

# Owner's Manual

## 5-port 10/100/1000Base-T + 1-slot Gigabit SFP Managed Industrial Gigabit Ethernet Switch

Model: NGI-M05-C1

### WARRANTY REGISTRATION

Register your product today and be automatically entered to win an ISOBAR® surge protector in our monthly drawing!

[tripplite.com/warranty](http://tripplite.com/warranty)



1111 W. 35th Street, Chicago, IL 60609 USA • [tripplite.com/support](http://tripplite.com/support)

Copyright © 2021 Tripp Lite. All rights reserved.



---

**Warning**

Take special care to read and understand all the content in the warning boxes.



---

**Warning**

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



---

**Warning**

Before working on 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.



---

**Warning**

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



---

**Warning**

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.



---

**Warning**

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



---

**Warning**

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



---

**Warning**

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.



---

**Warning**

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



---

**Warning**

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



---

**Warning**

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:

- ✓ **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- ✓ **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.**
- ✓ **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.**



---

**Warning**

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



---

**Warning**

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



---

**Warning**

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



---

**Warning**

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.



---

**Warning**

No user-serviceable parts inside. Do not open.



---

**Warning**

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.

# Table of Contents

|  |           |
|--|-----------|
| <b>1. ABOUT THIS MANUAL.....</b>                     | <b>12</b> |
| 1.1. INTRODUCTION.....                               | 12        |
| 1.2. PURPOSE .....                                   | 12        |
| 1.3. TERMS/ USAGE .....                              | 12        |
| <b>2. ABOUT THE NGI-M05-C1 .....</b>                 | <b>13</b> |
| 2.1. FEATURES .....                                  | 13        |
| 2.2. SPECIFICATIONS .....                            | 13        |
| <b>3. HARDWARE DESCRIPTION.....</b>                  | <b>15</b> |
| 3.1. CONNECTORS .....                                | 15        |
| 3.2. INSTALLATION .....                              | 16        |
| 3.3. LED INDICATORS.....                             | 21        |
| 3.4. DIP SWITCHES .....                              | 21        |
| <b>4. SYSTEM STATUS.....</b>                         | <b>23</b> |
| 4.1. CONSOLE PORT .....                              | 23        |
| 4.2. TELNET .....                                    | 23        |
| 4.3. HOW TO ENTER THE CLI? .....                     | 23        |
| 4.4. CLI COMMAND CONCEPT .....                       | 24        |
| 4.5. MANAGEMENT VIA INTERNET BROWSER INTERFACE ..... | 26        |
| 4.6. SYSTEM INFORMATION.....                         | 27        |
| 4.6.1. CLI CONFIGURATION .....                       | 27        |
| 4.6.2. WEB CONFIGURATION .....                       | 28        |
| <b>5. BASIC SETTINGS.....</b>                        | <b>30</b> |
| <b>5.1. SYSTEM SETTINGS .....</b>                    | <b>30</b> |
| 5.1.1. SYSTEM .....                                  | 30        |
| 5.1.1.1. CLI CONFIGURATION.....                      | 30        |
| 5.1.1.2. WEB CONFIGURATION .....                     | 32        |
| 5.1.2. JUMBO FRAME.....                              | 34        |
| 5.1.2.1. CLI CONFIGURATION.....                      | 34        |
| 5.1.2.2. WEB CONFIGURATION .....                     | 34        |
| 5.1.3. SNTP.....                                     | 35        |
| 5.1.3.1. CLI CONFIGURATION.....                      | 35        |
| 5.1.3.2. WEB CONFIGURATION .....                     | 37        |
| 5.1.4. MANAGEMENT HOST .....                         | 39        |
| 5.1.4.1. CLI CONFIGURATION.....                      | 39        |
| 5.1.4.2. WEB CONFIGURATION .....                     | 40        |
| <b>5.2. MAC MANAGEMENT .....</b>                     | <b>41</b> |
| 5.2.1. STATIC MAC.....                               | 42        |

|             |                                |           |
|-------------|--------------------------------|-----------|
| 5.2.1.1.    | CLI CONFIGURATION .....        | 42        |
| 5.2.1.2.    | WEB CONFIGURATION .....        | 42        |
| 5.2.2.      | MAC TABLE.....                 | 44        |
| 5.2.2.1.    | CLI CONFIGURATION .....        | 44        |
| 5.2.2.2.    | WEB CONFIGURATION .....        | 44        |
| 5.2.3.      | AGE TIME .....                 | 46        |
| 5.2.3.1.    | CLI CONFIGURATION .....        | 46        |
| 5.2.3.2.    | WEB CONFIGURATION .....        | 46        |
| <b>5.3.</b> | <b>PORT MIRROR .....</b>       | <b>47</b> |
| 5.3.1.      | CLI CONFIGURATION .....        | 47        |
| 5.3.2.      | WEB CONFIGURATION .....        | 48        |
| <b>5.4.</b> | <b>PORT SETTINGS .....</b>     | <b>50</b> |
| 5.4.1.      | GENERAL SETTINGS .....         | 51        |
| 5.4.1.1.    | CLI CONFIGURATION .....        | 51        |
| 5.4.1.2.    | WEB CONFIGURATION .....        | 54        |
| 5.4.2.      | INFORMATION .....              | 55        |
| 5.4.2.1.    | CLI CONFIGURATION .....        | 55        |
| 5.4.2.2.    | WEB CONFIGURATION .....        | 56        |
| <b>6.</b>   | <b>ADVANCED SETTINGS.....</b>  | <b>58</b> |
| <b>6.1.</b> | <b>BANDWIDTH CONTROL .....</b> | <b>58</b> |
| 6.1.1.      | QoS .....                      | 58        |
| 6.1.1.1.    | PORT PRIORITY .....            | 61        |
| 6.1.1.1.1.  | CLI CONFIGURATION .....        | 61        |
| 6.1.1.1.2.  | WEB CONFIGURATION .....        | 61        |
| 6.1.1.2.    | IP DIFFSERV (DSCP) .....       | 63        |
| 6.1.1.2.1.  | CLI CONFIGURATION .....        | 64        |
| 6.1.1.2.2.  | WEB CONFIGURATION .....        | 65        |
| 6.1.1.3.    | PRIORITY/QUEUE MAPPING .....   | 66        |
| 6.1.1.3.1.  | CLI CONFIGURATION .....        | 66        |
| 6.1.1.3.2.  | WEB CONFIGURATION .....        | 67        |
| 6.1.1.4.    | SCHEDULE MODE .....            | 68        |
| 6.1.1.4.1.  | CLI CONFIGURATION .....        | 68        |
| 6.1.1.4.2.  | WEB CONFIGURATION .....        | 69        |
| 6.1.2.      | RATE LIMITATION .....          | 70        |
| 6.1.2.1.    | STORM CONTROL .....            | 70        |
| 6.1.2.1.1.  | CLI CONFIGURATION .....        | 70        |
| 6.1.2.1.2.  | WEB CONFIGURATION .....        | 72        |
| 6.1.2.2.    | BANDWIDTH LIMITATION .....     | 73        |
| 6.1.2.2.1.  | CLI CONFIGURATION .....        | 73        |
| 6.1.2.2.2.  | WEB CONFIGURATION .....        | 74        |
| <b>6.2.</b> | <b>IGMP SNOOPING .....</b>     | <b>75</b> |
| 6.2.1.      | IGMP SNOOPING.....             | 75        |
| 6.2.1.1.    | GENERAL SETTINGS .....         | 77        |
| 6.2.1.1.1.  | CLI CONFIGURATION .....        | 77        |
| 6.2.1.1.2.  | WEB CONFIGURATION .....        | 77        |
| 6.2.1.2.    | PORT SETTINGS .....            | 79        |
| 6.2.1.2.1.  | CLI CONFIGURATION .....        | 79        |
| 6.2.1.2.2.  | WEB CONFIGURATION .....        | 81        |
| 6.2.1.3.    | QUERIER SETTINGS .....         | 83        |

|   |            |
|---|------------|
| 6.2.1.3.1. CLI CONFIGURATION .....        | 83         |
| 6.2.1.3.2. WEB CONFIGURATION .....        | 84         |
| 6.2.2. IGMP SNOOPING FILTERING.....       | 85         |
| 6.2.2.1. GENERAL SETTINGS .....           | 85         |
| 6.2.2.1.1. CLI CONFIGURATION .....        | 85         |
| 6.2.2.1.2. WEB CONFIGURATION .....        | 85         |
| <b>6.2.2.2. MULTICAST GROUP .....</b>     | <b>87</b>  |
| 6.2.2.2.1. CLI CONFIGURATION .....        | 87         |
| 6.2.2.2.2. WEB CONFIGURATION .....        | 87         |
| <b>6.2.2.3. PORT SETTINGS .....</b>       | <b>88</b>  |
| 6.2.2.3.1. CLI CONFIGURATION .....        | 88         |
| 6.2.2.3.2. WEB CONFIGURATION .....        | 89         |
| 6.2.3. MULTICAST ADDRESS .....            | 90         |
| 6.2.3.1. CLI CONFIGURATION .....          | 91         |
| 6.2.3.2. WEB CONFIGURATION .....          | 92         |
| <b>6.3. VLAN .....</b>                    | <b>93</b>  |
| 6.3.1. PORT ISOLATION .....               | 93         |
| 6.3.1.1. CLI CONFIGURATIONS .....         | 93         |
| 6.3.1.2. WEB CONFIGURATIONS.....          | 94         |
| 6.3.2. 802.1Q VLAN.....                   | 95         |
| 6.3.2.1. VLAN SETTINGS.....               | 96         |
| 6.3.2.1.1. CLI CONFIGURATIONS .....       | 96         |
| 6.3.2.1.2. WEB CONFIGURATIONS.....        | 97         |
| 6.3.2.2. TAG SETTINGS.....                | 99         |
| 6.3.2.2.1. CLI CONFIGURATIONS .....       | 99         |
| 6.3.2.2.2. WEB CONFIGURATIONS.....        | 100        |
| 6.3.2.3. PORT SETTINGS .....              | 101        |
| 6.3.2.3.1. CLI CONFIGURATIONS .....       | 101        |
| 6.3.2.3.2. WEB CONFIGURATIONS.....        | 102        |
| 6.3.3. MAC VLAN .....                     | 103        |
| 6.3.3.1. CLI CONFIGURATIONS .....         | 103        |
| 6.3.3.2. WEB CONFIGURATIONS.....          | 104        |
| 6.3.4. Q-IN-Q VLAN (VLAN STACKING) .....  | 105        |
| 6.3.4.1. VLAN STACKING.....               | 107        |
| 6.3.4.1.1. CLI CONFIGURATIONS .....       | 107        |
| 6.3.4.1.2. WEB CONFIGURATIONS.....        | 108        |
| 6.3.4.2. PORT-BASED Q-IN-Q.....           | 109        |
| 6.3.4.2.1. CLI CONFIGURATIONS .....       | 110        |
| 6.3.4.2.2. WEB CONFIGURATIONS.....        | 111        |
| <b>6.4. DHCP OPTION (OPTION 82) .....</b> | <b>113</b> |
| 6.4.1. CLI CONFIGURATIONS .....           | 115        |
| 6.4.2. WEB CONFIGURATIONS.....            | 116        |
| <b>6.5. DHCP RELAY .....</b>              | <b>118</b> |
| 6.5.1. CLI CONFIGURATIONS .....           | 119        |
| 6.5.2. WEB CONFIGURATIONS.....            | 120        |
| <b>6.6. DUAL HOMING.....</b>              | <b>121</b> |
| 6.6.1. CLI CONFIGURATIONS .....           | 123        |
| 6.6.2. WEB CONFIGURATIONS.....            | 124        |
| <b>6.7. EEE .....</b>                     | <b>126</b> |
| 6.7.1. CLI CONFIGURATIONS .....           | 126        |
| 6.7.2. WEB CONFIGURATIONS.....            | 126        |

|                                     |            |
|-------------------------------------|------------|
| <b>6.8. ERPS</b> .....              | <b>128</b> |
| 6.8.1. RING SETTINGS .....          | 130        |
| 6.8.1.1. CLI CONFIGURATIONS .....   | 130        |
| 6.8.1.2. WEB CONFIGURATIONS.....    | 131        |
| 6.8.2. INSTANCE .....               | 133        |
| 6.8.2.1. CLI CONFIGURATIONS .....   | 133        |
| 6.8.2.2. WEB CONFIGURATIONS.....    | 134        |
| <b>6.9. LINK AGGREGATION</b> .....  | <b>135</b> |
| 6.9.1. STATIC TRUNK.....            | 135        |
| 6.9.1.1. CLI CONFIGURATIONS .....   | 135        |
| 6.9.1.2. WEB CONFIGURATIONS.....    | 136        |
| 6.9.2. LACP .....                   | 137        |
| 6.9.2.1. CLI CONFIGURATIONS .....   | 138        |
| 6.9.2.2. WEB CONFIGURATIONS.....    | 139        |
| 6.9.3. LACP INFORMATION .....       | 140        |
| 6.9.3.1. CLI CONFIGURATIONS .....   | 140        |
| 6.9.3.2. WEB CONFIGURATIONS.....    | 140        |
| <b>6.10. LOOP DETECTION</b> .....   | <b>142</b> |
| 6.10.1. CLI CONFIGURATIONS .....    | 142        |
| 6.10.2. WEB CONFIGURATIONS.....     | 144        |
| <b>6.11. MODBUS TCP</b> .....       | <b>146</b> |
| 6.11.1. CLI CONFIGURATIONS .....    | 149        |
| 6.11.2. WEB CONFIGURATIONS.....     | 150        |
| <b>6.12. STP / RSTP</b> .....       | <b>152</b> |
| 6.12.1. GENERAL SETTINGS .....      | 157        |
| 6.12.1.1. CLI CONFIGURATIONS .....  | 157        |
| 6.12.1.2. WEB CONFIGURATIONS.....   | 158        |
| 6.12.2. PORT PARAMETERS .....       | 159        |
| 6.12.2.1. CLI CONFIGURATIONS .....  | 159        |
| 6.12.2.2. WEB CONFIGURATIONS.....   | 161        |
| 6.12.3. STP STATUS .....            | 163        |
| 6.12.3.1. CLI CONFIGURATIONS .....  | 163        |
| 6.12.3.2. WEB CONFIGURATIONS.....   | 163        |
| <br>                                |            |
| <b>7. SECURITY</b> .....            | <b>165</b> |
| <br>                                |            |
| <b>7.1. IP SOURCE GUARD</b> .....   | <b>165</b> |
| 7.1.1. DHCP SNOOPING .....          | 165        |
| 7.1.1.1. DHCP SNOOPING .....        | 168        |
| 7.1.1.1.1. CLI CONFIGURATIONS ..... | 168        |
| 7.1.1.1.2. WEB CONFIGURATIONS.....  | 169        |
| 7.1.1.2. PORT SETTINGS .....        | 170        |
| 7.1.1.2.1. CLI CONFIGURATIONS ..... | 170        |
| 7.1.1.2.2. WEB CONFIGURATIONS.....  | 171        |
| 7.1.1.3. SERVER SCREENING .....     | 172        |
| 7.1.1.3.1. CLI CONFIGURATIONS ..... | 172        |
| 7.1.1.3.2. WEB CONFIGURATIONS.....  | 172        |
| 7.1.2. BINDING TABLE .....          | 173        |
| 7.1.2.1. STATIC ENTRY .....         | 173        |
| 7.1.2.1.1. CLI CONFIGURATIONS ..... | 173        |
| 7.1.2.1.2. WEB CONFIGURATIONS.....  | 174        |

|             |                                  |            |
|-------------|----------------------------------|------------|
| 7.1.2.2.    | BINDING TABLE .....              | 175        |
| 7.1.2.2.1.  | CLI CONFIGURATIONS .....         | 175        |
| 7.1.2.2.2.  | WEB CONFIGURATIONS.....          | 175        |
| 7.1.3.      | ARP INSPECTION.....              | 176        |
| 7.1.3.1.    | ARP INSPECTION.....              | 177        |
| 7.1.3.1.1.  | CLI CONFIGURATIONS .....         | 177        |
| 7.1.3.1.2.  | WEB CONFIGURATIONS.....          | 178        |
| 7.1.3.2.    | FILTER TABLE .....               | 180        |
| 7.1.3.2.1.  | CLI CONFIGURATIONS .....         | 180        |
| 7.1.3.2.2.  | WEB CONFIGURATIONS.....          | 181        |
| <b>7.2.</b> | <b>ACCESS CONTROL LIST .....</b> | <b>182</b> |
| 7.2.1.      | CLI CONFIGURATIONS .....         | 183        |
| 7.2.2.      | WEB CONFIGURATIONS.....          | 185        |
| <b>7.3.</b> | <b>802.1x.....</b>               | <b>188</b> |
| 7.3.1.      | GLOBAL SETTINGS .....            | 191        |
| 7.3.1.1.    | CLI CONFIGURATIONS .....         | 191        |
| 7.3.1.2.    | WEB CONFIGURATIONS.....          | 192        |
| 7.3.2.      | PORT SETTINGS .....              | 194        |
| 7.3.2.1.    | CLI CONFIGURATIONS .....         | 194        |
| 7.3.2.2.    | WEB CONFIGURATIONS.....          | 195        |
| <b>7.4.</b> | <b>PORT SECURITY.....</b>        | <b>197</b> |
| 7.4.1.      | CLI CONFIGURATIONS .....         | 197        |
| 7.4.2.      | WEB CONFIGURATIONS.....          | 198        |
| <b>8.</b>   | <b>MONITOR.....</b>              | <b>199</b> |
| <b>8.1.</b> | <b>ALARM.....</b>                | <b>199</b> |
| 8.1.1.      | CLI CONFIGURATIONS .....         | 199        |
| 8.1.2.      | WEB CONFIGURATIONS.....          | 199        |
| <b>8.2.</b> | <b>PORT STATISTICS .....</b>     | <b>200</b> |
| 8.2.1.      | CLI CONFIGURATIONS .....         | 200        |
| 8.2.2.      | WEB CONFIGURATIONS.....          | 200        |
| <b>8.3.</b> | <b>PORT UTILIZATION .....</b>    | <b>201</b> |
| 8.3.1.      | CLI CONFIGURATIONS .....         | 201        |
| 8.3.2.      | WEB CONFIGURATIONS.....          | 201        |
| <b>8.4.</b> | <b>RMON STATISTICS .....</b>     | <b>202</b> |
| 8.4.1.      | CLI CONFIGURATIONS .....         | 202        |
| 8.4.2.      | WEB CONFIGURATIONS.....          | 202        |
| <b>8.5.</b> | <b>SFP INFORMATION .....</b>     | <b>203</b> |
| 8.5.1.      | CLI CONFIGURATIONS .....         | 203        |
| 8.5.2.      | WEB CONFIGURATIONS.....          | 203        |
| <b>8.6.</b> | <b>TRAFFIC MONITOR.....</b>      | <b>204</b> |
| 8.6.1.      | CLI CONFIGURATIONS .....         | 204        |
| 8.6.2.      | WEB CONFIGURATIONS.....          | 205        |
| <b>9.</b>   | <b>MANAGEMENT .....</b>          | <b>207</b> |
| <b>9.1.</b> | <b>SNMP.....</b>                 | <b>207</b> |
| 9.1.1.      | SNMP.....                        | 207        |
| 9.1.1.1.    | SNMP SETTINGS .....              | 207        |
| 9.1.1.1.1.  | CLI CONFIGURATIONS .....         | 207        |

|                                     |            |
|-------------------------------------|------------|
| 9.1.1.1.2. WEB CONFIGURATIONS.....  | 209        |
| 9.1.1.2. COMMUNITY NAME.....        | 210        |
| 9.1.1.2.1. CLI CONFIGURATIONS ..... | 210        |
| 9.1.1.2.2. WEB CONFIGURATIONS.....  | 211        |
| 9.1.2. SNMP TRAP .....              | 213        |
| 9.1.2.1. RECEIVER SETTINGS .....    | 213        |
| 9.1.2.1.1. CLI CONFIGURATIONS ..... | 213        |
| 9.1.2.1.2. WEB CONFIGURATIONS.....  | 213        |
| 9.1.2.2. EVENT SETTINGS.....        | 214        |
| 9.1.2.2.1. CLI CONFIGURATIONS ..... | 215        |
| 9.1.2.2.2. WEB CONFIGURATIONS.....  | 216        |
| 9.1.2.3. PORT EVENT SETTINGS .....  | 216        |
| 9.1.2.3.1. CLI CONFIGURATIONS ..... | 216        |
| 9.1.2.3.2. WEB CONFIGURATIONS.....  | 218        |
| 9.1.3. SNMPV3 .....                 | 219        |
| 9.1.3.1. SNMPV3 GROUP.....          | 219        |
| 9.1.3.1.1. CLI CONFIGURATIONS ..... | 219        |
| 9.1.3.1.2. WEB CONFIGURATIONS.....  | 219        |
| 9.1.3.2. SNMPV3 USER.....           | 220        |
| 9.1.3.2.1. CLI CONFIGURATIONS ..... | 220        |
| 9.1.3.2.2. WEB CONFIGURATIONS.....  | 221        |
| 9.1.3.3. SNMPV3 VIEW .....          | 222        |
| 9.1.3.3.1. CLI CONFIGURATIONS ..... | 222        |
| 9.1.3.3.2. WEB CONFIGURATIONS.....  | 222        |
| <b>9.2. AUTO PROVISION .....</b>    | <b>223</b> |
| 9.2.1. CLI CONFIGURATIONS .....     | 224        |
| 9.2.2. WEB CONFIGURATIONS.....      | 225        |
| <b>9.3. MAIL ALARM.....</b>         | <b>225</b> |
| 9.3.1. CLI CONFIGURATIONS .....     | 226        |
| 9.3.2. WEB CONFIGURATIONS.....      | 227        |
| <b>9.4. MAINTENANCE .....</b>       | <b>229</b> |
| 9.4.1. CONFIGURATION .....          | 229        |
| 9.4.1.1. CLI CONFIGURATIONS .....   | 229        |
| 9.4.1.2. WEB CONFIGURATIONS.....    | 230        |
| 9.4.2. FIRMWARE .....               | 231        |
| 9.4.2.1. CLI CONFIGURATIONS .....   | 231        |
| 9.4.2.2. WEB CONFIGURATIONS.....    | 232        |
| 9.4.3. REBOOT .....                 | 233        |
| 9.4.3.1. CLI CONFIGURATIONS .....   | 233        |
| 9.4.3.2. WEB CONFIGURATIONS.....    | 233        |
| 9.4.4. SERVER CONTROL.....          | 234        |
| 9.4.4.1. CLI CONFIGURATIONS .....   | 234        |
| 9.4.4.2. WEB CONFIGURATIONS.....    | 235        |
| <b>9.5. SYS LOG .....</b>           | <b>236</b> |
| 9.5.1. CLI CONFIGURATIONS .....     | 236        |
| 9.5.2. WEB CONFIGURATIONS.....      | 237        |
| <b>9.6. USER ACCOUNT .....</b>      | <b>238</b> |
| 9.6.1. CLI CONFIGURATION.....       | 238        |
| 9.6.2. WEB CONFIGURATION .....      | 239        |
| <b>9.7. DEVICE MANAGEMENT .....</b> | <b>240</b> |
| 9.7.1. LLDP .....                   | 240        |

|              |   |            |
|--------------|---|------------|
| 9.7.1.1.     | CLI CONFIGURATION .....                         | 240        |
| 9.7.1.2.     | WEB CONFIGURATION .....                         | 241        |
| 9.7.2.       | MANUAL REGISTRATION .....                       | 243        |
| 9.7.2.1.     | CLI CONFIGURATIONS .....                        | 243        |
| 9.7.2.2.     | WEB CONFIGURATIONS.....                         | 243        |
| 9.7.3.       | ONVIF .....                                     | 245        |
| 9.7.3.1.     | CLI CONFIGURATIONS .....                        | 245        |
| 9.7.3.2.     | WEB CONFIGURATIONS.....                         | 245        |
| <b>9.8.</b>  | <b>TOPOLOGY MAP .....</b>                       | <b>247</b> |
| 9.8.1.       | BACKGROUND CONFIGURATION .....                  | 249        |
| 9.8.2.       | CLIENT-SWITCH MANAGEMENT .....                  | 251        |
| <b>10.</b>   | <b>MISC .....</b>                               | <b>251</b> |
| <b>10.1.</b> | <b>CABLE TEST .....</b>                         | <b>251</b> |
| 10.1.1.      | CLI CONFIGURATIONS .....                        | 251        |
|              | <b>WARRANTY &amp; PRODUCT REGISTRATION.....</b> | <b>255</b> |

## **1. About this Manual**

### **1.1. Introduction**

The NGI-M05-C1 managed industrial switch is engineered with rugged hardware to meet the high reliability requirements of Industrial applications. Built in a well-protected IP-30 aluminum housing, the switch withstands in operating temperatures ranging from -40°C to 75°C and operates consistently even in harsh industrial environments. The NGI-M05-C1 supports QoS, IGMP snooping, SFP DDMI and other device management features to fulfill the needs of high performance managed Industrial networks.

The switch is complied with 4-10/100/1000Base-T copper ports to deliver gigabit performance for most demanding industrial applications. Two gigabit fiber slots of the switch can be configured as dual fiber ring ports to quickly recover network failures and provide an easy way to establish redundant gigabit network. Thus, NGI-M05-C1 ensures a reliable and highly available managed industrial network.

### **1.2. Purpose**

This guide describes how to install and configure the NGI-M05-C1 Industrial Managed Switch.

### **1.3. Terms/ Usage**

In this manual, the term “Switch” (first letter upper case) refers to the NGI-M05-C1 Switch, and “switch” (first letter lower case) refers to other switches.

## **2. About the NGI-M05-C1**

### **2.1. Features**

#### **Network Functions**

Port-based Mirroring  
256 Active VLAN  
IGMP Snooping v1/v2/v3  
IGMP Querier  
DHCP Relay/Option 82  
Link Aggregation  
Link Layer Discovery Protocol  
Loop Detection, Auto Recovery Timer  
STP/RSTP  
SFP DDMI Support  
RMON Statistics

#### **Network Security**

Access Control List (L2/L3/L4)  
Port Security  
802.1x Port Authentication  
DHCP Snooping

#### **Traffic Management & QoS**

Port Priority  
Rate Limitation  
Storm Control  
Port Isolation  
802.1Q Tag-based VLAN  
Auto MDI/MDI-X

#### **Network Management**

Command Line Interface, Telnet  
Web GUI  
SNMP v1/v2c  
Management VLAN  
System log  
Firmware Upgradable  
Configuration Upload/Download  
LED, SNMP trap and email alarm

### **2.2. Specifications**

#### **IEEE Standards**

|              |                                      |
|--------------|--------------------------------------|
| IEEE 802.3   | 10Base-T                             |
| IEEE 802.3u  | 100Base-TX/FX                        |
| IEEE 802.3ab | 1000Base-T                           |
| IEEE 802.3z  | 1000Base-SX/LX                       |
| IEEE 802.3x  | Flow Control                         |
| IEEE 802.3   | Nway Auto-negotiation                |
| IEEE 802.3az | EEE, Energy Efficient Ethernet       |
| IEEE 802.1ab | Link Layer Discovery Protocol MED    |
| IEEE 802.1p  | Class of Service, priority protocols |
| IEEE 802.1D  | Spanning Tree Protocol               |
| IEEE 802.1w  | Rapid Spanning Tree Protocol         |
| IEEE 802.1Q  | VLAN tagging                         |
| IEEE 802.1X  | Network Access Control               |

### **Performance**

|                    |                                  |
|--------------------|----------------------------------|
| Switching fabric   | 12 Gbps                          |
| L2 forwarding      | 8.92 Mpps                        |
| Packet buffer size | 4.1Mbits                         |
| MAC entries        | 08 K                             |
| Jumbo frame        | 10 K                             |
| Throughput         | 1,488,000pps when 1000Mbps speed |

### **Physical ports**

|                          |   |
|--------------------------|---|
| 10/100/1000Base-T (RJ45) | 5 |
| Gigabit SFP slots        | 1 |

### **Power**

Input Voltage:

- Primary inputs 20~57VDC at a maximum of 1.5A
- Redundant inputs 20~57VDC at a maximum of 1.5A

Connection:

|                                |   |
|--------------------------------|---|
| Removable 6-pin terminal block | one   |
| Overload current protection    | Support   |
| Reverse polarity protection    | Support   |
| Relay output                   | One with current carrying capacity of 1 A @ 24VDC |
| System-power consumption       | 10W   |

### **Mechanical**

|                   |  |
|-------------------|--|
| Dimension (WxHxD) | 31 x 136 x 109.5 mm (1.22 x 5.36 x 4.31 in.) |
| Weight            | 395 g (0.87 lb.)                             |
| Mounting          | DIN-Rail                                     |
| Housing           | IP30 protection                              |

### **Operating Requirement**

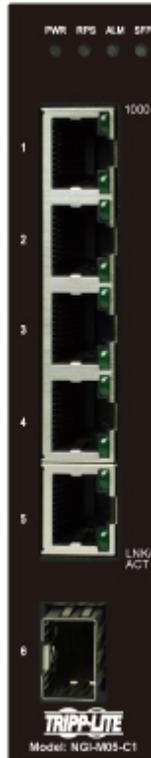
|                            |                                |
|----------------------------|--------------------------------|
| Wide operating temperature | -40°C to 75°C (-40°F to 167°F) |
| Storage temperature        | -40°C to 85°C (-40°F to 185°F) |
| Operating humidity         | 5% to 95% RH (Non Condensing)  |
| Storage humidity           | 5% to 95% RH (Non Condensing)  |

### **DIN RAIL Recommendation**

Steel with electrolytic zinc plating  
Stand-off rackets: 45<sup>0</sup> Angle and Straight  
Complies with DIN 50045, 50022 and 50035 standards

### 3. Hardware Description

#### NGI-M05-C1 Front Panel



5 10/100/1000Base-T ports & 1 Gigabit SFP slots  
Managed Industrial Ethernet Switch

#### 3.1. Connectors

The Switch 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 10Mbps, 100Mbps or 1000Mbps, and can operate in half- and full-duplex transfer modes. These ports also offer automatic MDI/MDI-X crossover detection that gives true “plug-and-play” capability – just plug the network cables into the ports and the ports will adjust according to the end-node devices. The following are recommended cabling for the RJ45 connectors: (1) 10Mbps – Cat 3 or better; (2) 100/1000Mbps – Cat 5e or better.

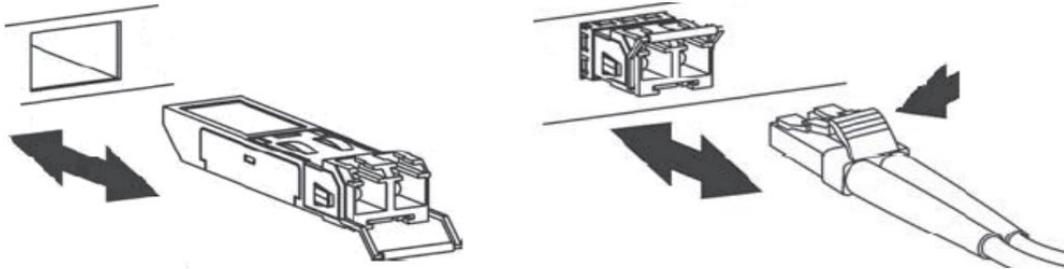
##### SFP Slots for SFP modules

The four SFP slots are designed to Gigabit SFP modules that support network speed of 1000Mbps.

##### 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 module's mouth.
4. Align the fiber cable's connector with the SFP module's mouth 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 Switch to be sure that the connection is valid. (Refer to the LED chart).

### 3.2. Installation

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

- ✓ Install the Switch in an appropriate place. See Technical Specifications for the acceptable temperature and humidity ranges.
- ✓ Install the Switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- ✓ Leave at least 10cm of space at the front and rear of the unit for ventilation.

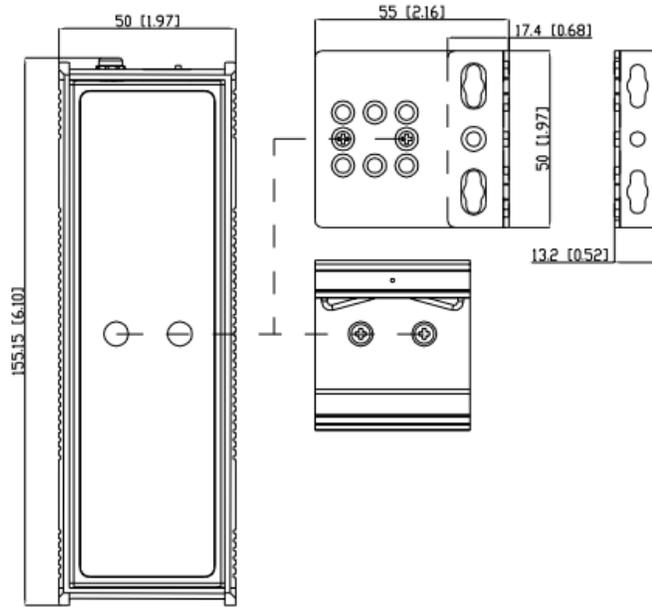
#### ATTENTION



The NGI-M05-C1 Series is an open type device and NGI-M05-C1 Series shall be DIN-Rail mounted or wall mounted (optional) in cabinet or enclosure.

#### Hardware Installation

- ✓ Step 1: Unpack the device and other contents of the package.
- ✓ Step 2: Fasten DIN-Rail or Wall-mount kit on the rear of the NGI-M05-C1.



- ✓ Connect the 20~57V DC power supply to the PWR & RPS terminal block or 4-pin power adapter to DC jack receiver on the top of the Switch (Refer to “**Wiring Redundant Power Inputs**”).
- ✓ Step 4: Connect the Ethernet (RJ45) port to the networking device and check the LED status to confirm the connection is established.

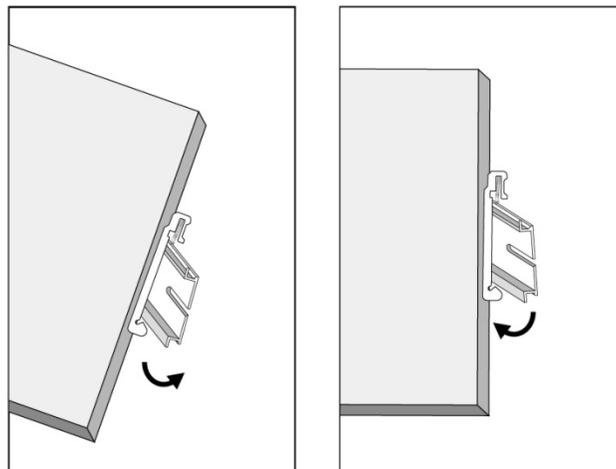
### DIN Rail Installation

The NGI-M05-C1 has a DIN rail bracket on the back of the Switch.

**Location:** The NGI-M05-C1 can be DIN-Rail-mounted in cabinet or enclosure.

### Mounting the Switch

Place the NGI-M05-C1 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.



## Dismounting the Switch

Pull out the lower edge of the switch and then remove the switch from the DIN rail.

**Ground the Switch:** Before powering on the switch, ground the switch to earth.

Ensure the rack on which the switch is to be mounted is properly grounded and in compliance 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).

### ATTENTION



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

### 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 (167°F).

### ATTENTION



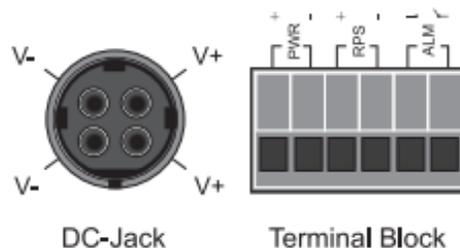
A corrosion-free mounting rail is advisable.

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

## Wiring Power Inputs

You can use either “DC-Jack” or “Terminal Block (PWR)” for primary power and “Terminal Block (RPS)” for secondary power source, to be a Redundant Power Input.

Top views of DC-Jack and Terminal Block are shown as pictures:



follow the steps below:

- ✓ **Step 1:** Insert the positive/negative DC wires into the V+/V- terminal, respectively.

- ✓ **Step 2:** Use your finger to press the green plug on top of terminal block connector to insert power cables.
- ✓ **Step 3:** Insert the terminal block connector which includes “PWR” and “RPS” into the terminal block receptor which is located on the top panel.
- ✓ **Option 2:** Insert the “DC-Jack” connector into “DC-Jack” receiver and “Terminal Block (RPS)” into terminal block receptor.

**WARNING**



- Use **copper** conductors only, **60/75°C (140/167°F)**, tighten to **0.56 N•m (5 lb•in)**.
- The wire gauge for the terminal block should range between **12~18 AWG**.

**Redundant Power Input:** You can use “Terminal Block (PWR)” as primary power or “Terminal Block (PWR)” for redundant power.

***Connect power cables to terminal block:** Use your finger to press the orange plug on top of terminal block connector to insert power cables*

**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.

**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.

### Wiring the Alarm Contact:

The Alarm Contact consists of the two last contacts of the terminal block on switch's top panel.

**ALM:** The two last contacts of the 6-contact terminal block connector are used to detect both power faults and port faults. The two wires attached to the ALM contacts form an open circuit when:

1. The Switch has lost power from one of the DC power inputs.

OR

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

If neither of these two conditions is satisfied, the Fault circuit will be closed.

### WARNING



- Use **copper** conductors only, **60/75°C (140/167°F)**, tighten to **0.56 N•m (5 lb•in)**.
- The wire gauge for the terminal block should range between **12~18 AWG**.

### Powering On the Unit

The Switch accepts the power input voltage from 20~57VDC.

- ✓ Insert the power cables into the terminal block located on the top of the device.
- ✓ Check the front-panel LEDs as the device is powered on to verify that the Power LED is lit. If not, check that the power cable is correctly and securely plugged in.

**Notice:** 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 go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.**

### DI Interface Setting:

DI is an interface that adds the ability to input and output digital signals in parallel. Using a digital input makes it possible to monitor (read) the statuses of the external sensors (i.e door sensors, water sensors) from remote site.

### Reset Button

There has "Reset" button in front of Switch which can help to manually hardware reboot.



### 3.3. LED Indicators

This Switch is equipped with Unit LEDs to enable you to determine the status of the Switch, as well as Port LEDs to display what is happening in all your connections. They are as follows:

|                             |             |  |
|-----------------------------|-------------|--|
| PWR<br>(Green)              | Illuminated | Power On by terminal block PWR or DC-Jack            |
|                             | Off         | Terminal block PWR/DC-Jack fails or is not available |
| RPS<br>(Green)              | Illuminated | Power On by terminal block RPS                       |
|                             | Off         | Terminal block RPS fails or is not available         |
| ALM<br>(Red)                | Illuminated | PWR/RPS fails or not available                       |
|                             | Off         | No power lost or DIP function is disabled            |
| 10/100/1000<br>Mbps (Green) | Illuminated | Copper port speeds at 1000Mbps                       |
|                             | Off         | Copper port speeds at 10/100Mbps                     |
| LNK/ACT<br>(Green)          | Illuminated | Copper port link-up                                  |
|                             | Blinking    | Data is transmitting / receiving                     |
|                             | Off         | Port disconnected or link failed                     |
| SFP<br>(Green)              | Illuminated | SFP port speeds at 1000Mbps                          |
|                             | Blinking    | Data is transmitting / receiving                     |
|                             | Off         | Port disconnected or link failed                     |

#### Notice:

- ✓ **PWR**: Primary Power
- ✓ **RPS**: Redundant Power Supply
- ✓ **ALM**: Alarm

### 3.4. DIP Switches

**Power: DIP 1 and DIP 2 is for primary power and redundant power supply.**

| No | Name | Description                                  |
|----|------|--|
| 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<br>OFF: Redundant power alarm reporting is disabled |

## 4. System Status

### 4.1. Console Port

- Connect your computer to the console port on the Switch using the appropriate cable.
- Use terminal emulation software with the following settings:

**Default Settings for the Console Port**

| Setting             | Default Value |
|---------------------|---------------|
| Terminal Emulation  | VT100         |
| Baud Rate           | 38400         |
| Parity              | None          |
| Number of Data Bits | 8             |
| Number of Stop Bits | 1             |
| Flow Control        | None          |

- Press [ENTER] to open the login screen.

| Setting          | Default Value |
|------------------|---------------|
| Default Username | admin         |
| Default Password | admin         |

### 4.2. Telnet

- Connect your computer to one of the Ethernet ports.
- Open a Telnet session to the Switch's IP address. If this is your first login, use the default values.

**Default Management IP Address**

| Setting          | Default Value |
|------------------|---------------|
| IP Address       | 192.168.0.254 |
| Subnet Mask      | 255.255.255.0 |
| Default Gateway  | 0.0.0.0       |
| Management VLAN  | 1             |
| Default Username | admin         |
| Default Password | admin         |

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

### 4.3. How to enter the CLI?

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

*Please press Enter to activate this console.*

Input **"admin"** to enter the CLI mode when below message is displayed on the screen.  
**L2SWITCH login:**

You can execute a few limited commands when CLI prompt is displayed as below.

**L2SWITCH>**

If you want to execute more powerful commands, you must enter the privileged mode.

Input command “**enable**”

**L2SWITCH>enable**

Input a valid username and password when below prompt are displayed.

**user: admin**

**password: admin**

**L2SWITCH#**

#### 4.4. CLI Command Concept

| Node      | Command              | Description   |
|-----------|----------------------|---|
| enable    | show hostname        | This command displays the system’s network name.                    |
| configure | reboot               | This command reboots the system.                                    |
| eth0      | ip address A.B.C.D/M | This command configures a static IP and subnet mask for the system. |
| interface | show                 | This command displays the current port configurations.              |
| acl       | show                 | This command displays the current access control profile.           |
| vlan      | show                 | This command displays the current VLAN configurations.              |

#### The Node Type:

- enable  
Its command prompt is “**L2SWITCH#**”.  
It means these commands can be executed in this command prompt.
- configure  
Its command prompt is “**L2SWITCH(config)#**”.  
It means these commands can be executed in this command prompt.  
In **Enable** code, executing command “**configure terminal**” enter the configure node.  
**L2SWITCH#configure terminal**
- eth0  
Its command prompt is “**L2SWITCH(config-if)#**”.  
It means these commands can be executed in this command prompt.  
In **Configure** code, executing command “**interface eth0**” enter the eth0 interface node.  
**L2SWITCH(config)#interface eth0**  
**L2SWITCH(config-if)#**

- interface  
 Its command prompt is “***L2SWITCH(config-if)#***”.  
 It means these commands can be executed in this command prompt.  
 In **Configure** code, executing command “***interface gigaethernet1/0/5***” enter the interface port 5 node.  
 Or  
 In **Configure** code, executing command “***interface fastethernet1/0/5***” enter the interface port 5 node.  
 Note: depend 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  
 Its command prompt is “***L2SWITCH(config-vlan)#***”.  
 It means these commands can be executed in this command prompt.  
 In **Configure** code, executing command “***vlan 2***” enter the vlan 2 node.  
 Note: where the “2” is the vlan ID.

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

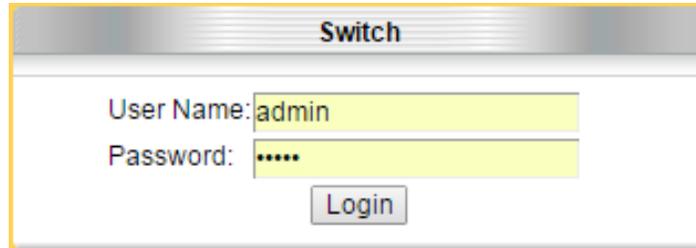
- acl  
 Its command prompt is “***L2SWITCH(config-acl)#***”.  
 It means these commands can be executed in this command prompt.  
 In **Configure** code, executing command “***access-list test***” enter the access-list test node.  
 Note: where the “*test*” is the profile name.

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

#### 4.5. Management via Internet Browser Interface

From a PC, open your Web browser, type the following in the Web address (or location) box: *http://192.168.0.254* and then press <Enter>.

This is the factory default IP address for the Switch. A login dialog is displayed, as shown in the figure:



| Parameter | Description          |
|-----------|----------------------|
| User ID   | Enter the user name. |
| Password  | Enter the password.  |

Enter your user name/password, and then click **Login**.

Use the defaults the first time you log into the program. You can change the password at any time through CLI / GUI interface.

**Default:**

Username: admin

Password: admin

## 4.6. System Information

### 4.6.1. CLI Configuration

| Node   | Command             | Description  |
|--------|---------------------|--|
| enable | show hostname       | This command displays the system's network name.   |
| enable | show interface eth0 | This command will display the interface et0 information.   |
| enable | show model          | This command will display information of switch like vendor, product, mac-address, serial boot code, firmware version etc... |
| enable | show running-config | This command displays the current operating configurations.  |
| enable | show system-info    | This command will display information of CPU loading and memory usage. etc...  |
| enable | show uptime         | This command will display the time from the system power up.   |

#### 4.6.2. 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



| Parameter                 | Description   |
|---------------------------|---|
| <b>System Information</b> |   |
| Model Name                | This field displays the model name of the Switch.                     |
| Host name                 | This field displays the name of the Switch.                           |
| Boot Code Version         | This field displays the boot code version.                            |
| Firmware Version          | This field displays the version of the firmware.                      |
| Built Date                | This field displays the built date of the firmware.                   |
| DHCP Client               | This field displays whether the DHCP client is enabled on the Switch. |
| IP Address                | This field indicates the IP address of the Switch.                    |
| Subnet Mask               | This field indicates the subnet mask of the Switch.                   |

|                      |  |
|----------------------|--|
| Default Gateway      | This field indicates the default gateway of the Switch.  |
| MAC Address          | This field displays the MAC (Media Access Control) address of the Switch.  |
| Serial Number        | The serial number assigned by manufacture for identification of the unit.  |
| Management VLAN      | This field displays the VLAN ID that is used for the Switch management purposes.   |
| CPU Loading          | This field displays the percentage of your Switch's system load.   |
| Memory Information   | This field displays the total memory the Switch has and the memory which is currently available ( <b>Free</b> ) and occupied ( <b>Usage</b> ). |
| Current Time         | This field displays current date (yyyy-mm-dd) and time (hh:mm:ss).   |
| System Uptime        | The time elapsed since the last boot of the operating system.  |
| DHCPv6 Client        | This field displays whether the DHCPv6 client is enabled on the Switch.  |
| IPv6 Local Address   | This field displays the Switch's local IP address for IPv6.  |
| IPv6 Default Gateway | This field displays the default gateway for IPv6.  |
| IPv6 Global Address  | This field displays the Switch's global IP address for IPv6.   |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.  |

## 5. Basic Settings

### 5.1. System Settings

#### 5.1.1. System

##### Management VLAN

To specify a VLAN group which can access the Switch.

- The valid VLAN range is from 1 to 4094.
- If you want to configure a management VLAN, the management VLAN should be created first and the management VLAN should have at least one member port.

##### Host Name

The **hostname** is same as the SNMP system name. Its length is up to 64 characters. The first 16 characters of the hostname will be configured as the CLI prompt.

##### Notices:

The default Hostname is L2SWITCH

The default DHCP client is disabled

The default Static IP is 192.168.0.254

Subnet Mask is 255.255.255.0

Default Gateway is 0.0.0.0

Management VLAN is 1

#### 5.1.1.1. CLI Configuration

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show interface eth0                                | This command displays the eth0 configurations.   |
| enable    | configure terminal                                 | This command changes the node to configure node.   |
| configure | hostname STRINGS                                   | This command sets the system's network name.   |
| configure | interface eth0                                     | This command enters the eth0 interface node to configure the system IP.  |
| eth0      | show   | This command displays the eth0 configurations.   |
| eth0      | ip address A.B.C.D/M                               | This command configures a static IP and subnet mask for the system.  |
| eth0      | ip address default-gateway A.B.C.D                 | This command configures the system default gateway.  |
| eth0      | ip dhcp client (disable enable renew next_restart) | This command configures a DHCP client function for the system.<br><b>disable:</b> Use a static IP address on the switch. |

|      |   |   |
|------|---|---|
|      |   | <b>enable &amp; renew:</b> Use DHCP client to get an IP address from DHCP server.<br><b>next_restart:</b> The settings will take effect on next system restart.   |
| eth0 | management vlan <1-4094>  | This command configures the management vlan.  |
| eth0 | ip ipv6-address<br>AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH/M              | This command configures a global scope of IPv6 address and subnet mask for the system.  |
| eth0 | ip ipv6-addressdefault-gateway<br>AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH | This command configures a default gateway for the system.   |
| eth0 | ip ipv6-dhcp client<br>(disable enable renew next_restart)                | This command configures a DHCPv6 client function for the system.<br><b>disable:</b> Use a static IP address on the switch.<br><b>enable &amp; renew:</b> Use DHCPv6 client to get an IP address from DHCPv6 server.<br><b>next_restart:</b> The settings will take effect on next system restart. |

**Example:** The procedures to configure an IP address for the Switch.

- ✓ To enter the configure node.  
L2SWITCH#configure terminal  
L2SWITCH(config)#
- ✓ To enter the ETH0 interface node.  
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 Switch.  
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 Switch.
  - Please set the static global IPv6 address first.  
L2SWITCH(config-if)#ip ipv6-address 3ffe::1235/64
  - And the set the IPv6 default gateway address.  
L2SWITCH(config-if)#ip ipv6-address default-gateway 3ffe::1234

### 5.1.1.2. Web Configuration

**System Settings**

| System  | Jumbo Frame   | SNTP | Management Host |
|---|---|------|-----------------|
| <b>System Settings</b>  |   |      |                 |
| Hostname  | <input type="text" value="L2SWITCH"/>                                       |      |                 |
| Management VLAN   | <input type="text" value="1"/>  |      |                 |
| <b>IPv4 Settings</b>  |   |      |                 |
| DHCP Client   | <input type="button" value="Enable"/> <input type="button" value="Renew"/>  |      |                 |
| IP Address  | <input type="text" value="192.168.202.65"/>                                 |      |                 |
| Subnet Mask   | <input type="text" value="255.255.255.0"/>                                  |      |                 |
| Default Gateway   | <input type="text" value="192.168.202.1"/>                                  |      |                 |
| <b>IPv6 Settings</b>  |   |      |                 |
| DHCPv6 Client   | <input type="button" value="Disable"/> <input type="button" value="Renew"/> |      |                 |
| Global Address  | <input type="text"/>  |      |                 |
| Default Gateway   | <input type="button" value="Set"/> <input type="text"/>                     |      |                 |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> |   |      |                 |

| Parameter              | Description   |
|------------------------|---|
| <b>System Settings</b> |   |
| Hostname               | The field configures a hostname for the system.   |
| Management VLAN        | The field configures a VLAN group to manage the Switch.   |
| <b>IPv4 Settings</b>   |   |
| DHCP Client            | Select <b>Enable</b> to allow the Switch to automatically get an IP address from a DHCP server. Click <b>Renew</b> to have the Switch re-get an IP address from the DHCP server. Select <b>Disable</b> if you want to configure the Switch's IP address manually. |
| IP Address             | Configures an IPv4 address for your Switch in dotted decimal notation. For example, 192.168.0.254.  |
| Subnet Mask            | Enter the IP subnet mask of your Switch 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.   |
| <b>IPv6 Settings</b>   |   |

|                 |   |
|-----------------|---|
| DHCPv6 Client   | Select <b>Enable</b> to allow the Switch to automatically get an IP address from a DHCPv6 server. Click <b>Renew</b> to have the Switch re-get an IP address from the DHCP server. Select <b>Disable</b> if you want to configure the Switch's IP address manually. |
| Global Address  | Configure a global IPv6 address for the Switch.   |
| Default Gateway | <b>Set</b> – Set an IPv6 default gateway for the Switch.<br><b>Unset</b> – Unset the IPv6 default gateway for the Switch.   |
| Apply           | Click <b>Apply</b> to take effect the settings.   |
| Refresh         | Click <b>Refresh</b> to begin configuring this screen afresh.   |

### 5.1.2. 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.

**Notice:**

- ✓ 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 10240, 1522, 1536, 1552, 9216.

#### 5.1.2.1. CLI Configuration

| Node      | Command                                   | Description  |
|-----------|---|--|
| enable    | show jumboframe                           | This command displays the current jumbo frame settings.                          |
| enable    | configure terminal                        | This command changes the mode to config mode.                                    |
| configure | jumboframe<br>(1522 1536 1552 9216 10240) | This command configures the maximum number of bytes of frame size for all ports. |

#### 5.1.2.2. Web Configuration

**System Settings**

System
Jumbo Frame
SNTP
Management Host

**Jumbo Frame Setting**

Frame Size

| Parameter                   | Description   |
|-----------------------------|---|
| <b>Jumbo Frame Settings</b> |   |
| Frame Size                  | This field configures the maximum number of bytes of frame size for the Switch.<br>(available size:1522/1536/1552/9216/10240) |
| Apply                       | Click <b>Apply</b> to take effect the settings.   |
| Refresh                     | Click <b>Refresh</b> to begin configuring this screen afresh.   |

### 5.1.3. 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.

**Note:**

1. The SNTP server always replies the UTC current time.
2. When the Switch receives the SNTP reply time, the Switch will adjust the time with the time zone configuration and then configure the time to the Switch.
3. If the time server's IP address is not configured, the Switch will not send any SNTP request packets.
4. If no SNTP reply packets, the Switch will retry every 10 seconds forever.
5. If the Switch has received SNTP reply, the Switch will re-get the time from NTP server every 24 hours.
6. If the time zone and time NTP server have been changed, the Switch will repeat the query process.
7. No default SNTP server.

#### 5.1.3.1. CLI Configuration

| Node      | Command                     | Description  |
|-----------|-----------------------------|--|
| enable    | show time                   | This command displays current time and time configurations.  |
| enable    | configure terminal          | This command changes the node to configure node.   |
| configure | time<br>HOUR:MINUTE:SECOND  | Sets the current time on the Switch.<br><i>hour:</i> 0-23<br><i>min:</i> 0-59<br><i>sec:</i> 0-59<br>Note: If you configure Daylight Saving Time after you configure the time, the Switch will apply Daylight Saving Time. |
| configure | time date<br>YEAR/MONTH/DAY | Sets the current date on the Switch.<br><i>year:</i> 1970-<br><i>month:</i> 1-12   |

|           |   |   |
|-----------|---|---|
|           |   | <i>day: 1-31</i>  |
| configure | time daylight-saving-time   | This command enables the daylight saving time.  |
| configure | no time daylight-saving-time  | This command disables daylight saving on the Switch.  |
| configure | time daylight-saving-time start-date<br>(first second third fourth last)(Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH HOUR | This command sets the start time of the Daylight Saving Time.   |
| configure | time daylight-saving-time end-date<br>(first second third fourth last)(Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH HOUR   | This command sets the end time of the Daylight Saving Time.   |
| configure | time ntp-server (disable enable)  | This command disables / enables the NTP server state.   |
| configure | time ntp-server IP_ADDRESS  | This command sets the IP address of your time server.   |
| configure | time ntp-server domain-name STRING  | This command 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.<br>Valid Range: -1200 ~ +1200. |

**Example:**

```
L2SWITCH(config)#time ntp-server 192.5.41.41
L2SWITCH(config)#time timezone +0800
L2SWITCH(config)#time ntp-server enable
L2SWITCH(config)#time daylight-saving-time start-date first Monday 6 0
L2SWITCH(config)#time daylight-saving-time end-date last Saturday 10 0
```

### 5.1.3.2. Web Configuration

**System Settings**

| System  | Jumbo Frame                                | SNTP   | Management Host         |
|---|--|--------|-------------------------|
| <b>Current Time and Date</b>  |  |        |                         |
| Current Time  | 00:25:59 (UTC+0)                           |        |                         |
| Current Date  | 2020-01-01                                 |        |                         |
| <b>Time and Date Settings</b>   |  |        |                         |
| <input checked="" type="radio"/> <b>Manual</b>                              |  |        |                         |
| New Time  | 2020                                       | .      | 1                       |
|   | .  | 1      | /                       |
|   | 0  | :      | 25                      |
|   | :  | 59     | (yyyy.mm.dd / hh:mm:ss) |
| <input type="radio"/> <b>Enable Network Time Protocol</b>                   |  |        |                         |
| NTP Server  | <input type="radio"/> ntp0.fau.de - Europe |        |                         |
|   | <input checked="" type="radio"/> IPv4      |        |                         |
|   | 0.0.0.0                                    |        |                         |
| Time Zone   | +0000 (+hh / -hh / +hhmm / -hhmm)          |        |                         |
| <b>Daylight Saving Settings</b>   |  |        |                         |
| State   | Disable                                    |        |                         |
| Start Date  | First                                      | Sunday | of January at 0 o'clock |
| End Date  | First                                      | Sunday | of January at 0 o'clock |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> |  |        |                         |

| Parameter                    | Description   |
|------------------------------|---|
| <b>Current Time and Date</b> |   |
| Current Time                 | This field displays the time you open / refresh this menu.  |
| Current Date                 | This field displays the date you open / refresh this menu.  |
| <b>Time and Date Setting</b> |   |
| 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 <b>Current Date</b> and <b>Current Time</b> fields after you click <b>Apply</b> . |
| 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 IPv6 address or type the domain name of your time  |

|                                 |  |
|---------------------------------|--|
|                                 | server. The Switch 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.  |
| <b>Daylight Saving Settings</b> |  |
| State                           | Select <b>Enable</b> if you want to use Daylight Saving Time. Otherwise, select <b>Disable</b> to turn it off.   |
| Start Date                      | <p>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:</p> <p>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 <b>Second, Sunday, March</b> and <b>2:00</b>.</p> <p>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 <b>Last, Sunday, March</b> and the last field depends on your time zone. In Germany for instance, you would select <b>2:00</b> because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p> |
| End Date                        | <p>Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving Time. The time field uses the 24 hour format.</p> <p>Here are a couple of examples:</p> <p>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 <b>First, Sunday, November</b> and <b>2:00</b>.</p> <p>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 <b>Last, Sunday, October</b> and the last field depends on your time zone. In Germany for instance, you would select <b>2:00</b> because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>               |
| Apply                           | Click <b>Apply</b> to take effect the settings.  |
| Refresh                         | Click <b>Refresh</b> to begin configuring this screen afresh.  |

#### 5.1.4. Management Host

The feature limits the hosts which can manage the Switch. The default has no management host. That is, any hosts can manage the Switch via **telnet** or **web browser**. If user has configured one or more management host, the Switch can be managed by these hosts only. The feature allow user to configure management IP up to 10 entries.

#### Notices:

This feature allows user to configure management host up to 10 entries.

The default is none, any host can manage the Switch via telnet or web browser.

##### 5.1.4.1. CLI Configuration

| Node      | Command                          | Description   |
|-----------|----------------------------------|---|
| enable    | show interface eth0              | This command displays the eth0 configurations.                                      |
| enable    | configure terminal               | This command changes the node to configure node.                                    |
| configure | interface eth0                   | This command enters the eth0 interface node to configure the system configurations. |
| eth0      | management host                  | This command configures a static IP and subnet mask for the system.                 |
| eth0      | show                             | The command displays the all of the interface eth0 configurations.                  |
| eth0      | management host A.B.C.D          | The command adds a management host address.   |
| eth0      | management subnet-host A.B.C.D/M | The command adds a management host address with a subnet mask.                      |
| eth0      | no management host A.B.C.D       | The command deletes a management host address.                                      |

#### Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#management 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
      DHCP Server port(s): 1-6
Eth0      DHCP client: 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 HWaddr 00:0B: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  
 UP BROADCAST RUNNING ALLMULTI MULTICAST MTU:1500  
 Metric:1 ASYMMETRY:0  
 RX packets:17931 errors:0 dropped:6680 overruns:0 frame:0  
 TX packets:6500 errors:0 dropped:0 overruns:0 carrier:0  
 collisions:0 txqueuelen:500  
 RX bytes:3565872 (3.4 Mb) TX bytes:1173040 (1.1 Mb)

### 5.1.4.2. Web Configuration

**System Settings**

| System  | Jumbo Frame              | SNTP   | Management Host |
|---|--------------------------|--|-----------------|
| <b>Management Host Settings</b>                             |                          |  |                 |
| Management Host: <input style="width: 150px;" type="text"/> |                          | Subnet Mask: <input style="width: 80px;" type="text"/> |                 |
| <input type="button" value="Apply"/>                        |                          | <input type="button" value="Refresh"/>                 |                 |
| <b>Management Host List</b>                                 |                          |  |                 |
| No.   | Management Host(IP/Mask) | Action   |                 |
| 1   | 192.168.202.1/24         | <input type="button" value="Delete"/>                  |                 |

| Parameter                       | Description   |
|---------------------------------|---|
| <b>Management Host Settings</b> |   |
| Management Host                 | This field configures a management host in dotted decimal notation. For example, 192.168.0.254.   |
| Subnet Mask                     | This field configures the number of mask bit which allows to configure a range of hosts. If you do not specify value, the system will give 32 for the host automatically. |
| Apply                           | Click <b>Apply</b> to take effect the settings.   |
| Refresh                         | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>Management Host List</b>     |   |
| No.                             | This field displays a sequential number for each management host.   |
| Management Host (IP/Mask)       | This field displays the management host and the number of mask bit.   |
| Action                          | Click <b>Delete</b> to remove the specified entry.  |

## 5.2. MAC Management

### Dynamic Address

The MAC addresses are learnt by the switch. When the switch 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 switch. The static address can be removed by user only.

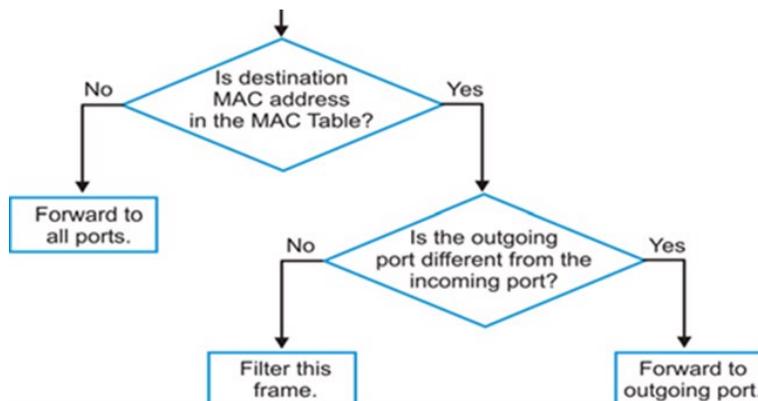
The maximum static address entry is up to 256.

The switch supports up to 16K address table. The static address and the dynamic address share the same table.

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

The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

1. The Switch examines a received frame and learns the port from which this source MAC address came.
2. The Switch checks to see if the frame's destination MAC address matches a source MAC address already learnt in the **MAC Table**.
  - ✓ If the Switch has already learnt the port for this MAC address, then it forwards the frame to that port.
  - ✓ If the Switch has not already learnt the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
  - ✓ If the Switch 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.



**Figure: MAC Table Flowchart**

**Notices:**

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

**5.2.1. 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.

**5.2.1.1. CLI Configuration**

| Node      | Command   | Description  |
|-----------|---|--|
| enable    | show mac-address-table (static dynamic)                     | This command displays the current <b>static/dynamic</b> unicast address entries. |
| enable    | configure terminal  | This command changes the node to configure node.                                 |
| configure | mac-address-table static MACADDR vlan <1-4094> port PORT_ID | This command configures a static unicast entry.                                  |
| configure | no mac-address-table static MACADDR vlan <1-4094>           | This command removes a static unicast entry from the address table.              |

**5.2.1.2. Web Configuration**

**MAC Management**

Static MAC
MAC Table
Age Time

Static MAC Settings

| MAC Address                               | VLAN ID                                   | Port                                       |
|---|---|--|
| <input style="width: 100%;" type="text"/> | <input style="width: 100%;" type="text"/> | 1 <span style="font-size: small;">▼</span> |

Static MAC Table

| MAC Address       | VLAN ID | Port | Action                                |
|-------------------|---------|------|---------------------------------------|
| 00:0b:04:11:22:33 | 1       | 1    | <input type="button" value="Delete"/> |
| 00:0b:04:84:16:24 | 1       | CPU  |                                       |

Total Counts: 2

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

| <b>Static MAC Settings</b> |   |
|----------------------------|---|
| MAC Address                | Enter the MAC address of a computer or device that you want to add to the MAC address table.<br>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 <b>Apply</b> to take effect the settings.   |
| Refresh                    | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>Static MAC Table</b>    |   |
| MAC Address                | This field displays the MAC address of a manually entered MAC address entry.  |
| VLAN ID                    | This field displays the VID of a manually entered MAC address entry.  |
| Port                       | This field displays the port number of a manually entered MAC address entry. The MAC address with port CPU means the Switch's MAC addresses itself. |
| Action                     | Click <b>Delete</b> to remove this manually entered MAC address entry from the MAC address table.   |

## 5.2.2. MAC Table

### 5.2.2.1. CLI Configuration

| Node      | Command                                 | Description  |
|-----------|---|--|
| enable    | show mac-address-table (static dynamic) | This command displays the current <b>static/dynamic</b> unicast address entries.       |
| enable    | show mac-address-table mac MACADDR      | This command displays information of a specific MAC.                                   |
| enable    | show mac-address-table port PORT_ID     | This command displays the current unicast address entries learnt by the specific port. |
| enable    | configure terminal                      | This command changes the node to configure node.                                       |
| configure | clear mac address-table dynamic         | This command clears the dynamic address entries.                                       |

### 5.2.2.2. Web Configuration

**MAC Management**

Static MAC
MAC Table
Age Time

**MAC Table**

Show Type: All Apply Refresh Clear

| MAC Address       | Type    | VLAN ID | Port/Trunk ID |
|-------------------|---------|---------|---------------|
| 00:0b:04:00:00:05 | Static  | 1       | CPU           |
| 18:31:bf:92:d4:a2 | Dynamic | 1       | 1             |
| a0:8c:fd:ec:12:f8 | Dynamic | 1       | 1             |
| 00:0b:04:00:01:5e | Dynamic | 1       | 1             |
| 00:0b:04:90:60:21 | Dynamic | 1       | 1             |
| bc:ee:7b:db:a2:9e | Dynamic | 1       | 1             |
| f4:6d:04:e6:f9:59 | Dynamic | 1       | 1             |

Total Counts: 7

Page UP
Page Down
Page: 1/1
Page: 1 Apply

| Parameter        | Description   |
|------------------|---|
| <b>Mac Table</b> |   |
| Show Type Apply  | Select <b>All, Static, Dynamic or Port</b> and then click <b>Apply</b> to display the corresponding MAC address entries on this screen. |
| Refresh          | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| MAC Address      | This field displays a MAC address.  |
| Type             | This field displays whether this entry was entered manually (Static) or whether it was learned by the Switch (Dynamic).                 |

|                 |  |
|-----------------|--|
| VLAN ID         | This field displays the VLAN ID of the MAC address entry.  |
| Port / Trunk ID | This field displays the port number / Trunk ID the MAC address entry is associated.<br>It displays CPU if it is the entry for the Switch itself.<br>The CPU means that it is the Switch's MAC. |
| Total Counts    | This field displays the total entries in the MAC table.  |

### 5.2.3. Age Time

#### 5.2.3.1. CLI Configuration

| Node      | Command                            | Description   |
|-----------|------------------------------------|---|
| enable    | show mac-address-table aging-time  | This command displays the current MAC address table age time.                           |
| enable    | configure terminal                 | This command changes the node to configure node.  |
| configure | mac-address-table aging-time VALUE | This command configures the mac table aging time. The range is 20 to 500 or 0: disable. |

**Example:**

```
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.
```

#### 5.2.3.2. Web Configuration

**MAC Management**

Static MAC    MAC Table    **Age Time**

**Age Time Settings**

Age Time:  (sec) (Range: 20-500 or 0:disable)

| Parameter                | Description  |
|--------------------------|--|
| <b>Age Time Settings</b> |  |
| Age Time                 | Configure the age time; the valid range is from 20 to 500 seconds. The default value is 300 seconds. 0 means that the system will not age out any entries. |
| Apply                    | Click <b>Apply</b> to take effect the settings.  |
| Refresh                  | Click <b>Refresh</b> to begin configuring this screen afresh.  |

### 5.3. Port Mirror

#### Port-Based Mirroring

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 will be copied to the monitor port.

#### Notices:

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 will be removed from the source ports automatically.

#### 5.3.1. CLI Configuration

| Node      | Command  | Description   |
|-----------|--|---|
| enable    | show mirror  | This command displays the current port mirroring configurations.                                    |
| enable    | configure terminal   | This command changes the node to configure node.  |
| configure | mirror<br>(disable enable)                                     | This command <b>disables</b> / <b>enables</b> the port mirroring on the switch.                     |
| configure | mirror destination<br>port PORT_ID                             | This command specifies the <b>monitor port</b> for the port mirroring.                              |
| configure | mirror source ports<br>PORT_LIST mode<br>(both ingress egress) | This command <b>adds</b> a port or a range of ports as the source ports of the port mirroring.      |
| configure | no mirror source ports<br>PORT_LIST                            | This command <b>removes</b> a port or a range of ports from the source ports of the port mirroring. |

#### Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#mirror destination port 9
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.
```

### 5.3.2. Web Configuration

**Port Mirror**

**Port Mirroring Settings**

State Disable ▾

Monitor to Port 1 ▾

---

All Ports : - ▾

| Source Port | Mirror Mode | Source Port | Mirror Mode |
|-------------|-------------|-------------|-------------|
| 1           | Disable ▾   | 2           | Disable ▾   |
| 3           | Disable ▾   | 4           | Disable ▾   |
| 5           | Disable ▾   | 6           | Disable ▾   |

| Parameter                      | Description  |
|--------------------------------|--|
| <b>Port Mirroring Settings</b> |  |
| State                          | Select <b>Enable</b> to turn on port mirroring or select <b>Disable</b> 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.<br>Use this field only if you want to make some settings the same for all ports.<br>Use this field first to set the common settings and then make adjustments on a port-by-port basis.  |
| Source Port                    | This field displays the number of a port.  |
| Mirror Mode                    | Select <b>Ingress</b> , <b>Egress</b> or <b>Both</b> to only copy the ingress (incoming), egress (outgoing) or both (incoming and outgoing) traffic from the specified source ports to the monitor port.<br>Select <b>Disable</b> to not copy any traffic from the specified source ports to the monitor port. |
| Apply                          | Click <b>Apply</b> to take effect the settings.  |

Refresh

Click **Refresh** to begin configuring this screen afresh.

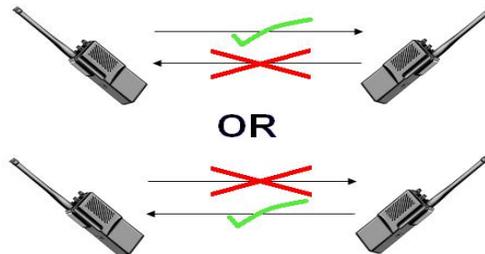
## 5.4. Port Settings

- 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.

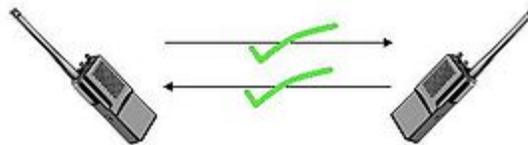
### Half Duplex:

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 direction 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.



- Loopback Test

A loopback test is a test in which a signal is sent from a communications device and returned (looped back) to it as a way to determine whether the device is working right or as a way to pin down a failing node in a network. One type of loopback test is performed using a special plug, called a **wrap plug** that is inserted in a port on a communications device. The effect of a wrap plug is to cause transmitted (output) data to be returned as received (input) data, simulating a complete communications circuit using a single computer.

- 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-MDIX was developed by HP engineers Dan Dove and Bruce Melvin.

- 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 Switch 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 Switch determines the connection speed by detecting the signal on the cable and using **half-duplex** mode. When the Switch'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 Switch uses IEEE802.3x flow control in full duplex mode and backpressure 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.

**Note: 1000 Base-T does not support force mode.**

## 5.4.1. General Settings

### 5.4.1.1. CLI Configuration

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show interface IFNAME  | This command displays the current port configurations.                       |
| enable    | configure terminal   | This command changes the node to configure node.                             |
| configure | interface IFNAME   | This command enters the interface configure node.                            |
| interface | show   | This command displays the current port configurations.                       |
| interface | loopback (none  mac)   | This command tests the loopback mode of operation for the specific port.     |
| interface | flowcontrol (off   on)   | This command <b>disables</b> / <b>enables</b> the flow control for the port. |
| interface | speed (auto 10-full   10-full-n   10-half   10-half-n   100-full | This command configures the speed and duplex for the ports.                  |

|           |  |  |
|-----------|--|--|
|           | 100-full-n   100-half   100-half-n   1000-full   1000-full-n)  | <p>auto: Auto negotiation mode.</p> <p>10-full: 10Mbps Full duplex force mode.</p> <p>10-full-n: 10Mbps Full duplex auto negotiation mode.</p> <p>10-half: 10Mbps Half duplex force mode.</p> <p>10-half-n: 10Mbps Half duplex auto negotiation mode.</p> <p>100-full: 100Mbps Full duplex force mode.</p> <p>100-full-n: 100Mbps Full duplex auto negotiation mode.</p> <p>100-half: 100Mbps Half duplex force mode.</p> <p>100-half-n: 100Mbps Half duplex auto negotiation mode.</p> <p>1000-full: 1000Mbps Full duplex force mode.</p> <p>1000-full-n: 1000Mbps Full duplex auto negotiation mode.</p> |
| interface | shutdown   | This command disables the specific port.   |
| interface | no shutdown  | This command enables the specific port.  |
| configure | interface range<br>gigabitethernet1/0/PORTLISTS  | This command enters the if-range configure node.   |
| if-range  | shutdown   | This command disables the specific ports.  |
| if-range  | no shutdown  | This command enables the specific ports.   |
| if-range  | speed (auto 10-full   10-full-n   10-half   10-half-n   100-full   100-full-n   100-half   100-half-n   1000-full   1000-full-n) | <p>This command configures the speed and duplex for the ports.</p> <p>auto: Auto negotiation mode.</p> <p>10-full: 10Mbps Full duplex force mode.</p> <p>10-full-n: 10Mbps Full duplex auto negotiation mode.</p> <p>10-half: 10Mbps Half duplex force mode.</p> <p>10-half-n: 10Mbps Half duplex auto negotiation mode.</p> <p>100-full: 100Mbps Full duplex force mode.</p> <p>100-full-n: 100Mbps Full duplex auto negotiation mode.</p> <p>100-half: 100Mbps Half duplex force mode.</p> <p>100-half-n: 100Mbps Half duplex auto negotiation mode.</p>   |

|  |  |  |
|--|--|--|
|  |  | 1000-full:1000Mbps Full duplex force mode.<br>1000-full-n: 1000Mbps Full duplex auto negotiation mode. |
|--|--|--|

### 5.4.1.2. Web Configuration

**Port Settings**

General Settings
Information

Port Settings

| Port  | State                               | Speed/Duplex                      | Flow Control                    |
|---|-------------------------------------|-----------------------------------|---------------------------------|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="Enable"/> | <input type="text" value="Auto"/> | <input type="text" value="On"/> |

Port Status

| Port | State   | Speed/Duplex | Flow Control | Link Status       |
|------|---------|--------------|--------------|-------------------|
| 1    | Enabled | Auto         | On           | 1000M / Full / On |
| 2    | Enabled | Auto         | On           | Link Down         |
| 3    | Enabled | Auto         | On           | Link Down         |
| 4    | Enabled | Auto         | On           | Link Down         |
| 5    | Enabled | Auto         | On           | Link Down         |
| 6    | Enabled | Auto         | On           | Link Down         |

| Parameter            | Description   |
|----------------------|---|
| <b>Port Settings</b> |   |
| Port                 | Select a port or a range ports you want to configure on this screen.  |
| State                | Select <b>Enable</b> to activate the port or <b>Disable</b> to deactivate the port.   |
| Speed/Duplex         | Select the speed and duplex mode of the port. The choices are: <ul style="list-style-type: none"> <li>• <b>Auto</b></li> <li>• <b>10 Mbps / Full Duplex</b></li> <li>• <b>10 Mbps / Full Duplex / Nway</b></li> <li>• <b>10 Mbps / Half Duplex</b></li> <li>• <b>10 Mbps / Half Duplex / Nway</b></li> <li>• <b>100 Mbps / Full Duplex</b></li> <li>• <b>100 Mbps / Full Duplex / Nway</b></li> <li>• <b>100 Mbps / Half Duplex</b></li> <li>• <b>100 Mbps / Half Duplex / Nway</b></li> <li>• <b>1000 Mbps / Full Duplex</b></li> <li>• <b>1000 Mbps / Full Duplex / Nway</b></li> </ul> |
| Flow Control         | Select <b>On</b> to enable access to buffering resources for the port thus ensuring lossless operation across network switches. Otherwise, select <b>Off</b> to disable it.   |
| Apply                | Click <b>Apply</b> to take effect the settings.   |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.   |

| Port Status  |  |
|--------------|--|
| Port         | This field displays the port number.   |
| State        | This field displays whether the port is enabled or disabled.   |
| Speed/Duplex | This field displays the speed either <b>10M</b> , <b>100M</b> or <b>1000M</b> and the duplex mode <b>Full</b> or <b>Half</b> .   |
| Flow Control | This field displays whether the port's flow control is <b>On</b> or <b>Off</b> .   |
| Link Status  | This field 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 <b>Link Down</b> if the port is disabled or not connected to any device. |

## 5.4.2. Information

### 5.4.2.1. CLI Configuration

| Node      | Command   | Description   |
|-----------|---|---|
| enable    | show interface IFNAME                           | This command displays the current port configurations.  |
| enable    | configure terminal                              | This command changes the node to configure node.  |
| configure | interface IFNAME                                | This command enters the interface configure node.   |
| interface | show  | This command displays the current port configurations.  |
| interface | description STRING                              | This command configures a description for the specific port. The length of description is up to 240 characters. |
| interface | no description                                  | This command configures the default port description.   |
| interface | alias STRING                                    | This command configures an alias for the specific port. The length of alias is up to 64 characters.             |
| interface | no alias  | This command reset the alias to default.  |
| configure | interface range<br>gigabitethernet1/0/PORTLISTS | This command enters the if-range configure node.  |
| if-range  | description STRINGs                             | This command configures a description for the specific ports.   |
| if-range  | no description                                  | This command configures the default port description for the specific ports.                                    |

|          |              |  |
|----------|--------------|--|
| if-range | alias STRING | This command configures an alias for the specific ports. The length of alias is up to 64 characters. |
| if-range | no alias     | This command reset the alias to default.   |

#### 5.4.2.2. Web Configuration

**Port Settings**

General Settings
Information

Port Settings

| Port  | Description                                       | Alias   |
|---|---|---|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="gigabitethernet1/0/1"/> | <input type="text" value="gigabitethernet1/0/1"/> |

Port Status

| Port | Description          | Alias                | Status   | Uptime        | Medium Mode |
|------|----------------------|----------------------|----------|---------------|-------------|
| 1    | gigabitethernet1/0/1 | gigabitethernet1/0/1 | Normally | 0 days 0:1:37 | Copper      |
| 2    | gigabitethernet1/0/2 | gigabitethernet1/0/2 | Normally | 0 days 0:0:0  | Copper      |
| 3    | gigabitethernet1/0/3 | gigabitethernet1/0/3 | Normally | 0 days 0:0:0  | Copper      |
| 4    | gigabitethernet1/0/4 | gigabitethernet1/0/4 | Normally | 0 days 0:0:0  | Copper      |
| 5    | gigabitethernet1/0/5 | gigabitethernet1/0/5 | Normally | 0 days 0:0:0  | Copper      |
| 6    | gigabitethernet1/0/6 | gigabitethernet1/0/6 | Normally | 0 days 0:0:0  | Fiber       |

| Parameter            | Description  |
|----------------------|--|
| <b>Port Settings</b> |  |
| Port                 | Select a port or a range ports you want to configure on this screen. |
| Description          | Configures a meaningful name for the port(s).                        |
| Alias                | Configures an alias for the port(s).                                 |
| Apply                | Click <b>Apply</b> to take effect the settings.                      |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.        |
| <b>Port Status</b>   |  |
| Port                 | This field displays the port number.                                 |
| Description          | The meaningful name for the port.                                    |
| Alias                | The alias name for the port.   |

|             |  |
|-------------|--|
| Status      | The field displays the detail port status if the port is blocked by some protocol. |
| Uptime      | The sustained time from last link up.  |
| Medium Mode | The current working medium mode, copper or fiber, for the port.                    |

## 6. Advanced Settings

### 6.1. Bandwidth Control

#### 6.1.1. 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 Switch supports 802.1p priority queuing. The Switch 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 Switch's priority queues as follows:

|          |     |   |   |   |   |   |   |   |
|----------|-----|---|---|---|---|---|---|---|
| Priority | : 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Queue    | : 2 | 0 | 1 | 3 | 4 | 5 | 6 | 7 |

Priority scheduling is implemented by the priority queues stated above. The Switch 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 Switch 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 Switch allows you to choose one of the following methods for assigning priority to incoming packets on the Switch:

- **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 Switch.
- **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 Switch. The Switch 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 Switch.*

### 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         |

### 6.1.1.1. Port Priority

#### 6.1.1.1.1. CLI Configuration

| Node      | Command                | Description  |
|-----------|------------------------|--|
| enable    | show interface IFNAME  | This command displays the current port configurations.   |
| enable    | configure terminal     | This command changes the node to configure node.   |
| configure | interface IFNAME       | This command enters the interface configure node.  |
| interface | default-priority <0-7> | This command allows the user to specify a default priority handling of untagged packets received by the Switch. 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    | This command configures the default priority (0) for the specific port.  |

#### 6.1.1.1.2. Web Configuration

**QoS**

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

**Port Priority Settings**

All Ports 802.1p priority :

| Port | 802.1p priority                | Port | 802.1p priority                |
|------|--------------------------------|------|--------------------------------|
| 1    | <input type="text" value="0"/> | 2    | <input type="text" value="0"/> |
| 3    | <input type="text" value="0"/> | 4    | <input type="text" value="0"/> |
| 5    | <input type="text" value="0"/> | 6    | <input type="text" value="0"/> |

| Parameter                     | Description  |
|-------------------------------|--|
| <b>Port Priority Settings</b> |  |
| 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                          | This field displays the number of a port.  |
| 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 <b>Apply</b> to take effect the settings.               |
| Refresh | Click <b>Refresh</b> to begin configuring this screen afresh. |

### 6.1.1.2. 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 tradeoff between low-delay, high-reliability, and high-throughput.

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

|            |   |   |   |   |   |   |   |
|------------|---|---|---|---|---|---|---|
| Bit 0      | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| PRECEDENCE |   |   | D | T | R | 0 | 0 |

### 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.

#### 6.1.1.2.1. CLI Configuration

| Node      | Command                                | Description  |
|-----------|--|--|
| enable    | show diffserv                          | This command displays DiffServ configurations.                       |
| enable    | configure terminal                     | This command changes the node to configure node.                     |
| configure | diffserv<br>(disable enable)           | This command <b>disables</b> / <b>enables</b> the DiffServ function. |
| configure | diffserv dscp <0-63><br>priority <0-7> | This command sets the DSCP-to-IEEE 802.1q mappings.                  |

### 6.1.1.2.2. Web Configuration

**QoS**

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

**DSCP Settings**

Mode Tag Over DSCP ▾

| DSCP    | Priority   | DSCP    | Priority   | DSCP    | Priority   | DSCP    | Priority   |
|---------|--|---------|--|---------|--|---------|--|
| DSCP 0  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 1  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 2  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 3  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 4  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 5  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 6  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 7  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 8  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 9  | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 10 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 11 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 12 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 13 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 14 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 15 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 16 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 17 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 18 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 19 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 20 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 21 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 22 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 23 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 24 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 25 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 26 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 27 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 28 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 29 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 30 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 31 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 32 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 33 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 34 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 35 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 36 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 37 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 38 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 39 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 40 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 41 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 42 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 43 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 44 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 45 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 46 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 47 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 48 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 49 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 50 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 51 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 52 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 53 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 54 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 55 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 56 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 57 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 58 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 59 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |
| DSCP 60 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 61 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 62 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> | DSCP 63 | <span style="border: 1px solid #ccc; padding: 2px;">0 ▾</span> |

Apply
Refresh

| Parameter            | Description   |
|----------------------|---|
| <b>DSCP Settings</b> |   |
| Mode                 | “Tag Over DSCP” or “DSCP Over Tag”. “Tag Over DSCP” means the 802.1p tag has higher priority than DSCP.     |
| Priority             | This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority). |
| Apply                | Click <b>Apply</b> to take effect the settings.   |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.   |

### 6.1.1.3. Priority/Queue Mapping

#### 6.1.1.3.1. CLI Configuration

| Node      | Command                      | Description  |
|-----------|------------------------------|--|
| enable    | show queue cos-map           | This command displays the current 802.1p priority mapping to the service queue.      |
| enable    | configure terminal           | This command changes the node to configure node.                                     |
| configure | queue cos-map <0-7><br><0-7> | This command configures the 802.1p priority mapping to the service queue.            |
| configure | no queue cos-map             | This command 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
```

### 6.1.1.3.2. Web Configuration

**QoS**

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

**Priority/Queue Mapping Settings**

| Priority | Queue ID |
|----------|----------|
| 0        | 1 ▾      |
| 1        | 0 ▾      |
| 2        | 2 ▾      |
| 3        | 3 ▾      |
| 4        | 4 ▾      |
| 5        | 5 ▾      |
| 6        | 6 ▾      |
| 7        | 7 ▾      |

| Parameter                              | Description   |
|--|---|
| <b>Priority/Queue Mapping Settings</b> |   |
| Reset to Default                       | Click this button to reset the priority to queue mappings to the defaults.                                  |
| Priority                               | This field 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 <b>Apply</b> to take effect the settings.   |
| Refresh                                | Click <b>Refresh</b> to begin configuring this screen afresh.   |

#### 6.1.1.4. 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.

- **Weighted Fair Queuing (WFQ)**

WFQ is a data packet scheduling technique allowing different scheduling priorities to statistically multiplexed data flows. It provides traffic priority management that automatically sorts among individual traffic streams without requiring an access list. WFQ decides which queue is selected in one slot time to guarantee the minimal packet rate of one queue. Thus, WFQ allows Internet operators to define traffic classes and then assign different bandwidth proportions.

##### 6.1.1.4.1. CLI Configuration

| Node      | Command             | Description  |
|-----------|---------------------|--|
| enable    | show qos mode       | This command displays the current QoS scheduling mode of IEEE 802.1p.  |
| enable    | configure terminal  | This command changes the node to configure node.   |
| configure | qos mode high-first | This command 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> | This command configures the QoS scheduling mode to Weighted Round Robin.          |
| configure | qos mode wfq-queue weights <1-127> <1-127> <1-127> <1-127> <1-127> <1-127> | This command configures the QoS scheduling mode to <b>Weighted Fair Queuing</b> . |

#### 6.1.1.4.2. Web Configuration

**QoS**

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

Schedule Mode Settings

Schedule Mode:  ▼

| Queue ID | Weight Value(Range:1~127) |
|----------|---------------------------|
| 0        | <input type="text"/>      |
| 1        | <input type="text"/>      |
| 2        | <input type="text"/>      |
| 3        | <input type="text"/>      |
| 4        | <input type="text"/>      |
| 5        | <input type="text"/>      |
| 6        | <input type="text"/>      |
| 7        | <input type="text"/>      |

| Parameter                     | Description   |
|-------------------------------|---|
| <b>Schedule Mode Settings</b> |   |
| Schedule Mode                 | <p>Select <b>High First(SPQ)</b> or <b>Weighted Round Robin (WRR)</b>.<br/>           Note: Queue weights can only be changed when <b>Weighted Round Robin</b> is selected.</p> <p><b>High First(SPQ=Strict Priority Queue):</b><br/>           Packets with higher priority levels are always transmitted before packets with lower priority levels.</p> <p><b>Weighted Round Robin</b> scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue <b>Weight</b> field). Queues with larger weights get more service than queues with smaller weights.</p> <p><b>Weighted Fair Queuing (WFQ):</b></p> |

|              |   |
|--------------|---|
| Queue ID     | This field 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 <b>Weighted Round Robin</b> is selected. Bandwidth is divided across the different traffic queues according to their weights. |
| Apply        | Click <b>Apply</b> to take effect the settings.   |
| Refresh      | Click <b>Refresh</b> to begin configuring this screen afresh.   |

## 6.1.2. Rate Limitation

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

Broadcast storm control limits the number of broadcast, multicast and unknown unicast (also referred to as Destination Lookup Failure or DLF) packets the Switch receives per second on the ports. 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: pps.**

#### 6.1.2.1.1. CLI Configuration

| Node      | Command   | Description  |
|-----------|---|--|
| enable    | show storm-control  | This command displays the current storm control configurations.  |
| enable    | configure terminal  | This command changes the node to configure node.   |
| configure | storm-control rate <1-5000> type (broadcast   multicast  DLF) ports PORTLISTS | This command enables the bandwidth limit for broadcast or multicast or DLF packets and set the limitation. |

|           |  |   |
|-----------|--|---|
| configure | no storm-control type<br>(broadcast   multicast<br> DLF) ports PORTLISTS | This command disables the bandwidth limit<br>for broadcast or multicast or DLF packets. |
|-----------|--|---|

### 6.1.2.1.2. Web Configuration

**Rate Limitation**

Storm Control
Bandwidth Limitation

Storm Control Settings

| Port  | Rate                                 | Type                                   |
|---|--------------------------------------|--|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="0"/> (pps) | <input type="text" value="Broadcast"/> |

(Range:1~5000, 0:Disable)

Storm Control Status

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

| Parameter                     | Description   |
|-------------------------------|---|
| <b>Storm Control Settings</b> |   |
| 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 <b>Type</b> field) per second the Switch can receive per second.   |
| Type                          | Select <b>Broadcast</b> - to specify a limit for the amount of broadcast packets received per second.<br><b>Multicast</b> - to specify a limit for the amount of multicast packets received per second.<br><b>DLF</b> - to specify a limit for the amount of DLF packets received per second. |
| Apply                         | Click <b>Apply</b> to take effect the settings.   |
| Refresh                       | Click <b>Refresh</b> to begin configuring this screen afresh.   |

### 6.1.2.2. Bandwidth Limitation

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

Rate Limitation unit: 16 Kbits.

#### 6.1.2.2.1. CLI Configuration

| Node      | Command   | Description   |
|-----------|---|---|
| enable    | show bandwidth-limit                              | This command displays the current rate control configurations.                        |
| enable    | configure terminal                                | This command changes the node to configure node.                                      |
| configure | bandwidth-limit egress <0-62500> ports PORTLISTS  | This command enables the bandwidth limit for outgoing packets and set the limitation. |
| configure | no bandwidth-limit egress ports PORTLISTS         | This command disables the bandwidth limit for outgoing packets.                       |
| configure | bandwidth-limit ingress <0-62500> ports PORTLISTS | This command enables the bandwidth limit for incoming packets and set the limitation. |
| configure | no bandwidth-limit ingress ports PORTLISTS        | This command disables the bandwidth limit for incoming packets.                       |

#### Example:

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

### 6.1.2.2.2. Web Configuration

**Rate Limitation**

Storm Control
Bandwidth Limitation

**Bandwidth Limitation Settings**

| Port  | Ingress                                    | Egress                                     |
|---|--|--|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="0"/> * 16(Kbits) | <input type="text" value="0"/> * 16(Kbits) |

(Range:1~62500, 0:Disable)

**Bandwidth Limitation Status**

| Port | Ingress (Kb) | Egress (Kb) | Port | Ingress (Kb) | Egress (Kb) |
|------|--------------|-------------|------|--------------|-------------|
| 1    | 0            | 0           | 2    | 0            | 0           |
| 3    | 0            | 0           | 4    | 0            | 0           |
| 5    | 0            | 0           | 6    | 0            | 0           |

| Parameter                            | Description   |
|--------------------------------------|---|
| <b>Bandwidth Limitation Settings</b> |   |
| Port                                 | Selects a port that you want to configure.                    |
| Ingress                              | Configures the rate limitation for the ingress packets.       |
| Egress                               | Configures the rate limitation for the egress packets.        |
| Apply                                | Click <b>Apply</b> to take effect the settings.               |
| Refresh                              | Click <b>Refresh</b> to begin configuring this screen afresh. |

## **6.2. IGMP Snooping**

### **6.2.1. IGMP Snooping**

The IGMP snooping is for multicast traffic. The Switch 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 Switch to learn multicast groups without you having to manually configure them.

The Switch 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 Switch to learn multicast groups without you having to manually configure them.

The Switch 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 Switch.

The Switch can perform IGMP snooping on up to 4094 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch 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 Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

#### **Configurations:**

Users can enable/disable the IGMP Snooping on the Switch. Users also can enable/disable the IGMP Snooping on a specific VLAN. If the IGMP Snooping on the Switch 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.

**Notices:** There are a global state and per VLAN states. When the global state is disabled, the IGMP snooping on the Switch 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.

## 6.2.1.1. General Settings

### 6.2.1.1.1. CLI Configuration

| Node      | Command   | Description   |
|-----------|---|---|
| enable    | show igmp-snooping                              | This command displays the current IGMP snooping configurations.   |
| enable    | configure terminal                              | This command changes the node to configure node.  |
| configure | igmp-snooping (disable enable)                  | This command <b>disables</b> / <b>enables</b> the IGMP snooping on the switch.  |
| configure | igmp-snooping vlan VLANLISTS                    | This command enables the IGMP snooping function on a VLAN or range of VLANs.  |
| configure | no igmp-snooping vlan VLANLISTS                 | This command disables the IGMP snooping function on a VLAN or range of VLANs.   |
| configure | igmp-snooping unknown-multicast (drop flooding) | This command configures the process for unknown multicast packets when the IGMP snooping function is enabled.<br><b>drop</b> : Drop all of the unknown multicast packets.<br><b>flooding</b> : Flooding the unknown multicast packets to all ports. |

#### Example:

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

### 6.2.1.1.2. Web Configuration

**IGMP Snooping**

General Settings
Port Settings
Querier Settings

IGMP Snooping Settings

IGMP Snooping State Disable ▾

IGMP Snooping VLAN State Add ▾

Unknown Multicast Packets Flooding ▾

IGMP Snooping Status

|                           |          |
|---------------------------|----------|
| IGMP Snooping State       | Disabled |
| Enabled on VLAN           | None     |
| Unknown Multicast Packets | Flooding |

| Parameter                     | Description   |
|-------------------------------|---|
| <b>IGMP Snooping Settings</b> |   |
| IGMP Snooping State           | Select <b>Enable</b> to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select <b>Disable</b> to deactivate the feature.  |
| IGMP Snooping VLAN State      | Select <b>Add</b> and enter VLANs upon which the Switch 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 <b>Delete</b> and enter VLANs on which to have the Switch not perform IGMP snooping. |
| Unknown Multicast Packets     | Specify the action to perform when the Switch receives an unknown multicast frame. Select <b>Drop</b> to discard the frame(s). Select <b>Flooding</b> to send the frame(s) to all ports.  |
| Apply                         | Click <b>Apply</b> to take effect the settings.   |
| Refresh                       | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>IGMP Snooping Status</b>   |   |
| IGMP Snooping State           | This field displays whether IGMP snooping is globally enabled or disabled.  |
| Enable on VLAN                | This field displays VLANs on which the Switch is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any VLAN yet.   |
| Unknown Multicast Packets     | This field displays whether the Switch is set to <b>drop</b> or <b>flooding</b> unknown multicast packets.  |

### 6.2.1.2. Port Settings

#### Immediate Leave

When you enable IGMP Immediate-Leave processing, the switch 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 switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the switch 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 switch 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 Switch uses the port as an IGMP query port if the port receives IGMP query packets.

- **Fixed:**

The Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). The Switch always forwards the client's **report/leave** packets to the port.

Normally, the port is connected to an IGMP server.

- **Edge:**

The Switch does not use the port as an IGMP query port. The IGMP query packets received by this port will be dropped.

Normally, the port is connected to an IGMP client.

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

#### 6.2.1.2.1. CLI Configuration

| Node   | Command            | Description   |
|--------|--------------------|---|
| enable | show igmp-snooping | This command displays the current IGMP snooping configurations. |
| enable | configure terminal | This command changes the node to configure node.                |

|           |   |  |
|-----------|---|--|
| configure | interface IFNAME                                    | This command enters the interface configure node.  |
| interface | igmp-immediate-leave                                | This command enables the IGMP Snooping immediate leave function for the specific port.   |
| interface | no igmp-immediate-leave                             | This command disables the IGMP Snooping immediate leave function for the specific port.  |
| interface | igmp-group-limit<br>VALUE                           | This command configures the maximum groups for the specific port.  |
| interface | no igmp-group-limit                                 | This command configures the default value for the limitation of the maximum groups for the specific port.  |
| interface | igmp-querier-mode<br>(auto fixed edge)              | This command specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch 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). |
| configure | interface range<br>gigabitethernet1/0/POR<br>TLISTS | This command enters the if-range configure node.   |
| if-range  | igmp-immediate-leave                                | This command enables the IGMP Snooping immediate leave function for the specific ports.  |
| if-range  | no igmp-immediate-leave                             | This command disables the IGMP Snooping immediate leave function for the specific ports.   |
| if-range  | igmp-group-limit<br>VALUE                           | This command configures the maximum groups for the specific port.  |
| if-range  | no igmp-group-limit                                 | This command configures the default value for the limitation of the maximum groups for the specific port.  |
| if-range  | igmp-querier-mode<br>(auto fixed edge)              | This command specifies whether or not and under what conditions the ports is (are) IGMP query port(s). The Switch 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).   |

**Example:**

```
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#igmp-immediate-leave
L2SWITCH(config-if)#igmp-querier-mode fixed
L2SWITCH(config-if)#igmp-snooping group-limit 20
```

### 6.2.1.2.2. Web Configuration

**IGMP Snooping**

General Settings
Port Settings
Querier Settings

**Port Settings**

| Port  | Querier Mode                      | Immediate Leave                      | Group Limit                      |
|---|-----------------------------------|--------------------------------------|----------------------------------|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="Auto"/> | <input type="text" value="Disable"/> | <input type="text" value="266"/> |

**Port Status**

| Port | Querier Mode | Immediate Leave | Group/Limit |
|------|--------------|-----------------|-------------|
| 1    | Auto         | Disable         | 0/266       |
| 2    | Auto         | Disable         | 0/266       |
| 3    | Auto         | Disable         | 0/266       |
| 4    | Auto         | Disable         | 0/266       |
| 5    | Auto         | Disable         | 0/266       |
| 6    | Auto         | Disable         | 0/266       |

| Parameter            | Description   |
|----------------------|---|
| <b>Port Settings</b> |   |
| Querier Mode         | Select the desired setting, <b>Auto</b> , <b>Fixed</b> , or <b>Edge</b> . <b>Auto</b> means the Switch uses the port as an IGMP query port if the port receives IGMP query packets. <b>Fixed</b> means the Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). <b>Edge</b> means the Switch does not use the port as an IGMP query port. In this case, the Switch does not keep a record of an IGMP router being connected to this port and the Switch 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 <b>Apply</b> to take effect the settings.   |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>Port Status</b>   |   |
| Port                 | The port ID.  |
| Querier Mode         | The Querier mode setting for the specific port.   |

|                 |  |
|-----------------|--|
| Immediate Leave | The Immediate Leave setting for the specific port.           |
| Group / Limit   | The current joining group count and the maximum group count. |

### 6.2.1.3. 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].

#### 6.2.1.3.1. CLI Configuration

| Node      | Command                                 | Description   |
|-----------|---|---|
| enable    | show igmp-snooping querier              | This command displays the current IGMP Queriers and the querier configurations.       |
| enable    | configure terminal                      | This command changes the node to configure node.                                      |
| configure | igmp-snooping querier (disable enable)  | This command disables / enables the IGMP snooping querier on the switch.              |
| configure | igmp-snooping querier vlan VLANLISTS    | This command enables the IGMP snooping querier function on a VLAN or range of VLANs.  |
| configure | no igmp-snooping querier vlan VLANLISTS | This command disables the IGMP snooping querier function on a VLAN or range of VLANs. |
| configure | igmp-snooping query interval <2-300>    | This command configures the query interval for the Querier. Unit: second.             |

### 6.2.1.3.2. Web Configuration

**IGMP Snooping**

General Settings
Port Settings
**Querier Settings**

**Querier Settings**

State  ▾

Query Interval  (sec)

VLAN State  ▾

**Querier Status**

|                 |           |
|-----------------|-----------|
| State           | Disable   |
| Query Interval  | 125 (sec) |
| Enabled on VLAN | None      |

| Parameter               | Description   |
|-------------------------|---|
| <b>Querier Settings</b> |   |
| State                   | This field configures the global Querier state.   |
| Query Interval          | This field configures the interval which Querier send query packet periodically.  |
| VLAN State              | This field enables the Querier state in a vlan or a range of vlan.  |
| Apply                   | Click <b>Apply</b> to take effect the settings.   |
| Refresh                 | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>Querier Status</b>   |   |
| State                   | This filed indicates the current global Querier status.   |
| Query Interval          | This field indicates the interval which Querier send query packet periodically.   |
| Enable on VLAN          | This field displays VLANs on which the Switch is to perform IGMP querier. None displays if you have not enabled IGMP querier on any VLAN yet. |

## 6.2.2. IGMP Snooping Filtering

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

### 6.2.2.1. General Settings

#### 6.2.2.1.1. CLI Configuration

| Node        | Command                                  | Description  |
|-------------|--|--|
| enable      | show igmp-snooping filtering             | This command displays the IGMP snooping filtering configurations.  |
| enable      | configure terminal                       | This command changes the node to configure node.   |
| configure   | igmp-snooping filtering (enable disable) | This command <b>enables/disables</b> the IGMP snooping filtering profiles on the Switch.                     |
| configure   | igmp-snooping filtering profile STRING   | This command creates a filtering profile and enters the IGMP snooping filtering profiles configuration node. |
| configure   | no igmp-snooping filtering all           | This command removes all of the IGMP snooping filtering profiles from the Switch.                            |
| configure   | no igmp-snooping filtering STRINGS       | This command removes the IGMP snooping filtering profiles by name from the Switch.                           |
| config-igmp | type (deny permit)                       | This command configures the type of deny or permit for the group.  |

#### 6.2.2.1.2. Web Configuration

**IGMP Filtering**

General Settings
Multicast Groups
Port Settings

**IGMP Filtering Settings**

IGMP Filtering State: Disable ▾

| Profile                                  | Type  |
|--|---|
| <input style="width: 95%;" type="text"/> | <span style="border: 1px solid #ccc; padding: 2px;">Deny ▾</span> |

Apply
Refresh

**IGMP Filtering Status**

| Profile                | Type | Ports | Action   |
|------------------------|------|-------|--|
| <a href="#">Justin</a> | Deny |       | <span style="border: 1px solid #ccc; padding: 2px 10px;">Delete</span> |

| Parameter                      | Description   |
|--------------------------------|---|
| <b>IGMP Filtering Settings</b> |   |
| IGMP Filtering State           | This field configures the global IGMP Filtering state.                      |
| Profile                        | This field creates the IGMP Filtering profile.                              |
| Type                           | The field configures the type of action for the profile.                    |
| Apply                          | Click <b>Apply</b> to take effect the settings.                             |
| Refresh                        | Click <b>Refresh</b> to begin configuring this screen afresh.               |
| <b>IGMP Filtering Status</b>   |   |
| Profile                        | The profile name.   |
| Type                           | The type of action.   |
| Ports                          | The field indicates the ports that the IGMP Filtering profile is activated. |
| Action                         | Click <b>Delete</b> to delete the profile.                                  |

## 6.2.2.2. Multicast Group

### 6.2.2.2.1. CLI Configuration

| Node        | Command  | Description  |
|-------------|--|--|
| enable      | show igmp-snooping filtering                                 | This command displays the IGMP snooping filtering configurations.  |
| enable      | configure terminal   | This command changes the node to configure node.   |
| configure   | igmp-snooping filtering profile STRING                       | This command creates a filtering profile and enters the IGMP snooping filtering profiles configuration node.                   |
| config-igmp | Group GROUP_ID start-address START-ADDR end-address END-ADDR | This command configures the group configurations, including group index and start multicast address and end multicast address. |
| config-igmp | no group GROUP-ID  | This command removes the group configurations.   |
| config-igmp | no group all   | This command removes all of the group configurations.  |

### 6.2.2.2.2. Web Configuration

**IGMP Filtering**

General Settings
Multicast Groups
Port Settings

Group Settings

Profile: Test1 ▼

| Group  | Start Address                            | End Address                              |
|--|--|--|
| <span style="border: 1px solid #ccc; padding: 2px;">1 ▼</span> | <input style="width: 80%;" type="text"/> | <input style="width: 80%;" type="text"/> |

Apply
Refresh

Group Status

| Profile               | Type | Group | Start Address | End Address | Action  |
|-----------------------|------|-------|---------------|-------------|---|
| <a href="#">Test1</a> | deny | 1     | 225.1.1.1     | 225.1.1.254 | <span style="border: 1px solid #ccc; padding: 2px 5px;">Delete</span> |
| <a href="#">Test1</a> | deny | 2     | 226.1.1.1     | 226.1.1.254 | <span style="border: 1px solid #ccc; padding: 2px 5px;">Delete</span> |
| <a href="#">Test2</a> | deny | 1     | 227.1.1.1     | 227.1.1.254 | <span style="border: 1px solid #ccc; padding: 2px 5px;">Delete</span> |
| <a href="#">Test2</a> | deny | 2     | 228.1.1.1     | 228.1.1.254 | <span style="border: 1px solid #ccc; padding: 2px 5px;">Delete</span> |

| Parameter             | Description   |
|-----------------------|---|
| <b>Group Settings</b> |   |
| Profile               | This field selects the profile which you want to configure the group. |
| Group                 | This field selects the group index.                                   |
| Start Address         | The field configures the first multicast address of the group.        |
| End Address           | The field configures the last multicast address of the group.         |
| Apply                 | Click <b>Apply</b> to take effect the settings.                       |
| Refresh               | Click <b>Refresh</b> to begin configuring this screen afresh.         |

### 6.2.2.3. Port Settings

#### 6.2.2.3.1. CLI Configuration

| Node      | Command                                      | Description   |
|-----------|--|---|
| enable    | show igmp-snooping filtering                 | This command displays the IGMP snooping filtering configurations.                 |
| enable    | configure terminal                           | This command changes the node to configure node.                                  |
| configure | interface IFNAME                             | This command enters the interface configure node.                                 |
| interface | igmp-snooping filtering profile STRING       | This command enables the IGMP snooping filtering profiles on the specific port.   |
| interface | no igmp-snooping filtering profile STRINGS   | This command disables the IGMP snooping filtering profiles on the specific port.  |
| configure | interface range gigabitethernet1/0/PORTLISTS | This command enters the if-range configure node.                                  |
| if-config | igmp-snooping filtering profile STRING       | This command enables the IGMP snooping filtering profiles on the range of ports.  |
| if-config | no igmp-snooping filtering profile STRINGS   | This command disables the IGMP snooping filtering profiles on the range of ports. |

### 6.2.2.3.2. Web Configuration

**IGMP Filtering**

General Settings
Multicast Groups
**Port Settings**

**Port Settings**

Profile :

Activate on Ports

Select All     Deselect All

1    2    3    4    5    6

**Port Status**

| Profile | Type | Port |
|---------|------|------|
|         |      |      |

| Parameter            | Description  |
|----------------------|--|
| <b>Port Settings</b> |  |
| Profile              | This field 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 <b>Apply</b> to take effect the settings.                          |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.            |

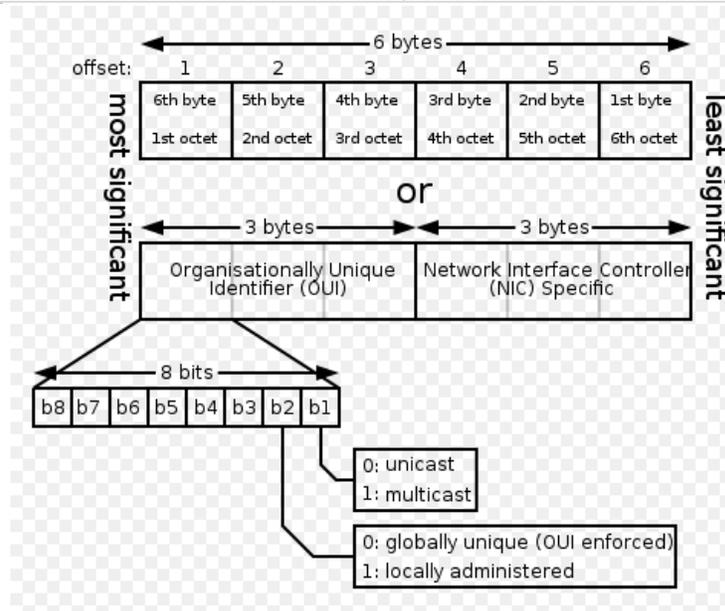
### 6.2.3. Multicast Address

A multicast address is associated with a group of interested receivers. According to RFC 3171, addresses 224.0.0.0 to 239.255.255.255, 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   |
|----------------|------------------------------|--|
| <b>Class A</b> | 1.0.0.1 to 126.255.255.254   | Supports 16 million hosts on each of 127 networks.             |
| <b>Class B</b> | 128.1.0.1 to 191.255.255.254 | Supports 65,000 hosts on each of 16,000 networks.              |
| <b>Class C</b> | 192.0.1.1 to 223.255.254.254 | Supports 254 hosts on each of 2 million networks.              |
| <b>Class D</b> | 224.0.0.0 to 239.255.255.255 | Reserved for multicast groups.                                 |
| <b>Class E</b> | 240.0.0.0 to 254.255.255.254 | Reserved for future use, or Research and Development Purposes. |



| <b>IP Multicast Address</b> | <b>Description</b>  |
|-----------------------------|---|
| 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 <u>RIP</u> 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.  |
| 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.   |

### 6.2.3.1. CLI Configuration

| <b>Node</b> | <b>Command</b>         | <b>Description</b>   |
|-------------|------------------------|--|
| enable      | show ip-multicast      | This command displays the IP multicast information.                      |
| enable      | show mac-address-table | This command displays the current unicast and multicast address entries. |
| enable      | configure terminal     | This command changes the node to configure node.                         |

|           |  |  |
|-----------|--|--|
| configure | ip-multicast IPADDR server IPADDR vlan <1-4094> port PORTLISTS | This command configures an IP multicast group. |
| configure | no ip-multicast IPADDR server IPADDR vlan <1-4094>             | This command deletes an IP multicast group.    |

### 6.2.3.2. Web Configuration

**Multicast Address**

**Static Multicast Address Settings**

| VLAN ID   | Group IP             | Source IP            | Port                 |
|---|----------------------|----------------------|----------------------|
| 1 ▾   | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> |                      |                      |                      |

**Multicast Address Table**

| VLAN ID | Group IP  | Source IP      | Status | Port | Action                                |
|---------|-----------|----------------|--------|------|---------------------------------------|
| 1       | 225.1.1.1 | 192.168.202.70 | Static | 1-4  | <input type="button" value="Delete"/> |
|         |           |                |        |      | Total Counts: <b>1</b>                |

| Parameter                                | Description   |
|--|---|
| <b>Static Multicast Address Settings</b> |   |
| 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 which send out the multicast stream. |
| Port                                     | Configures the member port(s) for the multicast address.              |
| Apply                                    | Click <b>Apply</b> to take effect the settings.                       |
| Refresh                                  | Click <b>Refresh</b> to begin configuring this screen afresh.         |

## 6.3. VLAN

### 6.3.1. Port Isolation

The port isolation is a port-based virtual LAN feature. It partitions the switching ports into virtual private domains designated on a per port basis. Data switching outside of the 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 Switch.

If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. CPU refers to the Switch 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 Switch 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
```

#### 6.3.1.1. CLI Configurations

| Node      | Command                        | Description   |
|-----------|--------------------------------|---|
| enable    | show port-isolation            | This command displays the current port isolation configurations.<br>“V” indicates the port's packets can be sent to that port.<br>“-” indicates the port's packets cannot be sent to that port. |
| enable    | configure terminal             | This command changes the node to configure node.  |
| configure | interface IFNAME               | This command enters the interface configure node.   |
| interface | port-isolation ports PORTLISTS | This command configures a port or a range of ports to egress traffic from the specific port.  |
| interface | no port-isolation              | This command configures all ports to egress traffic from the specific port.   |

### 6.3.1.2. Web Configurations

**Port Isolation**

**Port Isolation Settings**

Port                      From:  To:

Egress Port:

Select All       Deselect All

1  2  3  4  5  6  0 (CPU)

**Port Isolation Status**

| Port | Egress Port |   |   |   |   |   |   |
|------|-------------|---|---|---|---|---|---|
|      | 0           | 1 | 2 | 3 | 4 | 5 | 6 |
| 1    | v           | v | v | v | v | v | v |
| 2    | v           | v | v | v | v | v | v |
| 3    | v           | v | v | v | v | v | v |
| 4    | v           | v | v | v | v | v | v |
| 5    | v           | v | v | v | v | v | v |
| 6    | v           | v | v | v | v | v | v |

| Parameter                      | Description   |
|--------------------------------|---|
| <b>Port Isolation Settings</b> |   |
| Port                           | Select a port number to configure its port isolation settings.<br>Select <b>All Ports</b> to configure the port isolation settings for all ports on the Switch.   |
| Egress Port                    | An egress port is an outgoing port, that is, a port through which a data packet leaves.<br>Selecting a port as an outgoing port means it will communicate with the port currently being configured.   |
| Select All/<br>Deselect All    | Click <b>Select All</b> to mark all ports as egress ports and permit traffic.<br>Click <b>Deselect All</b> to unmark all ports and isolate them.<br>Deselecting all ports means the port being configured cannot communicate with any other port. |
| Apply                          | Click <b>Apply</b> to take effect the settings.   |
| Refresh                        | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>Port Isolation Status</b>   |   |
|                                | “V” indicates the port’s packets can be sent to that port.<br>“-” indicates the port’s packets cannot be sent to that port.   |

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

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

- 802.1Q Port 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 switch 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 switch 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), the performance is very good. An ASIC allows the port-to-VLAN mapping to be done at the hardware level.

**Notice:** The maximum VLAN group is 4094.

### 6.3.2.1. VLAN Settings

#### 6.3.2.1.1. CLI Configurations

| Node      | Command            | Description   |
|-----------|--------------------|---|
| enable    | show vlan          | This command displays all of the VLAN configurations. |
| enable    | show vlan <1-4094> | This command displays the VLAN configurations.        |
| enable    | configure terminal | This command changes the node to configure node.      |
| configure | vlan <1~4094>      | This command enables a VLAN and enters the VLAN node. |
| configure | no vlan <1~4094>   | This command deletes a VLAN.                          |

|            |                        |   |
|------------|------------------------|---|
| vlan       | show                   | This command displays the current VLAN configurations.  |
| vlan       | name STRING            | This command assigns a name for the specific VLAN.<br>The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_).<br>The maximum length of the name is 16 characters. |
| vlan       | no name                | This command configures the VLAN name to default.<br>Note: The default VLAN name is “VLAN”+vlan-ID, VLAN1, VLAN2,...  |
| vlan       | add PORTLISTS          | This command adds a port or a range of ports to the VLAN.   |
| vlan       | fixed PORTLISTS        | This command assigns ports for permanent member of the VLAN.  |
| vlan       | no fixed PORTLISTS     | This command removes all fixed member from the VLAN.  |
| configure  | vlan range VLANLIST    | This command configures a range of VLANs.   |
| configure  | no vlan range VLANLIST | This command removes a range of VLANs.  |
| vlan-range | add PORTLISTS          | This command adds a port or a range of ports to the VLANs.  |
| vlan-range | fixed PORTLISTS        | This command assigns ports for permanent member of the VLAN group.  |
| vlan-range | no fixed PORTLISTS     | This command removes all fixed member from the VLANs.   |

### 6.3.2.1.2. Web Configurations

**VLAN**

VLAN
Tag Settings
Port Settings

VLAN Settings

| VLAN ID   | VLAN Name                                  | Member Port                               |
|---|--|---|
| From: <input style="width: 50px;" type="text"/> To: <input style="width: 50px;" type="text"/> | <input style="width: 150px;" type="text"/> | <input style="width: 80px;" type="text"/> |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/>                   |  |   |

VLAN List

| VLAN ID | VLAN Name | VLAN Status | Member Port | Action |
|---------|-----------|-------------|-------------|--------|
| 1       | VLAN1     | Static      | 1-10        |        |

| Parameter            | Description   |
|----------------------|---|
| <b>VLAN Settings</b> |   |
| 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 Switch 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 <b>Apply</b> to take effect the settings.   |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>VLAN List</b>     |   |
| VLAN ID              | This field displays the index number of the VLAN entry. Click the number to modify the VLAN.  |
| VLAN Name            | This field displays the name of the VLAN.   |
| VLAN Status          | This field displays the status of the VLAN. <b>Static</b> or <b>Dynamic</b> (802.1Q VLAN).  |
| Member Port          | This field displays which ports have been assigned as members of the VLAN. This will display <b>None</b> if no ports have been assigned.  |
| Action               | Click <b>Delete</b> to remove the VLAN. The VLAN 1 cannot be deleted.   |

### 6.3.2.2. Tag Settings

#### 6.3.2.2.1. CLI Configurations

| Node      | Command               | Description  |
|-----------|-----------------------|--|
| enable    | show vlan             | This command displays all of the VLAN configurations.  |
| enable    | show vlan <1-4094>    | This command displays the VLAN configurations.   |
| enable    | configure terminal    | This command changes the node to configure node.   |
| configure | vlan <1~4094>         | This command enables a VLAN and enters the VLAN node.  |
| vlan      | show                  | This command displays the current VLAN configurations.   |
| vlan      | tagged PORTLISTS      | This command 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   | This command removes all tagged member from the VLAN.  |
| vlan      | untagged PORTLISTS    | This command 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 | This command 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
```

### 6.3.2.2.2. Web Configurations

**VLAN**

VLAN Settings
Tag Settings
Port Settings

**Tag Settings**

VLAN ID      From:     To:

Tag Port :

Select All       Deselect All

1  2  3  4  5  6

**Tag Status**

| VLAN ID | Tag Ports | UnTag Ports |
|---------|-----------|-------------|
| 1       |           | 1-6         |

| Parameter           | Description  |
|---------------------|--|
| <b>Tag Settings</b> |  |
| VLAN ID             | Select a VLAN ID to configure its port tagging settings.   |
| 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 <b>Select All</b> to mark all member ports as tag ports.   |
| Deselect All        | Click <b>Deselect All</b> to mark all member ports as untag ports.   |
| Apply               | Click <b>Apply</b> to take effect the settings.  |
| Refresh             | Click <b>Refresh</b> to begin configuring this screen afresh.  |
| <b>Tag Status</b>   |  |
| VLAN ID             | This field displays the VLAN ID.   |
| Tag Ports           | This field displays the ports that have been assigned as tag ports.  |
| Untag Ports         | This field displays the ports that have been assigned as untag ports.  |

### 6.3.2.3. Port Settings

#### 6.3.2.3.1. CLI Configurations

| Node      | Command   | Description  |
|-----------|---|--|
| enable    | show vlan                                       | This command displays all of the VLAN configurations.  |
| enable    | show vlan <1-4094>                              | This command displays the VLAN configurations.   |
| enable    | configure terminal                              | This command changes the node to configure node.   |
| configure | interface IFNAME                                | This command enters the interface configure node.  |
| interface | acceptable frame type<br>(all tagged untagged)  | This command configures the acceptable frame type.<br><b>all</b> - acceptable all frame types.<br><b>tagged</b> - acceptable tagged frame only.<br><b>untagged</b> – acceptable untagged frame only. |
| interface | pvid <1-4094>                                   | This command configures a VLAN ID for the port default VLAN ID.  |
| interface | no pvid   | This command configures 1 for the port default VLAN ID.  |
| configure | interface range<br>gigabitethernet1/0/PORTLISTS | This command enters the if-range configure node.   |
| if-range  | acceptable frame type<br>(all tagged untagged)  | This command configures the acceptable frame type.<br><b>all</b> - acceptable all frame types.<br><b>tagged</b> - acceptable tagged frame only.<br><b>untagged</b> – acceptable untagged frame only. |
| if-range  | pvid <1-4094>                                   | This command configures a VLAN ID for the port default VLAN ID.  |
| if-range  | no pvid   | This command configures 1 for the port default VLAN ID.  |

### 6.3.2.3.2. Web Configurations

**VLAN**

VLAN Settings
Tag Settings
Port Settings

**Port Settings**

| Port  | PVID                           | Acceptable Frame                 |
|---|--------------------------------|----------------------------------|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="1"/> | <input type="text" value="All"/> |

**Port Status**

| Port | PVID | Acceptable Frame | Port | PVID | Acceptable Frame |
|------|------|------------------|------|------|------------------|
| 1    | 1    | All              | 2    | 1    | All              |
| 3    | 1    | All              | 4    | 1    | All              |
| 5    | 1    | All              | 6    | 1    | All              |

| Parameter            | Description   |
|----------------------|---|
| <b>Port Settings</b> |   |
| Port                 | Select a port number to configure from the drop-down box. Select <b>All</b> to configure all ports at the same time.  |
| PVID                 | Select a <b>PVID</b> (Port VLAN ID number) from the drop-down box.  |
| Acceptable Frame     | Specify the type of frames allowed on a port. Choices are <b>All</b> , <b>VLAN Untagged Only</b> or <b>VLAN Tagged Only</b> .<br>- Select <b>All</b> from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting.<br>- Select <b>VLAN Tagged Only</b> to accept only tagged frames on this port. All untagged frames will be dropped.<br>- Select <b>VLAN Untagged Only</b> to accept only untagged frames on this port. All tagged frames will be dropped. |
| Apply                | Click <b>Apply</b> to take effect the settings.   |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>Port Status</b>   |   |
| Port                 | This field displays the port number.  |
| PVID                 | This field displays the Port VLAN ID number.  |
| Acceptable Frame     | This field displays the type of frames allowed on the port. This will either display <b>All</b> or <b>VLAN Tagged Only</b> or <b>VLAN Untagged Only</b> .   |

### 6.3.3. 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 Switch receives packets, it will compare MAC-based VLAN configurations. If the SA is matched the MAC-based VLAN configurations, the Switch replace the VLAN with user configured and then 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.

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

#### 6.3.3.1. CLI Configurations

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show mac-vlan  | This command displays the all of the mac-vlan configurations.  |
| enable    | configure terminal                                     | This command changes the node to configure node.   |
| configure | mac-vlan<br>STRINGS vlan<br><1-4094><br>priority <0-7> | This command 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<br>STRINGS                           | This command deletes a mac-vlan entry.   |
| configure | no mac-vlan all  | This command 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
```

### 6.3.3.2. Web Configurations

**MAC VLAN**

**MAC VLAN Settings**

| MAC Address                              | VLAN  | Priority   |
|--|---|--|
| <input style="width: 90%;" type="text"/> | <input style="width: 90%;" type="text"/> (1~4094) | <input style="width: 90%;" type="text" value="0"/> ▼ |

Ex: HH:HH:HH will only filter 3 bytes of source mac address.  
 HH:HH:HH:HH:HH will only filter 5 bytes of source mac address.  
 HH:HH:HH:HH:HH:HH will filter all bytes of source mac address.

**MAC VLAN Table**

| Index | MAC Address | VLAN | Priority | Action                                |
|-------|-------------|------|----------|---------------------------------------|
| 1     | 00:01:02    | 5    | 0        | <input type="button" value="Delete"/> |
| 2     | 00:0B:05:00 | 6    | 0        | <input type="button" value="Delete"/> |

| Parameter                | Description  |
|--------------------------|--|
| <b>MAC VLAN Settings</b> |  |
| 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 <b>Apply</b> to take effect the settings.                |
| Refresh                  | Click <b>Refresh</b> to begin configuring this screen afresh.  |
| Action                   | Click <b>Delete</b> to delete the MAC VLAN profile.            |

### 6.3.4. 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 Switch 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

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 switch. 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.

### 6.3.4.1. VLAN Stacking

#### 6.3.4.1.1. CLI Configurations

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show vlan-stacking                                 | This command displays the current vlan-stacking type.  |
| enable    | show vlan-stacking tpid-inform                     | This command displays the TPID configurations.   |
| enable    | configure terminal                                 | This command changes the node to configure node.   |
| configure | vlan-stacking (disable port-based selective)       | This command disable the vlan stacking or enable the vlan-stacking with port-based or selective on the switch. |
| configure | vlan-stacking tpid-table index <2-6> value STRINGS | This command configures TPID table.  |
| configure | interface IFNAME                                   | This command enters the interface configure node.  |
| interface | vlan-stacking tunnel-tpid index <1-6>              | This command sets TPID for a Q-in-Q tunnel port.   |
| configure | interface range gigabitethernet1/0/PORTLISTS       | This command enters the if-range configure node.   |
| if-range  | vlan-stacking tunnel-tpid index <1-6>              | This command sets TPID for a Q-in-Q tunnel port.   |

### 6.3.4.1.2. Web Configurations

**Q-in-Q**

VLAN Stacking

Port-based Q-in-Q

**VLAN Stacking Settings**

Action Disable ▼

| Tunnel TPID Index  | TPID  |
|--|---|
| <span style="border: 1px solid #ccc; padding: 2px;">0 (Default)</span> ▼ | <span style="border: 1px solid #ccc; padding: 2px;">88a8</span> (0000~ffff) |

| Port  | Tunnel TPID Index  |
|---|--|
| From: <span style="border: 1px solid #ccc; padding: 2px;">1</span> ▼ To: <span style="border: 1px solid #ccc; padding: 2px;">1</span> ▼ | <span style="border: 1px solid #ccc; padding: 2px;">0 (Default)</span> ▼ |

Apply
Refresh

**VLAN Stacking Status**

| Tunnel TPID Index | TPID |
|-------------------|------|
| 0                 | 88a8 |
| 1                 | 88a8 |
| 2                 | 88a8 |
| 3                 | 88a8 |

| Port | Tunnel TPID Index (TPID) | Port | Tunnel TPID Index (TPID) |
|------|--------------------------|------|--------------------------|
| 1    | 0 (88a8)                 | 2    | 0 (88a8)                 |
| 3    | 0 (88a8)                 | 4    | 0 (88a8)                 |
| 5    | 0 (88a8)                 | 6    | 0 (88a8)                 |

| Parameter  | Description   |
|--|---|
| <b>VLAN Stacking Settings</b>                            |   |
| Action   | Select one of the three modes, <b>Disable</b> or <b>Port-Based</b> or <b>Selective</b> for the VLAN stacking. |
| Configures the TPID Table: The TPID table has 6 entries. |   |
| Tunnel TPID Index  | Selects the table index.  |
| 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 <b>Apply</b> to take effect the settings.   |
| Refresh  | Click <b>Refresh</b> to begin configuring this screen afresh.   |

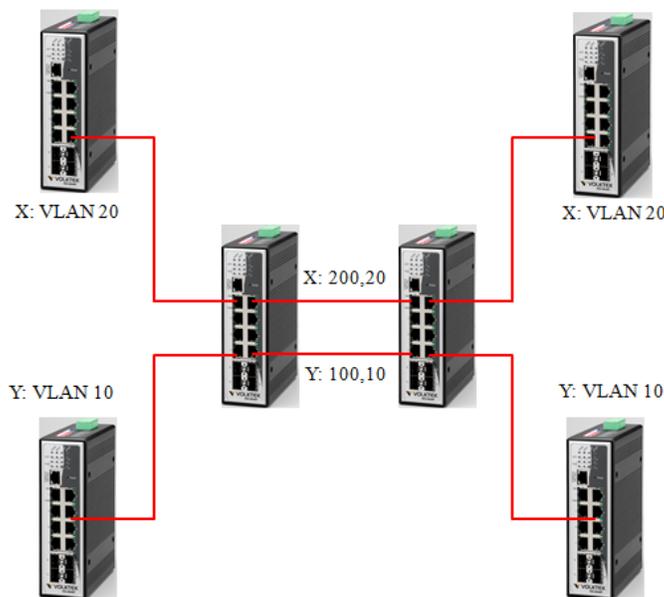
|        |   |
|--------|---|
| Action | Click <b>Delete</b> to delete the MAC VLAN profile. |
|--------|---|

### 6.3.4.2. Port-Based Q-in-Q

#### 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 **100** to distinguish customer **X** and tag **200** to distinguish 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 switch A with ports 1 on the Switch to tag incoming frames with the service provider's VID of 200 (ports are connected to customer X network) and configure port 7 to 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 gigabitEthernet1/0/1
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 gigabitEthernet1/0/2
L2SWITCH(config-if)# vlan-stacking port-based role tunnel
L2SWITCH(config-if)# vlan-stacking tunnel-tpid index 2
L2SWITCH(config)# interface gigabitEthernet1/0/5
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 gigabitEthernet1/0/6
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

```

#### 6.3.4.2.1. CLI Configurations

| Node      | Command                                 | Description   |
|-----------|---|---|
| enable    | show vlan-stacking portbased-qinq       | This command displays the port-based q-in-Q configurations. |
| enable    | configure terminal                      | This command changes the node to configure node.            |
| configure | interface IFNAME                        | This command enters the interface configure node.           |
| interface | vlan-stacking port-based priority <0~7> | This command sets the priority in port based Q-in-Q.        |

|           |   |   |
|-----------|---|---|
| interface | vlan-stacking port-based role<br>(tunnel access normal) | This command sets VLAN stacking port role.                          |
| interface | vlan-stacking port-based spvid<br><1~4096>              | This command sets the service provider's VID of the specified port. |
| interface | vlan-stacking tunnel-tpid index<br><1-6>                | This command sets TPID for a Q-in-Q tunnel port.                    |
| configure | interface range<br>gigabitethernet1/0/PORTLISTS         | This command enters the if-range configure node.                    |
| if-range  | vlan-stacking port-based priority<br><0~7>              | This command sets the priority in port based Q-in-Q.                |
| if-range  | vlan-stacking port-based role<br>(tunnel access normal) | This command sets VLAN stacking port role.                          |
| if-range  | vlan-stacking port-based spvid<br><1~4096>              | This command sets the service provider's VID of the specified port. |
| if-range  | vlan-stacking tunnel-tpid index<br><1-6>                | This command sets TPID for a Q-in-Q tunnel port.                    |

### 6.3.4.2.2. Web Configurations

**Q-in-Q**

VLAN Stacking **Port-based Q-in-Q**

Port-based Q-in-Q Settings

| Port          | Role   | SPVID      | Priority |
|---------------|--------|------------|----------|
| From: 1 To: 1 | Normal | 1 (1~4094) | 0        |

Apply Refresh

Port-based Q-in-Q Status

| Port | Role   | SPVID | Priority | Port | Role   | SPVID | Priority |
|------|--------|-------|----------|------|--------|-------|----------|
| 1    | Normal | 1     | 0        | 2    | Normal | 1     | 0        |
| 3    | Normal | 1     | 0        | 4    | Normal | 1     | 0        |
| 5    | Normal | 1     | 0        | 6    | Normal | 1     | 0        |

| Parameter                         | Description   |
|-----------------------------------|---|
| <b>Port-based Q-in-Q Settings</b> |   |
| Port                              | Selects a port or a range of ports which you want to configure.   |
| Role                              | Selects one of the three roles, <b>Normal</b> and <b>Access</b> and <b>Tunnel</b> , for the specific ports. |
| SPVID                             | Configures the service provider's VLAN.   |
| Priority                          | Configures the priority for the specific ports.   |

|         |   |
|---------|---|
| Apply   | Click <b>Apply</b> to take effect the settings.               |
| Refresh | Click <b>Refresh</b> to begin configuring this screen afresh. |
| Action  | Click <b>Delete</b> to delete the MAC VLAN profile.           |

#### 6.4. DHCP Option (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 switch will monitor the DHCP packets and append some information as below to the DHCPDISCOVER and DHCPREQUEST packets. The switch 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 switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

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

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the switch 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 switch adds the IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82 capable, it can use the remote ID, 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 unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch **removes** the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

#### Option Frame Format:

|      |     |                         |
|------|-----|-------------------------|
| 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<br>Sub-option Code | Sub-Option Description               |
|-------------------------------|--------------------------------------|
| -----<br>1                    | -----<br>Agent Circuit ID Sub-option |
| 2                             | Agent Remote ID Sub-option           |

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:

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

**6.4.1.CLI Configurations**

| Node      | Command                                   | Description   |
|-----------|---|---|
| enable    | show dhcp-options                         | This command displays the DHCP options configurations.                |
| enable    | configure terminal                        | This command changes the node to configure node.                      |
| configure | dhcp-options option82 (disable enable)    | This command disables / enables the DHCP option 82 on the Switch.     |
| configure | dhcp-options option82 circuit_id STRING   | This command configures the information of the circuit ID sub-option. |
| configure | no dhcp-options option82 circuit_id       | This command removes the information of the circuit ID sub-option.    |
| configure | dhcp-options option82 remote_id STRING    | This command configures the information of the remote ID sub-option.  |
| configure | no dhcp-options option82 remote_id        | This command removes the information of the remote ID sub-option.     |
| configure | dhcp-options option82 circuit_frame VALUE | This command configures the frame ID for the circuit sub-option.      |
| configure | dhcp-options option82 circuit_shelf VALUE | This command configures the shelf ID for the circuit sub-option.      |
| configure | dhcp-options option82 circuit_slot VALUE  | This command configures the slot ID for the circuit sub-option.       |

## 6.4.2. Web Configurations

**DHCP Options**

**DHCP Option 82 Settings**

Option 82 State:  ▾

Option 82 Frame:

Option 82 Shelf:

Option 82 Slot:

Circuit-ID String:

Remote-ID String:

**DHCP Option 82 Port Settings**

Port:  ▾

Option 82 State:  ▾

Circuit-ID String:

Remote-ID String:

**DHCP Option 82 Port Status**

| Port 1            |         |
|-------------------|---------|
| Option 82 State   | Disable |
| Circuit-ID String |         |
| Remote-ID String  |         |
| Port 2            |         |
| Option 82 State   | Disable |
| Circuit-ID String |         |
| Remote-ID String  |         |

| Parameter                           | Description  |
|-------------------------------------|--|
| <b>DHCP Option 82 Settings</b>      |  |
| State                               | Select this option to enable / disable the DHCP option 82 on the Switch. |
| 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.                      |
| <b>DHCP Option 82 Port Settings</b> |  |

|                                   |  |
|-----------------------------------|--|
| 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.  |
| Apply                             | Click <b>Apply</b> to take effect the settings.                            |
| Refresh                           | Click <b>Refresh</b> to begin configuring this screen afresh.              |
| <b>DHCP Option 82 Port Status</b> |  |
|                                   | The field displays all of the ports' configurations.                       |

## 6.5. 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.

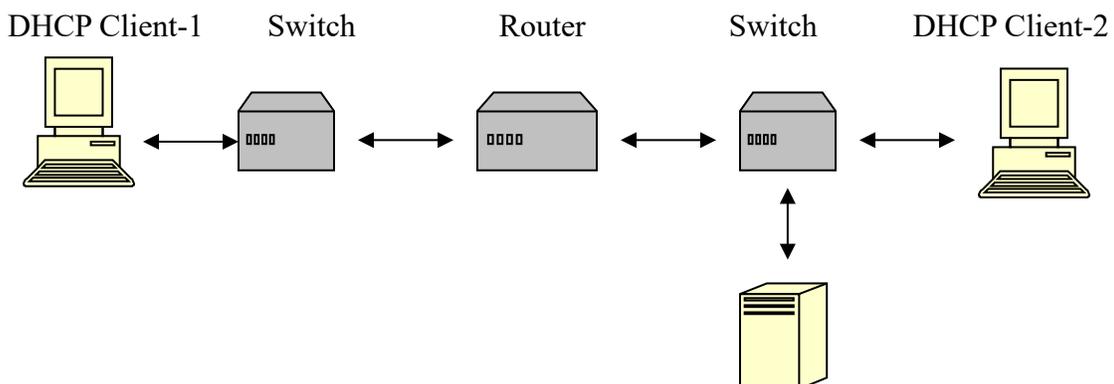
Most of the time in small networks DHCP uses broadcasts however there are some circumstances where unicast addresses will be used. A router for such a subnet receives the DHCP broadcasts, converts them to unicast (with a destination MAC/IP address of the configured DHCP server, source MAC/IP of the router 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 Switch. Users also can enable/disable the DHCP Relay on a specific VLAN. If the DHCP Relay on the Switch is disabled, the DHCP Relay is disabled on all VLANs even some of the VLAN DHCP Relay are enabled.

### Applications

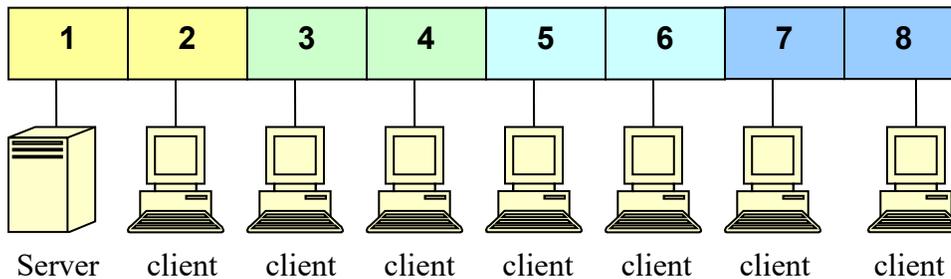
- Application-1 (Over a Router)  
The DHCP client-1 and DHCP client-2 are located in different IP segments. But they allocate IP address from the same DHCP server.



## DHCP Server

- Application-2 (Local in different VLANs)  
The DHCP client-1 and DHCP client-2 are located in different VLAN. But they allocate IP address from the same DHCP server.

### Switch DHCP Relay agent



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.*

### 6.5.1.CLI Configurations

| Node      | Command                        | Description  |
|-----------|--------------------------------|--|
| enable    | show dhcp relay                | This command displays the current configurations for the DHCP relay.         |
| enable    | configure terminal             | This command changes the node to configure node.                             |
| configure | dhcp relay (disable enable)    | This command disables/enables the DHCP relay on the switch.                  |
| configure | dhcp relay vlan VLAN_RANGE     | This command enables the DHCP relay function on a VLAN or a range of VLANs.  |
| configure | no dhcp relay vlan VLAN_RANGE  | This command disables the DHCP relay function on a VLAN or a range of VLANs. |
| configure | dhcp helper-address IP_ADDRESS | This command configures the DHCP server's IP address.                        |

|           |                        |  |
|-----------|------------------------|--|
| configure | no dhcp helper-address | This command 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
```

**6.5.2.Web Configurations**

**DHCP Relay**

**DHCP Relay Settings**

State:  ▾

VLAN State:  ▾

DHCP Server IP:

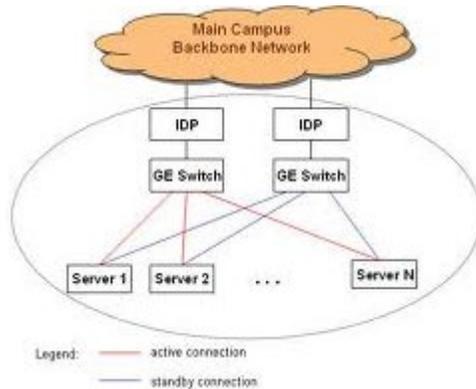
**DHCP Relay Status**

|                  |          |
|------------------|----------|
| DHCP Relay State | Disabled |
| Enabled on VLAN  | None     |
| DHCP Server IP   | 0.0.0.0  |

| Parameter                  | Description   |
|----------------------------|---|
| <b>DHCP Relay Settings</b> |   |
| State                      | Enables / disables the DHCP relay for the Switch.             |
| VLAN State                 | Enables / disables the DHCP relay on the specific VLAN(s).    |
| DHCP Server IP             | Configures the DHCP server's IP address.                      |
| Apply                      | Click <b>Apply</b> to take effect the settings.               |
| Refresh                    | Click <b>Refresh</b> to begin configuring this screen afresh. |

## 6.6. Dual Homing

Dual Homing, a network topology in which a device is connected to the network by the way of two independent access points (points of attachment). One access point is considered as a primary connection while other is standby. The standby access point is getting activated once primary connection fails.



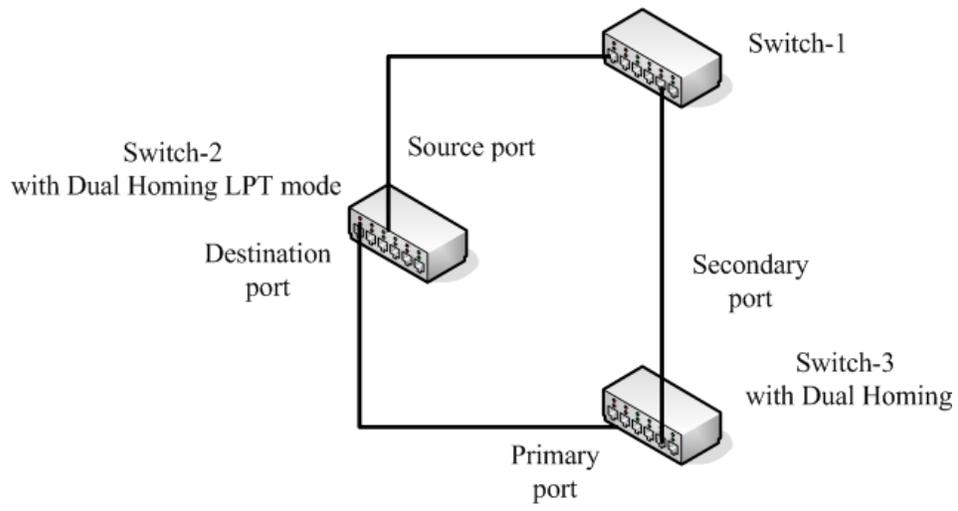
### How Dual-Homing Works?

Let us assume that both the primary and secondary connections are connected to Internet by means of different ways. For example, primary connection is connected to a physical network whereas the secondary one is attached to a wireless network. When dual homing feature is enabling, by default through primary connection the device will get connect to Internet at the same time the secondary connection will be shutdown. If the port or all the ports of primary connection are link-down then the device will replace its primary connection by the secondary one to connect with the Internet. If in any situation the secondary connection also link-down, device will do nothing. Secondary connection only works when primary connection is getting disconnect.

#### ● Dual Homing LPT Mode vs. Dual Homing :

The following figure is represented a ring connectivity between Switch-1, Switch-2 and Switch-3. In the discussed scenario, the Dual Homing LPT mode is enabled in the Switch-2 and Dual Homing is enabled in the Switch-3. Based on the mechanism of Dual Homing, the Secondary port of the Switch-3 will be shutdown which ensures a loop free ring connectivity.

Consider the scenario, if the source port between the Switch-2 and Switch-1 is link down, then the Destination port will automatically shutdown by the Dual Homing LPT mode. When the Switch-3 detects the Primary port gets link down, it will enable its Secondary port for continuing the communication. As a result, the hosts connected to the Switch-3 still can communicate with the hosts of Switch-1 without any interruption.



### 6.6.1.CLI Configurations

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show dual-homing                                       | This command displays the dual-homing information.   |
| enable    | configure terminal                                     | This command changes the node to configure node.   |
| configure | dual-homing<br>(disable enable)                        | This command disables / enables the dual-homing function for the system.   |
| configure | dual-homing<br>primary-channel<br>(port trunk) VALUE   | This command sets the dual-homing primary channel for the system. The channel can be a single port or a trunk group.   |
| configure | no dual-homing<br>primary-channel                      | This command removes the dual-homing primary channel for the system.   |
| configure | dual-homing<br>secondary-channel<br>(port trunk) VALUE | This command sets the dual-homing secondary channel for the system. The channel can be a single port or a trunk group. |
| configure | no dual-homing<br>secondary-channel                    | This command 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
```

## 6.6.2.Web Configurations

**Dual Homing**

**Dual Homing Settings**

State

Group ID

Group State

Primary Channel

Secondary Channel

**Dual Homing Status**

|                   |          |
|-------------------|----------|
| Group Id          | 1        |
| Group State       | Disabled |
| Primary Channel   | None     |
| Secondary Channel | None     |
| Group Id          | 2        |
| Group State       | Disabled |
| Primary Channel   | None     |
| Secondary Channel | None     |
| Group Id          | 3        |
| Group State       | Disabled |
| Primary Channel   | None     |
| Secondary Channel | None     |

| Parameter                   | Description   |
|-----------------------------|---|
| <b>Dual Homing Settings</b> |   |
| State                       | Enables / disables the Dual-Homing for the Switch.  |
| 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 <b>Apply</b> to take effect the settings.   |

Refresh

Click **Refresh** to begin configuring this screen afresh.

## 6.7. 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.

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

### 6.7.1. CLI Configurations

| Node      | Command               | Description  |
|-----------|-----------------------|--|
| enable    | show interface IFNAME | This command displays the current port configurations.         |
| enable    | configure terminal    | This command changes the node to configure node.               |
| configure | interface IFNAME      | This command enters the interface configure node.              |
| interface | eee (disable enable)  | This command enables / disables the EEE function on this port. |

Example:

- L2SWITCH#configure terminal
- L2SWITCH(config)#interface 1/0/1

### 6.7.2. Web Configurations

Energy Efficient Ethernet

Energy Efficient Ethernet Settings

EEE Ports State:(The feature for copper ports only.)

Select All  Deselect All

1  2  3  4  5

Apply Refresh

| Parameter                                 | Description   |
|---|---|
| <b>Energy Efficient Ethernet Settings</b> |   |
| 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 <b>Apply</b> to take effect the settings.                                |
| Refresh      | Click <b>Refresh</b> to begin configuring this screen afresh.                  |

## 6.8. 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 switch 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 Switch 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 switch fail (SF), manual switch (MS), or forced switch (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 switch 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 switch 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.

### **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.

**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.

Notice:

The ring ports should configure as below:

- Flow control off.
- 1000M Nway.
- Allow to enable up to 2 rings.

**6.8.1. Ring Settings**

**6.8.1.1. CLI Configurations**

| Node      | Command                 | Description  |
|-----------|-------------------------|--|
| enable    | show erps               | This command displays the ERPS configurations.   |
| enable    | configure terminal      | This command changes the node to configure node.   |
| configure | erps enable             | This command enables the global ERPS on the Switch.  |
| configure | no erps enable          | This command disables the global ERPS on the Switch.   |
| configure | erps ring-id <1-255>    | This command creates an ERPS ring and its ID and enter ERPS node.                              |
| configure | no erps ring-id <1-255> | This command creates an ERPS ring and enter ERPS node to configure detail ring configurations. |
| erps-ring | show                    | This command displays the configurations of the ring.  |
| erps-ring | control-vlan <1-4094>   | This command configures a control-vlan for the ERPS ring.                                      |
| erps-ring | guard-timer <10-2000>   | This command configures the Guard Timer for the ERPS ring. (default:500ms)                     |
| erps-ring | holdoff-timer <0-10000> | This command configures the Hold-off Timer for the ERPS ring. (default:0 ms)                   |

|           |   |   |
|-----------|---|---|
| erps-ring | left-port PORTID type<br>[owner neighbor normal]  | This command configures the left port and type for the ERPS ring.             |
| erps-ring | mel <0-7>   | This command configures a Control MEL for the ERPS ring.                      |
| erps-ring | name STRING                                       | This command configures a name for the ERPS ring.                             |
| erps-ring | revertive   | This command configures the revertive mode for the ERPS ring.                 |
| erps-ring | no revertive                                      | This command configures then on-revertive mode for the ERPS ring.             |
| erps-ring | right-port PORTID type<br>[owner neighbor normal] | This command configures the right port and type for the ERPS ring.            |
| erps-ring | ring enable                                       | This command enables the ring.  |
| erps-ring | no ring enable                                    | This command disables the ring.   |
| erps-ring | version (v1 v2)                                   | This command configures a version for the ERPS ring.                          |
| erps-ring | wtr-timer <5-720>                                 | This command configures the WTR Timer for the ERPS ring. (default: 5 minutes) |

### 6.8.1.2. Web Configurations

**ERPS**

Ring
Instance

**ERPS Global Settings**

Global State Disable ▾

**ERPS Ring Settings**

Ring ID  (1~255)

Ring Name

Instance  0 (0:Default, 0~30)

Control VLAN  (1~4094)

Holdoff Timer (ms)  0 (0~10000)

MEL  7 (0~7)

Left Port None ▾ Normal ▾

State Disable ▾

Revertive Enable ▾

Ring Type Major-ring ▾

Version v2 ▾

WTR Timer (sec)  300 (5~720)

Guard Timer (ms)  500 (10~2000)

Right Port None ▾ Normal ▾

Apply
Refresh

**ERPS Ring Status**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

| ERPS Global Settings |  |
|----------------------|--|
|----------------------|--|

|                           |   |
|---------------------------|---|
| Global State              | Enables/disables the global ERPS state.   |
| <b>ERPS Ring Settings</b> |   |
| 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 <b>Apply</b> to take effect the settings.   |
| Refresh                   | Click <b>Refresh</b> to begin configuring this screen afresh.   |

## 6.8.2. 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.

### 6.8.2.1. CLI Configurations

| Node             | Command  | Description   |
|------------------|--|---|
| enable           | show erps instance   | This command displays all of the ERPS instance configurations.                        |
| enable           | show erps instance <1-30>  | This command displays the specific ERPS instance configurations.                      |
| enable           | configure terminal   | This command changes the node to configure node.                                      |
| configure        | erps instance  | This command enters the instance configure node.                                      |
| config-erps-inst | instance <1-30><br>control-vlan <1-4094><br>data-vlan<br>VLANLISTS | This command configures a new instance and specifies its control VLAN and data VLANs. |
| config-erps-inst | no instance <1-30>   | This command removes an instance.   |
| config-erps-inst | show   | This command displays all of the instance configurations.                             |

## 6.8.2.2. Web Configurations

**ERPS**

Ring
Instance

**ERPS Instance Settings**

Instance  (1~30)

Control VLAN  (1~4094)      Data VLAN  (Multiple VLAN List, e.g. 1,2,5,10)

**ERPS Instance Status**

|              |   |           |   |
|--------------|---|-----------|---|
| Instance     | 1 | Data VLAN | 1 |
| Control VLAN | 2 | Data VLAN | 1 |

| Parameter                | Description  |
|--------------------------|--|
| <b>Instance Settings</b> |  |
| 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 <b>Apply</b> to take effect the settings.  |
| Refresh                  | Click <b>Refresh</b> to begin configuring this screen afresh.  |

## 6.9. Link Aggregation

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 Switch 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 Switch.

### 6.9.1. Static Trunk

#### 6.9.1.1. CLI Configurations

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show link-aggregation                              | The command displays the current trunk configurations.                 |
| enable    | configure terminal                                 | This command changes the node to configure node.                       |
| configure | link-aggregation [GROUP_ID] (disable   enable)     | The command disables / enables the trunk on the specific trunk group.  |
| configure | link-aggregation [GROUP_ID] load-balance (mac ip)  | The command configures the load balance algorithm for the trunk group. |
| configure | link-aggregation [GROUP_ID] interface PORTLISTS    | The command adds ports to a specific trunk group.                      |
| configure | no link-aggregation [GROUP_ID] interface PORTLISTS | The commands 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
```

## 6.9.1.2. Web Configurations

**Link Aggregation**

Static Trunk
LACP
LACP Info.

**Static Trunk Settings**

Group State Group 1 ▾ Disable ▾

Load Balance MAC ▾

Member Ports

Select All     Deselect All

1    2    3    4    5    6

**Trunk Group Status**

| Group ID | State    | Load Balance | Member Ports |
|----------|----------|--------------|--------------|
| 1        | Disabled | MAC          |              |
| 2        | Disabled | MAC          |              |
| 3        | Disabled | MAC          |              |

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

| Parameter                   | Description   |
|-----------------------------|---|
| <b>Trunk Group Settings</b> |   |
| Group State                 | Select the group ID to use for this trunk group, that is, one logical link containing multiple ports.<br>Select <b>Enable</b> to use this static trunk group. |
| Load Balance                | Configures the load balance algorithm ( <b>MAC/IP</b> ) for the specific trunk group.   |
| Member Ports                | Select the ports to be added to the static trunk group.   |
| Apply                       | Click <b>Apply</b> to take effect the settings.   |
| Refresh                     | Click <b>Refresh</b> to begin configuring this screen afresh.   |

## 6.9.2. LACP

The Switch 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.

Please note that:

- 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 switch 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.

### 6.9.2.1. CLI Configurations

| Node      | Command   | Description  |
|-----------|---|--|
| enable    | show lacp counters<br>[GROUP_ID]                    | This command displays the LACP counters for the specific group or all groups.                            |
| enable    | show lacp port_priority                             | This command c displays the port priority for the LACP.  |
| enable    | show lacp sys_id                                    | This command displays the actor's and partner's system ID.   |
| enable    | configure terminal                                  | This command changes the node to configure node.   |
| configure | lacp (disable   enable)                             | This command disables / enables the LACP on the switch.  |
| configure | lacp GROUP_ID<br>(disable   enable)                 | This command disables / enables the LACP on the specific trunk group.                                    |
| configure | clear lacp counters<br>[PORT_ID]                    | This command clears the LACP statistics for the specific port or all ports.                              |
| configure | lacp system-priority <1-65535>                      | This command configures the system priority for the LACP. Note: The default value is 32768.              |
| configure | no lacp system-priority                             | This command configures the default for the system priority for the LACP.                                |
| configure | interface IFNAME                                    | This command enters the interface configure node.  |
| interface | lacp port_priority <1-65535>                        | This command configures the priority for the specific port.<br><i>Note: The default value is 32768.</i>  |
| interface | no lacp port_priority                               | This command configures the default for the priority for the specific port.                              |
| configure | interface range<br>gigabitethernet1/0/POR<br>TLISTS | This command enters the if-range configure node.   |
| if-range  | lacp port_priority <1-65535>                        | This command configures the priority for the specific ports.<br><i>Note: The default value is 32768.</i> |
| if-range  | no lacp port_priority                               | This command configures the default for the priority for the specific ports.                             |

## 6.9.2.2. Web Configurations

**Link Aggregation**

Static Trunk
LACP
LACP Info.

**LACP Settings**

State Disable ▾  
 System Priority   
 Group LACP Group 1 ▾ Disable ▾  
 Port Priority From: - ▾ To: - ▾ :

**LACP Group Status**

| Group ID | LACP State |
|----------|------------|
| 1        | Disabled   |
| 2        | Disabled   |
| 3        | Disabled   |

**LACP Port Priority Status**

| Port | Priority | Port | Priority |
|------|----------|------|----------|
| 1    | 32768    | 2    | 32768    |
| 3    | 32768    | 4    | 32768    |
| 5    | 32768    | 6    | 32768    |

| Parameter            | Description  |
|----------------------|--|
| <b>LACP Settings</b> |  |
| State                | Select <b>Enable</b> from the drop down box to enable Link Aggregation Control Protocol (LACP).<br>Select <b>Disable</b> to not use LACP.  |
| System Priority      | LACP system priority is a number between 1 and 65,535. The switch 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 <b>Enable</b> or <b>Disable</b> 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 <b>Apply</b> to take effect the settings.  |

|         |   |
|---------|---|
| Refresh | Click <b>Refresh</b> to begin configuring this screen afresh. |
|---------|---|

**6.9.3. LACP Information**

**6.9.3.1. CLI Configurations**

| Node   | Command                       | Description   |
|--------|-------------------------------|---|
| enable | show lacp internal [GROUP_ID] | This command displays the LACP internal information for the specific group or all groups.   |
| enable | show lacp neighbor [GROUP_ID] | This command displays the LACP neighbor's information for the specific group or all groups. |

**6.9.3.2. Web Configurations**

**Link Aggregation**

Static Trunk
LACP
LACP Info.

LACP Information

Group ID

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

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

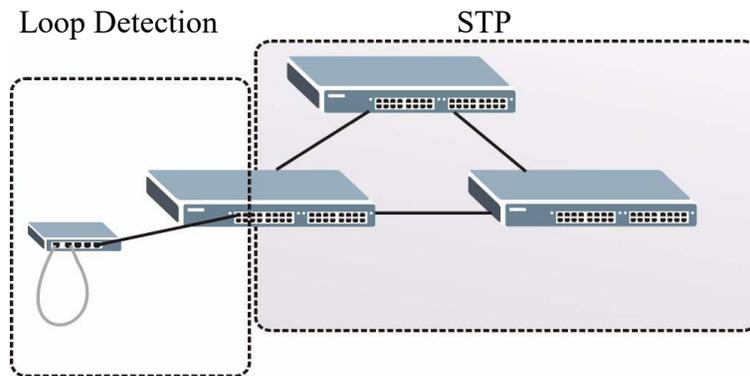
| Parameter                    | Description                                     |
|------------------------------|---|
| <b>LACP Information</b>      |   |
| Group ID                     | Select a LACP group that you want to view.      |
| Apply                        | Click <b>Apply</b> to take effect the settings. |
| <b>Neighbors Information</b> |   |
| 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 Switch's system ID.   |
| Port                        | The direct connected port Id of the neighbor Switch.   |
| Age                         | The available time period of the neighbor Switch LACP information.   |
| Port State                  | The direct connected port's state of the neighbor Switch.  |
| Port Priority               | The direct connected port's priority of the neighbor Switch.   |
| Oper Key                    | The Oper key of the neighbor Switch.   |
| <b>Internal Information</b> |  |
| 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.  |

## 6.10. 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 Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

The difference between the Loop Detection and STP:



The loop detection function sends probe packets periodically to detect if the port connect to a network in loop state. The Switch shuts down a port if the Switch detects that probe packets loop back to the same port of the Switch.

### Loop Recovery:

When the loop detection is enabled, the Switch will send one probe packets every two seconds and then listen this packet. If it receives the packet at the same port, the Switch will disable this port. After the time period, *recovery time*, the Switch will enable this port and do loop detection again.

The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop detection feature.

### 6.10.1. CLI Configurations

| Node      | Command                           | Description   |
|-----------|-----------------------------------|---|
| enable    | show loop-detection               | This command displays the current loop detection configurations.                    |
| enable    | configure terminal                | This command changes the node to configure node.                                    |
| configure | loop-detection (disable enable)   | This command disables / enables the loop detection on the switch.                   |
| configure | loop-detection address<br>MACADDR | This command configures the destination MAC for the loop detection special packets. |

|           |   |   |
|-----------|---|---|
| configure | no loop-detection address                       | This command configures the destination MAC to default (00:0b:04:AA:AA:AB).   |
| configure | interface IFNAME                                | This command enters the interface configure node.                             |
| interface | loop-detection (disable enable)                 | This command disables / enables the loop detection on the port.               |
| interface | no shutdown                                     | This command enables the port. It can unblock port blocked by loop detection. |
| interface | loop-detection recovery (disable enable)        | This command enables / disables the recovery function on the port.            |
| interface | loop-detection recovery time <1-60>             | This command configures the recovery period time.                             |
| configure | interface range<br>gigabitethernet1/0/PORTLISTS | This command enters the if-range configure node.                              |
| if-range  | loop-detection (disable enable)                 | This command disables / enables the loop detection on the ports.              |
| if-range  | loop-detection recovery (disable enable)        | This command enables / disables the recovery function on the port.            |
| if-range  | loop-detection recovery time <1-60>             | This command configures the recovery period time.                             |

**Example:**

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

## 6.10.2. Web Configurations

**Loop Detection**

**Loop Detection Settings**

State

MAC Address

| Port  | State                                | Recovery State                      | Recovery Time(min)                           |
|---|--------------------------------------|-------------------------------------|--|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="Disable"/> | <input type="text" value="Enable"/> | <input type="text" value="1"/> (Range: 1-60) |

**Loop Detection Status**

| Port | State    | Status | Manual Recovery                        | Recovery State | Recovery Time(min) |
|------|----------|--------|--|----------------|--------------------|
| 1    | Disabled | Normal | <input type="button" value="Unblock"/> | Enabled        | 1                  |
| 2    | Disabled | Normal | <input type="button" value="Unblock"/> | Enabled        | 1                  |
| 3    | Disabled | Normal | <input type="button" value="Unblock"/> | Enabled        | 1                  |
| 4    | Disabled | Normal | <input type="button" value="Unblock"/> | Enabled        | 1                  |
| 5    | Disabled | Normal | <input type="button" value="Unblock"/> | Enabled        | 1                  |
| 6    | Disabled | Normal | <input type="button" value="Unblock"/> | Enabled        | 1                  |

| Parameter                      | Description  |
|--------------------------------|--|
| <b>Loop Detection Settings</b> |  |
| State                          | Select this option to enable loop detection on the Switch.   |
| 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 detection protection.   |
| State                          | Select <b>Enable</b> to use the loop detection feature on the Switch.  |
| Recovery State                 | Select <b>Enable</b> to reactivate the port automatically after the designated recovery time has passed.                                 |
| Recovery Time                  | Specify the recovery time in minutes that the Switch will wait before reactivating the port. This can be between 1 to 60 minutes.        |
| Apply                          | Click <b>Apply</b> to take effect the settings.  |
| Refresh                        | Click <b>Refresh</b> to begin configuring this screen afresh.  |
| <b>Loop Detection Status</b>   |  |

|                     |  |
|---------------------|--|
| Port                | This field displays a port number.                                   |
| State               | This field displays if the loop detection feature is enabled.        |
| Status              | This field displays if the port is blocked.                          |
| Manual Recovery     | Clicks <b>Unblock</b> to reactivate the port immediately.            |
| Recovery State      | This field displays if the loop recovery feature is enabled.         |
| Recovery Time (min) | This field displays the recovery time for the loop recovery feature. |

### 6.11. Modbus TCP

Modbus TCP supports different types of data format for reading. The primary four types of them 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 Tripp Lite IE Switches

MODBUS base address of Tripp Lite switches is 1001(decimal) for Function Code 4.

| Address Offset            | Data Type | Interpretation | Description   |
|---------------------------|-----------|----------------|---|
| <b>System Information</b> |           |                |   |
| 0x0000                    | 1 word    | HEX            | Vendor ID = 0x0b04  |
| 0x0001                    | 16 words  | ASCII          | Vendor Name = "Tripp Lite"<br>Word 0 Hi byte = 'T'<br>Word 0 Lo byte = 'r'<br>Word 1 Hi byte = 'i'<br>Word 1 Lo byte = 'p'<br>Word 2 Hi byte = 'p'<br>Word 2 Lo byte = '<br>Word 3 Hi byte = 'L'<br>Word 3 Lo byte = 'i'<br>Word 4 Hi byte = 't'<br>Word 4 Lo byte = 'e'<br>Word 5 Hi byte = '\0'<br>Word 5 Lo byte = '\0'    |
| 0x0020                    | 16 words  | ASCII          | Product Name = "NGI-M05-C1"<br>Word 0 Hi byte = 'N'<br>Word 0 Lo byte = 'G'<br>Word 1 Hi byte = 'I'<br>Word 1 Lo byte = '-'<br>Word 2 Hi byte = 'M'<br>Word 2 Lo byte = '0'<br>Word 3 Hi byte = '5'<br>Word 3 Lo byte = '-'<br>Word 4 Hi byte = 'C'<br>Word 4 Lo byte = '1'<br>Word 5 Hi byte = '\0'<br>Word 5 Lo byte = '\0' |
| 0x0040                    | 7 words   |                | Product Serial Number   |

|                         |          |       |   |
|-------------------------|----------|-------|---|
|                         |          |       | Ex: Serial No=A00000000001  |
| 0x0050                  | 12 words | ASCII | Firmware Version="9015-000-1.0.0.S0"<br>Word 0 Hi byte = '9'<br>Word 0 Lo byte = '0'<br>Word 1 Hi byte = '1'<br>Word 1 Lo byte = '5'<br>Word 2 Hi byte = '-'<br>Word 2 Lo byte = '0'<br>Word 3 Hi byte = '0'<br>Word 3 Lo byte = '0'<br>Word 4 Hi byte = '-'<br>Word 4 Lo byte = '1'<br>Word 5 Hi byte = '.'<br>Word 5 Lo byte = '0'<br>Word 6 Hi byte = '.'<br>Word 6 Lo byte = '0'<br>Word 7 Hi byte = '.'<br>Word 7 Lo byte = 'S'<br>Word 8 Hi byte = '0'<br>Word 8 Lo byte = '\0' |
| 0x0060                  | 16 words | ASCII | Firmware Release Date="Mon Sep 30 18:51:45 2013"  |
| 0x0070                  | 3 words  | HEX   | Ethernet MAC Address<br>Ex: MAC = 00-01-02-03-04-05<br>Word 0 Hi byte = 0 x 00<br>Word 0 Lo byte = 0 x 01<br>Word 1 Hi byte = 0 x 02<br>Word 1 Lo byte = 0 x 03<br>Word 2 Hi byte = 0 x 04<br>Word 2 Lo byte = 0 x 05   |
| 0x0080                  | 1 word   | HEX   | Power 1(PWR) Alarm, DIP switch 1 need ON<br>0x0000: no alarm<br>0x0001: input voltage <44V<br>0x0002: input voltage > 57V<br>0x0003: No PWR input   |
| 0x0081                  | 1 word   | HEX   | Power 2(RPS) Alarm, DIP switch 1 need ON<br>0x0000: no alarm<br>0x0001: input voltage <44V<br>0x0002: input voltage > 57V<br>0x0003: No RPS input   |
| 0x0090                  | 1 word   | HEX   | Fault LED Status<br>0x0000: No<br>0x0001: Yes   |
| <b>Port Information</b> |          |       |   |
| 0x0100 to<br>0x0109     | 1 word   | HEX   | Port 1 to 10Link Status<br>0x0000: Link down<br>0x0001: 10M-Full-FC_ON (FC: Flow Control)<br>0x0002: 10M-Full-FC_OFF<br>0x0003: 10M-Half-FC_ON<br>0x0004: 10M-Half-FC_OFF<br>0x0005: 100M-Full-FC_ON<br>0x0006: 100M-Full-FC_OFF<br>0x0007: 100M-Half-FC_ON<br>0x0008: 100M-Half-FC_OFF<br>0x0009: 1000M-Full-FC_ON   |

|   |          |       |   |
|---|----------|-------|---|
|   |          |       | 0x000A: 1000M-Full-FC_OFF<br>0x000B: 1000M-Half-FC_ON<br>0x000C: 1000M-Half-FC_OFF<br>0xFFFF: No port   |
| 0x0200 to<br>0x0213 (port 1)<br>0x0220 to<br>0x0233 (port 2)<br>...<br>0x0320 to<br>0x0333 (port 6) | 20 words | ASCII | Port 1 to 6 Description<br>Port Description = "100TX,RJ45." Or<br>"1000TX,SFP."<br>Word 0 Hi byte = '1'<br>Word 0 Lo byte = '0'<br>Word 1 Hi byte = '0'<br>Word 1 Lo byte = 'T'<br>...<br>Word 4 Hi byte = '4'<br>Word 4 Lo byte = '5'<br>Word 5 Hi byte = '.'<br>Word 5 Lo byte = '\0' |
| 0x0400 to<br>0x0413 (port 1<br>to 6)  | 2 words  | HEX   | Port 1 to 6 Tx Packets<br>Ex: port 1 Tx Packet Amount = 0x87654321<br>Word 0 =8765<br>Word 1 = 4321   |
| 0x0440 to<br>0x0453 (port 1<br>to 6)  | 2 words  | HEX   | Port 1 to 6 Rx Packets<br>Ex: port 1 Rx Packet Amount = 0x123456<br>Word 0 = 0012<br>Word 1 = 3456  |
| 0x0480 to<br>0x0493 (port 1<br>to 6)  | 2 words  | HEX   | Port 1 to 6 Tx Error Packets<br>Ex: port 1 Tx Error Packet Amount =<br>0x87654321<br>Word 0 =8765<br>Word 1 = 4321  |
| 0x04C0 to<br>0x04D3 (port 1<br>to 6)  | 2 words  | HEX   | Port 1 to 6 Rx Error Packets<br>Ex: port 1 Rx Error Packet Amount = 0x123456<br>Word 0 = 0012<br>Word 1 = 3456  |
| <b>STP Information</b>  |          |       |   |
| 0x0500  | 1 word   | HEX   | STP Status:<br>0x0000 : STP is disabled.<br>0x0001 : STP<br>0x0002 : RSTP<br>0x0003 : MSTP  |
| <b>Xpress Ring Information</b>  |          |       |   |
| 0x0501  | 1 word   | HEX   | Xpress Ring Status on the Switch:<br>0x0000 : Disabled.<br>0x0001 : Enabled   |
| 0x0510  | 1 word   | HEX   | Status of Xpress-ring1 of the Switch<br>0x0000 : Disabled<br>0x0001 : Enabled   |
| 0x0511  | 1 word   | HEX   | Status of Xpress-ring2 of the Switch<br>0x0000 : Disabled<br>0x0001 : Enabled   |
| 0x0512  | 3 word   | HEX   | Destination MAC of the Xpress-ring1<br>Word 0 Lo byte = MAC0<br>Word 0 Hi byte = MAC1<br>Word 1Lo byte = MAC2<br>Word 1 Hi byte = MAC3<br>Word 2Lo byte = MAC4  |

|        |        |     |   |
|--------|--------|-----|---|
|        |        |     | Word 2 Hi byte = MAC5   |
| 0x0515 | 3 word | HEX | Destination MAC of the Xpress-ring2<br>Word 0 Lo byte = MAC0<br>Word 0 Hi byte = MAC1<br>Word 1Lo byte = MAC2<br>Word 1 Hi byte = MAC3<br>Word 2Lo byte = MAC4<br>Word 2 Hi byte = MAC5 |
| 0x0518 | 1 word | HEX | Primary Port of the Xpress-ring1<br>Word 0 Hi byte = Port ID.   |
| 0x0519 | 1 word | HEX | Secondary Port of the Xpress-ring1<br>Word 0 Hi byte = Port ID.   |
| 0x051a | 1 word | HEX | Primary Port of the Xpress-ring2<br>Word 0 Hi byte = Port ID.   |
| 0x051b | 1 word | HEX | Secondary Port of the Xpress-ring2<br>Word 0 Hi byte = Port ID.   |
| 0x051c | 1 word | HEX | Role of Xpress-ring1<br>0x0000 : Forwarder<br>0x0001 : Arbiter  |
| 0x051d | 1 word | HEX | Role of Xpress-ring2<br>0x0000 : Forwarder<br>0x0001 : Arbiter  |
| 0x051e | 1 word | HEX | Primary Port Status of Xpress-ring1<br>0x0000 : link down<br>0x0001 : forwarding<br>0x0002 : blocking   |
| 0x051f | 1 word | HEX | Secondary Port Status of Xpress-ring1<br>0x0000 : link down<br>0x0001 : forwarding<br>0x0002 : blocking   |
| 0x0520 | 1 word | HEX | Primary Port Status of Xpress-ring2<br>0x0000 : link down<br>0x0001 : forwarding<br>0x0002 : blocking   |
| 0x0521 | 1 word | HEX | Secondary Port Status of Xpress-ring2<br>0x0000 : link down<br>0x0001 : forwarding<br>0x0002 : blocking   |

### 6.11.1. CLI Configurations

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

| Node   | Command                                      | Description   |
|--------|--|---|
| enable | show modbus-tcp state                        | This command displays the current Modbus TCP configurations.  |
| enable | show modbus-tcp register-addr range NUMRANGE | This command displays the range of the Modbus TCP registrations.<br>Where NUMRANGE is the address range.<br>Format is: nnnn- <u>nnnn</u> , start <u>addr</u> -end <u>addr</u> . |
| enable | configure terminal                           | This command changes the node to configure node.  |

|           |                                |   |
|-----------|--------------------------------|---|
| configure | modbus-tcp<br>(disable enable) | This command disables / enables the Modbus TCP on the switch. |
|-----------|--------------------------------|---|

## 6.11.2. Web Configurations

**Modbus TCP**

**Modbus TCP Setting**

State

Connection : 0

**Modbus TCP Information**

| Read Input Registers (Function Code 04) |     |        |                |  |
|---|-----|--------|----------------|--|
| Modbus Address                          |     | Length | Interpretation | Description                              |
| Dec                                     | Hex | Word   |                |  |
| System Information                      |     |        |                |  |
| 1001                                    | 3e9 | 1      | HEX            | Vendor ID                                |
| 1002                                    | 3ea | 16     | ASCII          | Vendor Name                              |
| 1033                                    | 409 | 16     | ASCII          | Product Name                             |
| 1065                                    | 429 | 7      | ASCII          | Product Serial Number                    |
| 1081                                    | 439 | 12     | ASCII          | Firmware Version                         |
| 1097                                    | 449 | 16     | ASCII          | Firmware Release Date                    |
| 1113                                    | 459 | 3      | HEX            | Ethernet MAC Address                     |
| 1129                                    | 469 | 1      | HEX            | Power 1(PWR) Alarm, DIP switch 1 need ON |
| 1130                                    | 46a | 1      | HEX            | Power 2(RPS) Alarm, DIP switch 1 need ON |
| 1145                                    | 479 | 1      | HEX            | Fault LED Status                         |
| Port Information                        |     |        |                |  |
| 1257                                    | 4e9 | 1      | HEX            | Link Status of Port 1                    |

| Parameter                     | Description  |
|-------------------------------|--|
| <b>Modbus TCP Settings</b>    |  |
| State                         | Select this option to enable / disable the Modbus on the Switch. |
| Apply                         | Click <b>Apply</b> to take effect the settings.                  |
| Refresh                       | Click <b>Refresh</b> to begin configuring this screen afresh.    |
| <b>Modbus TCP Information</b> |  |

Download

Clicks the **Download** button to download all of the registers information to load host.

## 6.12. STP / RSTP

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch 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 Switch 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 Switch 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 | 4Mbps      | 250               | 100 to 1000       | 1 to 65535    |
| Path Cost | 10Mbps     | 100               | 50 to 600         | 1 to 65535    |
| Path Cost | 16Mbps     | 62                | 40 to 400         | 1 to 65535    |
| Path Cost | 100Mbps    | 19                | 10 to 60          | 1 to 65535    |
| Path Cost | 1Gbps      | 4                 | 3 to 10           | 1 to 65535    |
| Path Cost | 10Gbps     | 2                 | 1 to 5            | 1 to 65535    |

- On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root-path cost). If there is no root port, then this Switch 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 Switch will wait before changing states. This delay is required because every switch 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 30 seconds.

**Max Age:**

This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch 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 Switch 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 switch. 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 IEEE Standard 802.1D. 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 switch 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, making STP obsolete. 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 switch 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 switch. 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 switch port. If the port receives any BPDUs, the BPDUs will be dropped.

*Notice:*

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 switch. 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.

## 6.12.1. General Settings

### 6.12.1.1. CLI Configurations

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show spanning-tree active  | This command displays the spanning tree information and active ports' information. |
| enable    | show spanning-tree blocked ports   | This command displays the spanning tree information for only blocked port(s)       |
| enable    | show spanning-tree summary   | This command displays the summary of port states and configurations                |
| enable    | clear spanning-tree counters   | This command clears spanning-tree statistics for all ports.                        |
| enable    | clear spanning-tree counters PORT_ID   | This command clears spanning-tree statistics for a specific port.                  |
| enable    | configure terminal   | This command changes the node to configure node.                                   |
| configure | spanning-tree (disable   enable)   | This command disables / enables the spanning tree function for the system.         |
| configure | spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME | This command configures the bridge times(forward-delay, max-age, hello-time).      |
| configure | no spanning-tree algorithm-timer   | This command configures the default values for forward-time &max-age &hello-time.  |
| configure | spanning-tree forward-time <4-30>  | This command configures the bridge forward delay time (sec).                       |
| configure | no spanning-tree forward-time  | This command configures the default values for forward-time.                       |
| configure | spanning-tree hello-time <1-10>  | This command configures the bridge hello time (sec).                               |
| configure | no spanning-tree hello-time  | This command configures the default values for hello-time.                         |
| configure | spanning-tree max-age <6-40>   | This command configures the bridge message max-age time (sec).                     |
| configure | no spanning-tree max-age   | This command configures the default values for max-age time.                       |
| configure | spanning-tree mode (rstp stp)  | This command configures the spanning mode.   |
| configure | spanning-tree path-cost method (short long)                                  | This command configures the path-cost method.                                      |
| configure | spanning-tree priority <0-61440>   | This command configures the priority for the system.                               |
| configure | no spanning-tree priority  | This command configures the default values for the system priority.                |

## 6.12.1.2. Web Configurations

**Spanning Tree Protocol**

| General Settings  | Port Parameters                              | STP Status  |
|---|--|---|
| <b>STP Settings</b>   |  |   |
| State   | <input type="text" value="Disable"/>         |   |
| Mode  | <input type="text" value="RSTP"/>            |   |
| <b>STP Parameter Settings</b>   |  |   |
| Forward Delay (sec)   | <input type="text" value="15"/> (4~30)       | Relationships:<br>$2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$<br>$\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$ |
| Max Age (sec)   | <input type="text" value="20"/> (6~40)       |   |
| Hello Time (sec)  | <input type="text" value="2"/> (1~10)        |   |
| Priority  | <input type="text" value="32768"/> (0~61440) |   |
| Pathcost Method   | <input type="text" value="Short"/>           |   |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> |  |   |

| Parameter                     | Description  |
|-------------------------------|--|
| <b>STP Settings</b>           |  |
| State                         | Select <b>Enabled</b> to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).  |
| Mode                          | Select to use either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).  |
| <b>STP Parameter Settings</b> |  |
| Forward Time                  | This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch 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 30 seconds.  |
| Max Age                       | This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals.<br>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 Switch 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 switch. The allowed range is 1 to 10 seconds.   |

|          |   |
|----------|---|
| Priority | <p>Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.</p> <p>Enter a value from 0~61440.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge.</p> <p>Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.</p> |
| Pathcost | <p>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.</p>   |
| Apply    | <p>Click <b>Apply</b> to take effect the settings.</p>  |
| Refresh  | <p>Click <b>Refresh</b> to begin configuring this screen afresh.</p>  |

## 6.12.2. Port Parameters

### 6.12.2.1. CLI Configurations

| Node      | Command                                    | Description  |
|-----------|--|--|
| enable    | show spanning-tree blocked ports           | This command displays the spanning tree information for only blocked port(s).            |
| enable    | show spanning-tree port detail PORT_ID     | This command displays the spanning tree information for the interface port.              |
| enable    | configure terminal                         | This command changes the node to configure node.   |
| configure | interface IFNAME                           | This command enters the interface configure node.  |
| interface | spanning-tree (disable enable)             | This command configures enables/disables the STP function for the specific port.         |
| interface | spanning-tree bpdupfilter (disable enable) | This command configures enables/disables the bpdu filter function for the specific port. |
| interface | spanning-tree bpduguard (disable enable)   | This command configures enables/disables the bpdu guard function for the specific port.  |
| interface | spanning-tree rootguard (disable enable)   | This command enables/disables the BPDU Root guard port setting for the specific port.    |
| interface | spanning-tree edge-port (disable enable)   | This command enables/disables the edge port setting for the specific port.               |
| interface | spanning-tree cost VALUE                   | This command configures the cost for the specific port.                                  |

|           |   |  |
|-----------|---|--|
|           |   | Cost range:<br>16-bit based value range 1-65535,<br>32-bit based value range 1-200000000.  |
| interface | no spanning-tree cost                           | This command configures the path cost to default for the specific port.  |
| interface | spanning-tree port-priority <0-240>             | This command configures the port priority for the specific port.<br>Default: 128.  |
| interface | no spanning-tree port-priority                  | This command configures the port priority to default for the specific port.  |
| configure | interface range<br>gigabitethernet1/0/PORTLISTS | This command enters the if-range configure node.   |
| if-range  | spanning-tree(disable enable)                   | This command configures enables/disables the STP function for the specific port.   |
| if-range  | spanning-tree bpdudfilter (disable enable)      | This command configures enables/disables the bpdu filter function for the specific port.   |
| if-range  | spanning-tree bpduguard (disable enable)        | This command configures enables/disables the bpdu guard function for the specific port.  |
| if-range  | spanning-tree rootguard (disable enable)        | This command enables/disables the BPDU Root guard port setting for the specific port.  |
| if-range  | spanning-tree edge-port (disable enable)        | This command enables/disables the edge port setting for the specific port.   |
| if-range  | spanning-tree cost VALUE                        | This command configures the cost for the specific port.<br>Cost range:<br>16-bit based value range 1-65535,<br>32-bit based value range 1-200000000. |
| if-range  | no spanning-tree cost                           | This command configures the path cost to default for the specific port.  |
| if-range  | spanning-tree port-priority <0-240>             | This command configures the port priority for the specific port.<br>Default: 128.  |
| if-range  | no spanning-tree port-priority                  | This command configures the port priority to default for the specific port.  |

## 6.12.2.2. Web Configurations

**Spanning Tree Protocol**

General Settings
Port Parameters
STP Status

STP Port Settings

| Port              | Active   | Path Cost | Priority | Edge Port | BPDU Filter | BPDU Guard | ROOT Guard |
|-------------------|----------|-----------|----------|-----------|-------------|------------|------------|
| From: 1 ▼ To: 1 ▼ | Enable ▼ | 250       | 128      | Disable ▼ | Disable ▼   | Disable ▼  | Disable ▼  |

STP Port Status

| Port | Active  | Role | Status     | Path Cost | Priority | Edge Port | BPDU Filter | BPDU Guard | ROOT Guard |
|------|---------|------|------------|-----------|----------|-----------|-------------|------------|------------|
| 1    | Enabled | None | Discarding | 250       | 128      | Disabled  | Disabled    | Disabled   | Disabled   |
| 2    | Enabled | None | Discarding | 250       | 128      | Disabled  | Disabled    | Disabled   | Disabled   |
| 3    | Enabled | None | Discarding | 250       | 128      | Disabled  | Disabled    | Disabled   | Disabled   |
| 4    | Enabled | None | Discarding | 250       | 128      | Disabled  | Disabled    | Disabled   | Disabled   |
| 5    | Enabled | None | Discarding | 250       | 128      | Disabled  | Disabled    | Disabled   | Disabled   |
| 6    | Enabled | None | Discarding | 250       | 128      | Disabled  | Disabled    | Disabled   | Disabled   |

| Parameter                       | Description  |
|---------------------------------|--|
| <b>Port Parameters Settings</b> |  |
| Port                            | Selects a port that you want to configure.                           |
| Active                          | Enables/Disables the spanning tree function for the specific port.   |
| 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 <b>Apply</b> to take effect the settings.                      |
| Refresh                         | Click <b>Refresh</b> to begin configuring this screen afresh.        |
| <b>Port Status</b>              |  |
| Active                          | The state of the STP function.                                       |

|             |   |
|-------------|---|
| Role        | The port role. Should be one of the Alternated / Designated / Root / Backup / None.                           |
| 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.  |

### 6.12.3. STP Status

#### 6.12.3.1. CLI Configurations

| Node   | Command                   | Description  |
|--------|---------------------------|--|
| enable | show spanning-tree active | This command displays the spanning tree information and active ports' information. |

#### 6.12.3.2. Web Configurations

**Spanning Tree Protocol**

General Settings
Port Parameters
STP Status

**Current Root Status**

| MAC Address       | Priority | Max Age | Hello Time | Forward Delay |
|-------------------|----------|---------|------------|---------------|
| 00:0b:04:00:00:06 | 32768    | 20      | 2          | 15            |

**Current Bridge Status**

| MAC Address       | Priority | Max Age | Hello Time | Forward Delay | Path Cost | Root Port |
|-------------------|----------|---------|------------|---------------|-----------|-----------|
| 00:0b:04:00:00:06 | 32768    | 20      | 2          | 15            | 0         | 0         |

| Parameter                    | Description   |
|------------------------------|---|
| <b>Current Root Status</b>   |   |
| MAC address                  | This is the MAC address of the root bridge.   |
| Priority                     | <b>Root</b> refers to the base of the spanning tree (the root bridge). This field displays the root bridge's priority. This Switch may also be the root bridge.         |
| MAX Age                      | This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.                                   |
| Hello Time                   | This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay. |
| Forward Delay                | This is the time (in seconds) the root switch will wait before changing states.   |
| Apply                        | Click <b>Apply</b> to take effect the settings.   |
| Refresh                      | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>Current Bridge Status</b> |   |
| MAC address                  | This is the MAC address of the current bridge.  |

|               |   |
|---------------|---|
| Priority      | <p>Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.</p> <p>Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.</p>                  |
| MAX Age       | <p>This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals.</p> <p>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 Switch ports attached to the network.</p> |
| Hello Time    | <p>This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch.</p>   |
| Forward Delay | <p>This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch 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.</p>  |
| Path Cost     | <p>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.</p>   |
| Root Cost     | <p>This is the number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.</p>  |

## 7. Security

### 7.1. 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)

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

The switch drops a DHCP packet when one of these situations occurs:

- ✓ A packet from a DHCP server, such as a DHCP OFFER, DHCP ACK, DHCP NAK, or DHCP REQUEST 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. Untrusted 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 Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

*Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.*

**Untrusted ports** are connected to subscribers. The Switch 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 Switch stores the binding table in volatile memory. If the Switch 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 Switch.

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

#### **Notes:**

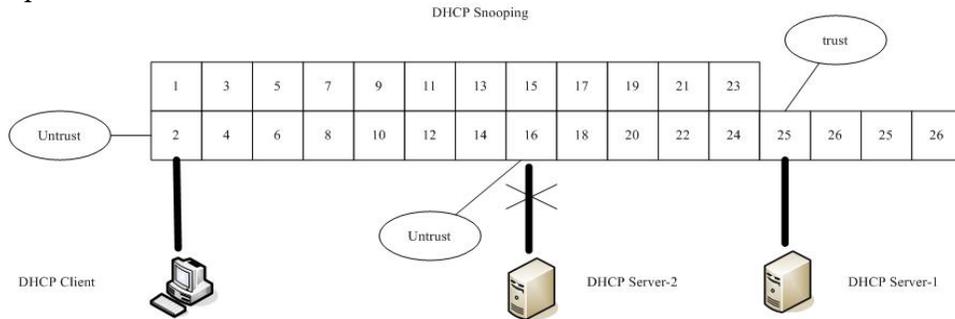
*The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.*

*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.



The DHCP server connected to an untrusted port will be filtered.

### Notices

There are a global state and per VLAN states.

When the global state is disabled, the DHCP Snooping on the Switch 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 : port 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-trust 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.

### 7.1.1.1. DHCP Snooping

#### 7.1.1.1.1. CLI Configurations

| Node      | Command                            | Description   |
|-----------|------------------------------------|---|
| enable    | show dhcp-snooping                 | This command displays the current DHCP snooping configurations.               |
| enable    | configure terminal                 | This command changes the node to configure node.                              |
| configure | dhcp-snooping<br>(disable enable)  | This command disables/enables the DHCP snooping on the switch.                |
| configure | dhcp-snooping vlan<br>VLANLISTS    | This command enables the DHCP snooping function on a VLAN or range of VLANs.  |
| configure | no dhcp-snooping vlan<br>VLANLISTS | This command 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
```

### 7.1.1.1.2. Web Configurations

**DHCP Snooping**

DHCP Snooping
Port Settings
Server Screening

**DHCP Snooping Settings**

State Disable ▾

VLAN State Add ▾

**DHCP Snooping Status**

|                     |          |
|---------------------|----------|
| DHCP Snooping State | Disabled |
| Enabled on VLAN     | None     |

| Parameter                     | Description   |
|-------------------------------|---|
| <b>DHCP Snooping Settings</b> |   |
| State                         | Select <b>Enable</b> to use DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLANs and specify trusted ports.<br>Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.<br>Select <b>Disable</b> to not use DHCP snooping. |
| VLAN State                    | Select <b>Add</b> and enter the VLAN IDs you want the Switch to enable DHCP snooping on. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-).<br>Select <b>Delete</b> and enter the VLAN IDs you no longer want the Switch to use DHCP snooping on.           |
| Apply                         | Click <b>Apply</b> to take effect the settings.   |
| Refresh                       | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>DHCP Snooping Status</b>   |   |
| DHCP Snooping State           | This field displays the current status of the DHCP snoopingfeature, <b>Enabled</b> or <b>Disabled</b> .   |
| Enabled on VLAN               | This field displays the VLAN IDs that have DHCP snooping enabled on them. This will display <b>None</b> if no VLANs have been set.  |

## 7.1.1.2. Port Settings

### 7.1.1.2.1. CLI Configurations

| Node      | Command   | Description  |
|-----------|---|--|
| enable    | show dhcp-snooping                              | This command displays the current DHCP snooping configurations.  |
| enable    | configure terminal                              | This command changes the node to configure node.   |
| configure | interface IFNAME                                | This command enters the interface configure node.  |
| interface | dhcp-snooping host count <1-32>                 | This command configures the maximum host count for the specific port.  |
| interface | no dhcp-snooping host count                     | This command configures the maximum host count to default for the specific port.<br>The default host count is 32.  |
| interface | dhcp-snooping trust                             | This command configures the trust port for the specific port.  |
| interface | no dhcp-snooping trust                          | This command configures the un-trust port for the specific port.   |
| configure | interface range<br>gigabitethernet1/0/PORTLISTS | This command enters the if-range configure node.   |
| if-range  | dhcp-snooping host count <1-32>                 | This command configures the maximum host count for the specific ports.   |
| if-range  | no dhcp-snooping host count                     | This command configures the maximum host count to default for the specific ports.<br>The default host count is 32. |
| if-range  | dhcp-snooping trust                             | This command configures the trust port for the specific ports.   |
| if-range  | no dhcp-snooping trust                          | This command configures the un-trust port for the specific ports.  |

## 7.1.1.2.2. Web Configurations

**DHCP Snooping**

DHCP Snooping
**Port Settings**
Server Screening

**Port Settings**

Port                      From:  To:

Trust                     

Maximum Host Count     (Range: 1-32)

**Port Status**

| 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                 |

| Parameter            | Description  |
|----------------------|--|
| <b>Port Settings</b> |  |
| 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 <b>Apply</b> to take effect the settings.  |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.                                    |

### 7.1.1.3. Server Screening

The Switch supports DHCP Server Screening, a feature that denies access to rogue DHCP servers. That is, when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients, the valid DHCP server's packets will be passed to the client.

If you want to enable this feature, you must enable the DHCP Snooping function first. The Switch allows users to configure up to three valid DHCP servers.

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

#### 7.1.1.3.1. CLI Configurations

| Node      | Command                        | Description                                       |
|-----------|--------------------------------|---|
| enable    | show dhcp-snooping server      | This command displays the valid DHCP server IP.   |
| enable    | configure terminal             | This command changes the node to configure node.  |
| configure | dhcp-snooping server IPADDR    | This command configures a valid DHCP server's IP. |
| configure | no dhcp-snooping server IPADDR | This command removes a valid DHCP server's IP.    |

#### 7.1.1.3.2. Web Configurations

**DHCP Snooping**

DHCP Snooping
Port Settings
Server Screening

**Server Screening Setting**

DHCP Server IP

**Server Screening List**

| No. | IP Address    | Action                                |
|-----|---------------|---------------------------------------|
| 1   | 192.168.202.1 | <input type="button" value="Delete"/> |

| Parameter                        | Description   |
|----------------------------------|---|
| <b>Server Screening Settings</b> |   |
| DHCP Server IP                   | This field configures the valid DHCP server's IP address.     |
| Apply                            | Click <b>Apply</b> to configure the settings.                 |
| Refresh                          | Click <b>Refresh</b> to begin configuring this screen afresh. |

| Server Screening List |  |
|-----------------------|--|
| No.                   | This field displays the index number of the DHCP server entry. Click the number to modify the entry. |
| IP Address            | This field displays the IP address of the DHCP server.   |
| Action                | Click <b>Delete</b> to remove a configured DHCP server.  |

### 7.1.2. 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.

#### 7.1.2.1. Static Entry

##### 7.1.2.1.1. CLI Configurations

| Node      | Command  | Description   |
|-----------|--|---|
| enable    | show dhcp-snooping binding   | This command displays the current DHCP snooping binding table.              |
| enable    | configure terminal   | This command changes the node to configure node.                            |
| configure | dhcp-snooping binding mac<br>MAC_ADDR ip IP_ADDR<br>vlan <1-4094> port PORT_NO | This command configures a static host into the DHCP snooping binding table. |
| configure | no dhcp-snooping binding mac<br>MACADDR  | This command 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
```

### 7.1.2.1.2. Web Configurations

#### DHCP Snooping Binding Table

Static Entry
Binding Table

**Static Entry Settings**

MAC Address

IP Address

VLAN ID

Port

**Static Binding Table**

| No. | MAC Address       | IP Address      | Lease(hour) | VLAN | Port | Type   | Action                                |
|-----|-------------------|-----------------|-------------|------|------|--------|---------------------------------------|
| 1   | 00:0b:04:11:22:33 | 192.168.202.111 | 0           | 1    | 1    | Static | <input type="button" value="Delete"/> |

| Parameter                    | Description   |
|------------------------------|---|
| <b>Static Entry Settings</b> |   |
| 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 <b>Apply</b> to take effect the settings.   |
| Refresh                      | Click <b>Refresh</b> to begin configuring this screen afresh.                                   |
| <b>Static Binding Table</b>  |   |
| No.                          | This field displays a sequential number for each binding. Click it to update an existing entry. |
| MAC Address                  | This field displays the source MAC address in the binding.                                      |
| IP Address                   | This field displays the IP address assigned to the MAC address in the binding.                  |
| Lease (Hour)                 | This field displays how long the binding is valid.  |
| VLAN                         | This field displays the source VLAN ID in the binding.  |
| Port                         | This field displays the port number in the binding.   |

|        |  |
|--------|--|
| Type   | This field displays how the Switch learned the binding.<br><b>Static:</b> This binding was learned from information provided manually by an administrator.<br><b>Dynamic:</b> This binding was learned by snooping DHCP packets. |
| Action | Click <b>Delete</b> to remove the specified entry.   |

### 7.1.2.2. Binding Table

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

#### 7.1.2.2.1. CLI Configurations

| Node   | Command                    | Description  |
|--------|----------------------------|--|
| enable | show dhcp-snooping binding | This command displays the current DHCP snooping binding table. |

#### 7.1.2.2.2. Web Configurations

**DHCP Snooping Binding Table**

Static Entry    Binding Table

DHCP Snooping Binding Table

Show Type:

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

| *All                     | MAC Address       | IP Address      | Lease(hour) | VLAN | Port | Type   |
|--------------------------|-------------------|-----------------|-------------|------|------|--------|
| <input type="checkbox"/> | 00:0b:04:11:22:33 | 192.168.202.111 | 0           | 1    | 1    | Static |

| Parameter                          | Description  |
|------------------------------------|--|
| <b>DHCP Snooping Binding Table</b> |  |
| MAC Address                        | This field displays the source MAC address in the binding.                     |
| IP Address                         | This field displays the IP address assigned to the MAC address in the binding. |
| Lease                              | This field displays how long the binding is valid.                             |
| VLAN                               | This field displays the source VLAN ID in the binding.                         |

|         |  |
|---------|--|
| Port    | This field displays the port number in the binding. If this field is blank, the binding applies to all ports.  |
| Type    | This field displays how the Switch learned the binding.<br><b>Static:</b> This binding was learned from information provided manually by an administrator.<br><b>Dynamic:</b> This binding was learned by snooping DHCP packets. |
| Apply   | Click <b>Apply</b> to configure the settings.  |
| Refresh | Click <b>Refresh</b> to begin configuring this screen afresh.  |

### 7.1.3. 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 switch 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 Switch does not discard ARP packets on trusted ports for any reasons.
- The Switch 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 Switch. Users also can enable/disable the ARP Inspection on a specific VLAN. If the ARP Inspection on the Switch is disabled, the ARP Inspection is disabled on all VLANs even some of the VLAN ARP Inspection are enabled.

#### Notices

There are a global state and per VLAN states.

- ✓ When the global state is disabled, the ARP Inspection on the Switch 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.

### 7.1.3.1. ARP Inspection

#### 7.1.3.1.1. CLI Configurations

| Node      | Command                          | Description  |
|-----------|----------------------------------|--|
| enable    | show arp-inspection              | This command displays the current ARP Inspection configurations.               |
| enable    | configure terminal               | This command changes the node to configure node.                               |
| configure | arp-inspection (disable enable)  | This command disables/enables the ARP Inspection function on the switch.       |
| configure | arp-inspection vlan VLANLISTS    | This command enables the ARP Inspection function on a VLAN or range of VLANs.  |
| configure | no arp-inspection vlan VLANLISTS | This command disables the ARP Inspection function on a VLAN or range of VLANs. |
| configure | interface IFNAME                 | This command enters the interface configure node.                              |
| interface | arp-inspection trust             | This command configures the trust port for the specific port.                  |
| interface | no arp-inspection trust          | This command 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
```

### 7.1.3.1.2. Web Configurations

**ARP Inspection**

ARP Inspection
Filter Table

**ARP Inspection Settings**

State

VLAN State

Trusted Ports

Select All     Deselect All

1    2    3    4    5    6

**ARP Inspection Status**

|                      |          |
|----------------------|----------|
| ARP Inspection State | Disabled |
| Enabled on VLAN      | None     |
| Trusted Ports        | None     |

| Parameter                      | Description  |
|--------------------------------|--|
| <b>ARP Inspection Settings</b> |  |
| State                          | Use this to <b>Enable</b> or <b>Disable</b> ARP inspection on the Switch.  |
| VLAN State                     | Enter the VLAN IDs you want the Switch to enable ARP Inspection for. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-).  |
| Trusted Ports                  | <p>Select the ports which are trusted and deselect the ports which are un-trusted.</p> <p>The Switch does not discard ARP packets on trusted ports for any reason.</p> <p>The Switch discards ARP packets on un-trusted ports in the following situations:</p> <ul style="list-style-type: none"> <li>• The sender's information in the ARP packet does not match any of the current bindings.</li> <li>• 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.</li> </ul> |
| Select All                     | Click this to set all ports to trusted.  |
| Deselect All                   | Click this to set all ports to un-trusted.   |
| Apply                          | Click <b>Apply</b> to take effect the settings.  |
| Refresh                        | Click <b>Refresh</b> to begin configuring this screen afresh.  |

| <b>ARP Inspection Status</b> |   |
|------------------------------|---|
| ARP Inspection State         | This field displays the current status of the ARP Inspection feature, <b>Enabled</b> or <b>Disabled</b> .                           |
| Enabled on VLAN              | This field displays the VLAN IDs that have ARP Inspection enabled on them. This will display <b>None</b> if no VLANs have been set. |
| Trusted Ports                | This field displays the ports which are trusted. This will display <b>None</b> if no ports are trusted.                             |

### 7.1.3.2. 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 Switch 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 switch 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 will create a filtered entry in the MAC address table.
- When Port link down and ARP Inspection was disabled, Switch will remove the MAC-filter entries learned by this port.
- When Port link down and ARP Inspection was enabled, Switch will remove 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 Switch receives unauthorized ARP packet, and it automatically creates a SYSLOG and drop this ARP packet. The SYSLOG event happens on the first time.

#### 7.1.3.2.1. CLI Configurations

| Node      | Command  | Description   |
|-----------|--|---|
| enable    | show arp-inspection mac-filter                         | This command displays the current ARP Inspection filtered MAC.                |
| enable    | configure terminal                                     | This command changes the node to configure node.                              |
| configure | arp-inspection mac-filter age <1-10080>                | This command configures the age time for the ARP inspection MAC filter entry. |
| configure | clear arp-inspection mac-filter                        | This command clears all of entries in the filter table.                       |
| configure | no arp-inspection mac-filter mac MACADDR vlan <1-4094> | This command removes an entry from the ARP inspection MAC filter table.       |

### 7.1.3.2.2. Web Configurations

**ARP Inspection**

|   |  |             |             |                    |                     |
|---|--|-------------|-------------|--------------------|---------------------|
| ARP Inspection  | <b>Filter Table</b>  |             |             |                    |                     |
| <b>Filter Age Time Settings</b>   |  |             |             |                    |                     |
| Filter Age Time   | <input style="width: 50px;" type="text" value="5"/> minutes (Range: 1-10080) |             |             |                    |                     |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> |  |             |             |                    |                     |
| <b>Filter Table</b>   |  |             |             |                    |                     |
| <b>No.</b>  | <b>MAC Address</b>   | <b>VLAN</b> | <b>Port</b> | <b>Expiry(min)</b> | <b>Action</b>       |
|   |  |             |             |                    | Total : 0 record(s) |

| Parameter                       | Description   |
|---------------------------------|---|
| <b>Filter Age Time Settings</b> |   |
| 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 Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. |
| Apply                           | Click <b>Apply</b> to take effect the settings.   |
| Refresh                         | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>Filter Table</b>             |   |
| No.                             | This field displays a sequential number for each MAC addressfilter.   |
| MAC Address                     | This field displays the source MAC address in the MAC addressfilter.  |
| VLAN                            | This field displays the source VLAN ID in the MAC address filter.   |
| Port                            | This field displays the source port of the discarded ARP packet.  |
| Expiry (min)                    | This field displays how long (in minutes) the MAC address filter remains in the Switch.   |
| Action                          | Click <b>Delete</b> to remove the record manually.  |
| Total                           | This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.   |

## 7.2. Access Control List

**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.

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: *source mac host MACADDR*
2. Filter a specific destination MAC address.  
Command: *destination mac host MACADDR*
3. Filter a range of source MAC address.  
Command: *source mac 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 ip host IPADDR*
3. Filter a range of source IP address.  
Command: *source ip IPADDR IPADDR*  
The second IPADDR is a mask, for example: 255.255.0.0
4. Filter a range of destination IP address.  
Command: *destination ip IPADDR IPADDR*

### L4 ACL Support:

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

### Notices:

- Maximum profile : 64.
- Maximum profile name length : 16.

- The ACL name should be the combination of the digit or the alphabet.

### 7.2.1. CLI Configurations

| Node      | Command  | Description   |
|-----------|--|---|
| enable    | show access-list                                 | This command displays all of the access control profiles.   |
| configure | access-list STRING                               | This command creates a new access control profile.<br>Where the STRING is the profile name.   |
| configure | no access-list<br>STRING                         | This command deletes an access control profile.   |
| acl       | show   | This command displays the current access control profile.   |
| acl       | action<br>(disable drop permit)                  | This command activates this profile.<br><b>disable</b> – disable the profile.<br><b>drop</b> – If packets match the profile, the packets will be dropped.<br><b>permit</b> – If packets match the profile, the packets will be forwarded. |
| acl       | destination mac host<br>MACADDR                  | This command configures the destination MAC and mask for the profile.   |
| acl       | destination mac<br>MACADDR<br>MACADDR            | This command configures the destination MAC and mask for the profile.   |
| acl       | destination mac<br>MACADDR<br>MACADDR<br>MACADDR | This command configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile.   |
| acl       | no destination mac                               | This command removes the destination MAC from the profile.  |
| acl       | ethertype STRING                                 | This command configures the ether type for the profile. Where the STRING is a hex-decimal value. e.g.: 08AA.  |
| acl       | no ethertype                                     | This command removes the limitation of the ether type from the profile.   |
| acl       | source mac host<br>MACADDR                       | This command configures the source MAC and mask for the profile.  |
| acl       | source mac<br>MACADDR<br>MACADDR                 | This command configures the source MAC and mask for the profile.  |
| acl       | no source mac                                    | This command removes the source MAC and mask from the profile.  |
| acl       | source ip host<br>IPADDR                         | This command configures the source IP address for the profile.  |

|     |                                 |  |
|-----|---------------------------------|--|
| acl | source ip IPADDR<br>IPMASK      | This command configures the source IP address and mask for the profile.      |
| acl | no source ip                    | This command removes the source IP address from the profile.                 |
| acl | destination ip host<br>IPADDR   | This command configures a specific destination IP address for the profile.   |
| acl | destination ip<br>IPADDR IPMASK | This command configures the destination IP address and mask for the profile. |
| acl | no destination ip               | This command removes the destination IP address from the profile.            |
| acl | l4-source-port<br>IPADDR        | This command configures UDP/TCP source port for the profile.                 |
| acl | no l4-source-port<br>IPADDR     | This command removes the UDP/TCP source port from the profile.               |
| acl | L4-destination-port<br>PORT     | This command configures the UDP/TCP destination port for the profile.        |
| acl | no l4-destination-port          | This command removes the UDP/TCP destination port from the profile.          |
| acl | vlan <1-4094>                   | This command configures the VLAN for the profile.                            |
| acl | no vlan                         | This command removes the limitation of the VLAN from the profile.            |
| acl | source interface<br>PORT_ID     | This command configures the source interface for the profile.                |
| acl | no source interface<br>PORT_ID  | This command 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

➔ The command will filter 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

➔ The command will filter 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

### 7.2.2. Web Configurations

**Access Control List**

**Access Control List Settings**

|                         |  |                         |                                      |
|-------------------------|--|-------------------------|--------------------------------------|
| Profile Name            | <input type="text"/>                                     | Action                  | <input type="text" value="Disable"/> |
| Ethernet Type           | <input type="text" value="Any"/>                         | VLAN                    | <input type="text" value="Any"/>     |
| Source MAC              | <input type="text" value="Any"/>                         | Mask of Source MAC      | <input type="text"/>                 |
| Destination MAC         | <input type="text" value="Any"/>                         | Mask of Destination MAC | <input type="text"/>                 |
| Source IP               | <input type="text" value="Any"/>                         | Mask of Source IP       | <input type="text"/>                 |
| Destination IP          | <input type="text" value="Any"/>                         | Mask of Destination IP  | <input type="text"/>                 |
| Source Application      | <input type="text" value="Any"/>                         |                         |                                      |
| Destination Application | <input type="text" value="Any"/>                         |                         |                                      |
| Source Interface        | <input type="text" value="Any"/> -- <input type="text"/> |                         |                                      |

**Access Control List Status**

|                    |        |                         |      |
|--------------------|--------|-------------------------|------|
| Profile Name       | Justin | Action                  | Dorp |
| Ethernet Type      | 0x0011 | VLAN                    | 1    |
| Source MAC         | Any    | Mask of Source MAC      | None |
| Destination MAC    | Any    | Mask of Destination MAC | None |
| Source IP          | Any    | Mask of Source IP       | None |
| Destination IP     | Any    | Mask of Destination IP  | None |
| Source Application | Any    | Destination Application | Any  |
| Source Interface   | Any    |                         |      |

| Parameter | Description                               |
|-----------|---|
| IP Type   | Selects IPv4 / IPv6 type for the profile. |

|                         |  |
|-------------------------|--|
| Profile Name            | The access control profile name.   |
| Action                  | Selects <b>Disables/Drop/Permits</b> action for the profile.   |
| 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.<br>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 for the profile.   |
| Mask of Destination MAC | Configures the bitmap mask of the destination MAC of the packets for the profile.<br>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.<br>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.<br>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.     |
| IP Protocol             | Configures the IP protocol type. The setting will be used for Source Application and Destination Application.<br>TCP:0x06. UDP:0x11.   |
| 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 <b>Apply</b> to take effect the settings.                                   |
| Refresh             | Click <b>Refresh</b> to begin configuring this screen afresh.                     |

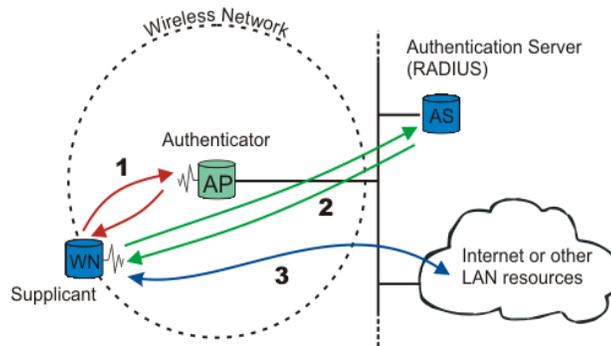
### 7.3. 802.1x

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 switch (authenticator) is enabled and set to the "**unauthorized**" state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is blocked at the network layer (Layer 3). The authenticator sends out the EAP-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 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password.



When the client provides the login credentials, the Switch 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 Switch, your Switch 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 switch 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 switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

### Port Parameters:

- **Admin Control Direction:**
  - both - 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 Switch 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 Switch 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.

### 7.3.1. Global Settings

#### 7.3.1.1. CLI Configurations

| Node      | Command   | Description   |
|-----------|---|---|
| enable    | show dot1x  | This command displays the current 802.1x configurations.                      |
| enable    | show dot1x username                                       | This command displays the current user accounts for the local authentication. |
| enable    | show dot1x accounting-record                              | This command displays the local accounting records.                           |
| enable    | configure terminal  | This command changes the node to configure node.                              |
| configure | dot1x authentication (disable enable)                     | This command enables/disables the 802.1x authentication on the switch.        |
| configure | dot1x authentic-method (local radius)                     | This command configures the authentic method of 802.1x.                       |
| configure | no dot1x authentic-method                                 | This command configures the authentic method of 802.1x to default.            |
| configure | dot1x accounting (disable enable)                         | This command <b>enables/disables</b> the dot1x local accounting records.      |
| configure | dot1x accounting-clean                                    | This command cleans all of the accounting records.                            |
| configure | dot1x default   | This command sets all of the configuration to default settings.               |
| configure | dot1x guest-vlan <1-4094>                                 | This command configures the guest vlan.                                       |
| configure | no dot1x guest-vlan                                       | This command removes the guest vlan.  |
| configure | dot1x radius primary-server-ip <IP> port PORTID           | This command configures the primary radius server.                            |
| configure | dot1x radius primary-server-ip <IP> port PORTID key KEY   | This command configures the primary radius server.                            |
| configure | no dot1x radius primary-server-ip                         | This command removes the secondary radius server.                             |
| configure | dot1x radius secondary-server-ip <IP> port PORTID         | This command configures the secondary radius server.                          |
| configure | dot1x radius secondary-server-ip <IP> port PORTID key KEY | This command configures the secondary radius server.                          |
| configure | no dot1x radius secondary-server-ip                       | This command removes the secondary radius server.                             |
| configure | dot1x username <USERNAME> <PASSWORD>                      | This command configures the user account for local authentication.            |

|           |                            |   |
|-----------|----------------------------|---|
| configure | no dot1x username <STRING> | This command deletes the user account for local authentication. |
|-----------|----------------------------|---|

### 7.3.1.2. Web Configurations

**802.1X**

| Configuration   | Port Settings   |
|---|---|
| <b>Global Settings</b>  |   |
| State   | Disable ▾   |
| Authentication Method   | Local ▾   |
| Guest VLAN  | 0   |
| Primary Radius Server   | IP : <input type="text"/> UDP Port : <input type="text"/> Shared Key : <input type="text"/> |
| Secondary Radius Server   | IP : <input type="text"/> UDP Port : <input type="text"/> Shared Key : <input type="text"/> |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> |   |
| <b>Global Status</b>  |   |
| State   | Disabled  |
| Authentication Method   | Local   |
| Guest VLAN  | 0   |
| Primary Radius Server   | IP : -      UDP Port : -      Shared Key : -  |
| Secondary Radius Server   | IP : -      UDP Port : -      Shared Key : -  |

| Parameter              | Description   |
|------------------------|---|
| <b>Global Settings</b> |   |
| State                  | Select <b>Enable</b> to permit 802.1x authentication on the Switch.<br>Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.  |
| Authentication Method  | Select whether to use <b>Local</b> or <b>RADIUS</b> as the authentication method.<br>The <b>Local</b> method of authentication uses the “guest” and “user” user groups of the user account database on the Switch itself to authenticate.<br>However, only a certain number of accounts can exist at one time.<br><b>RADIUS</b> 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.   |
| Primary Radius Server | When <b>RADIUS</b> is selected as the 802.1x authentication method, the <b>Primary Radius Server</b> 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 <b>1812</b> .   |
| Share Key             | Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch. |
| Second Radius Server  | This is the backup server used only when the <b>Primary Radius Server</b> is down.  |
| Apply                 | Click <b>Apply</b> to take effect the settings.   |
| Refresh               | Click <b>Refresh</b> to begin configuring this screen afresh.   |

## 7.3.2. Port Settings

### 7.3.2.1. CLI Configurations

| Node      | Command   | Description  |
|-----------|---|--|
| enable    | show dot1x  | This command displays the current 802.1x configurations.             |
| enable    | configure terminal  | This command changes the node to configure node.                     |
| configure | interface IFNAME  | This command enters the interface configure node.                    |
| interface | dot1x admin-control-direction (both in)                       | This command configures the control direction for blocking packets.  |
| interface | dot1x default   | This command sets the port configuration to default settings.        |
| interface | dot1x max-req <1-10>  | This command sets the max-req times for the port.                    |
| interface | dot1x port-control (auto force-authorized force-unauthorized) | This command configures the port control mode on the port.           |
| interface | dot1x authentication (disable enable)                         | This command enables/disables the 802.1x authentication on the port. |
| interface | dot1x reauthentication (disable enable)                       | This command enables/disables re-authentication on the port.         |
| interface | dot1x timeout quiet-period                                    | This command configures the quiet-period value on the port.          |
| interface | dot1x timeout server-timeout                                  | This command configures the server-timeout value on the port.        |
| interface | dot1x timeout reauth-period                                   | This command configures the reauth-period value on the port.         |
| interface | dot1x timeout supp-timeout                                    | This command configures the supp-timeout value on the port.          |
| interface | dot1x guest-vlan (disable enable)                             | This command disables / enables guest VLAN on the port.              |

### 7.3.2.2. Web Configurations

**802.1X**

Configuration
Port Settings

**Port Settings**

Port: From: 1 To: 1

802.1X State: Disable

| Admin Control Direction   | Reauthentication   | Port Control Mode   | Guest VLAN   | Max-req Times  |
|---|--|---|--|--|
| <span style="border: 1px solid #ccc; padding: 2px;">Both</span> | <span style="border: 1px solid #ccc; padding: 2px;">Disable</span> | <span style="border: 1px solid #ccc; padding: 2px;">Auto</span> | <span style="border: 1px solid #ccc; padding: 2px;">Disable</span> | <span style="border: 1px solid #ccc; padding: 2px;">2</span> |
| Reauth-period (sec)   | Quiet-period (sec)   | Supp-timeout (sec)  | Server-timeout (sec)   | Reset to Default   |
| <span style="border: 1px solid #ccc; padding: 2px;">3600</span> | <span style="border: 1px solid #ccc; padding: 2px;">20</span>      | <span style="border: 1px solid #ccc; padding: 2px;">30</span>   | <span style="border: 1px solid #ccc; padding: 2px;">16</span>      | <input type="checkbox"/>                                     |

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

Apply
Refresh

**Port Status**

| Port | 802.1X State | Admin Control Direction | Reauthentication | Port Control Mode | Guest VLAN | Max-req Times | Reauth-period | Quiet-period | Supp-timeout | Server-timeout |
|------|--------------|-------------------------|------------------|-------------------|------------|---------------|---------------|--------------|--------------|----------------|
| 1    | Disabled     | Both                    | Disabled         | Auto              | Disabled   | 2             | 3600          | 20           | 30           | 16             |
| 2    | Disabled     | Both                    | Disabled         | Auto              | Disabled   | 2             | 3600          | 20           | 30           | 16             |
| 3    | Disabled     | Both                    | Disabled         | Auto              | Disabled   | 2             | 3600          | 20           | 30           | 16             |
| 4    | Disabled     | Both                    | Disabled         | Auto              | Disabled   | 2             | 3600          | 20           | 30           | 16             |
| 5    | Disabled     | Both                    | Disabled         | Auto              | Disabled   | 2             | 3600          | 20           | 30           | 16             |
| 6    | Disabled     | Both                    | Disabled         | Auto              | Disabled   | 2             | 3600          | 20           | 30           | 16             |

| Parameter               | Description  |
|-------------------------|--|
| <b>Port Settings</b>    |  |
| Port                    | Select a port number to configure.   |
| 802.1x State            | Select <b>Enable</b> to permit 802.1x authentication on the port. You must first enable 802.1x authentication on the Switch before configuring it on each port.  |
| Admin Control Direction | Select <b>Both</b> to drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. Select <b>In</b> 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.  |
| Port Control Mode       | Select <b>Auto</b> to require authentication on the port. Select <b>Force Authorized</b> to always force this port to be authorized. Select <b>Force Unauthorized</b> to always force this port to be unauthorized. No packets can pass through this port. |

|                  |   |
|------------------|---|
| Guest VLAN       | Select <b>Disable</b> to disable Guest VLAN on the port.<br>Select <b>Enable</b> to enable Guest VLAN on the port.  |
| Max-req Time     | Specify the amount of times the Switch 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 Switch 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 Switch will wait before communicating with the server. The acceptable range for this field is 0 to 65535 seconds.  |
| Server timeout   | Specify how long the Switch to time out the Authentication Server. The acceptable range for this field is 0 to 65535 seconds.   |
| Reset to Default | Select this and click <b>Apply</b> to reset the custom 802.1x port authentication settings back to default.   |
| Apply            | Click <b>Apply</b> to take effect the settings.   |
| Refresh          | Click <b>Refresh</b> to begin configuring this screen afresh.   |

## 7.4. Port Security

The Switch will learn the MAC address of the device directly connected to a particular port and allow traffic through. Ask the question: “How do we control who and how many can connect to a switch port?” This is where port security can assist us. The Switch allow us to control which devices can connect to a switch port or how many of them can connect to it (such as when a hub or another switch is connected to the port).

Let’s say we have only one switch port left free and we need to connect five hosts to it. What can we do? 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 port of the Switch from disabled to enabled, all of the MAC learned by this port will be clear.*

### 7.4.1. CLI Configurations

| Node      | Command                                       | Description   |
|-----------|---|---|
| enable    | show port-security                            | This command displays the current port security configurations.                     |
| enable    | configure terminal                            | This command changes the node to configure node.                                    |
| configure | port-security (disable enable)                | This command enables / disables the global port security function.                  |
| configure | interface IFNAME                              | This command enters the interface configure node.                                   |
| interface | port-security (disable enable)                | This command enables / disables the port security function on the specific port.    |
| interface | port-security limit <1-1000>                  | This command configures the maximum MAC entries on the specific port.               |
| configure | interface range gigabitethernet1/0/ PORTLISTS | This command enters the if-range configure node.                                    |
| if-range  | port-security (disable enable)                | This command enables / disables the port security function for the specified ports. |
| if-range  | port-security limit <1-1000>                  | This command configures the maximum MAC entries for the specified ports.            |

## 7.4.2. Web Configurations

**Port Security**

**Port Security Settings**

Port Security Disable ▾

| Port  | State   | Maximum MAC  |
|---|---|--|
| From: <span style="border: 1px solid black; padding: 2px;">1 ▾</span> To: <span style="border: 1px solid black; padding: 2px;">1 ▾</span> | <span style="border: 1px solid black; padding: 2px;">Disable ▾</span> | <input style="width: 80px;" type="text" value="5"/> (1~1000) |

Apply
Refresh

**Port Security Status**

| Port | State   | Maximum MAC | Port | State   | Maximum MAC |
|------|---------|-------------|------|---------|-------------|
| 1    | Disable | 5           | 2    | Disable | 5           |
| 3    | Disable | 5           | 4    | Disable | 5           |
| 5    | Disable | 5           | 6    | Disable | 5           |

| Parameter                     | Description   |
|-------------------------------|---|
| <b>Port Security Settings</b> |   |
| Port Security                 | Select <b>Enable/Disable</b> to permit Port Security on the Switch.                           |
| Port                          | Select a port number to configure.  |
| State                         | Select <b>Enable/Disable</b> 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 <b>Apply</b> to take effect the settings.   |
| Refresh                       | Click <b>Refresh</b> to begin configuring this screen afresh.                                 |

## 8. Monitor

### 8.1. Alarm

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

**Notice:** The Alarm DIP switch allow users to configure if send alarm message when the corresponding event occurs.

#### For Example:

P1: ON, The Switch will send alarm message when port 1 is link down.

PWR: ON, The Switch will send alarm message when the main power supply disconnect.

RPS: ON, The Switch will send alarm message when the redundant power supply disconnect.

#### 8.1.1. CLI Configurations

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

#### 8.1.2. Web Configurations

**Alarm**

**Alarm Information**

|                        |           |
|------------------------|-----------|
| <b>Alarm Status</b>    | No Alarm. |
| <b>Alarm Reason(s)</b> |           |

**DIP switch Settings**

|                   |               |                   |               |
|-------------------|---------------|-------------------|---------------|
| <b>DIP switch</b> | <b>Status</b> | <b>DIP switch</b> | <b>Status</b> |
| PWR               | Disable       | RPS               | Disable       |

| Parameter                        | Description   |
|----------------------------------|---|
| <b>Alarm Information</b>         |   |
| Alarm Status                     | This field indicates if there is any alarm events.  |
| Alarm Reason(s)                  | This field displays all of the detail alarm events. |
| <b>Alarm DIP Switch Settings</b> |   |
| DIP Switch                       | The field displays the DIP Switch name.             |
| Status                           | The field indicates the DIP Switch current status.  |

## 8.2. Port Statistics

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

### 8.2.1. CLI Configurations

| Node   | Command              | Description  |
|--------|----------------------|--|
| enable | show port-statistics | This command displays the link up ports' statistics. |

### 8.2.2. Web Configurations

| Port Statistics |                |               |                 |                |                  |                 |                |               |
|-----------------|----------------|---------------|-----------------|----------------|------------------|-----------------|----------------|---------------|
| Port Statistics |                |               |                 |                |                  |                 |                |               |
| Port            | Transmit Drops | Receive Drops | Transmit Errors | Receive Errors | Transmit Packets | Receive Packets | Transmit Bytes | Receive Bytes |
| 4               | 0              | 0             | 0               | 0              | 482              | 250             | 63744          | 46402         |

| Parameter  | Description  |
|------------|--|
| Port       | Select a port or a range of ports to display their statistics. |
| Rx Packets | The field displays the received packet count.                  |
| Tx Packets | The field displays the transmitted packet count.               |
| Rx Bytes   | The field displays the received byte count.                    |
| Tx Bytes   | The field displays the transmitted byte count.                 |
| Rx Errors  | The field displays the received error count.                   |
| Tx Errors  | The field displays the transmitted error count.                |
| Rx Drops   | The field displays the received drop count.                    |
| Tx Drops   | The field displays the transmitted drop count.                 |
| Refresh    | Click this button to refresh the screen quickly.               |

### 8.3. Port Utilization

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

#### 8.3.1. CLI Configurations

| Node   | Command                               | Description   |
|--------|---------------------------------------|---|
| enable | show port-utilization (bps Kbps Mbps) | This command displays the link up ports' traffic utilization. |

#### 8.3.2. Web Configurations

**Port Utilization**

Port Utilization

Unit

| Port | Speed | Rx Utilization (%) | Rx Utilization (bps) | Tx Utilization (%) | Tx Utilization (bps) |
|------|-------|--------------------|----------------------|--------------------|----------------------|
| 6    | 1000  | 0.00               | 3266                 | 0.00               | 0                    |

| Parameter               | Description   |
|-------------------------|---|
| <b>Port Utilization</b> |   |
| Unit                    | Select a unit for displaying the port utilization.                  |
| Port                    | Select a port or a range of ports to display their RMON statistics. |
| Speed                   | The current port speed.   |
| Rx Utilization (%)      | The port receiving traffic utilization in percentage.               |
| Rx Utilization (bps)    | The port receiving traffic utilization in bits per second.          |
| Tx Utilization (%)      | The port transmitting traffic utilization in percentage.            |
| Tx Utilization (bps)    | The port transmitting traffic utilization in bits per second.       |
| Apply                   | Click <b>Apply</b> to take effect the settings.                     |
| Refresh                 | Click <b>Refresh</b> to begin configuring this screen afresh.       |

## 8.4. RMON Statistics

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

### 8.4.1. CLI Configurations

| Node      | Command                        | Description   |
|-----------|--------------------------------|---|
| enable    | show rmon statistics           | This command displays the RMON statistics.                    |
| enable    | configure terminal             | This command changes the node to configure node.              |
| configure | clear rmon statistics [IFNAME] | This command clears one port's or all ports' RMON statistics. |

### 8.4.2. Web Configurations

**RMON Statistics**

RMON Statistics

Port

| Port 4 ( Active )                      |                   |         |                      |
|--|-------------------|---------|----------------------|
| Inbound                                | Total Octets      | 1787175 |                      |
|  | BroadcastPkts     | 1605    | UnicastPkts 1342     |
|  | Non-unicastPkts   | 5664    | MulticastPkts 4059   |
|  | FragmentsPkts     | 0       | UndersizePkts 0      |
|  | OversizePkts      | 0       | DiscardsPkts 0       |
|  | ErrorPkts         | 0       | UnknownProtos 0      |
|  | AlignError        | 0       | CRCAAlignErrors 0    |
|  | Jabbers           | 0       | DropEvents 0         |
| Outbound                               | Total Octets      | 306298  |                      |
|  | BroadcastPkts     | 5       | UnicastPkts 478      |
|  | Non-unicastPkts   | 357     | Collisions 0         |
|  | LateCollision     | 0       | SingleCollision 0    |
|  | MultipleCollision | 0       | DiscardsPkts 0       |
|  | ErrorPkts         | 0       |                      |
| # of packets received with a length of | 64 Octets         | 3033    | 65to127 Octets 1468  |
|  | 128to255 Octets   | 1058    | 256to511 Octets 563  |
|  | 512to1023 Octets  | 1582    | 1024toMax Octets 137 |

| Parameter | Description   |
|-----------|---|
| Port      | Select a port or a range of ports to display their RMON statistics. |
| Show      | Show them.  |
| Clear     | Clear the RMON statistics for the port or a range of ports.         |

## 8.5. 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.

### 8.5.1. CLI Configurations

| Node   | Command                    | Description                                |
|--------|----------------------------|--|
| enable | show sfp info port PORT_ID | This command displays the SFP information. |
| enable | show sfp ddmi port PORT_ID | This command displays the SFP DDMI status. |

### 8.5.2. Web Configurations

**SFP Information**

**SFP Information**

Port

| SFP Information   |     |
|-------------------|-----|
| Fiber Cable       | N/A |
| Connector         | N/A |
| Wavelength(nm)    | N/A |
| Transfer Distance | N/A |
| DDM Supported     | N/A |
| Vendor Name       | N/A |
| Vendor PN         | N/A |
| Vendor rev        | N/A |
| Vendor SN         | N/A |
| Date code         | N/A |

| Parameter              | Description  |
|------------------------|--|
| <b>SFP Information</b> |  |
| Port                   | Select a port number to configure.                 |
| Apply                  | Click <b>Apply</b> to display the SFP information. |
| <b>SFP Information</b> |  |
| 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.        |

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

## 8.6. Traffic Monitor

The function can be enabled / disabled on a specific port or globally be enabled disabled on the Switch. 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.

### 8.6.1. CLI Configurations

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show traffic-monitor   | This command displays the traffic monitor configurations and current status.   |
| enable    | configure terminal   | This command changes the node to configure node.   |
| configure | traffic-monitor (disable enable)                               | This command enables / disables the traffic monitor on the Switch.   |
| configure | interface IFNAME   | This command enters the interface configure node.  |
| interface | traffic-monitor (disable enable)                               | This command enables / disables the traffic monitor on the port.   |
| interface | traffic-monitor rate RATE_LIMIT type (bcast mcast bcast+mcast) | This command configures the packet rate and packet type for the traffic monitor on the port.<br><b>bcast</b> – Broadcast packets.<br><b>mcast</b> – Multicast packets.<br><b>bcast+ mcast</b> - Broadcast packets and Multicast packets. |
| interface | traffic-monitor recovery (disable enable)                      | This command enables / disables the recovery function for the traffic monitor on the port.   |
| interface | traffic-monitor recovery time <1-60>                           | This command configures the recovery time for the traffic monitor on the port.   |
| interface | traffic-monitor quarantine times <1-20>                        | This command configures the quarantine times for the traffic monitor on the port.  |

|           |  |  |
|-----------|--|--|
| configure | interface range<br>gigabitethernet1/0/<br>PORTLISTS                        | This command enters the if-range configure node.   |
| if-range  | traffic-monitor<br>(disable enable)  | This command enables / disables the traffic monitor on the port.   |
| if-range  | traffic-monitor<br>rateRATE_LIMIT<br>type<br>(bcast mcast bcast+mc<br>ast) | This command configures the packet rate and packet type for the traffic monitor on the port.<br><b>bcast</b> – Broadcast packets.<br><b>mcast</b> – Multicast packets.<br><b>bcast+ mcast</b> - Broadcast packets and Multicast packets. |
| if-range  | traffic-monitor<br>recovery<br>(disable enable)                            | This command enables / disables the recovery function for the traffic monitor on the port.   |
| if-range  | traffic-monitor<br>recovery time <1-60>                                    | This command configures the recovery time for the traffic monitor on the port.   |
| if-range  | traffic-monitor<br>quarantine times<br><1-20>                              | This command configures the quarantine times for the traffic monitor on the port.  |

## 8.6.2. Web Configurations

**Traffic Monitor**

**Traffic Monitor Settings**

State Disable ▾

| Port  | State   | Packet Type   | Packet Rate (pps)                                     | Recovery State   | Recovery Time(min)                                  | Quarantine Times                                    |
|---|---|---|---|--|---|---|
| From: <span style="border: 1px solid black; padding: 2px;">1 ▾</span> To: <span style="border: 1px solid black; padding: 2px;">1 ▾</span> | <span style="border: 1px solid black; padding: 2px;">Disable ▾</span> | <span style="border: 1px solid black; padding: 2px;">Broadcast ▾</span> | <input style="width: 50px;" type="text" value="100"/> | <span style="border: 1px solid black; padding: 2px;">Enable ▾</span> | <input style="width: 50px;" type="text" value="1"/> | <input style="width: 50px;" type="text" value="3"/> |

Apply Refresh

| Port  | Manual Recovery  |
|---|--|
| From: <span style="border: 1px solid black; padding: 2px;">1 ▾</span> To: <span style="border: 1px solid black; padding: 2px;">1 ▾</span> | <span style="border: 1px solid black; padding: 2px;">None ▾</span> |

Apply

**Traffic Monitor Status**

| Port | State    | Status | Packet Type | Packet Rate(pps) | Recovery State | Recovery Time(min) | Quarantine Times |
|------|----------|--------|-------------|------------------|----------------|--------------------|------------------|
| 1    | Disabled | Normal | Broadcast   | 100              | Enabled        | 1                  | 3                |
| 2    | Disabled | Normal | Broadcast   | 100              | Enabled        | 1                  | 3                |
| 3    | Disabled | Normal | Broadcast   | 100              | Enabled        | 1                  | 3                |
| 4    | Disabled | Normal | Broadcast   | 100              | Enabled        | 1                  | 3                |
| 5    | Disabled | Normal | Broadcast   | 100              | Enabled        | 1                  | 3                |
| 6    | Disabled | Normal | Broadcast   | 100              | Enabled        | 1                  | 3                |

| Parameter                       | Description   |
|---------------------------------|---|
| <b>Traffic Monitor Settings</b> |   |
| 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). |
| Quarantine Times                | Configures the quarantine times for the traffic monitor on these ports. (Range: 1 – 20 times).        |
| Apply                           | Click <b>Apply</b> to take effect the settings.   |
| Refresh                         | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| Manual Recovery                 | Select <b>Unblock</b> to enable these ports blocked by traffic monitor.                               |
| Apply                           | Click <b>Apply</b> to take effect the settings.   |

## 9. Management

### 9.1. 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 and Number of Mask Bit:

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 192.168.1.102/24, 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 Switch.

#### 9.1.1. SNMP

##### 9.1.1.1. SNMP Settings

##### 9.1.1.1.1. CLI Configurations

| Node   | Command   | Description                                    |
|--------|-----------|--|
| enable | show snmp | This command displays the SNMP configurations. |

|           |                                   |   |
|-----------|-----------------------------------|---|
| enable    | configure terminal                | This command changes the node to configure node.  |
| configure | snmp (disable enable)             | This command disables/enables the SNMP on the switch.                                     |
| configure | snmp system-contact<br>STRING     | This command configures contact information for the system.                               |
| configure | snmp system-location<br>STRING    | This command configures the location information for the system.                          |
| configure | snmp system-name<br>STRING        | This command configures a name for the system. (The System Name is same as the host name) |
| configure | no snmp system-contact<br>STRING  | This command resets the contact information for the system.                               |
| configure | no snmp system-location<br>STRING | This command resets the location information for the system.                              |
| configure | no snmp system-name<br>STRING     | This command resets the system name for the system.                                       |

**Example:**

```
L2SWITCH#configure terminal
L2SWITCH(config)#snmp enable
L2SWITCH(config)#snmp system-contact IT engineer
L2SWITCH(config)#snmp system-location Branch-Office
```

### 9.1.1.1.2. Web Configurations

**SNMP**

SNMP SettingsCommunity Name

**SNMP Settings**

|                 |                                       |
|-----------------|---------------------------------------|
| SNMP State      | <input type="text" value="Disable"/>  |
| System Name     | <input type="text" value="L2SWITCH"/> |
| System Location | <input type="text"/>                  |
| System Contact  | <input type="text"/>                  |

| Parameter            | Description  |
|----------------------|--|
| <b>SNMP Settings</b> |  |
| SNMP State           | Select <b>Enable</b> to activate SNMP on the Switch.<br>Select <b>Disable</b> to not use SNMP on the Switch. |
| System Name          | Type a System Name for the Switch.<br>(The System Name is same as the host name).                            |
| System Location      | Type a System Location for the Switch.   |
| System Contact       | Type a System Contact for the Switch.  |
| Apply                | Click <b>Apply</b> to take effect the settings.  |
| Refresh              | Click <b>Refresh</b> to begin configuring this screen afresh.  |

### 9.1.1.2. Community Name

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

Network ID of Trusted Host:

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

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 Switch.

#### 9.1.1.2.1. CLI Configurations

| Node      | Command   | Description                                      |
|-----------|---|--|
| enable    | show snmp   | This command displays the SNMP configurations.   |
| enable    | configure terminal                                      | This command changes the node to configure node. |
| configure | snmp community<br>STRING (ro rw)<br>trusted-host IPADDR | This command configures the SNMP community name. |

#### Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#snmp community public rw trusted-host 192.168.200.106/24
```

## 9.1.1.2.2. Web Configurations

**SNMP**

SNMP Settings
Community Name

Community Name Settings

| Community String     | Rights      | IP Version | Network ID of Trusted Host | Number of Mask Bit   |
|----------------------|-------------|------------|----------------------------|----------------------|
| <input type="text"/> | Read-Only ▾ | IPv4 ▾     | <input type="text"/>       | <input type="text"/> |

Community Name List

| No.               | Community String | Rights    | IP Version | Network ID of Trusted Host | Number of Mask Bit | Action                                |
|-------------------|------------------|-----------|------------|----------------------------|--------------------|---------------------------------------|
| <a href="#">1</a> | 111              | Read-Only | IPv4       | 192.168.202.0              | 24                 | <input type="button" value="Delete"/> |
| <a href="#">2</a> | 666              | Read-Only | IPv6       | 2100::                     | 64                 | <input type="button" value="Delete"/> |

| Parameter                      | Description  |
|--------------------------------|--|
| <b>Community Name Settings</b> |  |
| Community String               | Enter a Community string, this will act as a password for requests from the management station.<br>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 Switch.<br>Select Read-Write to allow the SNMP manager using this string to create or edit MIBs (configure settings on the Switch).   |
| IP Version                     | Selects the IP type, IPv4 or IPv6.   |
| 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.   |
| Number of Mask Bit             | Type the number of Mask Bit for the IP address of the remote SNMP.   |
| Apply                          | Click <b>Apply</b> to take effect the settings.  |
| Refresh                        | Click <b>Refresh</b> to begin configuring this screen afresh.  |
| <b>Community Name List</b>     |  |

|                            |   |
|----------------------------|---|
| No.                        | This field indicates the community number. It is used for identification only. Click on the individual community number to edit the community settings. |
| Community String           | This field displays the SNMP community string. An SNMP community string is a text string that acts as a password.                                       |
| Right                      | This field displays the community string's rights. This will be <b>Read Only</b> or <b>Read Write</b> .   |
| IP Version                 | This field displays the IP type.  |
| Network ID of Trusted Host | This field displays the IP address of the remote SNMP management station after it has been modified by the subnet mask.                                 |
| Number of Mask Bit         | This field displays the number of Mask Bit for the IP address of the remote SNMP management station.  |
| Action                     | Click <b>Delete</b> to remove a specific Community String.  |

## 9.1.2. SNMP Trap

### 9.1.2.1. Receiver Settings

#### 9.1.2.1.1. CLI Configurations

| Node      | Command   | Description   |
|-----------|---|---|
| enable    | show snmp   | This command displays the SNMP configurations.  |
| enable    | configure terminal                                | This command changes the node to configure node.  |
| configure | snmp trap-receiver IPADDR (v1 v2c) COMMUNITY      | This command 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 | This command configures the trap IPv6 receiver's configurations, including the IP address, version (v1 or v2c) and community. |

#### Example:

```
L2SWITCH#configure terminal
```

```
L2SWITCH(config)#snmp trap-receiver 192.168.200.106 v2c public
```

#### 9.1.2.1.2. Web Configurations

**SNMP Trap**

Trap Receiver
Trap Event
Port Trap Event

**Trap Receiver Settings**

| IP Version | IP Address           | Version | Community String     |
|------------|----------------------|---------|----------------------|
| IPv4 ▾     | <input type="text"/> | v1 ▾    | <input type="text"/> |

**Trap Receiver List**

| No.               | IP Version | IP Address      | Version | Community String | Action                                |
|-------------------|------------|-----------------|---------|------------------|---------------------------------------|
| <a href="#">1</a> | IPv4       | 192.168.202.154 | v1      | public           | <input type="button" value="Delete"/> |

| Parameter                     | Description   |
|-------------------------------|---|
| <b>Trap Receiver Settings</b> |   |
| IP Version                    | Selects the IP version, IPv4 or IPv6.                                       |
| 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. <b>v1</b> or <b>v2c</b> .          |
| Community String          | Specify the community string used with this remote trap station.  |
| Apply                     | Click <b>Apply</b> to take effect the settings.   |
| Refresh                   | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>Trap Receiver List</b> |   |
| No.                       | This field displays the index number of the trap receiver entry. Click the number to modify the entry.  |
| IP Version                | This field displays the IP address version.   |
| IP Address                | This field displays the IP address of the remote trap station.  |
| Version                   | This field displays the version of Simple Network Management Protocol in use. <b>v1</b> or <b>v2c</b> . |
| Community String          | This field displays the community string used with this remote trap station.                            |
| Action                    | Click <b>Delete</b> to remove a configured trap receiver station.                                       |

### 9.1.2.2. Event Settings

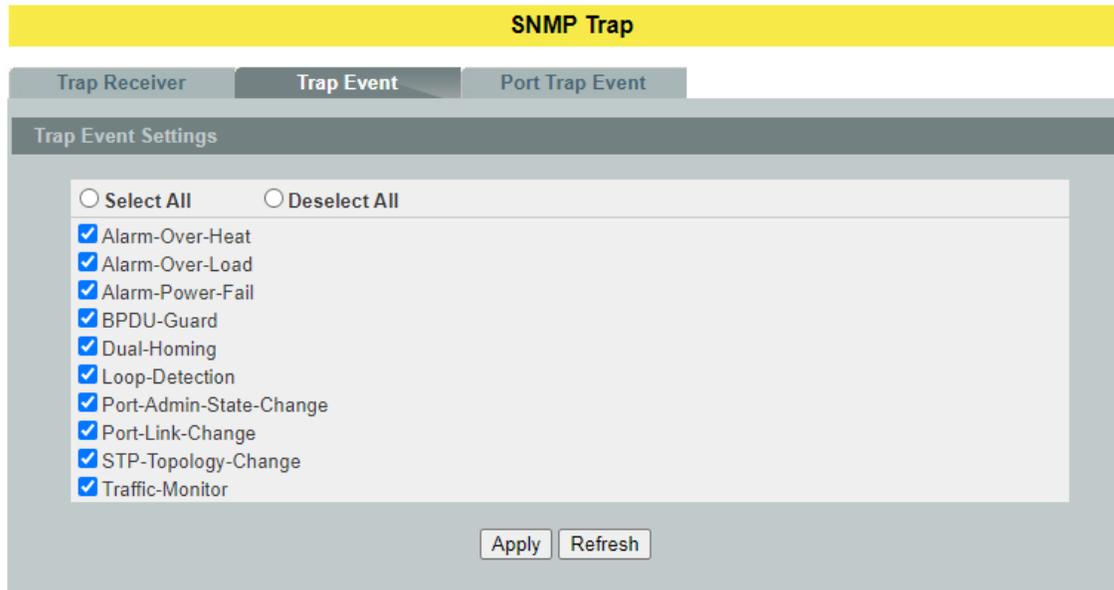
The features allow users to enable/disable individual trap notification.

|                         |  |
|-------------------------|--|
| 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. |
| bpd                     | - Trap when port is blocked by BPDU Guard/BPDU 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.<br>(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.  |

### 9.1.2.2.1. CLI Configurations

| Node      | Command  | Description   |
|-----------|--|---|
| enable    | show snmp trap-event                                     | This command displays the SNMP configurations.  |
| enable    | configure terminal                                       | This command changes the node to configure node.  |
| configure | snmp trap-event alarm-over-heat (disable/enable)         | This command enables/disables the alarm-over-heat trap.                                   |
| configure | snmp trap-event alarm-over-load (disable/enable)         | This command enables/disables the alarm-over-load trap.                                   |
| configure | snmp trap-event alarm-power-fail (enable/enable)         | This command enables/disables the alarm-power-fail trap.                                  |
| configure | snmp trap-event bpdu (disable/enable)                    | This command enables/disables the BPDU port state change/BPDU Root Guard/BPDU Guard trap. |
| configure | snmp trap-event dual-homing (disable/enable)             | This command enables/disables the dual-homing trap.                                       |
| configure | snmp trap-event dying-gasp (disable/enable)              | This command enables/disables the dying-gasp trap.  |
| configure | snmp trap-event loop-detection (disable/enable)          | This command enables/disables the loop-detection trap.                                    |
| configure | snmp trap-event pd-alive (disable/enable)                | This command enables/disables the pd-alive trap.  |
| configure | snmp trap-event port-admin-state-change (disable/enable) | This command enables/disables the port-admin-state-change trap.                           |
| configure | snmp trap-event port-link-change (disable/enable)        | This command enables/disables the port-link-change trap.                                  |
| configure | snmp trap-event power-source-change (disable/enable)     | This command enables/disables the power-source-change trap.                               |
| configure | snmp trap-event stp-topology-change (disable/enable)     | This command enables/disables the stp-topology-change trap.                               |
| configure | snmp trap-event traffic-monitor (disable/enable)         | This command enables/disables the traffic-monitor trap.                                   |
| configure | snmp trap-event xpress-ring (disable/enable)             | This command enables/disables the xpress-ring trap.                                       |

### 9.1.2.2.2. Web Configurations



| Parameter                        | Description   |
|----------------------------------|---|
| <b>Trap Event State Settings</b> |   |
| Select all                       | Enables all of trap events.                                   |
| Deselect All                     | Disables all os trap events.                                  |
| Apply                            | Click <b>Apply</b> to take effect the settings.               |
| Refresh                          | Click <b>Refresh</b> to begin configuring this screen afresh. |

### 9.1.2.3. Port Event Settings

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

#### 9.1.2.3.1. CLI Configurations

| Node      | Command                         | Description  |
|-----------|---------------------------------|--|
| enable    | show snmp port-link-change-trap | This command displays the SNMP port link-change trap configurations. |
| enable    | configure terminal              | This command changes the node to configure node.                     |
| configure | interface IFNAME                | This command enters the interface configure node.                    |
| interface | snmp port-link-change-trap      | This command enables the link change trap on the specific port.      |

|           |   |   |
|-----------|---|---|
| interface | no snmp port-link-change-trap                   | This command disables the link change trap on the specific port.  |
| configure | interface range<br>gigabitethernet1/0/PORTLISTS | This command enters the if-range configure node.                  |
| if-range  | snmp port-link-change-trap                      | This command enables the link change trap on the specific ports.  |
| if-range  | no snmp port-link-change-trap                   | This command disables the link change trap on the specific ports. |

### 9.1.2.3.2. Web Configurations

**SNMP Trap**

Trap Receiver
Trap Event
Port Trap Event

**Port Link-Change Trap Settings**

| Port  | State                               |
|---|-------------------------------------|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="Enable"/> |

**Port Link-Change Trap Status**

| Port | State   | Port | State   |
|------|---------|------|---------|
| 1    | Enabled | 2    | Enabled |
| 3    | Enabled | 4    | Enabled |
| 5    | Enabled | 6    | Enabled |

| Parameter                             | Description  |
|---------------------------------------|--|
| <b>Port Link-Change Trap Settings</b> |  |
| Port                                  | Selects a port or a range of ports to configure the port event trap. |
| State                                 | Enables / Disable the port link change trap.                         |
| <b>Port Link-Change Trap Status</b>   |  |
| Port                                  | The port ID.   |
| State                                 | The state of the port.   |

### 9.1.3. SNMPv3

#### 9.1.3.1. SNMPv3 Group

##### 9.1.3.1.1. CLI Configurations

| Node      | Command   | Description   |
|-----------|---|---|
| enable    | show snmp group   | This command displays all snmp v3 groups.             |
| enable    | configure terminal  | This command changes the node to configure node.      |
| 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   | This command removes a v3 group from switch.          |

##### 9.1.3.1.2. Web Configurations

**SNMPv3**

Group Settings
User Settings
View Settings

**Group Settings**

Group Name

Security Level noauth ▼

Read View

Write View

Notify View

**Group Status**

| Group Name | Security Model | Security Level | Read View | Write View | Notify View | Action |
|------------|----------------|----------------|-----------|------------|-------------|--------|
| Empty!     |                |                |           |            |             |        |

| Parameter  | Description             |
|------------|-------------------------|
| Group Name | Enter the v3 user name. |

|                            |   |
|----------------------------|---|
| Security Level             | Select the security level of the v3 group to use.   |
| Read View                  | Note that if a group is defined without a read view than all objects are available to read. (default value is <b>none</b> .)                                      |
| 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 <b>none</b> .) |
| Notify View                | By using a notify view, a group determines the list of notifications its users can receive. (default value is <b>none</b> .)                                      |
| Apply                      | Click <b>Apply</b> to take effect the settings.   |
| Refresh                    | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>SNMPv3 Group Status</b> |   |
| Group Name                 | This field displays the v3 user name.   |
| Security Model             | This field displays the security model of the group.<br>Always displayed <b>v3: User-based Security Model (USM)</b>   |
| Security Level             | This field displays the security level to this group.   |
| Read View                  | These fields display the View list of this group.   |
| Write View                 |   |
| Notify View                |   |
| Action                     | Click <b>Delete</b> to remove a v3 group.   |

### 9.1.3.2. SNMPv3 User

#### 9.1.3.2.1. CLI Configurations

| Node      | Command  | Description   |
|-----------|--|---|
| enable    | configure terminal   | This command changes the node to configure node.        |
| configure | snmp user USERNAME<br>GROUPNAME noauth                                   | Configures v3 user of non-authentication.               |
| configure | snmp user USERNAME<br>GROUPNAME auth<br>(MD5 SHA) STRINGS                | Configures v3 user of authentication.                   |
| configure | snmp user USERNAME<br>GROUPNAME priv<br>(MD5 SHA) STRINGS des<br>STRINGS | Configures v3 user osnmf authentication and encryption. |
| configure | no snmp user USERNAME<br>GROUPNAME                                       | This command removes a v3 user from switch.             |

### 9.1.3.2.2. Web Configurations

**SNMPv3**

Group Settings
User Settings
View Settings

**User Settings**

Username

Group Name

Security Levelnoauth ▾

Auth AlgorithmMD5 ▾

Auth Password

Priv AlgorithmDES ▾

Priv Password

**User Status**

| Username | Group Name | Auth Protocol | Priv Protocol | Rowstatus | Action |
|----------|------------|---------------|---------------|-----------|--------|
| Empty!   |            |               |               |           |        |

| 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.<br><b>noauth</b> means no authentication and no encryption.<br><b>auth</b> means messages are authenticated but not encrypted.<br><b>priv</b> means messages are authenticated and encrypted. |
| Auth Algorithm            | Select <b>MD5</b> or <b>SHA</b> Algorithm when security level is <b>auth</b> or <b>priv</b> .  |
| Auth Password             | Set the password for this user when security level is <b>auth</b> or <b>priv</b> . (pass phrases must be at least 8 characters long!)  |
| Priv Algorithm            | Select <b>DES</b> encryption when security level is <b>priv</b> .  |
| Priv Password             | Set the password for this user when security level is <b>priv</b> . (pass phrases must be at least 8 characters long!)   |
| Apply                     | Click <b>Apply</b> to take effect the settings.  |
| Refresh                   | Click <b>Refresh</b> to begin configuring this screen afresh.  |
| <b>SNMPv3 User Status</b> |  |

|               |   |
|---------------|---|
| User Name     | This field displays the v3 user name.                         |
| Group Name    | This field displays the group name which the v3 user mapping. |
| Auth Protocol | These fields display the security level to this v3 user.      |
| Priv Protocol |   |
| Rowstatus     | This field displays the v3 user rowstatus.                    |
| Action        | Click <b>Delete</b> to remove a v3 user.                      |

### 9.1.3.3. SNMPv3 View

#### 9.1.3.3.1. CLI Configurations

| Node      | Command  | Description                                      |
|-----------|--|--|
| enable    | show snmp view                                 | This command displays all snmp v3 view.          |
| enable    | configure terminal                             | This command changes the node to configure node. |
| configure | snmp view VIEWNAME STRINGS (included excluded) | To identify the subtree.                         |
| configure | no snmp view VIEWNAME STRINGS                  | This command removes a v3 view from switch.      |

#### 9.1.3.3.2. Web Configurations

**SNMPv3**

Group Settings
User Settings
View Settings

**View Settings**

View Name

View Subtree

View Type included ▼

**View Status**

| View Name | View Subtree | View Type | Action |
|-----------|--------------|-----------|--------|
| Empty!    |              |           |        |

| Parameter | Description  |
|-----------|--|
| 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 <b>included</b> or <b>excluded</b> to define subtree adding to the view or not. |
| Apply                     | Click <b>Apply</b> to take effect the settings.  |
| Refresh                   | Click <b>Refresh</b> to begin configuring this screen afresh.                          |
| <b>SNMPv3 View Status</b> |  |
| View Name                 | This field displays the v3 view name.  |
| View Subtree              | This field displays the subtree.   |
| View Type                 | This field displays the subtree adding to the view or not.                             |
| Action                    | Click <b>Delete</b> to remove a v3 view.   |

## 9.2. 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 Switch will download 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: ***9015-8GT2GS\_Autoprovision.txt***

The contents of the file are listed below:

```
AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version=9015-000-1.1.0.S0
Firmware_Image_File=9015-000-1.1.0.S0.fw
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File=9015-000-1.1.0.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 “INS-8648P\_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 switch; otherwise, wait 24 hours and go back to step 1.

### 9.2.1. CLI Configurations

| Node           | Command  | Description  |
|----------------|--|--|
| enable         | show auto-provision                            | This command displays the current auto provision configurations.         |
| configure      | auto-provision                                 | This command enters the auto-provision node.                             |
| auto-provision | show   | This command displays the current auto provision configurations.         |
| auto-provision | active (enable disable)                        | This command enables/disables the auto provision function.               |
| auto-provision | server-addressIPADDR                           | This command configures the auto provision server's IP.                  |
| auto-provision | protocol (tftp http ftp)                       | The command configurations the upgrade protocol.                         |
| auto-provision | FTP-user username<br>STRING password<br>STRING | The command configurations the username and password for the FTP server. |
| auto-provision | folder STRING                                  | The command configurations the folder for the auto provision server.     |
| auto-provision | no folder                                      | The command configurations the folder to default.                        |
| auto-provision | no FTP-user                                    | The command configurations the username and password to default.         |

## 9.2.2. Web Configurations

**Auto Provision**

**Auto Provision Settings**

|             |                                      |
|-------------|--------------------------------------|
| State       | <input type="text" value="Disable"/> |
| Status      | Disabled                             |
| Version     | 0                                    |
| Protocol    | <input type="text" value="TFTP"/>    |
| Server IP   | <input type="text" value="IPv4"/>    |
|             | <input type="text" value="0.0.0.0"/> |
| User Name   | <input type="text"/>                 |
| Password    | <input type="text"/>                 |
| Folder Path | <input type="text"/>                 |

| Parameter                      | Description  |
|--------------------------------|--|
| <b>Auto Provision Settings</b> |  |
| State                          | The field enables / disables the auto provision function.        |
| Status                         | The field displays the state machine status of auto provision.   |
| Version                        | The field displays the auto provision version of current system. |
| Protocol                       | The field configures the protocol for file transfer.             |
| Server IP                      | The field configures the IP format.                              |
|                                | The field configures the IP address of IPv4 or IPv6.             |
| User Name                      | FTP user name.   |
| Password                       | FTP password.  |
| Folder Path                    | Configurations the folder for the auto provision server.         |
| Apply                          | Click <b>Apply</b> to take effect the settings.                  |
| Refresh                        | Click <b>Refresh</b> to begin configuring this screen afresh.    |

## 9.3. Mail Alarm

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

- Alarm : The hardware monitor alarm.

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

### ● Reference

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

### 9.3.1. CLI Configurations

| Node   | Command            | Description  |
|--------|--------------------|--|
| enable | show mail-alarm    | This command displays the Mail Alarm configurations. |
| enable | configure terminal | This command changes the node to configure node.     |

|           |   |  |
|-----------|---|--|
| configure | mail-alarm (disable enable)   | This command disables / enables the Mail Alarm function.   |
| configure | mail-alarm auth-account   | This command configures the Mail server authentication account.  |
| configure | mail-alarm mail-from  | This command configures the mail sender.   |
| configure | mail-alarm mail-to  | This command configures the mail receiver.   |
| configure | mail-alarm server (ip domain-name) STRINGS server-port VALUE  | This command configures the mail server IP address / domain name and the TCP port.                           |
| configure | mail-alarm server (ip domain-name) STRINGS server-port default  | This command 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) | This command disables / enables mail trap events.  |
| configure | mail-alarm utf8-encoding (disable enable)   | This command disables / enables the UTF8 encoding for mail content.  |

### 9.3.2. Web Configurations

**Mail Alarm**

**Mail Alarm Settings**

State:

Server:   Server Port:  (Default:25)

Account Name:  Account Password:

Mail From:

Mail To:

UTF-8 Encoding:

Mail Event State:

Select All     Deselect All

- Alarm
- Configuration Change
- Firmware Upgrade
- Port Blocked
- Port Link Change
- System Reboot
- User Login

| Parameter                  | Description   |
|----------------------------|---|
| <b>Mail Alarm Settings</b> |   |
| State                      | Enable / disable the Mail Alarm function.   |
| Server                     | Selects one of below options:<br>IP: The mail server's IP format is IPv4.<br>Domain Name: The mail server's IP format is a domain name. |
| Server Port                | Specifies the TCP port for the SMTP.  |
| 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 function.   |
| Trap State                 | Enables / disables the mail trap event states.  |
| Apply                      | Click <b>Apply</b> to take effect the settings.   |
| Refresh                    | Click <b>Refresh</b> to begin configuring this screen afresh.   |

## 9.4. Maintenance

### 9.4.1. Configuration

#### 9.4.1.1. CLI Configurations

| Node      | Command  | Description   |
|-----------|--|---|
| enable    | configure terminal                                   | This command changes the node to configure node.  |
| configure | write memory   | This command writes current operating configurations to the configuration file.   |
| configure | archive download-config <URL PATH>                   | This command downloads a new copy of configuration file to replace the <b>startup-config</b> from TFTP server. Where <URL PATH> can be:<br>ftp://user:pass@192.168.1.1/file<br>http://192.168.1.1/file<br>tftp://192.168.1.1/file |
| configure | archive upload-config <URL PATH>                     | This command uploads the current <b>startup-config</b> configurations file to a TFTP server.  |
| configure | archive download-running-config <URL PATH>           | This command downloads a new copy of running configuration file from TFTP server. Where <URL PATH> can be:<br>ftp://user:pass@192.168.1.1/file<br>http://192.168.1.1/file<br>tftp://192.168.1.1/file                              |
| configure | reload default-config                                | This command copies a <b>user-default-config</b> file to replace the <b>startup-config</b> file.<br><i>Note: The system will reboot automatically to take effect the configurations.</i>  |
| configure | archive download-config URL_PATH user-default-config | This command downloads configure file to <b>user-default-config</b> .   |
| configure | copy factory-default-config to user-default-config   | This command copies <b>factory-default-config</b> file to <b>user-default-config</b> file.  |
| configure | copy startup-config to user-default-config           | This command copies the <b>startup-config</b> file to <b>user-default-config</b> 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 Switch boot 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.

#### 9.4.1.2. Web Configurations

The screenshot shows a web interface with a yellow 'Maintenance' header. Below it are four tabs: 'Configuration' (selected), 'Firmware', 'Reboot', and 'Server'. The 'Configuration' tab contains three sections:

- Save Configuration:** A section with the text 'Save the parameter settings of the Switch :' and a 'Save' button.
- Upload and Download Configuration:** A section with two radio buttons. The first is selected and labeled 'Upload configuration file to your Switch.' It includes a 'File path' field with a 'Choose File' button and 'No file chosen' text, and an 'Upload' button. The second radio button is labeled 'Press "Download" to save configuration file to your PC.' and has a 'Download' button.
- Reset Configuration:** A section with the text 'Reset the factory default settings of the Switch : - IP address will be 192.168.0.254' and a 'Reset' button.

#### Save Configurations

This screenshot shows a close-up of the 'Save Configurations' section. It features a dark grey header with the text 'Save Configurations'. Below the header, the text 'Save the parameter settings of the Switch :' is displayed, followed by a 'Save' button.

Press the Save button to save the current settings to the NV-RAM (flash).

## Upload / Download Configurations to /from a your server

Follow the steps below to save the configuration file to your PC.

- Select the “Press “Download” to save configurations file to your PC”.
- Click the “Download” button to start the process.

Follow the steps below to load the configuration file from your PC to the Switch.

- Select the “Upload configurations file to your Switch”.
- Select the full path to your configuration file.
- Click the Upload button to start the process.

## Reset the factory default settings of the Switch

Press the Reset button to set the settings to factory default configurations.

### 9.4.2. Firmware

#### 9.4.2.1. CLI Configurations

| Node      | Command                             | Description  |
|-----------|-------------------------------------|--|
| enable    | configure terminal                  | This command changes the node to configure node.   |
| configure | archive download-fw <URL PATH>      | This command downloads a new copy of firmware file from TFTP / FTP / HTTP server.<br>Where <URL PATH> can be:<br>ftp://user:pass@192.168.1.1/file<br>http://192.168.1.1/file<br>tftp://192.168.1.1/file      |
| configure | archive ipv6-download-fw <URL PATH> | This command downloads a new copy of firmware file from IPv6 TFTP / FTP / HTTP server.<br>Where <URL PATH> can be:<br>ftp://user:pass@192.168.1.1/file<br>http://192.168.1.1/file<br>tftp://192.168.1.1/file |

|           |   |  |
|-----------|---|--|
| configure | archive download-secondary-fw <URL PATH>      | This command downloads a new copy of firmware file for secondary image from TFTP / FTP / HTTP server.<br>Where <URL PATH> can be:<br>ftp://user:pass@192.168.1.1/file<br>http://192.168.1.1/file<br>tftp://192.168.1.1/file      |
| configure | archive ipv6-download-secondary-fw <URL PATH> | This command downloads a new copy of firmware file for secondary image from IPv6 TFTP / FTP / HTTP server.<br>Where <URL PATH> can be:<br>ftp://user:pass@192.168.1.1/file<br>http://192.168.1.1/file<br>tftp://192.168.1.1/file |

### 9.4.2.2. Web Configurations

Type the path and file name of the firmware file you wish to upload to the Switch in the **File path** text box or click **Browse** to locate it. Click **Upgrade** to load the new firmware.

**Maintenance**

Configuration
Firmware
Reboot
Server

Upgrade Firmware

File path

Choose File

No file chosen

Upgrade

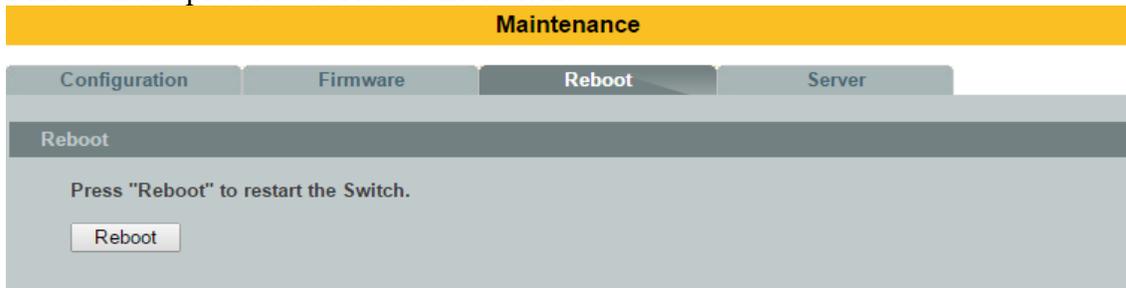
### 9.4.3. Reboot

#### 9.4.3.1. CLI Configurations

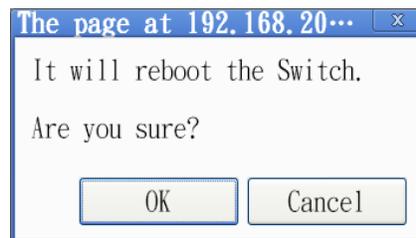
| Node      | Command            | Description                                      |
|-----------|--------------------|--|
| enable    | configure terminal | This command changes the node to configure node. |
| configure | reboot             | This command reboots the system.                 |

#### 9.4.3.2. Web Configurations

**Reboot** allows you to restart the Switch without physically turning the power off. Follow the steps below to reboot the Switch.



- In the **Reboot** screen, click the **Reboot** button. The following screen displays.



- Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

#### 9.4.4. Server Control

The function allows users to enable or disable the HTTP or HTTPS or SNMP v1/v2c or SNMP v3 or SSH or Telnet service individual using the CLI or GUI.

Notice:

##### **SNMP state v.s snmp\_v1v2c v.s snmp\_v3**

- The global SNMP state has the highest priority.
- If the global SNMP state is disabled, the snmp v1 / v2c /v3 will be disabled.
- If the global SNMP state is enabled, you can disable the snmp v1/v2c or snmp v3 individually.

##### 9.4.4.1. CLI Configurations

| Node      | Command                     | Description   |
|-----------|-----------------------------|---|
| enable    | show server status          | This command displays the current server status.            |
| enable    | configure terminal          | This command changes the node to configure node.            |
| configure | http server                 | This command enables the http on the Switch.                |
| configure | no http server              | This command disables the http on the Switch.               |
| configure | http server port<br>VALUE   | This command configures the TCP port for the HTTP server.   |
| configure | no http server port         | This command resets the HTTP TCP port to 80.                |
| configure | https server                | This command enables the https on the Switch.               |
| configure | no https server             | This command disables the https on the Switch.              |
| configure | ssh server                  | This command enables the ssh on the Switch.                 |
| configure | no ssh server               | This command disables the ssh on the Switch.                |
| configure | telnet server               | This command enables the telnet on the Switch.              |
| configure | no telnet server            | This command disables the telnet on the Switch.             |
| configure | telnet server port<br>VALUE | This command configures the TCP port for the TELNET server. |
| configure | no telnet server port       | This command resets the TELNET TCP port to 23.              |

## 9.4.4.2. Web Configurations

**Maintenance**

Configuration
Firmware
Reboot
**Server**

**Server Settings**

|                                 |                                     |                               |  |
|---------------------------------|-------------------------------------|-------------------------------|--|
| <b>HTTP Server State</b>        | <input type="text" value="Enable"/> | <b>HTTP Server TCP Port</b>   | <input type="text" value="80"/><br><small>(80,1025~9999)</small> |
| <b>HTTPS Server State</b>       | <input type="text" value="Enable"/> |                               |  |
| <b>SNMP v1/v2c Server State</b> | <input type="text" value="Enable"/> |                               |  |
| <b>SNMP v3 Server State</b>     | <input type="text" value="Enable"/> |                               |  |
| <b>SSH Server State</b>         | <input type="text" value="Enable"/> |                               |  |
| <b>TELNET Server State</b>      | <input type="text" value="Enable"/> | <b>TELNET Server TCP Port</b> | <input type="text" value="23"/><br><small>(23,1025~9999)</small> |

**Server Status**

|                                  |         |                               |    |
|----------------------------------|---------|-------------------------------|----|
| <b>HTTP Server Status</b>        | Enabled | <b>HTTP Server TCP Port</b>   | 80 |
| <b>HTTPS Server Status</b>       | Enabled |                               |    |
| <b>SNMP v1/v2c Server Status</b> | Enabled |                               |    |
| <b>SNMP v3 Server Status</b>     | Enabled |                               |    |
| <b>SSH Server Status</b>         | Enabled |                               |    |
| <b>TELNET Server Status</b>      | Enabled | <b>TELNET Server TCP Port</b> | 23 |

| Parameter              | Description  |
|------------------------|--|
| <b>Server Settings</b> |  |
| HTTP Server State      | Selects Enable or Disable to enable or disable the HTTP service.   |
| HTTP Server TCP Port   | Configures the TCP port for the HTTP service.                      |
| SSH Server State       | Selects Enable or Disable to enable or disable the SSH service.    |
| Telnet Server State    | Selects Enable or Disable to enable or disable the Telnet service. |
| TELNET Server TCP Port | Configures the TCP port for the Telnet service.                    |
| Apply                  | Click <b>Apply</b> to take effect the settings.                    |
| Refresh                | Click <b>Refresh</b> to begin configuring this screen afresh.      |

## 9.5. Sys log

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 message can be recorded in local NV-RAM or be sent to Syslog server. If you have configured server's IP address and have enabled the Syslog server function, the Switch will send a copy to the syslog server. The default setting of the Syslog server is disabled.

The log message file is limited in 2000 entries. If the log count reach to the 2000, the oldest one will be replaced.

### 9.5.1. CLI Configurations

| Node      | Command                               | Description   |
|-----------|---------------------------------------|---|
| enable    | show syslog                           | The command displays the entire log message recorded in the Switch.         |
| enable    | show syslog level LEVEL               | The command displays the log message with the LEVEL recorded in the Switch. |
| enable    | show syslog server                    | The command displays the syslog server configurations.                      |
| enable    | configure terminal                    | This command changes the node to configure node.                            |
| configure | clear syslog                          | The command clears the syslog message.                                      |
| configure | syslog-server (disable enable)        | The command disables / enables the syslog server function.                  |
| configure | syslog-server ipv4-ip IPADDR          | The command configures the syslog server's IP address in IPv4 format.       |
| configure | syslog-server ipv6-ip IPADDR          | The command configures the syslog server's IP address in IPv6 format.       |
| configure | syslog-server facility                | The command configures the syslog facility level.                           |
| configure | archive upload-syslog <URL PATH>      | This command uploads the syslog file to a TFTP server.                      |
| configure | archive ipv6-upload-syslog <URL PATH> | This command 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
```

## 9.5.2. Web Configurations

**Syslog**

**Syslog Server Settings**

Server IP

---

**Syslog**

Log Level

```

<4> 1999 Nov 12 10:00:57 4001c:Update System Firmware Succeeded!
<6> 1999 Nov 12 10:03:45 60004:System Warm Start!
<4> 1999 Nov 12 10:03:47 40005:Port 6 Link Up.
<6> 1999 Nov 12 10:05:43 60001:User(q) Login Succeeded!
<4> 1999 Nov 12 10:16:40 40004:Port 6 Link Down.
<4> 1999 Nov 12 10:17:06 40005:Port 6 Link Up.
<4> 1999 Nov 12 10:45:16 40004:Port 6 Link Down.
<4> 1999 Nov 12 10:45:43 40005:Port 6 Link Up.
<4> 1999 Nov 12 11:11:09 4001c:Update System Firmware Succeeded!
<6> 1999 Nov 12 11:14:02 60004:System Warm Start!
<4> 1999 Nov 12 11:14:04 40005:Port 6 Link Up.
<6> 1999 Nov 12 11:14:13 60001:User(q) Login Succeeded!
<4> 1999 Nov 12 11:30:37 4001c:Update System Firmware Succeeded!
<6> 1999 Nov 12 11:37:55 60003:System Cold Start!
<4> 1999 Nov 12 11:37:57 40005:Port 2 Link Up.
<4> 1999 Nov 12 11:38:00 40005:Port 8 Link Up.
<4> 1999 Nov 12 11:38:03 40005:Port 6 Link Up.
<6> 1999 Nov 12 11:38:41 be9968e4:User(q) Login Succeeded!

```

| Parameter | Description  |
|-----------|--|
| Server IP | Select IP type for the server's IP.<br>Enter the Syslog server IP address.<br>Select <b>Enable</b> to activate switch sent log message to Syslog server when any new log message occurred. |
| Facility  | Selects the facility level.  |
| Apply     | Click <b>Apply</b> to take effect the settings.  |
| Refresh   | Click <b>Refresh</b> to begin configuring this screen afresh.  |
| Log Level | Select <b>Alert/Critical/Error/Warning/Notice/Information</b> to choose which log message to want to see.  |
| Clear     | Click Clear to clear all of log message.   |
| Save      | Click Save to save all of log message into NV-RAM.   |

## 9.6. User Account

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

### Notices

- The Switch 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.

#### 9.6.1. CLI Configuration

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show user account  | This command displays the current user accounts.   |
| enable    | show dot1x username                                      | This command displays the dot1x user accounts.   |
| configure | add user<br>USERNAME<br>PASSWORD<br>(normal admin dot1x) | This command adds a new user account with choice of privileges <b>normal/admin/dot1x</b> . |
| configure | delete user<br>USERNAME                                  | This command deletes a present user account.   |
| configure | dot1x username<br>USERNAME<br>PASSWORD                   | This command creates a user account for DOT1X local authentication.                        |
| configure | no dot1x username<br>USERNAME                            | This command removed a user account for DOT1X local authentication.                        |

## 9.6.2. Web Configuration

**User Account**

**User Account Settings**

Username   
 User Password   
 User Authority Admin ▾

**User Account List**

| No. | Username | User Authority | Action                                |
|-----|----------|----------------|---------------------------------------|
| 1   | admin    | Admin          | <input type="button" value="Delete"/> |
| 2   | q        | Admin          | <input type="button" value="Delete"/> |

| Parameter                    | Description  |
|------------------------------|--|
| <b>User Account Settings</b> |  |
| 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: <b>admin</b> (read and write) or <b>normal</b> (read only) for this user account. |
| Apply                        | Click <b>Apply</b> to take effect the settings.  |
| Refresh                      | Click <b>Refresh</b> to begin configuring this screen afresh.  |
| <b>User Account List</b>     |  |
| No.                          | This field displays the index number of an entry.  |
| Name                         | This field displays the name of a user account.  |
| Authority                    | This field displays the associated group.  |
| Action                       | Click the <b>Delete</b> button to remove the user account.<br>Note: You cannot delete the last admin accounts.                 |

## 9.7. Device Management

The Topology map uses the LLDP, ONVIF and Manual Registration data to draw the map.

### 9.7.1. 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).

#### 9.7.1.1. CLI Configuration

| Node      | Command                                     | Description   |
|-----------|---|---|
| enable    | show lldp                                   | This command displays the LLDP configurations.  |
| enable    | show lldp neighbor                          | This command displays all of the ports' neighbor information.   |
| enable    | configure terminal                          | This command changes the node to configure node.  |
| configure | lldp (disable enable)                       | This command globally enables / disables the LLDP function on the Switch.   |
| configure | lldp tx-interval                            | This command configures the interval to transmit the LLDP packets.  |
| configure | lldp tx-hold                                | This command configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)  |
| configure | interface IFNAME                            | This command enters the interface configure node.   |
| interface | lldp-agent (disable enable rx-only tx-only) | This command configures the LLDP agent function.<br>disable – Disable the LLDP on the specific port.<br>enable – Transmit and Receive the LLDP packet on the specific port.<br>tx-only – Transmit the LLDP packet on the specific port only.<br>rx-only – Receive the LLDP packet on the specific port. |

|          |   |   |
|----------|---|---|
| config   | interface range<br>gigabitethernet1/0/<br>PORTLISTS | This command enters the if-range configure node.  |
| if-range | lldp-agent<br>(disable enable rx-<br>only tx-only)  | This command configures the LLDP agent function.<br>disable – Disable the LLDP on the specific port.<br>enable – Transmit and Receive the LLDP packet on the specific port.<br>tx-only – Transmit the LLDP packet on the specific port only.<br>rx-only – Receive the LLDP packet on the specific port. |

**Example:**

L2SWITCH(config)#*interface gigabitethernet1/0/ 1*

L2SWITCH(config-if)#*lldp-agent disable*

Success!

L2SWITCH(config)#*interface range gigabitethernet1/0/ 1-3*

L2SWITCH(config-if-range)#*lldp-agent enable*

Success!

### 9.7.1.2. Web Configuration

**Device Management**

LLDP
Manual Registration
ONVIF

**LLDP Settings**

State: Enable ▼  
 Tx Interval: 30 seconds (Range: 1-3600)  
 Tx Hold: 4 times (Range: 2-100)  
 Time To Live: 120 seconds

Apply
Refresh

**LLDP Neighbor Information**

| Local Port 2               |  |
|----------------------------|--|
| <b>Remote Port ID</b>      | GigabitEthernet1/0/8   |
| <b>Chassis ID</b>          | 00-06-87-89-68-a2  |
| <b>System Name</b>         | L2SWITCH   |
| <b>System Description</b>  | Tripp Lite Corporate./NGI-M08C4POE8-2/V1.0.0.S0/Thu May 13 11:10:15 CST 2021 |
| <b>System Capabilities</b> | Bridge/Switch (enabled)  |
| <b>Management IP</b>       | IPv4: 192.168.202.62   |

| Parameter                        | Description   |
|----------------------------------|---|
| <b>LLDP Settings</b>             |   |
| State                            | Globally enables / disables the LLDP on the Switch.   |
| Tx Interval                      | Configures the interval to transmit the LLDP packets.   |
| Tx Hold                          | Configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval) |
| Time To Live                     | The hold time for the Switch's information.   |
| Apply                            | Click <b>Apply</b> to take effect the settings.   |
| Refresh                          | Click <b>Refresh</b> to begin configuring this screen afresh.   |
| <b>LLDP Neighbor Information</b> |   |
| Local Port                       | The local port ID.  |
| Remote Port ID                   | The connected port ID.  |
| Chassis ID                       | The neighbor's chassis ID.  |
| System Name                      | The neighbor's system name.   |
| System Description               | The neighbor's system description.  |
| System Capabilities              | The neighbor's capability.  |
| Management IP                    | The neighbor management address.  |

## 9.7.2. 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, Switch and PC.

### 9.7.2.1. CLI Configurations

| Node      | Command  | Description  |
|-----------|--|--|
| enable    | show manual-registration-device  | This command displays the manual registration device configurations. |
| enable    | configure terminal   | This command changes the node to configure node.                     |
| configure | manual-registration-device type (ipcam plc switch pc) mac MACADDR ip IPADDR product-name STRINGS system-name STRINGS | This command configures a device for the Topology Map.               |
| configure | no manual-registration-device mac MACADDR  | This command removes a device from the Topology Map.                 |

### 9.7.2.2. Web Configurations

**Device Management**

LLDP
Manual Registration
ONVIF

**Manual Registration Settings**

| Type     | MAC Address          | IP                   | Product Name         | System Name          |
|----------|----------------------|----------------------|----------------------|----------------------|
| IP-Cam ▼ | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

**Manual Registration Table**

| Type   | MAC Address       | IP              | Product Name | System Name | Action                                |
|--------|-------------------|-----------------|--------------|-------------|---------------------------------------|
| IP-Cam | 00:0b:04:11:22:33 | 192.168.202.154 | Justin_PC    | L2SWITCH    | <input type="button" value="Delete"/> |

| Parameter                           | Description                              |
|-------------------------------------|--|
| <b>Manual Registration Settings</b> |  |
| Type                                | The kind of devices connected to switch. |
| MAC Address                         | The MAC address on the device.           |

|                                  |   |
|----------------------------------|---|
| Apply                            | Click <b>Apply</b> to take effect the settings.               |
| Refresh                          | Click <b>Refresh</b> to begin configuring this screen afresh. |
| <b>Manual Registration Table</b> |   |
| Type                             | The kind of devices connected to switch.                      |
| MAC Address                      | The MAC address on the ONVIF device.                          |
| Action                           | Whether to delete entered device or not.                      |

### 9.7.3. ONVIF

ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products.

The Switch use ONVIF to discovery if there is ONVIF device connected to the Switch.

#### ONVIF settings and ONVIF Neighbor

The page show the detail information about ONVIF settings and ONVIF devices connected to the Switch. The Switch displays ONVIF devices up to total port count, NGI-M05-C1 shows upto 10 ONVIF devices connected to it. If one or more ONVIF devices are connected to the same port it displays the last ONVIF device gets connect to it.

#### 9.7.3.1. CLI Configurations

| Node   | Command                    | Description   |
|--------|----------------------------|---|
| enable | show onvif                 | This command displays the ONVIF configurations.                                   |
| enable | configure terminal         | This command changes the node to configure node.                                  |
| config | onvif enable               | This command enables the ONVIF on the Switch.                                     |
| config | onvif tx-interval <6-3600> | This command configures the tx interval for the ONVIF.                            |
| config | no onvif enable            | This command disables the ONVIF on the Switch.                                    |
| config | no onvif tx-interval       | This command reset the tx interval to default for the ONVIF.(Default: 6 seconds). |

#### 9.7.3.2. Web Configurations

**Device Management**

LLDP
Manual Registration
ONVIF

**ONVIF Settings**

State

Tx Interval (sec)  (6~3600)

**ONVIF Neighbors**

| Parameter             | Description |
|-----------------------|-------------|
| <b>ONVIF Settings</b> |             |

|                                   |   |
|-----------------------------------|---|
| State                             | Select option to enable / disable the ONVIF feature on the Switch.                          |
| Tx Interval                       | Configures the sending ONVIF discovery packet interval.<br>Valid range is 6 ~ 3600 seconds. |
| Apply                             | Click <b>Apply</b> to take effect the settings.   |
| Refresh                           | Click <b>Refresh</b> to begin configuring this screen afresh.                               |
| <b>ONVIF Neighbor Information</b> |   |
| Port                              | The connected port of the ONVIF device.   |
| IP Address                        | The IP address of the ONVIF device.   |
| MAC Address                       | The MAC address on the ONVIF device.  |
| VLAN ID                           | The VLAN ID of the ONVIF device join.   |
| Product Name                      | Name of the product added.  |
| Product Type                      | What kind of product 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.  |

## 9.8. Topology Map

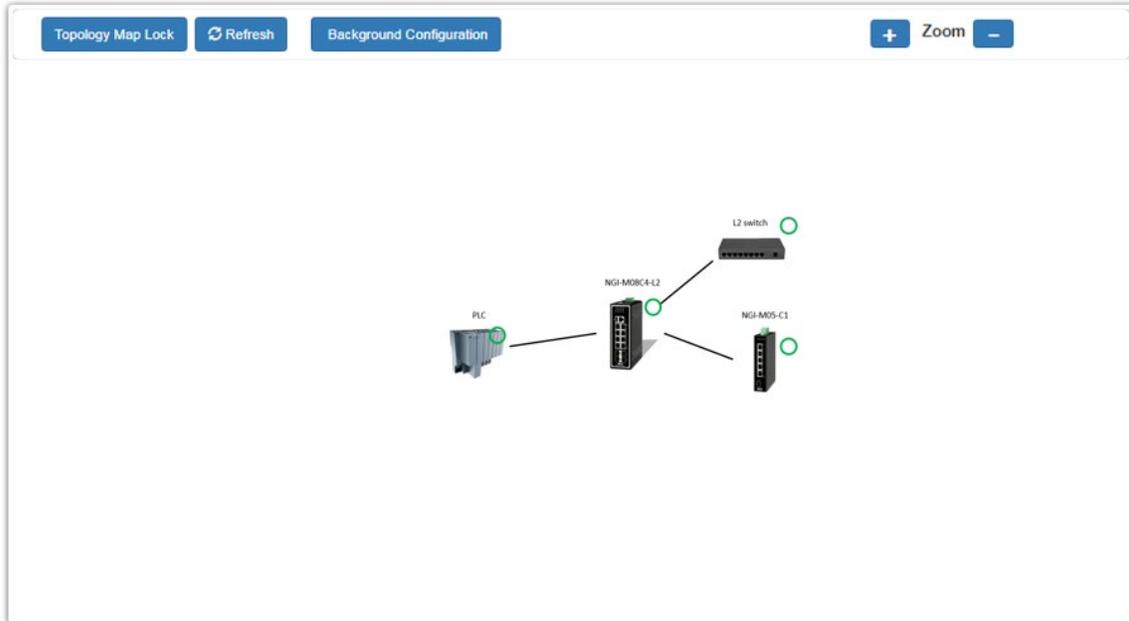
The Topology map is a feature to check neighbor devices' information or to configure them easily. Click the Topology map, the system will display topology as below.

All devices connect to the Switch directly and support LLDP will be displayed on the screen. Such as below figure, the NGI-M05-C1 is its neighbor device. When moving the mouse indicator on the NGI-M05-C1 icon, it will display information about the NGI-M05-C1. Left click the mouse on the NGI-M05-C1 icon. The browser will connect to the NGI-M05-C1. If the neighbor device is a Switch that supports the Netlite server function, right click the mouse. The menu will be displayed on the screen. You can then click the item you wish to configure the Switch.

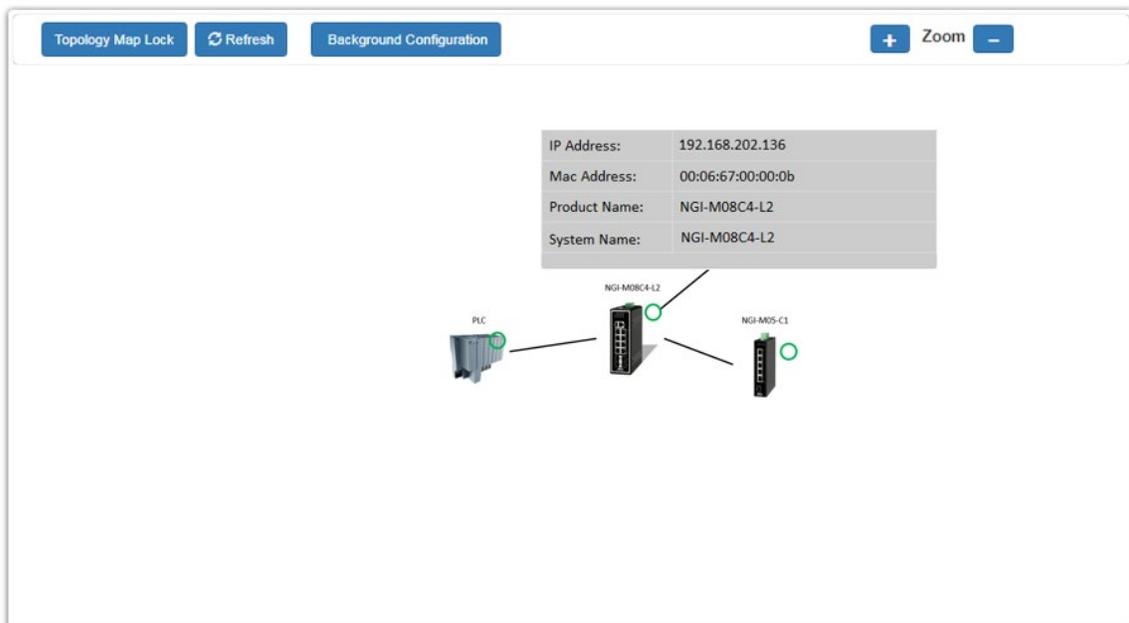
*Note: Topology map can be viewed only on Google or Firefox browsers.*



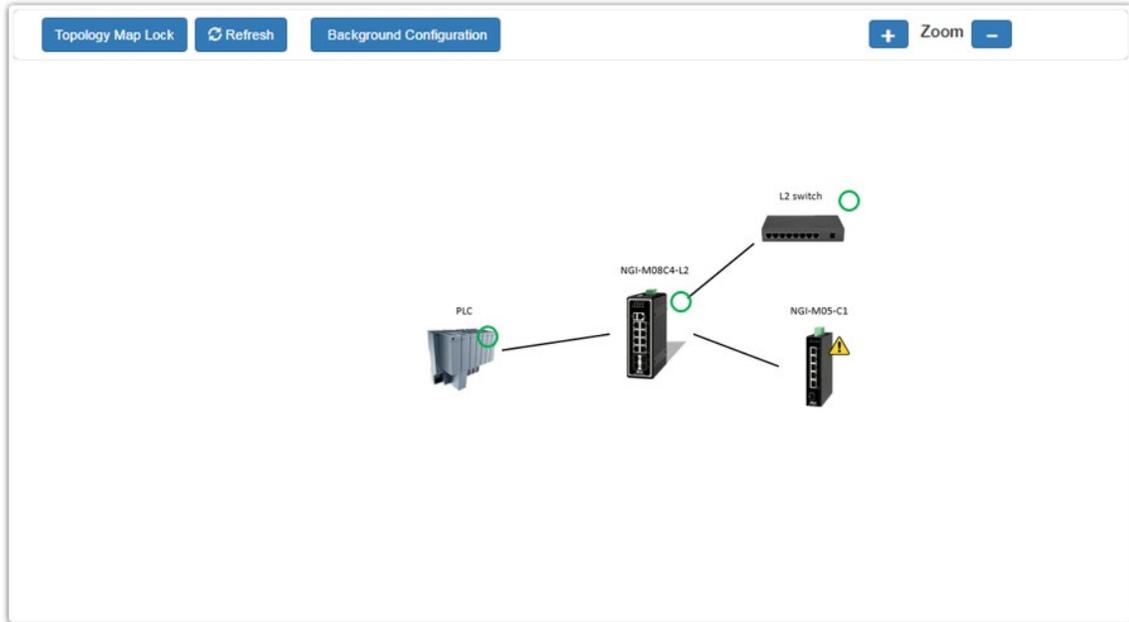
**When you click the “Topology Map Lock”, the screen will appear as below:  
The green circle on the devices indicates they are working normally.**



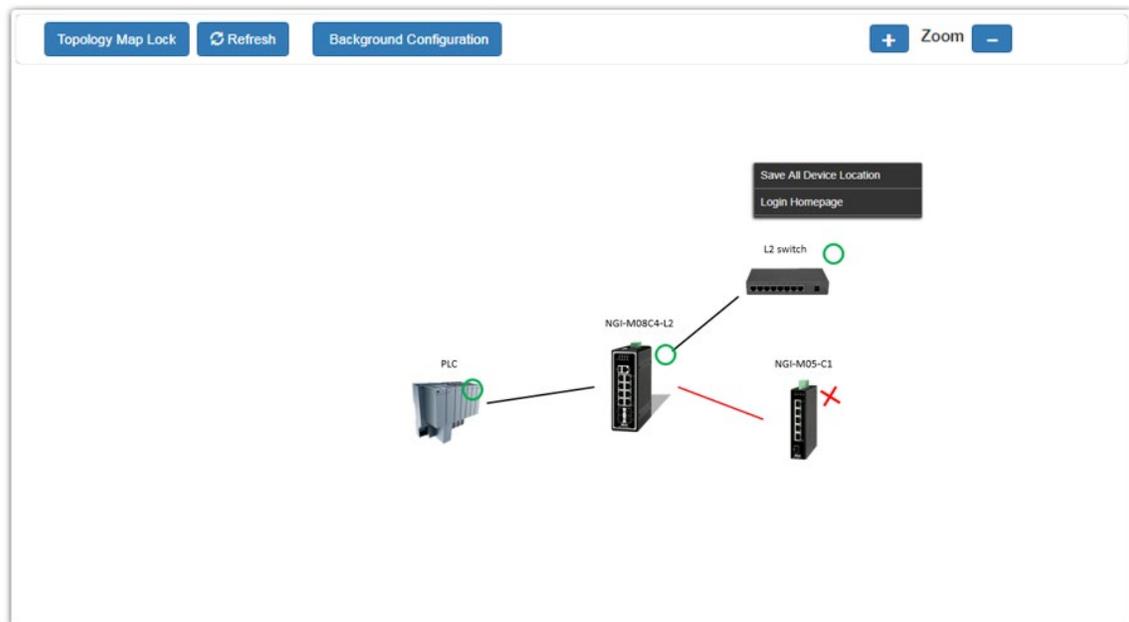
**You can view the basic details of the devices connected to the host, by placing the cursor on it.**



**When there is something wrong with the devices, the screen will appear so that you can find the details of events that have gone wrong and correct it.**

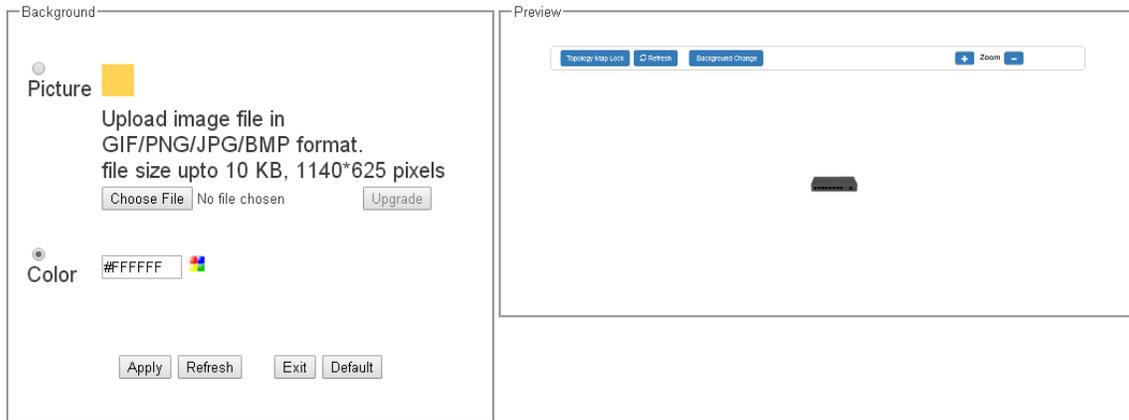


The red 'X' indicates that connection is lost with the host.



### 9.8.1. Background Configuration

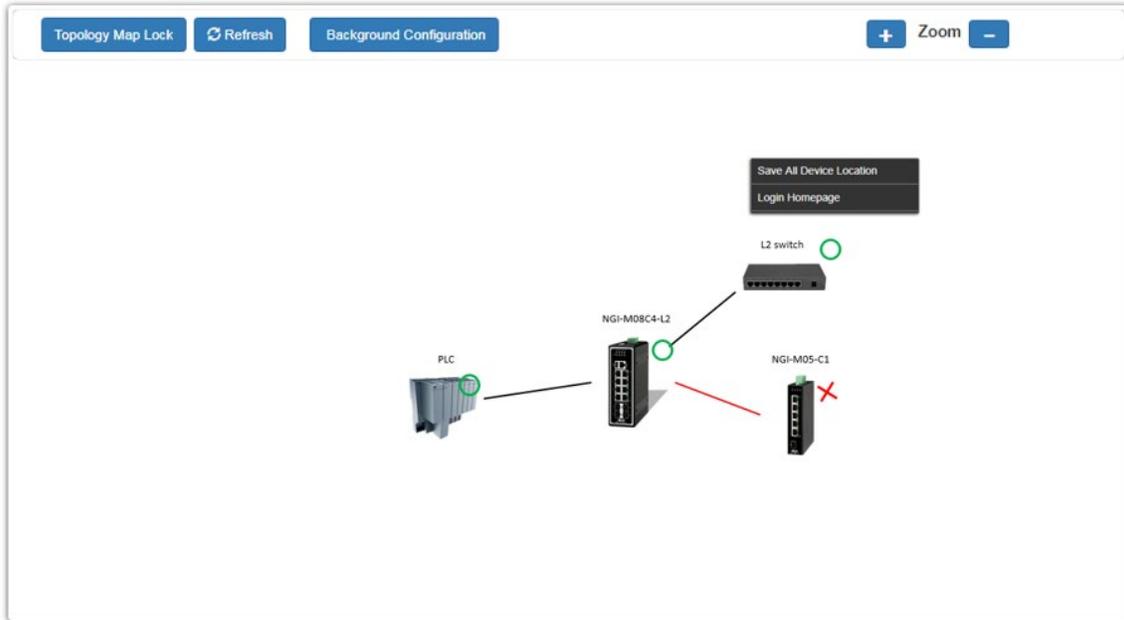
You can upload your company floor layout plan picture in to the background image so that you can identify easily where the switches has been placed.



- **Picture**  
To choose 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 Switch 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.

## 9.8.2. Client-Switch Management

By Right clicking on the non-Lite management switch (L2 Switch) you will get this menu and can configure as shown below.



Non-Lite management switch and other devices menu:

- Save All Device Location  
To fix the location of all devices on the map, so that it restores its places after refresh.
- Login Homepage  
To login to the client device Homepage, make the necessary changes after entering suitable username and password.

## 10. MISC

### 10.1. Cable Test

This feature determines the quality of the cables, shorts, 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 accessible through the CLI without any GUI support.*

#### 10.1.1. CLI Configurations

| Node   | Command            | Description                                      |
|--------|--------------------|--|
| Enable | configure terminal | This command changes the node to configure node. |

|           |                        |   |
|-----------|------------------------|---|
| configure | interface IFNAME       | This command enters the interface configure node. |
| Interface | show cable-test result | This command displays the cable test result.      |
| Interface | cable-test start       | This command starts to test the cable.            |

## WARRANTY & PRODUCT REGISTRATION

### 3-Year Limited Warranty

TRIPP LITE warrants its products to be free from defects in materials and workmanship for a period of three (3) years from the date of initial purchase. TRIPP LITE's obligation under this warranty is limited to repairing or replacing (at its sole option) any such defective products. To obtain service under this warranty, you must obtain a Returned Material Authorization (RMA) number from TRIPP LITE or an authorized TRIPP LITE service center. Products must be returned to TRIPP LITE or an authorized TRIPP LITE service center with transportation charges prepaid and must be accompanied by a brief description of the problem encountered and proof of date and place of purchase. This warranty does not apply to equipment which has been damaged by accident, negligence or misapplication or has been altered or modified in any way.

EXCEPT AS PROVIDED HEREIN, TRIPP LITE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Some states do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

EXCEPT AS PROVIDED ABOVE, IN NO EVENT WILL TRIPP LITE BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Specifically, TRIPP LITE is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise.

### PRODUCT REGISTRATION

Visit [www.tripplite.com/warranty](http://www.tripplite.com/warranty) today to register your new Tripp Lite product. You'll be automatically entered into a drawing for a chance to win a FREE Tripp Lite product!\*

\* No purchase necessary. Void where prohibited. Some restrictions apply. See website for details.

### Regulatory Compliance Identification Numbers

For the purpose of regulatory compliance certifications and identification, your Tripp Lite product has been assigned a unique series number. The series number can be found on the product nameplate label, along with all required approval markings and information. When requesting compliance information for this product, always refer to the series number. The series number should not be confused with the marketing name or model number of the product.

### FCC Notice, Class A

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**Note:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide

reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. 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 his own expense. The user must use shielded cables and connectors with this equipment. Any changes or modifications to this equipment not expressly approved by Tripp Lite could void the user's authority to operate this equipment.

Tripp Lite has a policy of continuous improvement. Specifications are subject to change without notice. Photos and illustrations may differ slightly from actual products.



1111 W. 35th Street, Chicago, IL 60609 USA • [triplite.com/support](http://triplite.com/support)

21-04-320 93-3EAD\_RevA