure	snmp group GROUPNAME noauth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of non- authentication.
configure	snmp group GROUPNAME auth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication.
configure	snmp group GROUPNAME priv (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication and encryption.
configure	no snmp group GROUPNAME	Removes a v3 group from ICRL2-M.

8.1.3.1.2. Web Configuration - SNMP / SNMPv3 / Group Settings



SNMP/ SNMPv3 / Group Settings	
Parameter	**Description**
Group Name	Enter the v3 user name.
Security Level	Select the security level of the v3 group to use.
Read View	If a group is defined without a read view than all objects are available to read. (default value is none.)
Write View	If no write or notify view is defined, no write access is granted and no objects can send notifications to members of the group. (default value is none.)
Notify View	By using a notify view, a group determines the list of notifications its users can receive.(default value is none.)
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
SNMPv3 Group Status	
Group Name	Displays the v3 user name.
Security Model	Displays the security model of the group. Always displayed v3: User-based Security Model (USM)
Security Level	Displays the security level to this group.
Read View Write View Notify View	Display the View list of this group.
Action	Click Delete to remove a v3 group.

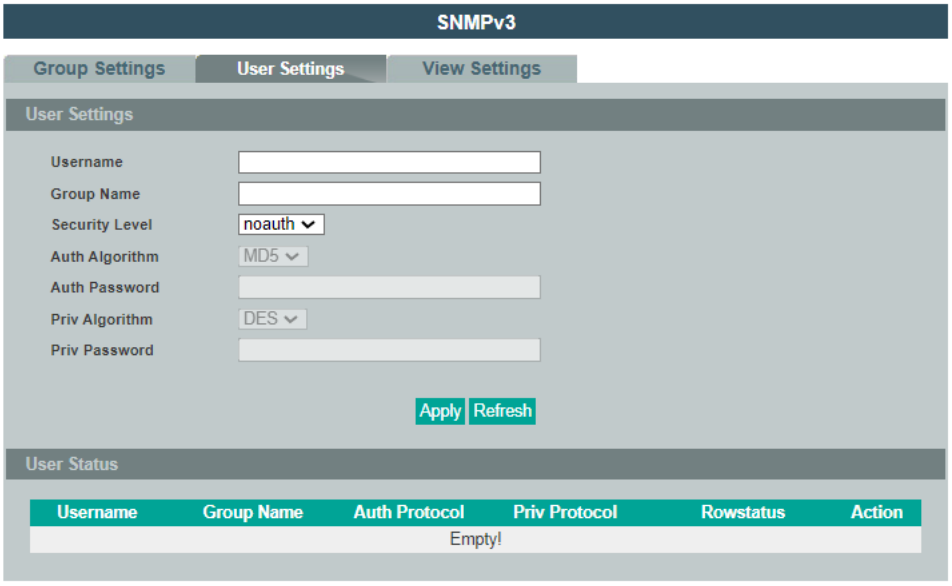
8.1.3.2. SNMP / SNMPv3 / User Settings

8.1.3.2.1. CLI Configurations - SNMP / SNMPv3 / User Settings

CLI SNMP / SNMPv3 / User Settings		
Mode	**Command**	**Description**
enable	show snmp user	Displays all snmp v3 users.
enable	configure terminal	Changes the mode to configure mode.
configure	snmp user USERNAME GROUPNAME noauth	Configures v3 user of non- authentication.
configure	snmp user USERNAME GROUPNAME auth (MD5 | SHA) STRINGS	Configures v3 user of authentication.

CLI SNMP / SNMPv3 / User Settings (Continued)		
Mode	**Command**	**Description**
configure	snmp user USERNAME GROUPNAME priv (MD5 | SHA) STRINGS des STRINGS	Configures v3 user osnmf authentication and encryption.
configure	no snmp user USERNAME GROUPNAME	Removes a v3 user from ICRL2-M.

8.1.3.2.2. Web Configuration - SNMP / SNMPv3 / User Settings



SNMP / SNMPv3 / User Settings	
Parameter	**Description**
User Name	Enter the v3 user name.
Group Name	Map the v3 user name into a group name.
Security Level	Select the security level of the v3 user to use. • **noauth** means no authentication and no encryption. • **auth** means messages are authenticated but not encrypted. • **priv** means messages are authenticated and encrypted.
Auth Algorithm	Select **MD5** or **SHA** Algorithm when security level is **auth** or **priv**.
Auth Password	Set the password for this user when security level is **auth** or **priv**. (pass phrases must be at least 8 characters long!)
Priv Algorithm	Select **DES** encryption when security level is **priv**.

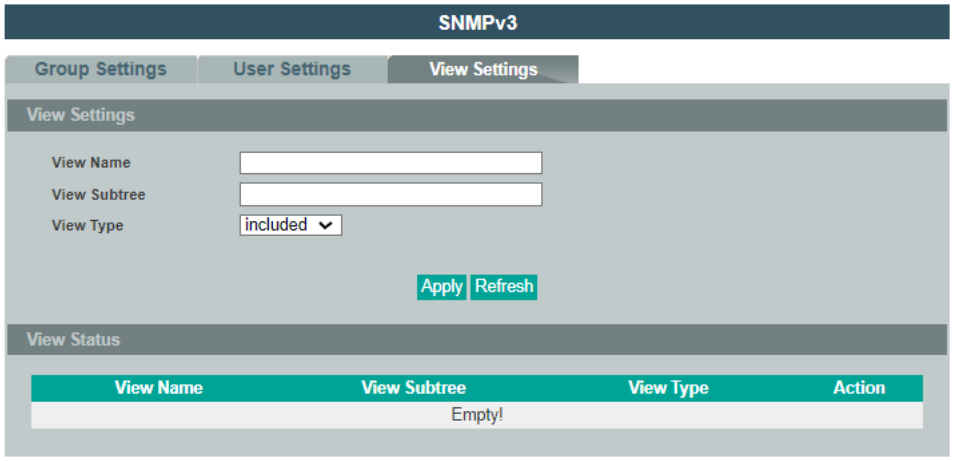
SNMP / SNMPv3 / User Settings (Continued)	
Parameter	**Description**
Priv Password	Set the password for this user when security level is **priv**. (pass phrases must be at least 8 characters long!)
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
SNMPv3 User Status	
User Name	Displays the v3 user name.
Group Name	Displays the group name which the v3 user mapping.
Auth Protocol Priv Protocol	Display the security level to this v3 user.
Rowstatus	Displays the v3 user row status.
Action	Click Delete to remove a v3 user.

8.1.3.3. SNMP / SNMPv3 / View Settings

8.1.3.3.1. CLI Configurations - SNMP / SNMPv3 / View Settings

CLI SNMP / SNMPv3 / View Settings		
Mode	**Command**	**Description**
enable	show snmp view	Displays all snmp v3 view.
enable	configure terminal	Changes the mode to configure mode.
configure	snmp view VIEWNAME STRINGS (included | excluded)	To identify the subtree.
configure	no snmp view VIEWNAME STRINGS	Removes a v3 view from ICRL2-M.

8.1.3.3.2. Web Configuration - SNMP / SNMPv3 / View Settings



SNMP / SNMPv3 / View Settings	
Parameter	**Description**
View Settings	
View Name	Enter the v3 view name for creating an entry in the SNMPv3 MIB view table.
View Subtree	The OID defining the root of the subtree to add to (or exclude from) the named view.
View Type	Select included or excluded to define subtree adding to the view or not.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
View Status	
View Name	Displays the v3 view name.
View Subtree	Displays the subtree.
View Type	Displays the subtree adding to the view or not.
Action	Click Delete to remove a v3 view.

8.2. Auto Provision

Auto provision is a service that service provider can quickly, easily and automatically configure remote device or doing firmware upgrade at remote side.

1. When the Auto Provision is enabled, the ICRL2-M downloads the auto provision information file from the auto provision server first.

   The file name is followed below naming rule:

   Model_Name_Autoprovision.txt

   For Example: ICRL2-M_Autoprovision.txt

   The contents of the file are listed below:

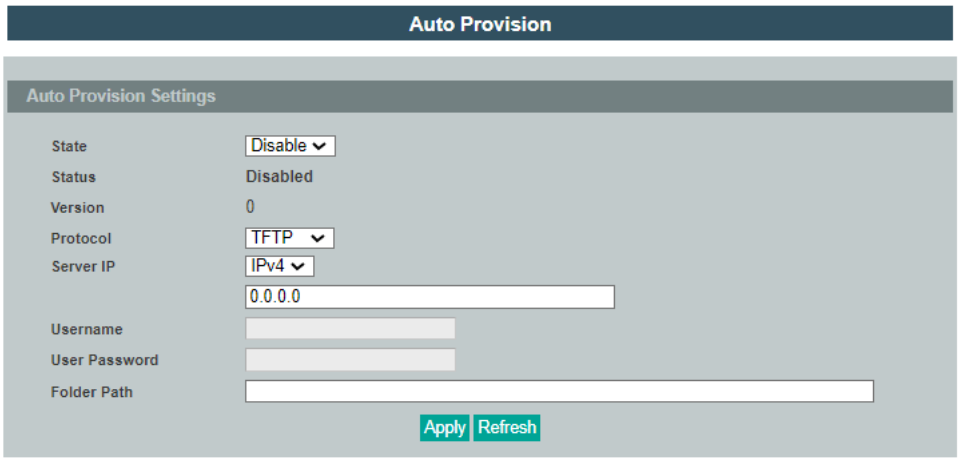
   AUTO_PROVISION_VER=1
   Firmware_Upgrade_State=1
   Firmware_Version=8648-000-1.4.1.S0
   Firmware_Image_File=8648-000-1.4.1.S0.fw
   Firmware_Reboot=1
   Global_Configuration_State=0
   Global_Configuration_File=8648-000-1.1.0.S0.save
   Global_Configuration_Reboot=0
   Specific_Configuration_State=0
   Specific_Configuration_Reboot=0
2. If AUTO_PROVISION_VER is biggest than current auto provision version, do step 3; otherwise, wait 24 hours and go back to step 1.
3. If the Firmware_Upgrade_State =1, do step 4; otherwise, do step 6.
4. If the Firmware_Version is difference than current firmware version, download the Firmware_Image_File and upgrade firmware.
5. If upgrade firmware succeeded and Firmware_Reboot=1, let reboot_flag=1.
6. If the Global_Configuration_State =1, download the Global_Configuration_File and upgrade configuration; otherwise, do step 8.
7. If upgrade configutation succeeded and Global_Configuration_Reboot =1, let reboot_flag=1.
8. If the Specific_Configuration_State =1, download the specific configuration file and upgrade configuration; otherwise do step 10. The naming is “Model_Name _” with 12-bit MAC digits ,example for following is “8648-A_00e04c8196b9.txt”
9. If upgrade configutation succeeded and Specific_Configuration_Reboot =1, let reboot_flag=1.
10. If reboot_flag=1, save running configuration and reboot the ICRL2-M; otherwise, wait 24 hours and go back to step 1.

Default Settings	
Auto provision configuration profile:	
Active	Disable
Version	0
Protocol	FTP
FTP user/pwd	/
Folder	
Server address	

8.2.1. CLI Configurations - Auto Provision

CLI Management / Auto Provision		
Mode	**Command**	**Description**
enable	show auto-provision	Displays the current auto provision configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	auto-provision	Enters the auto-provision mode.
auto-provision	show	Displays the current auto provision configurations.
auto-provision	active (enable | disable)	Enables/disables the auto provision function.
auto-provision	server-addressIPADDR	Configures the auto provision server's IP.
auto-provision	protocol (tftp | http | ftp)	Configures the upgrade protocol.
auto-provision	FTP-user username STRING password STRING	Configures the username and password for the FTP server.
auto-provision	folder STRING	Configures the folder for the auto provision server.
auto-provision	no folder	Configures the folder to default.
auto-provision	no FTP-user	Configures the username and password to default.

8.2.2. Web Configuration - Auto Provision



8/19/25

Auto Provision	
Parameter	**Description**
State	Enables/Disables auto provisioning.
Status	Displays if auto provisioning is enabled or disabled.
Version	Version of the auto provisioning file currently used. Correlates to the AUTO_PROVISION_VER value in the auto provision text file on the server.
Protocol	The protocol used to fetch the auto provision text file. Can be TFTP, FTP, or HTTP.
Server IP	The IP address of the TFTP, FTP, or HTTP server hosting the auto provision text file.
Username	The user name needed to log into the FTP server. Only used if Protocol is set to FTP.
User Password	The password needed to log into the FTP server. Only used if Protocol is set to FTP.
Folder Path	The path to the auto provision text file on the server.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

8.3. Mail Alarm

The feature sends an e-mail trap to a predefined administrator when some events occur. The events are listed below:

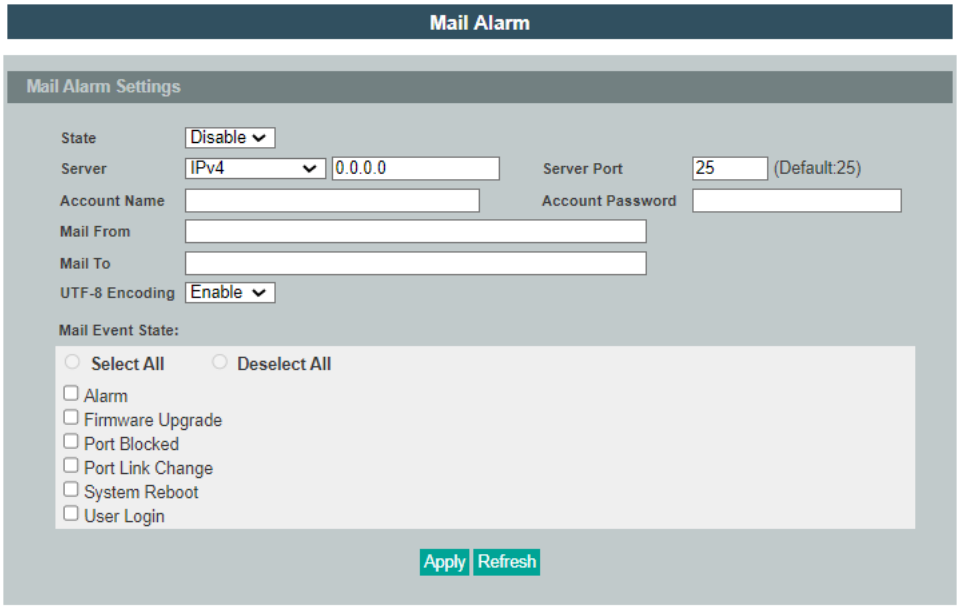
Mail Alarm Events	
Events	**Description**
System Reboot	The system warn start or cold start.
Port Link Change	A port link up or down.
Configuration Change	The system configurations in the NV-RAM have been updated.
Firmware Upgrade	The system firmware image has been updated.
User Login	A user login the system.
Port Blocked	A port is blocked by looping detection or BPDU Guard.

Mail Alarm Information			
Default Ports	**Server**	**Authentication**	**Port**
SMTP Server (Outgoing Messages)	Non-Encrypted	AUTH	25 (or 587)
	Secure (TLS)	StartTLS	587
	Secure (SSL)	SSL	465
POP3 Server (Incoming Messages)	Non-Encrypted	AUTH	110
	Secure (SSL)	SSL	995
Googlemail - Gmail	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	smtp.gmail.com	SSL	465
	smtp.gmail.com	StartTLS	587
POP3 Server (Incoming Messages)	pop.gmail.com	SSL	995
Outlook.com	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	smtp.live.com	StartTLS	587
POP3 Server (Incoming Messages)	pop3.live.com	SSL	995
Yahoo Mail	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	smtp.mail.yahoo.com	SSL	465
POP3 Server (Incoming Messages)	pop.mail.yahoo.com	SSL	995
Yahoo Mail Plus	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	plus.smtp.mail.yahoo.com	SSL	465
POP3 Server (Incoming Messages)	plus.pop.mail.yahoo.com	SSL	995

8.3.1. CLI Configurations - Mail Alarm

CLI Mail Alarm		
Mode	**Command**	**Description**
enable	show mail-alarm	Displays the Mail Alarm configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	mail-alarm (disable | enable)	Disables / enables the Mail Alarm function.
configure	mail-alarm auth-account	Configures the Mail server authentication account.
configure	mail-alarm mail-from	Configures the mail sender.
configure	mail-alarm mail-to	Configures the mail receiver.
configure	mail-alarm server (ip | ipv6 | domain-name) STRINGS server-port VALUE	Configures the mail server IP address / domain name and the TCP port.
configure	mail-alarm server (ip | ipv6 | domain-name) STRINGS server-port default	Configures the mail server IP address / domain name and configures 25 as the server's TCP port.
configure	mail-alarm trap-event (reboot | link-change | config. | firmware | login | port-blocked | alarm) (disable | enable)	Disables / enables mail trap events.
configure	mail-alarm utf8-encoding (disable | enable)	Disables / enables the UTF8 encoding for mail content.

8.3.2. Web Configuration - Mail Alarm



Mail Alarm	
Parameter	**Description**
State	Enable / disable the Mail Alarm function.
Server	Selects one of below options: • **IP**: The mail server's IP format is IPv4. • **Domain Name**: The mail server's IP format is a domain name.
Server Port	Specifies the TCP port for the SMTP server.
Account Name	Specifies the mail account name.
Account Password	Specifies the mail account password.
Mail From	Specifies the mail sender.
Mail To	Specifies the mail receiver.
UTF-8 Encoding	Enable / disable the UTF-8 encoding for mail content.
Mail Event State	Enables / disables the mail trap event states.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

8.4. Maintenance

8.4.1. Configuration

8.4.1.1. CLI Configurations - Maintenance / Configuration

CLI Maintenance / Configuration		
Mode	**Command**	**Description**
enable	configure terminal	Changes the mode to configure mode.
configure	write memory	Writes current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	Downloads a new copy of configuration file to replace the startup-config from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	Uploads the current startup-config configurations file to a TFTP server.
configure	archive download-running-config <URL PATH>	Downloads a new copy of running configuration file from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	reload default-config	Copies a user-default-config file to replace the startup-config file. ***Note:*** *The system reboots automatically to execute the default configuration.*
configure	archive download-config URL_PATH user-default-config	Downloads configure file to user-default-config.
configure	copy factory-default-config to user-default-config	Copies factory-default-config file to user-default-config file.
configure	copy startup-config to user-default-config	Copies the startup-config file to user-default-config file.

There are three configuration files:

startup-config.
user-default-config.
factory-default-config.

- When users execute the command, write memory, the system will save all of the running configurations to startup-config file.
- When the ICRL2-M boots up, it will load startup-config as the system configurations.
- When users execute the command, reload default-config, the system will copy user-default-config to startup-config.

How to build your own default configuration file?

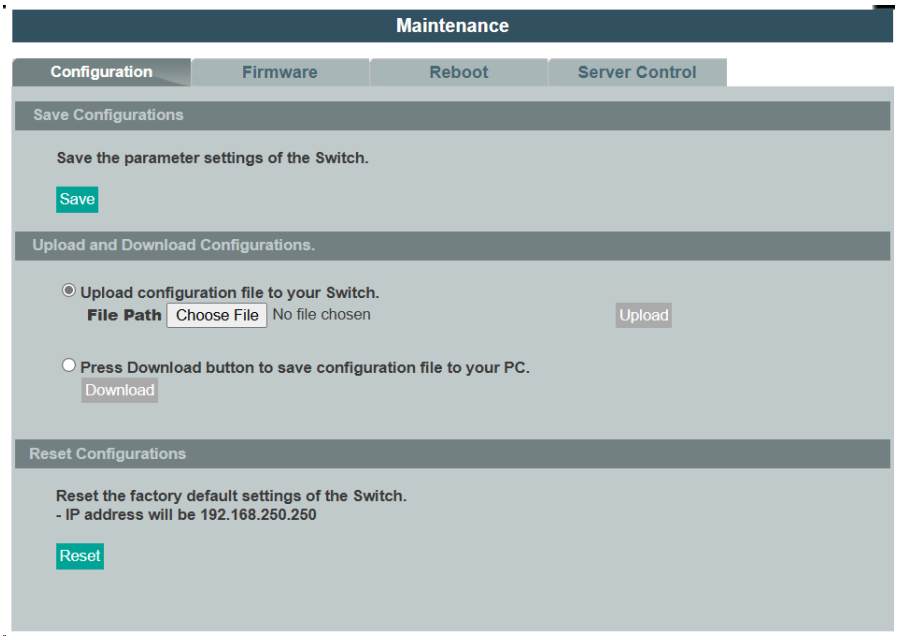
1. You can prepare a configuration file and then do below command,

   archive download-config URL_PATH user-default-config

2. You can login the system with console/Telnet/Http. And then follow below procedures:
   - To setup all configurations what you want.
   - Do the command, write memory, to save them to startup-config file.
   - Do the command, copy startup-config to user-default-config, to copy startup-config file to user-default-config file.

- The factory-default-config file for user special propose.

8.4.1.2. Web Configuration - Maintenance / Configuration



Maintenance / Configuration	
Parameter	**Description**
Save Configurations	
Save	Press the **Save** button to save the current settings to the NV-RAM (flash).
Upload and Download Configurations	
Upload configuration file to your switch	1. Select the **Upload configurations file to your switch.** 2. Choose the path to the saved configuration file. 3. Click the **Upload** button to start the process.
Press Download button to save configuration file to your PC	Click the **Download** button to start the process.
Reset Configuration	
Reset the factory default settings of the Switch. IP address 192.168.250.250	Press the **Reset** button to set the settings to factory default configurations.

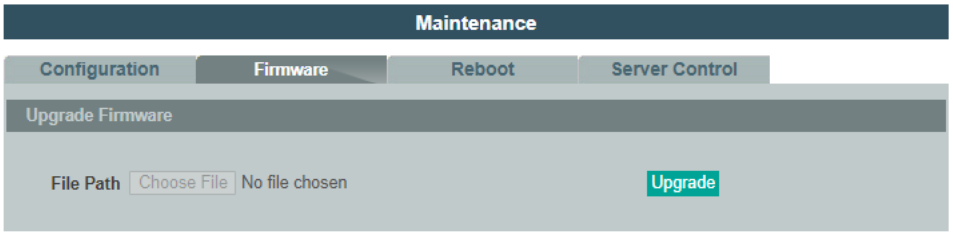
8.4.2. Maintenance / Firmware

8.4.2.1. CLI Configurations - Maintenance / Firmware

CLI Maintenance / Firmware		
Mode	**Command**	**Description**
enable	configure terminal	Changes the mode to configure mode.
configure	archive download-fw <URL PATH>	Downloads a new copy of firmware file from TFTP / FTP / HTTP server. Where <URL PATH> can be: • ftp://user:pass@192.168.1.1/file • http://192.168.1.1/file • tftp://192.168.1.1/file
configure	archive ipv6-download-fw <URL PATH>	Downloads a new copy of firmware file from IPv6 TFTP / FTP / HTTP server. Where <URL PATH> can be: • ftp://user:pass@192.168.1.1/file • http://192.168.1.1/file • tftp://192.168.1.1/file
configure	archive download-secondary-fw <URL PATH>	Downloads a new copy of firmware file for secondary image from TFTP / FTP / HTTP server. Where <URL PATH> can be: • ftp://user:pass@192.168.1.1/file • http://192.168.1.1/file • tftp://192.168.1.1/file
configure	archive ipv6-download-secondary-fw <URL PATH>	Downloads a new copy of firmware file for secondary image from IPv6 TFTP / FTP / HTTP server. Where <URL PATH> can be: • ftp://user:pass@192.168.1.1/file • http://192.168.1.1/file • tftp://192.168.1.1/file

8.4.2.2. Web Configuration - Maintenance / Firmware

Click **Browse** to locate the firmware file to upload and then click **Upgrade** to load the new firmware.



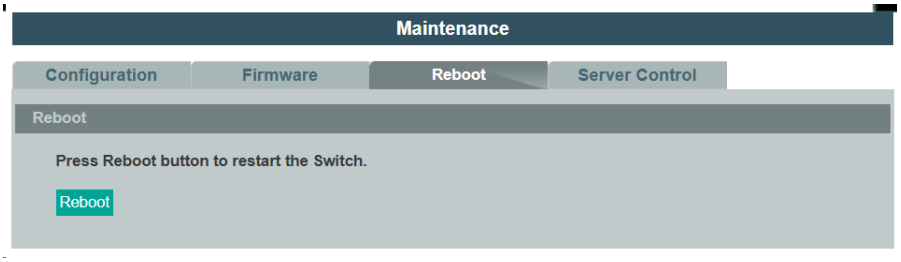
8.4.3. Maintenance / Reboot

8.4.3.1. CLI Configurations - Maintenance / Reboot

CLI Maintenance / Reboot		
Mode	**Command**	**Description**
enable	configure terminal	Changes the mode to configure mode.
configure	reboot	Reboots the system.

8.4.3.2. Web Configuration - Maintenance / Reboot

Reboot allows you to restart the ICRL2-M without physically turning the power off.



Follow these steps to reboot the ICRL2-M.

1. In the Reboot screen, click the **Reboot** button.
2. Click **OK** again and then wait for the ICRL2-M to restart. This takes up to two minutes. This does not affect the ICRL2-M's configuration.

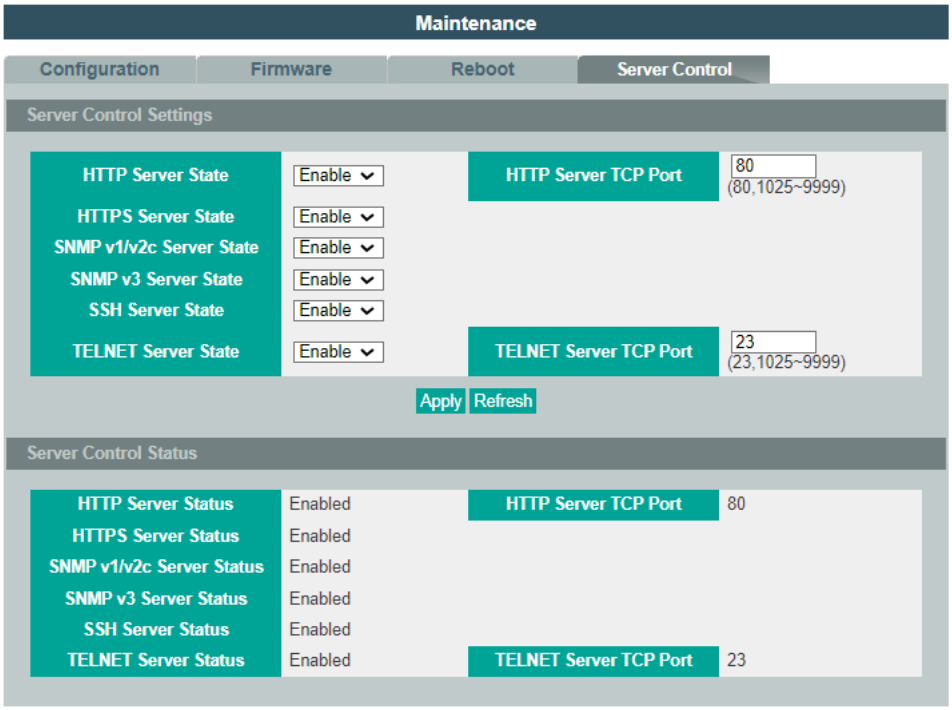
8.4.4. Maintenance / Server Control

The function allows users to enable or disable the SSH or Telnet or Web service individual using the CLI or GUI.

8.4.4.1. CLI Configurations - Maintenance / Server Control

CLI Management / Maintenance / Server		
Mode	**Command**	**Description**
enable	show server status	Displays the current server status.
enable	configure terminal	Changes the mode to configure mode.
configure	http server	Enables the http on the ICRL2-M.
configure	no http server	Disables the http on the ICRL2-M.
configure	http server port VALUE	Configures the TCP port for the HTTP server.
configure	no http server port	Resets the HTTP TCP port to 80.
configure	https server	Enables the https on the ICRL2-M.
configure	no https server	Disables the https on the ICRL2-M.
configure	ssh server	Enables the ssh on the ICRL2-M.
configure	no ssh server	Disables the ssh on the ICRL2-M.
configure	telnet server	Enables the telnet on the ICRL2-M.
configure	no telnet server	Disables the telnet on the ICRL2-M.
configure	telnet server port VALUE	Configures the TCP port for the TELNET server.
configure	no telnet server port	Resets the TELNET TCP port to 23.

8.4.4.2. Web Configuration - Maintenance / Server Control



Maintenance / Server Control	
Parameter	**Description**
HTTP Server State	Select **Enable** or **Disable** to enable or disable the HTTP service.
HTTP Server TCP Port	Configure the TCP port for the HTTP service.
SSH Server State	Select **Enable** or **Disable** to enable or disable the SSH service.
Telnet Server State	Select **Enable** or **Disable** to enable or disable the Telnet service.
TELNET Server TCP Port	Configure the TCP port for the Telnet service.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

8.5. Syslog

The syslog function records some of system information for debugging purpose. Each log message recorded with one of these levels, Alert / Critical / Error / Warning / Notice / Information. The syslog function can be enabled or disabled. The default setting is disabled. The log message is recorded in the ICRL2-M file system. If the syslog server's IP address has been configured, the ICRL2-M sends a copy to the syslog server.

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

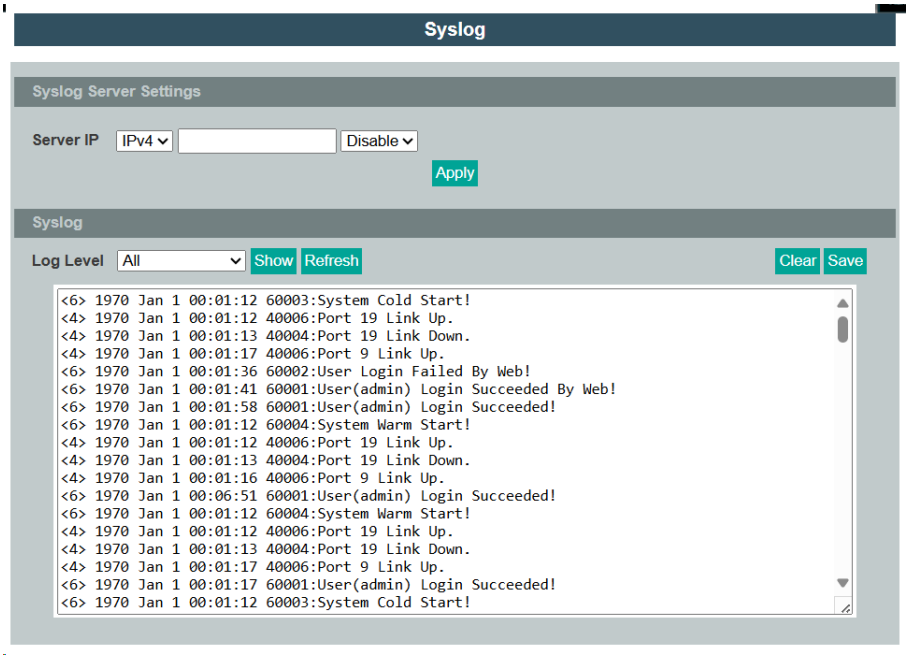
8.5.1. CLI Configurations - Syslog

CLI Syslog		
Mode	**Command**	**Description**
enable	show syslog	Displays the entire log message recorded in the ICRL2-M.
enable	show syslog level LEVEL	Displays the log message with the LEVEL recorded in the ICRL2-M.
enable	show syslog server	Displays the syslog server configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	clear syslog	Clears the syslog message.
configure	syslog-server (disable | enable)	Disables / enables the syslog server function.
configure	syslog-server ipv4-ip IPADDR	Configures the syslog server's IP address in IPv4 format.
configure	syslog-server ipv6-ip IPADDR	Configures the syslog server's IP address in IPv6 format.
configure	syslog-server facility	Configures the syslog facility level.
configure	archive upload-syslog <URL PATH>	Uploads the syslog file to a TFTP server.
configure	archive ipv6-upload-syslog <URL PATH>	Uploads the syslog file to a IPv6 TFTP server.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#syslog-server ipv4-ip 192.168.200.106
L2SWITCH(config)#syslog-server enable

8.5.2. Web Configuration - Syslog



Syslog	
Parameter	**Description**
Server IP	Select IP type for the server's IP. Enter the Syslog server IP address. Select **Enable** to activate ICRL2-M sent log message to Syslog server when any new log message occurred.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Log Level	Select **Alert**/**Critical**/**Error**/**Warning**/**Notice**/**Information** to choose which log message to view.
Clear	Click **Clear** to clear all of log message.
Save	Click **Save** to save all of log message into NV-RAM.

8.6. USB Functions

The USB Functions is used on a network ICRL2-M for automatic execution of tasks, such as firmware upgrade, download configurations and system log.

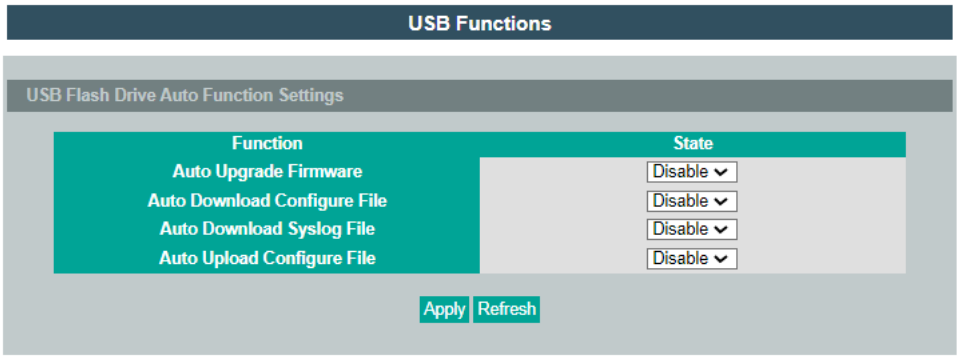
8.6.1. CLI Configurations - USB Functions

Management / USB Functions		
Mode	**Command**	**Description**
enable	show usb status	Displays the current USB function configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	usb auto-upgrade-fw (disable | enable)	Disables / enables the USB upgrade firmware automatically.
configure	usb auto-download-config (disable | enable)	Disables / enables the USB download configuration file automatically..
configure	usb auto-download-syslog (disable | enable)	Disables / enables the USB download syslog file automatically.

Example:

```
L2SWITCH#show usb status
 USB auto upgrade firmware State : Enabled
 USB auto download config State  : Enabled
 USB auto download syslog State : Enabled
L2SWITCH#configure terminal
L2SWITCH(config)#usb auto-upgrade-fw enable
L2SWITCH(config)#usb auto-download-config enable
L2SWITCH(config)#usb auto-download-syslog enable
```

8.6.2. Web Configuration - USB Functions



USB Functions	
Parameter	**Description**
Auto Upgrade Firmware	Select **Enable** to turn on automatic upgrade firmware or select **Disable** to turn it off.
Auto Download Config	Select **Enable** to turn on automatic download configurations or select **Disable** to turn it off.
Auto Download Syslog	Select **Enable** to turn on automatic download system log or select **Disable** to turn it off.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

8.7. User Account

The ICRL2-M allows users to create up to 6 user account. The user name and the password should be the combination of the digit or the alphabet. The last admin user account cannot be deleted. Users should input a valid user account to login the CLI or web management.

User Authority:

The ICRL2-M supports two types of the user account, admin and normal. The default user's account is username(admin) / password(admin).

- admin: read / write
- normal: read only
  - Cannot enter the privileged mode in CLI.
  - Cannot apply any configurations in web.

The ICRL2-M also supports backdoor user account. In case of that user forgot their user name or password, the ICRL2-M can generate a backdoor account with the system's MAC. Users can use the new user account to enter the ICRL2-M and then create a new user account.

User Account Default Settings	
Maximum user account	6
Maximum user name length	32
Maximum password length	32
Default user account for privileged mode	admin / admin

Note:

- The ICRL2-M allows users to create up to 6 user account.
- The user name and the password should be the combination of the digit or the alphabet.
- The last admin user account cannot be deleted.
- The maximum length of the username and password is 32 characters.

8.7.1. CLI Configurations - User Account

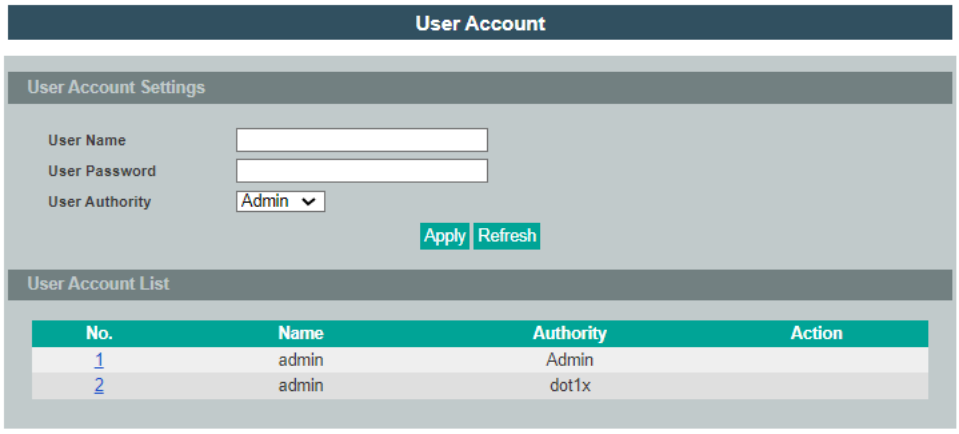
CLI User Account		
Mode	**Command**	**Description**
enable	show user account	Displays the current user accounts.
enable	show dot1x username	Displays the dot1x user accounts.
configure	add user USERNAME PASSWORD (normal | admin | dot1x)	Adds a new user account with choice of privileges normal/admin/dot1x.
configure	delete user USERNAME	Deletes a present user account.
configure	dot1x username USERNAME PASSWORD	Creates a user account for DOT1X local authentication.

CLI User Account (Continued)		
Mode	**Command**	**Description**
configure	no dot1x username USERNAME	Removes user account for DOT1X local authentication.

Example:

L2SWITCH#configure terminal
L2SWITCH(config)#add user q q admin
L2SWITCH(config)#add user 1 1 normal

8.7.2. Web Configuration - User Account



User Account	
Parameter	**Description**
User Account Settings	
User Name	Type a new username or modify an existing one.
User Password	Type a new password or modify an existing one. Enter up to 32 alphanumeric or digit characters.
User Authority	Select with which group the user associates: **admin** (read and write) or normal (read only) for this user account.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
User Account List	
Action	Click **Delete** to remove the user account. ***Note:*** *You cannot delete the last admin accounts.*

8.8. Device Management

8.8.1. LLDP

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802® LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

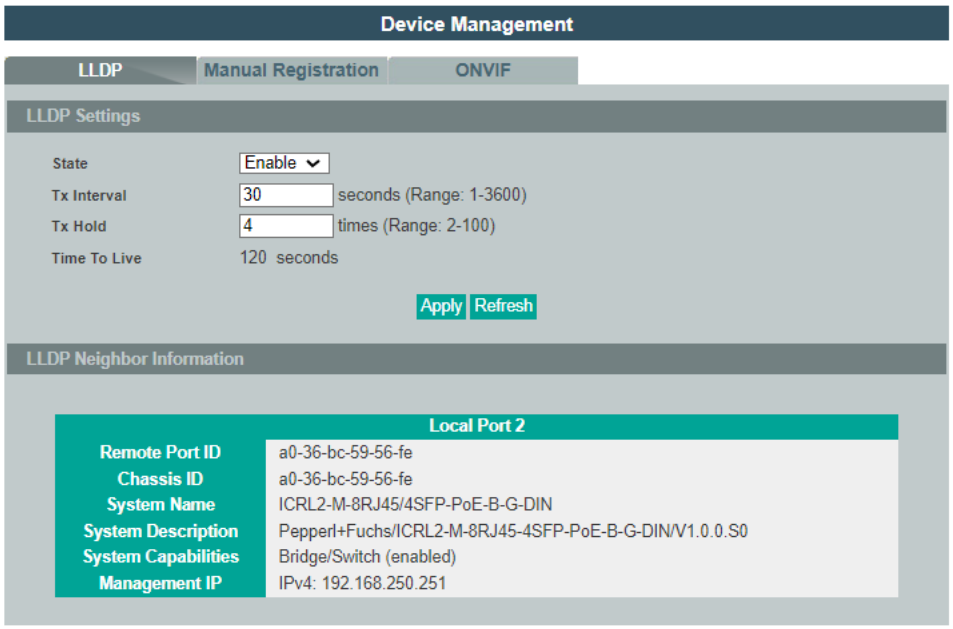
The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

8.8.1.1. CLI Configurations - Device Management / LLDP

CLI Device Management / LLDP		
Mode	**Command**	**Description**
enable	show lldp	Displays the LLDP configurations.
enable	show lldp neighbor	Displays all of the ports' neighbor information.
enable	configure terminal	Changes the mode to configure mode.
configure	lldp (disable | enable)	Globally enables / disables the LLDP function on the ICRL2-M.
configure	lldp tx-interval	Configures the interval to transmit the LLDP packets.
configure	lldp tx-hold	Configures the tx-hold time which determines the TTL of the ICRL2-M's message. (TTL=tx-hold * tx-interval)
configure	interface IFNAME	Enters the interface configure mode.
interface	lldp-agent (disable | enable | rx-only | tx-only)	Configures the LLDP agent function. • disable – Disable the LLDP on the specific port. • enable – Transmit and Receive the LLDP packet on the specific port. • tx-only – Transmit the LLDP packet on the specific port only. • rx-only – Receive the LLDP packet on the specific port.
config	interface range gigabitethernet1/ 0/ PORTLISTS	Enters the if-range configure mode.

CLI Device Management / LLDP (Continued)		
Mode	**Command**	**Description**
if-range	lldp-agent (disable | enable | rx-only | tx-only)	Configures the LLDP agent function. • disable – Disable the LLDP on the specific port. • enable – Transmit and Receive the LLDP packet on the specific port. • tx-only – Transmit the LLDP packet on the specific port only. • rx-only – Receive the LLDP packet on the specific port.

8.8.1.2. Web Configuration - Device Management / LLDP



Device Management / LLDP	
Parameter	**Description**
LLDP Settings	
State	Globally enables / disables the LLDP on the ICRL2-M.
Tx Interval	Configures the interval to transmit the LLDP packets.
Tx Hold	Configures the tx-hold time which determines the TTL of the ICRL2-M's message. (TTL=tx-hold * tx-interval)

Device Management / LLDP (Continued)	
Parameter	**Description**
Time To Live	The hold time for the ICRL2-M's information.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
LLDP Neighbor Information	
Local Port	Local port ID.
Remote Port ID	Connected port ID.
Chassis ID	Neighbor's chassis ID.
System Name	Neighbor's system name.
System Description	Neighbor's system description.
System Capabilities	Neighbor's capability.
Management IP	Neighbor management address.

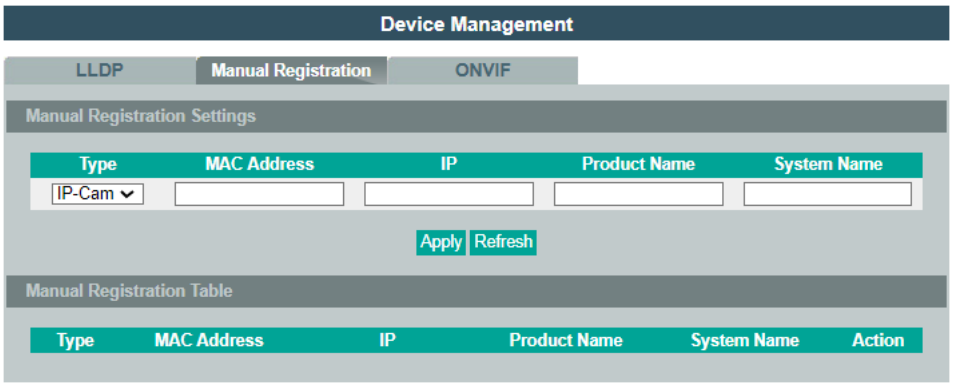
8.8.2. Manual Registration

If devices do not support LLDP and ONVIF, user has to enter the details of it by manually under manual registration. The function supports four types, IP-Cam, PLC, ICRL2-M and PC.

8.8.2.1. CLI Configuration - Device Management / Manual Registration

CLI Device Management / Manual Registration		
Mode	**Command**	**Description**
enable	show manual-registration-device	Displays the manual registration device configurations.
enable	configure terminal	Changes the mode to configure mode.
configure	manual-registration-device type (ipcam | plc | switch | pc) mac MACADDR ip IPADDR product-name STRINGS system-name STRINGS	Configures a device for the Topology Map.
configure	no manual-registration-device mac MACADDR	Removes a device from the Topology Map.

8.8.2.2. Web Configuration - Device Management / Manual Registration



Device Management / Manual Registration	
Parameter	**Description**
Manual Registration Settings	
Type	Devices connected to ICRL2-M.
MAC Address	MAC address of the device.
Product Name	Product name of the device.

Device Management / Manual Registration (Continued)	
Parameter	**Description**
System Name	System name of the device.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.
Manual Registration Table	
Action	Click Delete to delete this device.

8.8.3. Device Management / ONVIF

8.8.3.1. CLI Configurations - Device Management / ONVIF

CLI Device Management / ONVIF		
Mode	**Command**	**Description**
enable	show onvif	Displays the ONVIF configurations.
enable	configure terminal	Changes the mode to configure mode.
config	onvif enable	Enables the ONVIF on the ICRL2-M.
config	onvif tx-interval <6-3600>	Configures the tx interval for the ONVIF.
config	no onvif enable	Disables the ONVIF on the ICRL2-M.
config	no onvif tx-interval	Resets the tx interval to default for the ONVIF.(Default: 6 seconds).

8.8.3.2. Web Configuration - Device Management / ONVIF

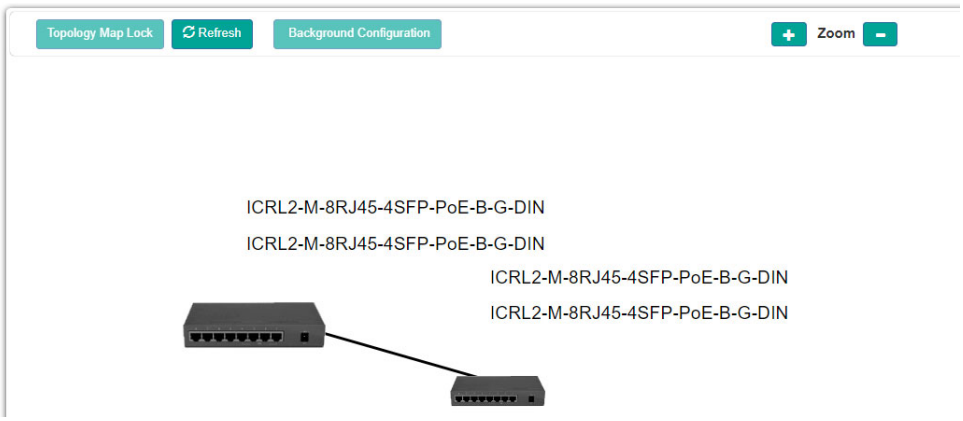


Device Management / ONVIF	
Parameter	**Description**
ONVIF Settings	
State	Select option to enable / disable the ONVIF feature on the ICRL2-M.
Tx Interval	Configures the sending ONVIF discovery packet interval. Valid range is 6 ~ 3600 seconds.
Apply	Click **Apply** to change the settings.
Refresh	Click **Refresh** to reload the running configuration values.

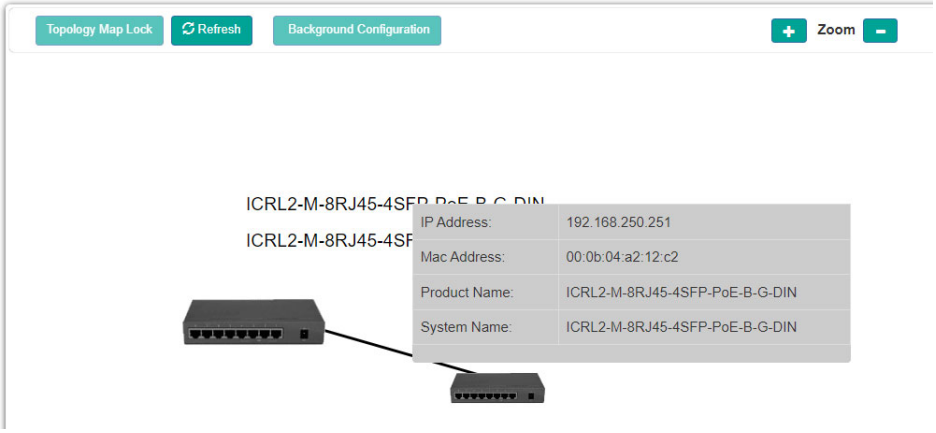
Device Management / ONVIF (Continued)	
Parameter	**Description**
ONVIF Neighbor Information	
Port	Connected port of the ONVIF device.
IP Address	IP address of the ONVIF device.
MAC Address	MAC address on the ONVIF device.
VLAN ID	VLAN ID of the ONVIF device join.
Product Name	Name of the product added.
Product Type	Identifies the device that is added.
Model	Model of the product.
Location	Location where it is placed.
Web Service Address	Address of the web service of that camera.

8.9. Topology Map

Click the “Topology Map Lock” to view the following information. You can use Zoom to adjust the view.



You can view the basic details of the devices connected to the host, by placing the cursor on it.



When there is something wrong with the devices so that you can find the details of events that have gone wrong, and correct it. A red ‘X’ indicates that connection is lost with the host.

You can upload your company floor layout plan picture in to the background image so that you can identify easily where the ICRL2-M has been placed.

- Picture: To choice a file which you want to display it in the background and the Preview window will display your select immediately. If you click the “Upgrade” button, the file will be download to the ICRL2-M and it will be applied on next reboot.
- Color: Allow user to select standard color for the background and the Preview window will display your select immediately.

9. Technical Support

This section contains troubleshooting information for your ICRL2-M. You should review the following subsections before calling Technical Support because they will request that you perform many of the procedures or verifications before they will be able to help you diagnose a problem.

If you cannot diagnose the problem, you can contact Technical Support.

9.1. Cable Test

This feature determines the quality of the cables, shorts, and cable impedance mismatch, bad connectors, termination mismatch, and bad magnetics. The feature can work on the copper Ethernet cable only. The cable testers can measure the signal strength and attenuation of the cable during transmission.

Note: *Cable tester can only accesable through the CLI without any GUI support.*

CLI Configurations		
Mode	**Command**	**Description**
Enable	configure terminal	Changes the node to configure node.
configure	interface IFNAME	Enters the interface configure node.
Interface	show cable-test result	Displays the cable test result.
Interface	cable-test start	Starts to test the cable.

9.2. Support Contact Information

Refer to https://www.pepperl-fuchs.com for detailed information.

Location	Email	Phone
Twinsburg OH USA	sales@us.pepperl-fuchs.com	+1 330 425-3555
Mannheim Germany	info@de.pepperl-fuchs.com	+49 621 776-0

FACTORY AUTOMATION – SENSING YOUR NEEDS





Worldwide Headquarters
Pepperl+Fuchs Group
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

TDOCT-9236_ENG
8/19/25

Subject to modifications
Copyright PEPPERL+FUCHS • Printed in Germany