



User Manual

Surveillance Switch

DSS-200G Series

Information in this document is subject to change without notice.

© 2023 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-Link logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

FCC Warning

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 this user's guide, 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.

CE Mark Warning

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

Warning!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstörungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo caso, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l'utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l'utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Table of Contents

| | |
|--|-----------|
| 1. Introduction | 1 |
| Audience | 1 |
| Standard Mode and Surveillance Mode | 1 |
| Other Documentation | 2 |
| Conventions | 2 |
| Notes, Notices, and Cautions | 2 |
| 2. Product Introduction | 3 |
| DSS-200G-10MP | 4 |
| Front Panel | 4 |
| Rear Panel | 7 |
| DSS-200G-10MPP | 7 |
| Front Panel | 7 |
| Rear Panel | 10 |
| DSS-200G-28MP | 11 |
| Front Panel | 11 |
| Rear Panel | 14 |
| DSS-200G-28MPP | 15 |
| Front Panel | 15 |
| Rear Panel | 18 |
| 3. Hardware Installation | 19 |
| Step1: Unpacking | 19 |
| Packing Contents | 19 |
| Step2: Switch Installation | 19 |
| Desktop or Shelf Installation | 19 |
| Rack Installation | 19 |
| Step 3: Plugging in the AC Power Cord | 21 |
| Power Failure | 21 |
| Grounding the Switch | 21 |
| Connecting the Alarm Cable | 22 |
| Connecting the PoE Cable | 22 |
| 4. Web-based Switch Configuration | 25 |
| Management Options | 25 |
| Connecting using the Web User Interface | 25 |
| Logging onto the Web User Interface | 26 |
| Smart Wizard | 27 |
| Web User Interface – Standard Mode | 30 |
| Areas of the User Interface | 30 |
| Device Information | 30 |
| System | 31 |
| System Information Settings | 31 |
| Port Configuration | 33 |
| PoE | 35 |
| System Log | 38 |
| Time | 40 |
| Time Range | 42 |
| Management | 43 |

| | |
|--|-----------|
| User Account Settings | 43 |
| SNMP..... | 44 |
| SNMP Community Table Settings | 45 |
| HTTP/HTTPS..... | 47 |
| D-Link Discovery Protocol | 47 |
| Layer 2 Features | 49 |
| FDB..... | 49 |
| VLAN..... | 52 |
| Auto Surveillance VLAN | 58 |
| Voice VLAN..... | 60 |
| Spanning Tree | 63 |
| Loopback Detection | 65 |
| Link Aggregation | 67 |
| L2 Multicast Control | 70 |
| LLDP | 74 |
| QoS | 75 |
| 802.1p Priority..... | 75 |
| Port Rate Limiting | 76 |
| Security | 77 |
| Safeguard Engine Settings..... | 77 |
| Traffic Segmentation..... | 77 |
| Storm Control..... | 78 |
| DoS Attack Prevention Settings | 78 |
| Zone Defense Settings | 79 |
| SSL | 80 |
| OAM..... | 81 |
| Cable Diagnostics..... | 81 |
| Monitoring | 82 |
| Statistics..... | 82 |
| Mirror Settings | 82 |
| Green | 84 |
| Power Saving..... | 84 |
| EEE..... | 85 |
| ONVIF | 87 |
| Global Status | 87 |
| IP-Camera Information | 88 |
| Dip Switch | 89 |
| Dip Status | 89 |
| Extend..... | 90 |
| Save and Tools | 91 |
| Save Configuration | 91 |
| Firmware Information..... | 91 |
| Firmware Upgrade..... | 91 |
| Configuration Restore & Backup | 93 |
| Log Backup..... | 95 |
| Ping..... | 96 |
| Reset..... | 96 |
| Reboot System | 97 |
| 5. Surveillance | 98 |
| Web User Interface – Surveillance Mode | 98 |
| Areas of the User Interface..... | 99 |
| Surveillance Topology..... | 100 |

| | |
|---|------------|
| Enabling and Disabling PoE | 103 |
| Device Information | 104 |
| Port Information | 105 |
| Group Details | 107 |
| IP-Camera Information..... | 108 |
| PoE Information | 110 |
| PoE Scheduling | 112 |
| PD Alive | 114 |
| Time | 115 |
| Clock Settings | 115 |
| SNTP Settings | 115 |
| Surveillance Settings | 117 |
| Surveillance Log | 119 |
| Health Diagnostic..... | 120 |
| Save and Tools | 121 |
| Firmware Information..... | 121 |
| Firmware Upgrade..... | 121 |
| Configuration Restore & Backup | 123 |
| Reset..... | 123 |
| Reboot System | 124 |
| Help..... | 125 |
| Help..... | 125 |
| 6. Appendix A - Ethernet Technology | 126 |
| Gigabit Ethernet Technology | 126 |
| Fast Ethernet Technology | 126 |
| Switching Technology..... | 126 |
| 7. Appendix B - Technical Specifications | 128 |
| Hardware Specifications | 128 |
| Key Components / Performance | 128 |
| Port Functions..... | 128 |
| Physical & Environment..... | 128 |
| Emission (EMI) Certifications..... | 129 |
| Safety Certifications..... | 129 |
| Features | 129 |
| L2 Features..... | 129 |
| L2 Multicasting..... | 129 |
| VLAN..... | 129 |
| Quality of Service (QoS) | 129 |
| Security | 129 |
| Management..... | 129 |
| Power Saving..... | 129 |
| Surge Protection | 129 |
| 8. Appendix C –Rack Mount Instructions | 130 |
| 9. Appendix D – Surveillance Mode Defaults | 131 |

1. Introduction

This manual's command descriptions are based on the software release 1.00. The commands listed here are the subset of commands that are supported by the DSS-200G MP/MPP Series switch.

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the DSS-200G MP/MPP Series switch, which will be generally referred to simply as 'the switch' within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Standard Mode and Surveillance Mode

The DSS-200G MP/MPP Series switches support Standard Mode and Surveillance Mode Web UI types. Standard Mode is used to manage the network and system elements of the switch. Surveillance Mode is a dedicated user interface designed for monitoring and managing the surveillance and IP security devices on your network.

There are two methods to switch between the interface types. These are as follows:

- Re-run the Smart Wizard that is presented when you access the web interface of the device and choose Surveillance Mode option. See the

- Smart Wizard section of this manual for more information.
- Click the Standard Mode button in the toolbar. See the section of this manual for more information.

For more information, please refer to the Web UI Interface Guide for the appropriate Web UI mode.

Other Documentation

The documents below are a further source of information in regard to configuring and troubleshooting the switch. All the documents are available either from the CD, bundled with this switch, or from the D-Link website. Other documents related to this switch are:

- *D-LinkDSS-200G MP/MPP Series Standard Mode Web UI Reference Guide*
- *D-LinkDSS-200G MP/MPP Series Surveillance Mode Web UI Reference Guide*

Conventions

| Convention | Description |
|-----------------------------------|--|
| Boldface Font | Indicates a button, a toolbar icon, menu, or menu item. For example: Open the File menu and choose Cancel . Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: You have mail . Bold font is also used to represent filename, program names and commands. For example: use the copy command. |
| Initial capital letter | Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Press Enter. |
| Menu Name > Menu Option | Indicates the menu structure. Device > Port > Port Properties means the Port Properties menu option under the Port menu option that is located under the Device menu. |
| <i>Blue Courier Font</i> | This convention is used to represent an example of a screen console display including example entries of CLI command input with the corresponding output. |

Notes, Notices, and Cautions

Below are examples of the three types of indicators used in this manual. When administering your switch using the information in this document, you should pay special attention to these indicators. Each example below provides an explanatory remark regarding each type of indicator.



NOTE: A note indicates important information that helps you make better use of your device.



NOTICE: A notice indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



CAUTION: A caution indicates a potential for property damage, personal injury, or death.

2. Product Introduction

The DSS-200G MP/MPP series Surveillance Switch is a PoE switch with ONVIF support. This allows it to recognize ONVIF devices and integrate seamlessly with your surveillance network. Various power budgets support, including the high PoE (90 Watts) standard available on MPP series, makes the DSS-200G MP/MPP series a critical part of your surveillance infrastructure.

The DSS-200G MP/MPP series switches can change modes between 'Smart Switch' and 'Surveillance Switch' modes, making them suitable for a variety of applications. An intuitive web user interface provides advanced features available in the Standard Mode, with full PoE capabilities and high link speeds for fast deployment time for PoE devices.

The switches are designed to be energy efficient with the support for IEEE 802.3az Energy Efficient Ethernet (EEE) and D-Link Green Technologies. They include multiple features, such as cable length detection, port status detection and the ability to hibernate under low utilization. If the switch detects no activity on any of the switch ports, it can be hibernated to conserve power.

The DSS-200G MPP series provides multiple PoE ports that support IEEE 802.3bt to accommodate heavy-duty PoE devices with high power requirement. In addition, the ports of both the DSS-200G MP and MPP series are equipped with 6kV surge protection to protect damages from changes in the electrical current. Features such as automatic device identification, video traffic optimization and health diagnostic tools provide an intelligent and comprehensive solution to your enterprise network and surveillance infrastructure.

The switches support 802.1Q VLAN standard tagging to enhance network security and performance. The switches also support 802.1p priority queues, enabling users to run bandwidth-sensitive applications such as streaming multimedia by prioritizing that traffic in network. These functions allow switches to work seamlessly with VLAN and 802.1p traffic in the network. Furthermore, the Auto Surveillance VLAN can be used for assigning IP surveillance devices with a VLAN ID to prioritize video traffic.

DSS-200G-10MP

8 x 10/100/1000 Mbps PoE ports + 2 x 100/1000 Mbps SFP surveillance switch

Front Panel



Figure 2-1 DSS-200G-10MP Front Panel

Mode Button:

By pressing the Mode button over 2 seconds, the Port LED (ports 1~8) will switch between the Link (refer to the below **Link/Act/Speed LED**) and PoE mode to indicate the PoE ports (refer to the below **PoE LED**) status or link speed:

| PoE/Link Mode LED | Description |
|-------------------|---|
| Green | The Port LED indicator is in Link/Act/Speed mode. |
| Orange | The Port LED indicator is in PoE mode. |

Reset:

The Reset button has 3 modes:

| Reset Mode | Description |
|--------------------------|---|
| Reboot | Press the reset button and hold it for 1~5 seconds to reboot the device. |
| Reset to factory default | Press the reset button and hold it for longer than 5 seconds (the port LEDs should all flash orange) to reset the device to its factory defaults, which will erase all configuration changes. |
| Reset to loader mode | Press the reset button and hold it for longer than 10 seconds to enter the loader mode (the port LEDs should all flash orange and then green), which allows you to upgrade the firmware. |

Alert LED:

The Alert indicator is blinking red to indicate PoE malfunctioning events: PoE function startup failure, PoE function disabled due to thermal abnormality, PoE power denial, PoE power overload, and PoE power short circuit. The Alarm port on the back can also be connected to signify such events.

Power LED:

The power LED has two states to indicate the Switch power status.

| | |
|-------|---|
| Green | The Switch is powered on using normal power supply. |
| Off | The Switch is not powered on. |

PoE Budget LED (with % indicator):

The PoE Budget LED has 4 states to indicate the total PoE consumption level.

| LED | Description |
|--------|--|
| Red | When the PoE power consumption is between 75% and 100% of the total power (130W), the PoE indicator is steady red. |
| Orange | When the PoE power consumption is between 50% and 75% of the total power (130W), the PoE indicator is steady orange. |
| Green | When the PoE power consumption is between 25% and 50% of the total power (130W), the PoE indicator is steady green. |
| Green | When the PoE power consumption is lower than 25% of the total power (130W), the PoE indicator is steady green. |

Link/Act/Speed LED (Ports 1-8):

Ports 1-8 are 10/100/1000 Mbps RJ45 ports that comply with 802.3at/802.3af and can supply 30 W/15 W power to the powered devices (PD). The Port LED can be switched between the PoE mode and Link mode. When in Link Mode, the Port LED has the following states:

| LED | Description |
|-----------------|--|
| Solid Orange | An active link operating at 10/100 Mbps on the port. |
| Flashing Orange | The port is transmitting data at 10/100 Mbps. |
| Off | There is no active link on the port. |
| Solid Green | An active link operating at 1000 Mbps on the port. |
| Flashing Green | The port is transmitting data at 1000 Mbps. |

Link/Act/Speed LED (Ports 9-10):

Ports 9-10 are 100/1000 Mbps SFP ports that comply with 802.3u and 802.3z.

| LED | Description |
|-----------------|---|
| Solid Orange | An active link operating at 100 Mbps on the port. |
| Flashing Orange | The port is transmitting data at 100 Mbps. |
| Off | There is no active link on the port. |

| | |
|----------------|--|
| Solid Green | An active link operating at 1000 Mbps on the port. |
| Flashing Green | The port is transmitting data at 1000 Mbps. |

PoE LED (Ports 1-8):

Ports 1-8 comply with 802.3at/802.3af and can supply 30 W/15 W power to the powered devices (PD). The Port LED can be switched between the PoE mode and Link Mode. When in PoE Mode, the Port LED has the following states:

| LED | Description |
|----------------|---|
| Solid Green | A PD is connected and consumes power from the Switch. |
| Flashing Green | The port is transmitting power to the PD. |
| Off | There is no PD connected to the port. |

DIP Switch:

The DIP switch is a convenient mechanism to enable or disable the advanced functions of the Switch. The DIP switch is turned off by default. The following describes the functions of the 5 switches:

| LED | Description |
|-----------|---|
| QoS | If the QoS switch is enabled, incoming packets of the controlled ports (ports 1-8) are forwarded according to the assigned port number with Port 1 having the highest priority. |
| Extend | If the PoE Extend switch is enabled, the enabled PoE ports (ports 1-4) can power devices with 20 W through a 250-meter network cable (Cat 5e or above) at a speed of up to 10 Mbps. |
| Isolation | If the Isolation switch is enabled, the LAN ports (ports 1-8) will be isolated from one another. The LAN ports can only communicate with the uplink SFP ports. |
| PD-Alive | If the PD-Alive is enabled, the PoE ports (ports 1-8) can detect whether the connected PDs are alive and automatically reboot the connected PDs once they become unresponsive. |
| STP | If the STP switch is enabled, the STP function is enabled on the uplink ports (ports 9-10). Network connectivity can be automatically restored through redundant paths in case of a link failure. |

Rear Panel

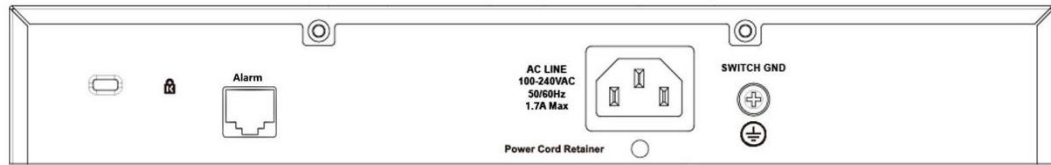


Figure 2-2 DSS-200G-10MP Rear Panel

Power: Connect the supplied AC power cable to this port.



CAUTION: The SFP ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.



CAUTION: This equipment is to be connected only to PoE networks without routing to the outside plant.

DSS-200G-10MPP

8 x 10/100/1000 Mbps PoE ports + 2 x 100/1000 Mbps SFP ports surveillance switch

Front Panel



Figure 2-3 DSS-200G-10MPP Front Panel

Mode Button:

By pressing the Mode button over 2 seconds, the Port LED (ports 1~8) will switch between the Link (refer to the below **Link/Act/Speed LED**) and PoE mode to indicate the PoE ports (refer to the below **PoE LED**) status or link speed:

| PoE/Link Mode LED | Description |
|-------------------|---|
| Green | The Port LED indicator is in Link/Act/Speed mode. |
| Orange | The Port LED indicator is in PoE mode. |

Reset:

The Reset button has 3 modes:

| Reset Mode | Description |
|--------------------------|---|
| Reboot | Press the reset button and hold it for 1~5 seconds to reboot the device. |
| Reset to factory default | Press the reset button and hold it for longer than 5 seconds (the port LEDs should all flash orange) to reset the device to its factory defaults, which will erase all configuration changes. |
| Reset to loader mode | Press the reset button and hold it for longer than 10 seconds to enter the loader mode (the port LEDs should all flash orange and then green), which allows you to upgrade the firmware. |

Alert LED:

Blinking Red: The Alert indicator is blinking red to indicate PoE malfunctioning events: PoE function startup failure, PoE function disabled due to thermal abnormality, PoE power denial, PoE power overload, and PoE power short circuit. The Alarm port on the back can also be connected to signify such events.

Power LED:

The power LED has two states to indicate the Switch power status.

| | |
|-------|---|
| Green | The Switch is powered on using normal power supply. |
| Off | The Switch is not powered on. |

PoE Budget LED (with % indicator):

The PoE Budget LED has 4 states to indicate the total PoE consumption level.

| LED | Description |
|--------------|--|
| Solid Red | When the PoE power consumption is between 75% and 100% of the total power (242W), the PoE indicator is steady red. |
| Solid Orange | When the PoE power consumption is between 50% and 75% of the total power (242W), the PoE indicator is steady orange. |
| Solid Green | When the PoE power consumption is between 25% and 50% of the total power (242W), the PoE indicator is steady green. |
| Solid Green | When the PoE power consumption is lower than 25% of the total power (242W), the PoE indicator is steady green. |

Link/Act/Speed LED (Ports 1-8):

Ports 1-8 comply with 802.3at and can supply up to 90 W power to the powered devices (PD). The Port LED can be switched between the PoE mode and Link Mode. When in Link Mode, the Port LED has the following states:

| LED | Description |
|-----------------|--|
| Solid Orange | An active link operating at 10/100 Mbps on the port. |
| Flashing Orange | The port is transmitting data at 10/100 Mbps. |
| Off | There is no active link on the port. |
| Solid Green | An active link operating at 1000 Mbps on the port. |
| Flashing Green | The port is transmitting data at 1000 Mbps. |

PoE LED (Ports 1- 8):

Ports 1-8 comply with 802.3bt and can supply 90 W power to the powered devices (PD). The Port LED can be switched between the PoE mode and Link Mode. When in PoE Mode, the Port LED has the following states:

| LED | Description |
|----------------|---|
| Solid Green | A PD is connected and consumes power from the Switch. |
| Flashing Green | The port is transmitting power to the PD. |
| Off | There is no PD connected to the port. |

Link/Act/Speed LED (Ports 9-10):

Ports 9-10 are 100/1000 Mbps SFP ports that comply with 802.3u and 802.3z.

| LED | Description |
|-----------------|--|
| Solid Orange | An active link operating at 100 Mbps on the port. |
| Flashing Orange | The port is transmitting data at 100 Mbps. |
| Off | There is no active link on the port. |
| Solid Green | An active link operating at 1000 Mbps on the port. |
| Flashing Green | The port is transmitting data at 1000 Mbps. |

DIP Switch:

The DIP switch is a convenient mechanism to enable or disable the advanced functions of the Switch. The DIP switch is turned off by default. The following describes the functions of the 5 switches:

| LED | Description |
|-----------|---|
| QoS | If the QoS switch is enabled, incoming packets of the controlled ports (ports 1-24) are forwarded according to the port priority based on the assigned port number (with Port 1 having the highest priority). |
| Extend | If the PoE Extend switch is enabled, the enabled PoE ports (ports 1-4) can power devices with 20 W through a 250-meter network cable (Cat 5e or above) at a speed of up to 10 Mbps. |
| Isolation | If the Isolation switch is enabled, the LAN ports (ports 1-8) will be isolated from one another. The LAN ports can only communicate with the uplink SFP ports. |
| PD-Alive | If the PD-Alive is enabled, the PoE ports (ports 1-8) can detect whether the connected PDs are alive and automatically reboot the connected PDs once they become unresponsive. |
| STP | If the STP switch is enabled, the STP function is enabled on the uplink ports (ports 9-10). Network connectivity can be automatically restored through redundant paths in case of a link failure. |

Rear Panel

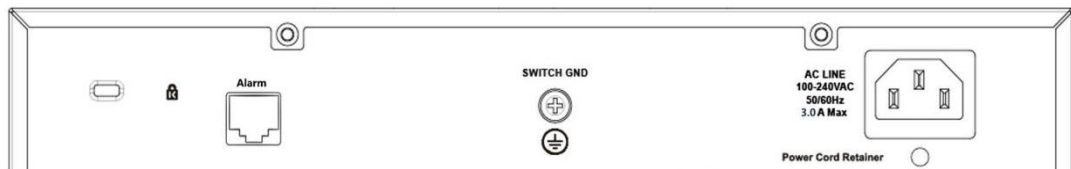


Figure 2-4 DSS-200G-10MPP Rear Panel

Power: Connect the supplied AC power cable to this port.



CAUTION: The SFP ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.



CAUTION: This equipment is to be connected only to PoE networks without routing to the outside plant.

DSS-200G-28MP

24 x 10/100/1000 Mbps PoE ports + 4 x 1000BASE-T/SFP Combo ports surveillance switch

Front Panel



Figure 2-5 DSS-200G-28MP Front Panel

Mode Button:

By pressing the Mode button over 2 seconds, the Port LED (ports 1~24) will switch between the Link (refer to the below **Link/Act/Speed LED**) and PoE mode to indicate the PoE ports (refer to the below **PoE LED**) status or link speed:

| PoE/Link Mode LED | Description |
|-------------------|---|
| Green | The Port LED indicator is in Link/Act/Speed mode. |
| Orange | The Port LED indicator is in PoE mode. |

Reset:

The Reset button has 3 modes:

| Reset Mode | Description |
|--------------------------|---|
| Reboot | Press the reset button and hold it for 1~5 seconds to reboot the device. |
| Reset to factory default | Press the reset button and hold it for longer than 5 seconds (the port LEDs should all flash orange) to reset the device to its factory defaults, which will erase all configuration changes. |
| Reset to loader mode | Press the reset button and hold it for longer than 10 seconds to enter the loader mode (the port LEDs should all flash orange and then green), which allows you to upgrade the firmware. |

Alert LED:

The Alert indicator is blinking red to indicate PoE malfunctioning events: PoE function startup failure, PoE function disabled due to thermal abnormality, PoE power denial, PoE power overload, and PoE power short circuit. The Alarm port on the back can also be connected to signify such events.

Power LED:

The power LED has two states to indicate the Switch power status.

| | |
|-------|---|
| Green | The Switch is powered on using normal power supply. |
| Off | The Switch is not powered on. |

PoE Budget LED (with % indicator):

The PoE Budget LED has 4 states to indicate the total PoE consumption level.

| LED | Description |
|--------------|--|
| Solid Red | When the PoE power consumption is between 75% and 100% of the total power (370W), the PoE indicator is steady red |
| Solid Orange | When the PoE power consumption is between 50% and 75% of the total power (370W), the PoE indicator is steady orange. |
| Solid Green | When the PoE power consumption is between 25% and 50% of the total power (370W), the PoE indicator is steady green. |
| Solid Green | When the PoE power consumption is lower than 25% of the total power (370W), the PoE indicator is steady green. |

Link/Act/Speed LED (Ports 1-24):

Ports 1-24 comply with 802.3at/af and can supply 30 W/15 W power to the powered devices (PD). The Port LED can be switched between the PoE mode and Link Mode. When in Link Mode, the Port LED has the following states:

| LED | Description |
|-----------------|--|
| Solid Orange | An active link operating at 10/100 Mbps on the port. |
| Flashing Orange | The port is transmitting data at 10/100 Mbps. |
| Off | There is no active link on the port. |
| Solid Green | An active link operating at 1000 Mbps on the port. |
| Flashing Green | The port is transmitting data at 1000 Mbps. |

SFP LED (Combo SFP Ports 25-28):

Ports 25-28 are 1000Base-T/SFP combo ports that comply with 802.3ab, 802.3u, and 802.3z.

| LED | Description |
|-----------------|---|
| Solid Orange | An active link operating at 100 Mbps on the port. |
| Flashing Orange | The port is transmitting data at 100 Mbps. |
| Off | There is no active link on the port. |

| | |
|----------------|--|
| Solid Green | An active link operating at 1000 Mbps on the port. |
| Flashing Green | The port is transmitting data at 1000 Mbps. |

PoE LED (Ports 1- 24):

Ports 1-24 comply with 802.3at/af and can supply 30 W/15 W power to the powered devices (PD). The Port LED can be switched between the PoE mode and Link Mode. When in PoE Mode, the Port LED has the following states:

| LED | Description |
|----------------|---|
| Solid Green | A PD is connected and consumes power from the Switch. |
| Flashing Green | The port is transmitting power to the PD. |
| Off | There is no PD connected to the port. |

DIP Switch :

The DIP switch is a convenient mechanism to enable or disable the advanced functions of the Switch. The DIP switch is turned off by default. The following describes the functions of the 5 switches:

| LED | Description |
|-----------|---|
| QoS | If the QoS switch is enabled, incoming packets of the controlled ports (ports 1-24) are forwarded according to the port priority based on the assigned port number (with Port 1 having the highest priority). |
| Extend | If the PoE Extend switch is enabled, the enabled PoE ports (ports 1-8) can power devices with 20 W through a 250-meter network cable (Cat 5e or above) at a speed of up to 10 Mbps. |
| Isolation | If the Isolation switch is enabled, the LAN ports (ports 1-24) will be isolated from one another. The LAN ports can only communicate with the uplink SFP ports. |
| PD-Alive | If the PD-Alive is enabled, the PoE ports (ports 1-24) can detect whether the connected PDs are alive and automatically reboot the connected PDs once they become unresponsive. |
| STP | If the STP switch is enabled, the STP function is enabled on the uplink ports (ports 25-28). Network connectivity can be automatically restored through redundant paths in case of a link failure. |

Rear Panel

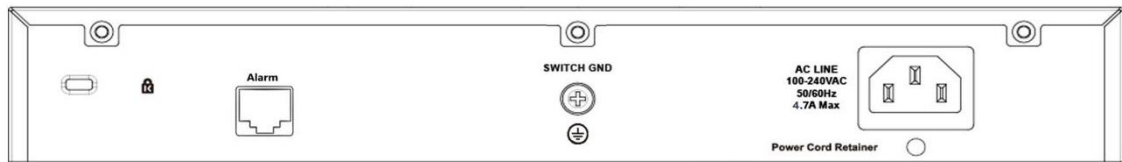


Figure 2-6 DSS-200G-28MP Rear Panel

Power: Connect the supplied AC power cable to this port.



CAUTION: The SFP ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.



CAUTION: This equipment is to be connected only to PoE networks without routing to the outside plant.

DSS-200G-28MPP

24 x 10/100/1000 Mbps PoE ports + 4 x 1000BASE-T/SFP Combo ports surveillance switch

Front Panel



Figure 2-7 DSS-200G-28MPP Front Panel

Mode Button:

By pressing the Mode button over 2 seconds, the Port LED (ports 1~24) will switch between the Link (refer to the below **Link/Act/Speed LED**) and PoE mode to indicate the PoE ports (refer to the below **PoE LED**) status or link speed:

| PoE/Link Mode LED | Description |
|-------------------|---|
| Green | The Port LED indicator is in Link/Act/Speed mode. |
| Orange | The Port LED indicator is in PoE mode. |

Reset:

The Reset button has 3 modes:

| Reset Mode | Description |
|--------------------------|---|
| Reboot | Press the reset button and hold it for 1~5 seconds to reboot the device. |
| Reset to factory default | Press the reset button and hold it for longer than 5 seconds (the port LEDs should all flash orange) to reset the device to its factory defaults, which will erase all configuration changes. |
| Reset to loader mode | Press the reset button and hold it for longer than 10 seconds to enter the loader mode (the port LEDs should all flash orange and then green), which allows you to upgrade the firmware. |

Alert LED:

The Alert indicator is blinking red to indicate PoE malfunctioning events: PoE function startup failure, PoE function disabled due to thermal abnormality, PoE power denial, PoE power

overload, and PoE power short circuit. The Alarm port on the back can also be connected to signify such events.

Power LED:

The power LED has two states to indicate the Switch power status.

| | |
|-------|---|
| Green | The Switch is powered on using normal power supply. |
| Off | The Switch is not powered on. |

PoE Budget LED (with % indicator):

The PoE Budget LED has 4 states to indicate the total PoE consumption level.

| LED | Description |
|--------------|--|
| Solid Red | When the PoE power consumption is between 75% and 100% of the total power (518W), the PoE indicator is steady red |
| Solid Orange | When the PoE power consumption is between 50% and 75% of the total power (518W), the PoE indicator is steady orange. |
| Solid Green | When the PoE power consumption is between 25% and 50% of the total power (518W), the PoE indicator is steady green. |
| Solid Green | When the PoE power consumption is lower than 25% of the total power (518W), the PoE indicator is steady green. |

Link/Act/Speed LED (Ports 1-24):

Ports 1-8 comply with 802.3bt and can supply up to 90 W power to the powered devices (PD). Ports 9-24 comply with 802.3at/af and can supply up to 30 W/15 W power to the powered devices (PD). The Port LED can be switched between the PoE mode and Link Mode. When in Link Mode, the Port LED has the following states:

| LED | Description |
|-----------------|--|
| Solid Orange | An active link operating at 10/100 Mbps on the port. |
| Flashing Orange | The port is transmitting data at 10/100 Mbps. |
| Off | There is no active link on the port. |
| Solid Green | An active link operating at 1000 Mbps on the port. |
| Flashing Green | The port is transmitting data at 1000 Mbps. |

SFP LED (Combo SFP Ports 25-28):

Ports 25-28 are 1000Base-T/SFP combo ports that comply with 802.3ab, 802.3u, and 802.3z.

| LED | Description |
|-----|-------------|
|-----|-------------|

| | |
|-----------------|--|
| Solid Orange | An active link operating at 100 Mbps on the port. |
| Flashing Orange | The port is transmitting data at 100 Mbps. |
| Off | There is no active link on the port. |
| Solid Green | An active link operating at 1000 Mbps on the port. |
| Flashing Green | The port is transmitting data at 1000 Mbps. |

PoE LED (Ports 1- 24):

Ports 1-8 comply with 802.3bt and can supply up to 90 W power to the powered devices (PD). Ports 9-24 comply with 802.3at/af and can supply up to 30 W/15 W power to the powered devices (PD). The Port LED can be switched between the PoE mode and Link Mode. When in PoE Mode, the Port LED has the following states:

| LED | Description |
|----------------|---|
| Solid Green | A PD is connected and consumes power from the Switch. |
| Flashing Green | The port is transmitting power to the PD. |
| Off | There is no PD connected to the port. |

DIP Switch :

The DIP switch is a convenient mechanism to enable or disable the advanced functions of the Switch. The DIP switch is turned off by default. The following describes the functions of the 5 switches:

| LED | Description |
|-----------|---|
| QoS | If the QoS switch is enabled, incoming packets of the controlled ports (ports 1-24) are forwarded according to the port priority based on the assigned port number (with Port 1 having the highest priority). |
| Extend | If the PoE Extend switch is enabled, the enabled PoE ports (ports 1-8) can power devices with 20 W through a 250-meter network cable (Cat 5e or above) at a speed of up to 10 Mbps. |
| Isolation | If the Isolation switch is enabled, the LAN ports (ports 1-24) will be isolated from one another. The LAN ports can only communicate with the uplink SFP ports. |
| PD-Alive | If the PD-Alive is enabled, the PoE ports (ports 1-24) can detect whether the connected PDs are alive and automatically reboot the connected PDs once they become unresponsive. |
| STP | If the STP switch is enabled, the STP function is enabled on the uplink ports (ports 25-28). Network connectivity can be automatically restored through redundant paths in case of a link failure. |

Rear Panel

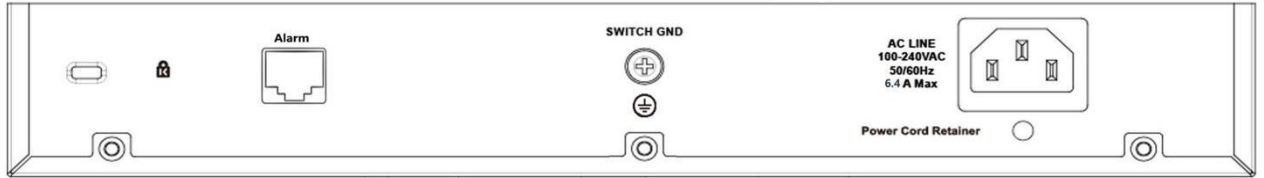


Figure 2-8 DSS-200G-28MPP Rear Panel

Power: Connect the supplied AC power cable to this port.



CAUTION: The SFP ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.



CAUTION: This equipment is to be connected only to PoE networks without routing to the outside plant.

3. Hardware Installation

This chapter provides unpacking and installation information for the D-Link switch.

Step1: Unpacking

Open the shipping carton and carefully unpack its contents. Please consult the packing list located below to make sure all items are present and undamaged. If any item is missing or damaged, please contact your local D-Link reseller for a replacement.

Packing Contents

- One D-Link DSS-200G MP/MPP series switch
- One AC power cord
- Four rubber feet
- Rackmount kit
- One accessory kit for a ground screw
- Quick Installation Guide

Step2: Switch Installation

For safe switch installation and operation, it is recommended that you:

- Visually inspect the power cord to see that it is secured fully to the AC power connector.
- Make sure that there is proper heat dissipation and adequate ventilation around the switch.
- Do not place heavy objects on the switch.

Desktop or Shelf Installation

When installing the switch on a desktop or shelf, the rubber feet included with the device must be attached on the bottom at each corner of the device's base. Allow enough ventilation space between the device and the objects around it.



Figure 3-1 Attach the adhesive rubber pads to the bottom

Rack Installation

The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment.



CAUTION: Ensure the power cable is disconnected before installing the switch.

To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided.



Figure 3-2 Attach the mounting brackets to the switch

Then, use the screws provided with the equipment rack to mount the switch in the rack.

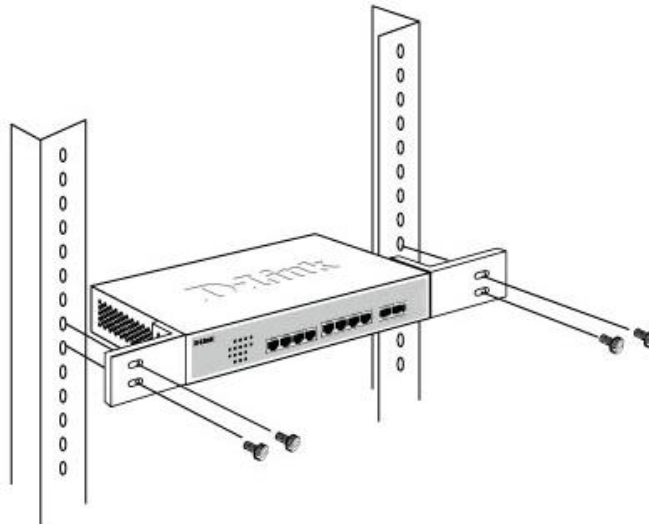


Figure 3-3 Mount the switch in the rack or chassis

Please be aware of following safety Instructions when installing:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

Step 3: Plugging in the AC Power Cord

Users may now connect the AC power cord into the rear of the switch and to an electrical outlet (preferably one that is grounded and surge protected).

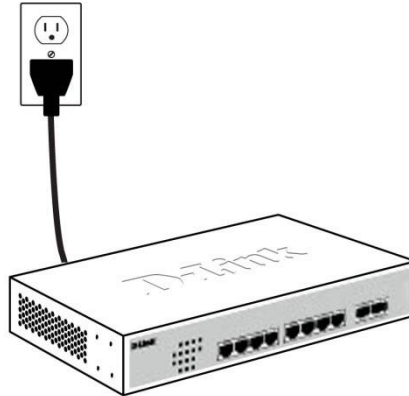


Figure 3-4 Plugging the switch into an outlet

Power Failure

As a precaution, the switch should be unplugged in case of power failure. When power is resumed, the switch should be plugged back in.

Grounding the Switch

This section describes how to connect the DSS-200G MP/MPP series switch to ground. You must complete this procedure before powering your switch.

Required Tools and Equipment

- Ground screws (included in the accessory kit): One M4 x 8 mm (metric) pan-head screw
- Ground cable (not included in the accessory kit): The grounding cable should be sized according to local and national installation requirements. Depending on the power supply and system, a 12 to 6 AWG copper conductor is required for U.S installation. Commercially available 6 AWG wire is recommended. The length of the cable depends on the proximity of the switch to proper grounding facilities.
- A screwdriver (not included in the accessory kit)

Follow these steps to ground the switch:

Step 1: Verify that the switch is not connected to a power supply.

Step 2: Use the ground cable to place the #8 terminal lug ring on top of the ground-screw opening, as seen in the figure below.

Step 3: Insert the ground screw into the ground-screw opening.

Step 4: Using a screwdriver, tighten the ground screw to secure the ground cable to the switch.

Step 5: Attach the terminal lug ring at the other end of the grounding cable to an appropriate grounding stud or bolt on rack where the switch is installed.

Step 6: Verify if the connections at the ground connector on the switch and the rack are securely attached.

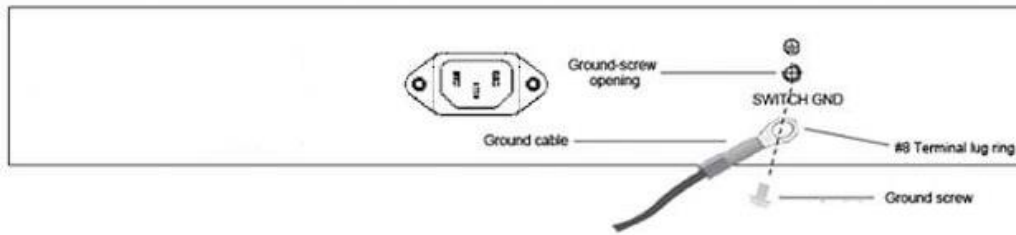


Figure 3-5 Ground cable, screw and #8 terminal lug rings



CAUTION: This equipment is to be connected only to PoE networks without routing to the outside plant.

Connecting the Alarm Cable

The system can send out alarms through system logs and traps and it can also trigger an alarm device such as a siren. The alarm port activates alarms when the front Alert LED flashes due to PoE malfunctioning events. The alarm port has an RJ45 connector; however, its pinout is not the same as the common RJ45 connector for connecting a network cable. Only the first 2 pins (of the 8 pins) can be used to connect to the alarm device.

Connecting the PoE Cable

The DSS-200G MP/MPP Series switches support the IEEE 802.3af and 802.3at Power over Ethernet (PoE) standards. The DSS-200G MPP Series also support the IEEE 802.3bt standard.

The ports and power ratings per switch are as follows:

| Switch Model | Port Numbers | Power Rating |
|----------------|-----------------|--------------|
| DSS-200G-10MP | 1 - 8 | 30 W |
| DSS-200G-10MPP | 1 - 8 | 90 W |
| DSS-200G-28MP | 1 - 24 | 30 W |
| DSS-200G-28MPP | 1 - 8 9 - 24 | 90 W 30 W |

Power can be supplied at 48VDC to Powered Devices (PDs) over Category 5 or Category 6 UTP Ethernet cables. The switches follow the standard PSE (Power Sourcing Equipment) pinout *Alternative B*.

The DSS-200G MP/MPP Series switches include the following PoE features:

- Auto-discovery recognizes the connection of a PD (Powered Device) and automatically sends power to it.
- The Auto-disable feature occurs under two conditions: firstly, if the total power consumption exceeds the system power limit; and secondly, if the per port power consumption exceeds the per port power limit.
- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

Based on 802.3af/at/bt PDs receive power according to the following classification:

PSE provides power according to the following classification:

| Class | Maximum power used by PD |
|-------|--------------------------|
| 0 | 12.95W |
| 1 | 3.84W |
| 2 | 6.49W |
| 3 | 13 W |
| 4 | 25.5W |
| 5 | 40 W |
| 6 | 51 W |
| 7 | 62 W |
| 8 | 71.3 W |

| Class | Max power supplied by PSE |
|-------|---------------------------|
| 0 | 16.2W |
| 1 | 4 W |
| 2 | 7 W |
| 3 | 15.4 W |
| 4 | 30 W |
| 5 | 45 W |
| 6 | 60 W |
| 7 | 90 W |

PoE Ports Signal Definition:

The DSS-200G MP/MPP Series switches power through the pin as follows:

- DSS-200G-10MP: Front 4 ports (ports 1-4): Pin 1/2&4/5 are positive (V+), Pin 3/6&7/8 are negative (V-); For the last four ports (ports 5-8): Pin 4/5 is positive (V+) and Pin 7/8 is negative (V-) (compliant with 802.3at).
- DSS-200G-10MPP: Pin 3/6&4/5 positive (V+), 1/2&7/8 negative (V-) (compliant with 802.3bt).
- DSS-200G-28MP: Front 8 ports (ports 1-8): Pin 1/2&4/5 is positive (V+) and Pin 3/6&7/8 is negative (V-); For the last 16 ports (ports 9-24), Pin 4/5 is positive and Pin 7/8 is negative (compliant with 802.3at).
- DSS-200G-28MPP: Front 8 ports (ports 1-8): Pin 3/6&4/5 are positive (V+) and Pin 1/2&7/8 are negative (V-) (compliant with 802.3bt); For the last 16 ports (ports 9-24), Pin 4/5 is positive (V+) and Pin 7/8 is negative (V-) (compliant with 802.3at).

DSS-200G-10MP / DSS-200G-28MP

DSS-200G-10MP (ports 1-8) / DSS-200G-28MP (ports 1-24): These ports support 802.3af/at to provide a maximum of 15 W or 30 W power supply to the connected PDs. In addition, DSS-200G-10MP (ports 1-4) and DSS-200G-28MP (ports 1-8) can also be configured to support PoE up to a maximum of 20 W with an extended distance using a network cable (250 meters) at the speed of 10 Mbps. The pin assignments for these ports are as follows:

| Contact | MDI | PoE 802.3at | PoE with 8-core Power Supply |
|---------|-----------------|-------------|------------------------------|
| 1 | TD+ (transmit) | | DC+ |
| 2 | TD - (transmit) | | DC+ |
| 3 | RD+ (receive) | | DC- |
| 4 | 1000BASE-T | DC+ | DC+ |
| 5 | 1000BASE-T | DC+ | DC+ |
| 6 | RD - (receive) | | DC- |
| 7 | 1000BASE-T | DC- | DC- |
| 8 | 1000BASE-T | DC- | DC- |

DSS-200G-10MPP / DSS-200G-28MPP

DSS-200G-10MPP (ports 1-8) / DSS-200G-28MPP (ports 1-24): Ports 1-8 of DSS-200G-10MPP and DSS-200G-28MPP support 802.3bt to provide a maximum of 90 W power supply to the connected

PDs. Whereas Ports 9-24 of DSS-200G-28MPP support 802.3af/at to provide 15 W or 30 W power supply to the connected PDs.

In addition, DSS-200G-10MPP (ports 1-8) and DSS-200G-28MPP (ports 1-8) can also be configured to support PoE up to a maximum of 20 W with an extended distance using a network cable (250 meters) at the speed of 10 Mbps. The pin assignments for these ports are as follows:

| Contact | MDI | PoE 802.3at | 802.3bt |
|---------|-----------------|-------------|---------|
| 1 | TD+ (transmit) | | DC- |
| 2 | TD - (transmit) | | DC- |
| 3 | RD+ (receive) | | DC+ |
| 4 | 1000BASE-T | DC+ | DC+ |
| 5 | 1000BASE-T | DC+ | DC+ |
| 6 | RD - (receive) | | DC+ |
| 7 | 1000BASE-T | DC- | DC- |
| 8 | 1000BASE-T | DC- | DC- |

4. Web-based Switch Configuration

Management Options

Connecting using the Web User Interface

Logging onto the Web User Interface

Smart Wizard

Web User Interface – Standard Mode

Management Options

The switch provides multiple access platforms that can be used to configure, manage and monitor networking features available on the switch. Currently there are three management platforms available and they are described below.

Web-based Management Interface

After successfully installing the switch, the user can configure the switch, monitor the LED panel, and display statistics graphically using a Web browser, such as Microsoft® Internet Explorer, Opera Firefox, Safari, or Google Chrome.

SNMP-based Management

The switch can be managed with an SNMP-compatible console program. The switch supports SNMP version 1.0, and version 2c. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Connecting using the Web User Interface

Most software functions of the DSS-200G MP/MPP series switches can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the switch from remote stations anywhere on the network through a standard web browser. The web browser acts as a universal access tool and can communicate directly with the switch using the HTTP or HTTPS protocol.

You need the following equipment to begin the web configuration of your device:

- A PC with a RJ-45 Ethernet connection
- A standard Ethernet cable



Figure 4-1 Connecting to a DSS-200G MP/MPP series switch

Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.

Logging onto the Web User Interface

To access the Web UI, simply open a web browser and enter the switch's default IP address into the address bar. Make sure that the IP address of the management PC is in the same subnet as the IP address of the switch you are trying to connect to.



NOTE: The default IP address of the switch is **10.90.90.90**, with a subnet mask of **255.0.0.0**.



NOTE: The default username is '**admin**' and password is '**admin**'.

After successfully connecting to the Web UI, the Smart Wizard will be launched.

Smart Wizard

The Smart Wizard is a configuration utility that is launched the first time the Web UI is accessed. It allows users to configure basic settings such as the switch mode, management IP and password. It can also be used to switch between Standard Mode and Surveillance Mode Web UI types.

Step 1 – Web Mode

The initial page allows the user to choose between Standard Mode and Surveillance Mode on the switch. This can be changed at any time by returning to the Smart Wizard.

For more information on the Surveillance Mode features of the switch, please refer to the **Web User Interface – Surveillance Mode** section.

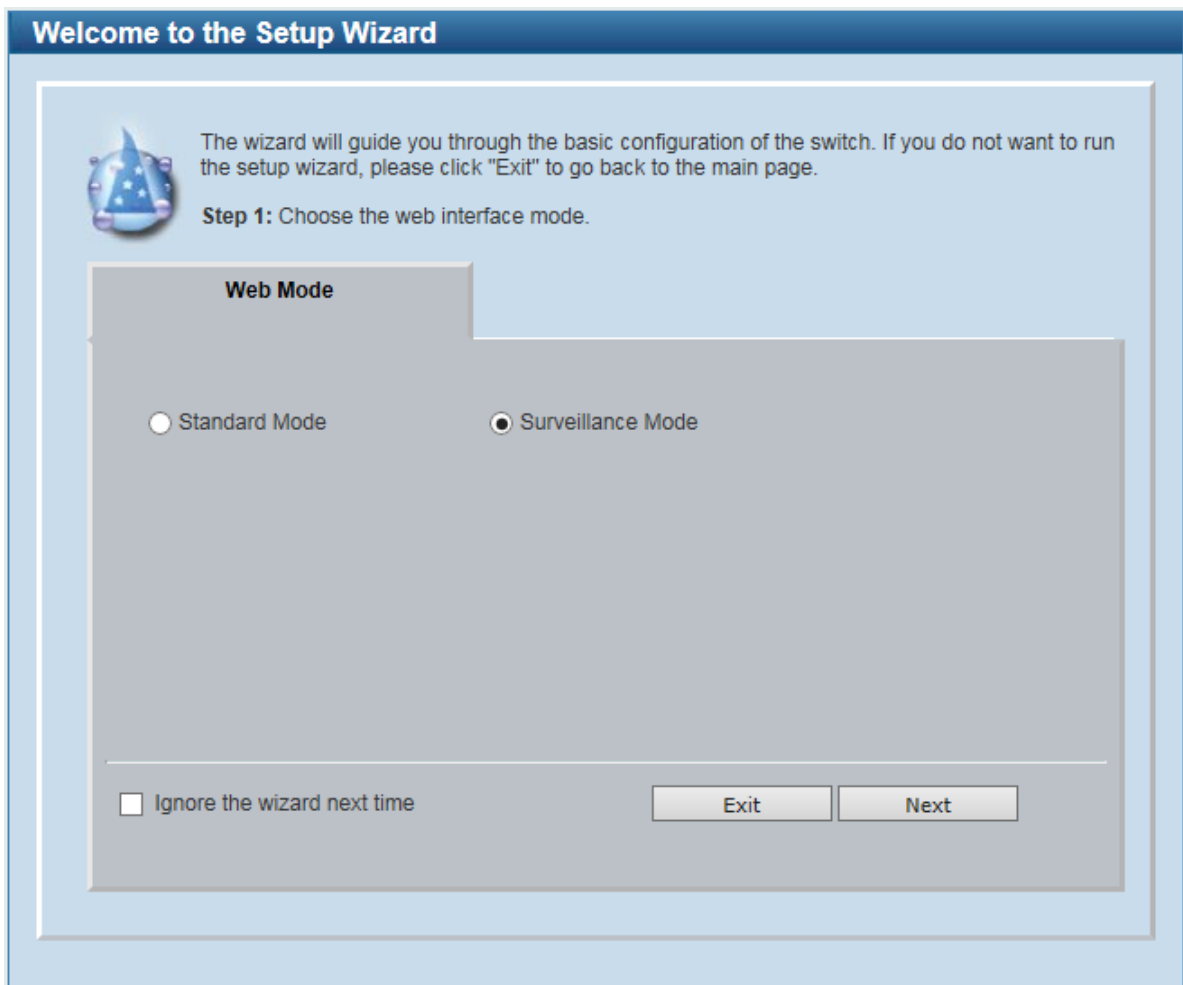


Figure 4-2 Web Mode window

The fields that can be configured are described below:

| Parameter | Description |
|-----------------|--|
| Web Mode | Select the Surveillance Mode option to continue the Smart Wizard in Surveillance Mode. Please refer to the Standard Mode Web UI Reference Guide for more information on Standard Mode. |

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Standard Mode Web UI.

Click the **Next** button to accept the changes made and continue to the next step.

Step 2 – System IP Information

In this window, the user can configure the IP address assignment method, the static IP address, net mask and gateway address.



NOTE: The switch will probe IP cameras every 30 seconds. If an IP camera is not in the same subnet as the switch, the IP camera will not be automatically discovered. Place the switch management IP in the same subnet as the IP cameras for the cameras to be automatically added to the Surveillance Mode Web UI.

Figure 4-3 System IP Information window

The fields that can be configured are described below:

| Parameter | Description |
|-------------------|--|
| Static | Select this option to manually configure and use IP address settings on this switch. |
| DHCP | Select this option to obtain IP address settings from a DHCP server. |
| IP Address | Enter the IP address of the switch here. |
| Netmask | Select the net mask option here. |
| Gateway | Enter the default gateway IP address here. |

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Standard Mode Web UI.

Click the **Next** button to accept the changes made and continue to the next step.

Step 3 – Password

In this window, the user can set the password used with the admin account.

The screenshot shows a web-based configuration window titled "Welcome to the Setup Wizard". The main content area is titled "Step 3: Set the password for admin access." and contains a "Password" section with two input fields: "Password" and "Confirm Password". At the bottom of the window, there is a checkbox labeled "Ignore the wizard next time" and three buttons: "Exit", "Back", and "Apply & Save".

Figure 4-4 Admin Password window

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Standard Mode Web UI.

Click the **Apply & Save** button to accept the changes made, and then continue to the Web UI.



NOTE: Standard Mode and Surveillance Mode Web UIs share the same configuration files. Any features enabled in one interface will be made available in the other interface, for example: PoE scheduling, SNMP settings and the surveillance VLAN in use.



NOTE: Settings are saved between interface types. It is possible to switch interface types and re-run the Smart Wizard without losing settings saved in one version of the interface.

Web User Interface – Standard Mode

By clicking the **Exit** button in the Smart Wizard, you will enter the Web-based Management interface.

Areas of the User Interface

The figure below shows the user interface. Two distinct areas divide the user interface, as described in the table.

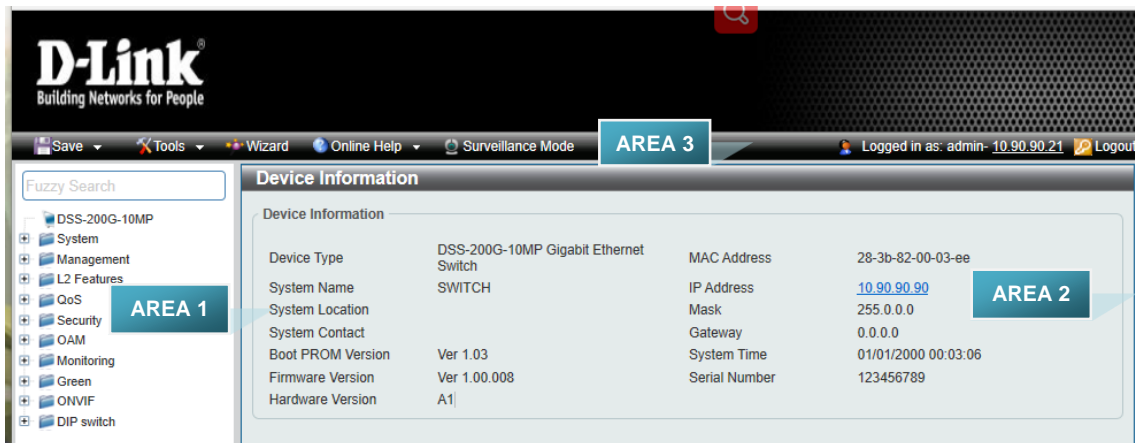


Figure 4-5 Main Web UI window

| Area Number | Description |
|-------------|--|
| AREA 1 | The navigation menu is displayed in this area. Click on the links and navigate the folder structure to display information on the main page. |
| AREA 2 | This is the main page for displaying information and configuration options for the switch. The page displayed here is based on the selection in AREA 1 . |
| AREA 3 | This area displays a toolbar used to access Save and Tools menus. It also provides access to the Setup Wizard and selection between Surveillance and Standard Mode . |

Device Information

Device information such as firmware version, MAC address and serial number are displayed in this window. It appears automatically when you log in to the switch. To return to the Device Information window after viewing other windows, click the model number of the switch at the top of the navigation menu.

| Device Information | | | |
|--------------------|---------------------------------------|---------------|-----------------------------|
| Device Information | | | |
| Device Type | DSS-200G-10MP Gigabit Ethernet Switch | MAC Address | 28-3b-82-00-03-ee |
| System Name | SWITCH | IP Address | 10.90.90.90 |
| System Location | | Mask | 255.0.0.0 |
| System Contact | | Gateway | 0.0.0.0 |
| Boot PROM Version | Ver 1.03 | System Time | 01/01/2000 00:03:06 |
| Firmware Version | Ver 1.00.008 | Serial Number | 123456789 |
| Hardware Version | A1 | | |

Figure 4-6 Devie Info

System

System Information Settings

Port Configuration

PoE

System Log

Time

Time Range

System Information Settings

System Information

The user can enter a System Name, System Location, and System Contact to aid in defining the switch.

To view the following window, click **System > System Information Settings > System Information**, as shown below:

| System Information | |
|--------------------------------------|---------------------------------------|
| System Information | |
| System Name | <input type="text" value="SWITCH"/> |
| System Location | <input type="text" value="32 chars"/> |
| System Contact | <input type="text" value="32 chars"/> |
| <input type="button" value="Apply"/> | |

Figure 4-7 System Information window

The fields that can be configured are described below:

| Parameter | Description |
|------------------------|--|
| System Name | Enter a system name for the switch, if so desired. This name will identify it on the switch network. |
| System Location | Enter the location of the switch, if so desired. |
| System Contact | Enter a contact name for the switch, if so desired. |

Click the **Apply** button to accept the changes made.

IPv4 Interface

This window is used to configure the IPv4 settings of the switch.

To view the following window, click **System > System Information Settings > IPv4 Interface**, as shown below:

Figure 4-8 Peripheral Settings window

The fields that can be configured are described below:

| Parameter | Description |
|-------------------------------|--|
| Get IP From | Select DHCP to automatically obtain an IP address. Select Static to manually configure the IP address settings. BOOTP allows the switch to get an IP configuration using the BOOTP protocol. |
| IP Address | If Static is selected, enter the IP address of the switch. If DHCP or BOOTP is selected, the automatically obtained IP address will be displayed. |
| Mask | If Static is selected, enter the IP address of the switch. If DHCP or BOOTP is selected, the automatically obtained network mask will be displayed. |
| Gateway | If Static is selected, enter the IP address of the switch. If DHCP or BOOTP is selected, the automatically obtained gateway will be displayed. |
| DHCP Retry Time(5-120) | If DHCP is selected, enter the number of times to retry obtaining an IP address. |

Click the **Apply** button to accept the changes made.

IPv6 Interface

This window is used to configure the IPv6 settings of the switch.

To view the following window, click **System > System Information Settings > IPv6 Interface**, as shown below:

Figure 4-9 Peripheral Settings window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| IPv6 State | Select whether to Enable or Disable IPv6 functionality. |
| Static IPv6 Address | If enabled, enter the static IPv6 address of the switch. |

Click the **Apply** button to accept the changes made.

Port Configuration

Port Settings

This window is used to view and configure the switch's port settings.

To view the following window, click **System > Port Configuration > Port Settings**, as shown below:

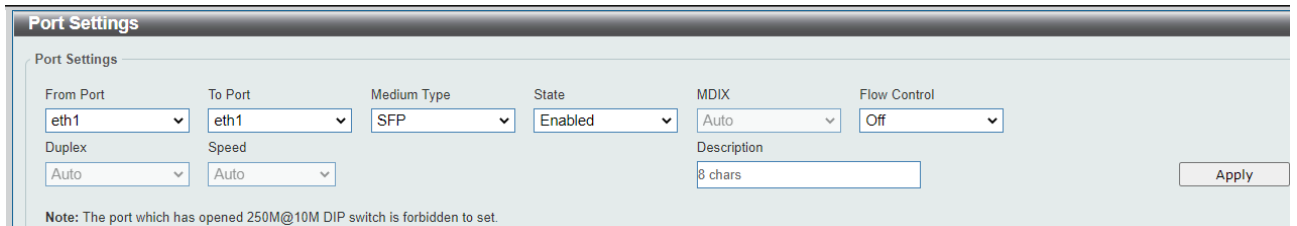


Figure 4-10 Port Settings window

Note: Ports that support PoE Extent cannot be configured if the Dip Switch on the front panel has been turned on.

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| Medium Type | Select the port type to RJ45 or SFP. |
| State | Select this option to enable or disable the physical port here. |
| MDIX | Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are Auto , Normal , and Cross . Auto - Select this option for auto-sensing of the optimal type of cabling. Normal - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC's NIC using a straight-through cable or a port (in the MDIX mode) on another switch through a cross-over cable. Cross - Select this option for cross cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another switch through a straight cable. |
| Flow Control | Select to either turn flow control On or Off here. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use back-pressure flow control, and Auto ports use an automatic selection of the two. |
| Duplex | Select the duplex mode used here. Options to choose from are Auto , Half , and Full . |
| Speed | Select the port speed option here. This option will manually force the connected on the selected port to only connect at the speed specified here. Options to choose from are Auto , 10M , 100M . 1000M speed is only available when Auto is selected. |
| Description | Enter a 8 characters description for the corresponding port here. |

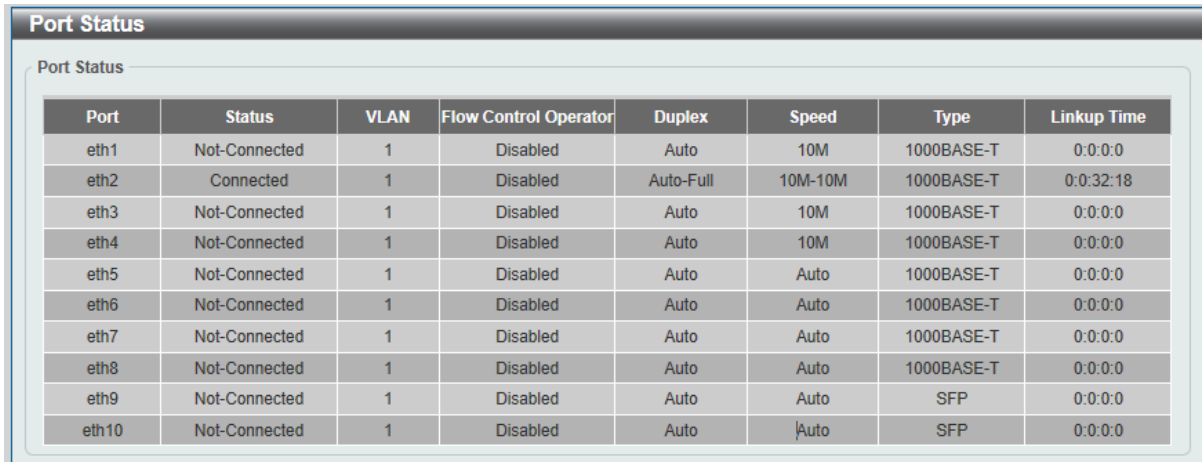
Click the **Apply** button to accept the changes made.

Note: The SFP ports on the DSS-200G MP/MPP series only support **Auto** for duplex and speed. Also, the fiber ports on the DSS-200G MP/MPP series does not support MDIX.

Port Status

This window is used to view switch port status.

To view the following window, click **System > Port Configuration > Port Status**, as shown below:



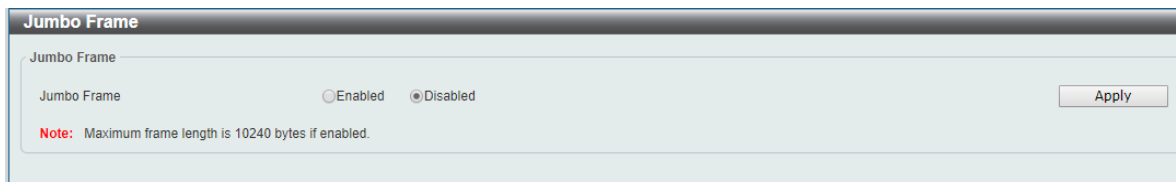
| Port | Status | VLAN | Flow Control Operator | Duplex | Speed | Type | Linkup Time |
|-------|---------------|------|-----------------------|-----------|---------|------------|-------------|
| eth1 | Not-Connected | 1 | Disabled | Auto | 10M | 1000BASE-T | 0:0:0:0 |
| eth2 | Connected | 1 | Disabled | Auto-Full | 10M-10M | 1000BASE-T | 0:0:32:18 |
| eth3 | Not-Connected | 1 | Disabled | Auto | 10M | 1000BASE-T | 0:0:0:0 |
| eth4 | Not-Connected | 1 | Disabled | Auto | 10M | 1000BASE-T | 0:0:0:0 |
| eth5 | Not-Connected | 1 | Disabled | Auto | Auto | 1000BASE-T | 0:0:0:0 |
| eth6 | Not-Connected | 1 | Disabled | Auto | Auto | 1000BASE-T | 0:0:0:0 |
| eth7 | Not-Connected | 1 | Disabled | Auto | Auto | 1000BASE-T | 0:0:0:0 |
| eth8 | Not-Connected | 1 | Disabled | Auto | Auto | 1000BASE-T | 0:0:0:0 |
| eth9 | Not-Connected | 1 | Disabled | Auto | Auto | SFP | 0:0:0:0 |
| eth10 | Not-Connected | 1 | Disabled | Auto | Auto | SFP | 0:0:0:0 |

Figure 4-11 Port Status window

Jumbo Frame

This window is used to view and configure the Jumbo Frame size and settings. The switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1,518 bytes of payload. The switch supports jumbo frames with a maximum frame size of up to 10240 bytes.

To view the following window, click **System > Port Configuration > Jumbo Frame**, as shown below:



Jumbo Frame

Jumbo Frame Enabled Disabled

Note: Maximum frame length is 10240 bytes if enabled.

Figure 4-12 Jumbo Frame window

The fields that can be configured are described below:

| Parameter | Description |
|-------------|---|
| Jumbo Frame | Select whether to Enable or Disable support for Jumbo Frames on the switch. |

Click the **Apply** button to accept the changes made.

PoE

PoE System

This window is used to configure the PoE system and display the detailed power information and PoE Trap parameters for PoE modules.

To view the following window, click **System > PoE > PoE System**, as shown below:

| Power Budget (W) | Delivered (W) | Usage Threshold (%) | Trap State |
|------------------|---------------|---------------------|------------|
| 370 | 0.0 | 99 | Disabled |

Figure 4-13 PoE System window

The fields that can be configured are described below:

| Parameter | Description |
|------------------------|---|
| Usage Threshold | Enter the usage threshold to generate a log and send the corresponding standard notification. |
| Trap State | Select this option to enable or disable the sending of PoE notifications. |

Click the **Apply** button to accept the changes made.

PoE Configuration

This window is used to configure the PoE port.

To view the following window, click **System > PoE > PoE Configuration**, as shown below:

Figure 4-14 PoE Configuration window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| Priority | Select the priority for provisioning power to the port. Options to choose from are Critical , High and Low . |
| State | Select this option to enable or disable the PoE functionality. Options to choose from are Disabled or Enabled . |
| 4-Pair State | Enable or disable the 8-core power supply using the 4 pairs of the Ethernet cable: Null, Disabled, 60 W enabled, or 90 W enabled. |

| | |
|---------------------------------|--|
| | Note: For the Null option, specify the Power Limit level or enter the Max Wattage as described below manually. The 60 W and 90 W options are only available for models and the respective ports that support 802.3bt. |
| Power Limit | Select the power management mode for the PoE ports. Options to choose from are Auto , Class 1 , Class 2 , Class 3 , and Class 4 . Auto means 30,000, Class 1 means 4000, Class 2 means 7000, Class 3 means 16000, and Class 4 means 30,000 mW power limit. |
| 4-Pair State | Enable or disable the 8-core power supply using the 4 pairs of the Ethernet cable: Null, Disabled, 60 W enabled, or 90 W enabled. Note: For the Null option, specify the Power limit level or enter the Max Wattage below manually. |
| Max Wattage (1000-30000) | When selecting Auto in the Mode drop-down list, this option appears. Tick the check box and enter the maximum wattage of power that can be provisioned to the auto-detected PD. If the value is not entered, the class of the PD automatically determines the maximum wattage which can be provisioned. The valid range for maximum wattage is between 1000 mW and 30000 mW. |
| Time Range | Select the Time range from the drop down list. Note: The Time range drop down menu will only have available options if a time range has been created. |

Click the **Delete Time Range** button to clear the setting in the corresponding Time Range field.

Click the **Apply** button to accept the changes made.

Note: The **Max Wattage** option will only be available if the check box next to the input field is enabled. When enabled, the Power Limit drop down menu will not be available.

Note: If the switch failed to supply power to the IEEE 802.3at/bt PD (Powered Device):

1. Check if the PD connected to the port supports the IEEE 802.3at/bt standard.
2. Manually configure the corresponding port's power limit value to 30, 60 or 90 Watts according to the port's PoE capability.

PD Alive

This window is used to configure the PD Alive function for PDs connected to the PoE ports. The ping function is used to check if PDs, connected to the PoE ports, are active or not. When PDs appear to be inactive, the specified action (Reboot, Notify, or Both) will be taken.

To view the following window, click on the **System > PoE > PD Alive Configuration** enters the navigation menu:

PD Alive

PD Alive Configuration

From Port: eth1 To Port: eth1 PD Alive State: Disabled PD IP Address:

Poll Interval (10-300): 30 sec Retry Count (0-5): 2 Waiting Time (30-300): 90 sec Action: Both

Apply

| Port | PD Alive State | PD IP Address | Poll Interval | Retry Count | Waiting Time | Action |
|------|----------------|---------------|---------------|-------------|--------------|--------|
| eth1 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth2 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth3 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth4 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth5 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth6 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth7 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth8 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |

Figure 4-15 PD Alive Configuration window

The fields that can be configured are described below:

| Parameter | Description |
|-------------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| PD Alive State | Select to enable or disable the PD Alive function on the specified port(s). Note that a port's PD Alive state cannot be disabled if the DIP Switch on the front panel has been turned on. |
| PD IP Address | Enter the IP address of the PD here. |
| Pool interval (10-300) | Enter the poll interval here. This is the interval between ping messages from the system to PDs connected to the PoE port(s). The range is from 10 to 300 seconds. |
| Retry Count (0-5) | Enter the retry count here. This is the amount of ping messages that will be sent (at each interval) when PDs are not responding. The range is from 0 to 5. |
| Waiting Time (30-300) | Enter the waiting time here. This is how long the system will wait before sending ping messages to the PD connected to the PoE port after a 'Reset' action was taken. The range is from 30 to 300 seconds. |
| Action | Select the action that will be taken here. Options to choose from are Reset , Notify , and Both . Reset - Specifies to reset the PoE port state (turn PoE off and on). Notify - Specifies to send logs and traps to notify the administrator. Both - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on). |

Click the **Apply** button to accept the changes made.

System Log

System Log Settings

This window is used to view and configure the system's log settings.

To view the following window, click **System > System Log > System Log Settings**, as shown below:

Figure 4-16 System Log Settings window

The fields that can be configured for **Global State** are described below:

| Parameter | Description |
|-------------------|---|
| System Log | Select this option to enable or disable the System Log functionality. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Buffer Log Settings** are described below:

| Parameter | Description |
|-------------------------|---|
| Buffer Log State | Select this option to enable or disable the Buffer Log State. |

Click the **Apply** button to accept the changes made.

System Log Server Settings

This window is used to view and configure system log's server settings.

To view the following window, click **System > System Log > System Log Server Settings**, as shown below:

Figure 4-17 System Log Server Settings window

The fields that can be configured are described below:

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

| | |
|----------------------------------|--|
| Host IPv4 Address | Enter the system log server's IPv4 address here. |
| UDP Port (514,1024-65535) | Enter the system log server's UDP port number here. This value must be 514 or between 1024 and 65535. |
| Facility | Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local 0 to Local 7). |
| Severity | Select the severity value of the type of information that will be logged. Options to choose from are Warning, informational, and All The possible levels are: Warning - The lowest level of a device warning. The device is functioning, but an operational problem has occurred. Informational - Provides device information. All - Displays all levels of system logs. |

Click the **Apply** button to accept the changes made.

System Log

This window is used to view and clear the system log.

To view the following window, click **System > System Log > System Log**, as shown below:

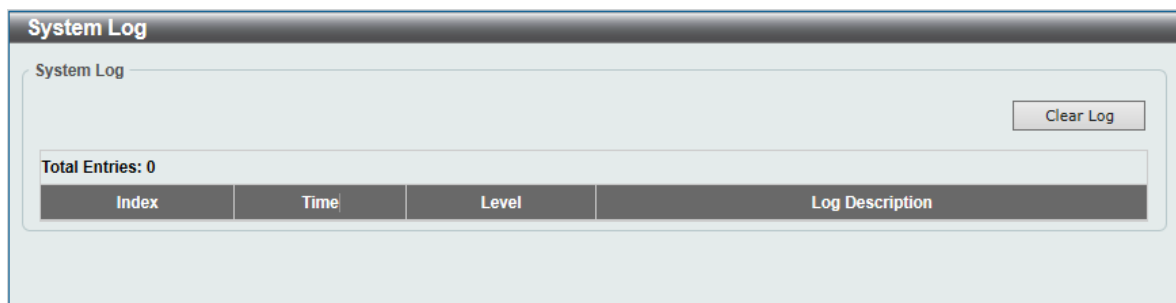


Figure 4-18 System Log window

Click the **Clear Log** button to clear the system log entries displayed in the table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Time

The Simple Network Time Protocol (SNTP) is a protocol for system clock synchronization through the Internet.

Clock Settings

This window is used to configure the time settings for the switch manually.

To view the following window, click **System > Time > Clock Settings**, as shown below:

Figure 4-19 Clock Settings window

The fields that can be configured are described below:

| Parameter | Description |
|------------------------------|--|
| Time (HH:MM:SS) | Enter the current time in hours, minutes, and seconds. |
| Date (DD / MM / YYYY) | Enter the current day, month, and year to update the system clock. |

Click the **Apply** button to accept the changes made.

Time Zone Settings

This window is used to configure time zones and Daylight Savings Time settings for SNTP.

To view the following window, click **System > Time > Time Zone Settings**, as shown below:

Figure 4-20 Time Zone Settings window

The fields that can be configured are described below:

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

| | |
|--------------------------|--|
| Summer Time State | Select the summer time setting. Options to choose from are Disabled , and Date Setting . Disabled - Select to disable the summer time setting. Date Setting - Select to configure the summer time that should start and end on the specified date. |
| Time Zone | Select to specify your local time zone's offset from Coordinated Universal Time (UTC). |

The fields that can be configured for **Date Setting** are described below:

| Parameter | Description |
|--------------------------------|---|
| From: Date of the Month | Select date of the month that summer time will start. |
| From: Month | Select the month that summer time will start. |
| From: Time (HH:MM) | Select the time of the day that summer time will start. |
| To: Date of the Month | Select date of the month that summer time will end. |
| To: Month | Select the month that summer time will end. |
| To: Time (HH:MM) | Select the time of the day that summer time will end. |
| Offset | Enter the number of minutes to add during summer time. The default value is 30. The range of this offset is 30, 60, 90 and 120. |

Click the **Apply** button to accept the changes made.

SNTP Settings

This window is used to configure the time settings for the switch.

To view the following window, click **System > Time > SNTP Settings**, as shown below:

Figure 4-21 SNTP Settings window

The fields that can be configured for **SNTP Global Settings** are described below:

| Parameter | Description |
|---------------------------------|---|
| Current Time Source | This will indicate the current time source and will change from System Clock to SNTP when SNTP is configured and functioning. |
| SNTP State | Select this option to enable or disable SNTP. |
| Poll Interval (30-99999) | Select the Poll Interval range from 30 to 99999. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for **SNTP Server Setting** are described below:

| Parameter | Description |
|---------------------|---|
| Server | You can configure information about the primary and backup servers that provide clock services. |
| IPv4 Address | Enter the IP address of the SNTP server which provides the clock synchronization. |

Click the **Apply** button to add the SNTP server.

Time Range

This window is used to view and configure the time range settings. The maximum number of time profiles supported by the switch is 8.

To view the following window, click **System > Time range**, as shown below:

Figure 4-22 Time range window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| Range Name | Enter the name of the time range. This name can be up to 8 characters long. |
| Days | Select the days of the week that will be used for this time range. Tick the Daily option to use this time range for every day of the week. |
| From Time / To Time | Select the starting and ending time of the day that will be used for this time range. The first drop-down menu selects the hour and the second drop-down menu selects the minute. |

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Management

User Account Settings

SNMP

HTTP/HTTPS

D-Link Discovery Protocol

User Account Settings

This window is used to configure the user accounts. The active user account sessions can be viewed.

There are several configuration options available in the Web User Interface (Web UI). The set of configuration options available to the user depends on the account's **Privilege Level**.



NOTE: By default, the admin account is created on the switch.

To view the following window, click **Management > User Account Settings**, as shown below:

| User Name | Privilege | Password | |
|-----------|------------|----------|--------|
| admin | Read-Write | ***** | Delete |
| user | Read-Only | ***** | Delete |

Figure 4-23 User Account Settings window

The fields that can be configured are described below:

| Parameter | Description |
|------------------|---|
| User Name | Select the user account name here. |
| Password | Enter the password for the account here. The password must contain 8 to 30 characters and include both letters and numbers. |

Click the **Apply** button to accept the changes made.

Note: Only one user can be logged into the switch at any time.

SNMP

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch supports the SNMP versions 1, and 2c. The two versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v2c, user authentication is accomplished using 'community string', which function like passwords. The remote user SNMP application and the switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

Traps

Traps are messages that alert network personnel of events that occur on the switch. The events can be as serious as a reboot (someone accidentally turned OFF the switch), or less serious like a port status change. The switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, and Topology Change.

MIBs

The switch in the Management Information Base (MIB) stores management and counter information. The switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the switch also supports its own proprietary enterprise MIB as an extended Management Information Base. Specifying the MIB Object Identifier may also retrieve the proprietary MIB. MIB values can be either read-only or read-write.

The switch supports the Simple Network Management Protocol (SNMP) versions 1, and 2c. The administrator can specify the SNMP version used to monitor and control the switch.

SNMP settings are configured using the menus located on the SNMP folder of the Web manager. Workstations on the network that are allowed SNMP privileged access to the switch can be restricted with the Management Station IP Address menu.

SNMP Global Settings

This window is used to configure the SNMP global settings and trap settings.

To view the following window, click **Management > SNMP > SNMP Global Settings**, as shown below:

Figure 4-24 SNMP Global Settings window

The fields that can be configured for **SNMP Global Settings** are described below:

| Parameter | Description |
|--------------------------|---|
| SNMP Global State | Select this option to enable or disable the SNMP feature. |

The fields that can be configured for **Trap Settings** are described below:

| Parameter | Description |
|---------------------------------|--|
| Trap Global State | Select this option to enable or disable the sending of all or specific SNMP notifications. |
| SNMP Authentication Trap | Tick this option to control the sending of SNMP authentication failure notifications. |
| Port Link Up | Tick this option to control the sending of port link up notifications. |
| Port Link Down | Tick this option to control the sending of port link down notifications. |
| Coldstart | Tick this option to control the sending of Cold Start notifications. |
| Warmstart | Tick this option to control the sending of Warm Start notifications. |

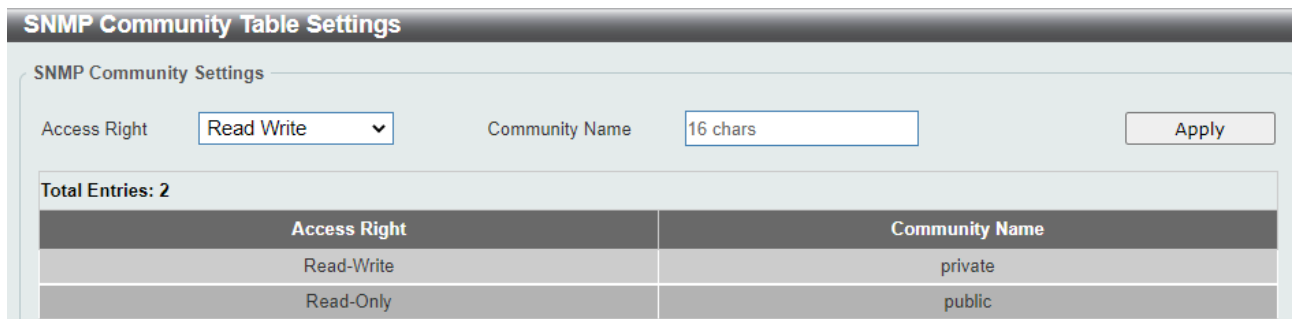
Click the **Apply** button to accept the changes made.

SNMP Community Table Settings

This window is used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the switch. One or more of the following characteristics can be associated with the community string:

- Read-write or Read-only level permission for the MIB objects accessible to the SNMP community.

To view the following window, click **Management > SNMP > SNMP Community Table Settings**, as shown below:



The screenshot shows the 'SNMP Community Table Settings' window. At the top, there is a section for 'SNMP Community Settings' with an 'Access Right' dropdown set to 'Read Write' and a 'Community Name' field containing '16 chars'. An 'Apply' button is located to the right. Below this is a table with the heading 'Total Entries: 2'. The table has two columns: 'Access Right' and 'Community Name'. The first row shows 'Read-Write' and 'private', and the second row shows 'Read-Only' and 'public'.

| Access Right | Community Name |
|--------------|----------------|
| Read-Write | private |
| Read-Only | public |

Figure 4-25 SNMP Community Table Settings window

The fields that can be configured are described below:

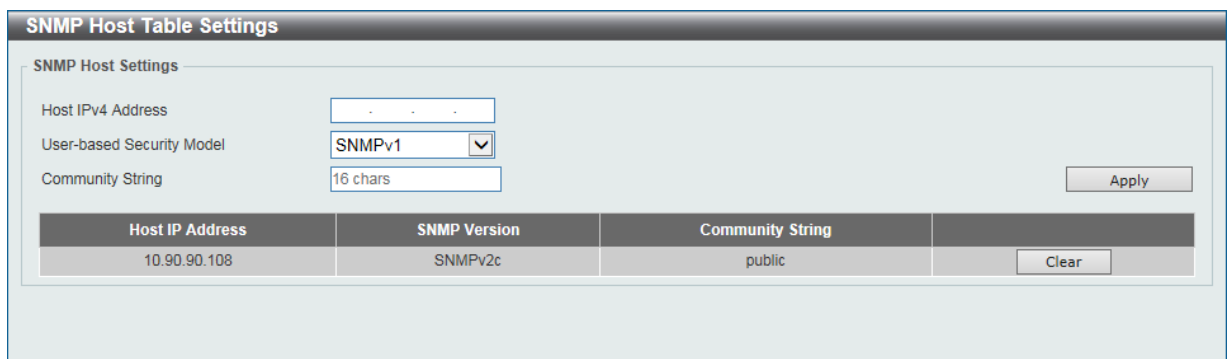
| Parameter | Description |
|-----------------------|--|
| Access Right | Select the access right here. Options to choose from are Read Only and Read Write . Read Only - SNMP community members using the community string created can only read the contents of the MIBs on the switch. Read Write -SNMP community members using the community string created can read from and write to the contents of the MIBs on the switch. |
| Community Name | Enter an alphanumeric string of up to 16 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the switch's SNMP agent. |

Click the **Apply** button to accept the changes made.

SNMP Host Table Settings

This window is used to configure and display the recipient of the SNMP notification.

To view the following window, click **Management > SNMP > SNMP Host Table Settings**, as shown below:



The screenshot shows the 'SNMP Host Table Settings' window. It has a section for 'SNMP Host Settings' with three fields: 'Host IPv4 Address' (empty), 'User-based Security Model' (dropdown set to 'SNMPv1'), and 'Community String' (field containing '16 chars'). An 'Apply' button is on the right. Below is a table with columns: 'Host IP Address', 'SNMP Version', 'Community String', and a 'Clear' button. The table contains one row with values: '10.90.90.108', 'SNMPv2c', and 'public'.

| Host IP Address | SNMP Version | Community String |
|-----------------|--------------|------------------|
| 10.90.90.108 | SNMPv2c | public |

Figure 4-26 SNMP Host Table Settings

The fields that can be configured are described below:

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

| | |
|----------------------------------|--|
| Host IPv4 Address | Enter the IPv4 address of the SNMP notification host. |
| User-based Security Model | Select the security model here. Options to choose from are SNMPv1 , and SNMPv2c . SNMPv1 - Select to allow the group user to use the SNMPv1 security model. SNMPv2c -Select to allow the group user to use the SNMPv2c security model. |
| Community String | Enter the community string to be sent with the notification packet. |

Click the **Apply** button to accept the changes made.

Click the **Clear** button to remove SNMP Host.

HTTP/HTTPS

This window is used to configure Web settings on the switch.

To view the following window, click **Management > HTTP/HTTPS**, as shown below:

Figure 4-27 HTTP/HTTPS window

The fields that can be configured for **HTTP/HTTPS Settings** are described below:

| Parameter | Description |
|---------------------------------------|---|
| Web Session | Select this option to enable the configuration through HTTP or HTTPS. Note: When switching from HTTP to HTTPS mode, the switch will take about 30 seconds to initialize the secured HTTP environment. |
| Web Session Timeout (60-36000) | Enter a value for the amount of time in seconds before the web session expires. |

Click the **Apply** button to accept the changes made.

Note: If the switch is in HTTPS mode, the firmware or configuration cannot be upgraded using regular HTTP.

D-Link Discovery Protocol

This window is used to configure and display D-Link Discovery Protocol (DDP).

To view the following window, click **Management > D-Link Discovery Protocol**, as shown below:

D-Link Discovery Protocol

D-Link Discovery Protocol
DDP Global Settings

D-Link Discovery Protocol State Enabled Disabled

Report Timer sec

DDP Port Settings

From Port To Port State

| Port | State |
|-------|---------|
| eth1 | Enabled |
| eth2 | Enabled |
| eth3 | Enabled |
| eth4 | Enabled |
| eth5 | Enabled |
| eth6 | Enabled |
| eth7 | Enabled |
| eth8 | Enabled |
| eth9 | Enabled |
| eth10 | Enabled |

Figure 4-28 D-Link Discovery Protocol window

The fields that can be configured for **D-Link Discovery Protocol** are described below:

| Parameter | Description |
|--|--|
| D-Link Discovery Protocol State | Select this option to enable or disable DDP global state. |
| Report Timer | Select the interval in seconds between two consecutive DDP report messages. Options to choose from are 30, 60, 90, 120, and Never. |

The fields that can be configured for **DDP Port Settings** are described below:

| Parameter | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| State | Select the port to enable or disable. |

Click the **Apply** button to accept the changes made.

Layer 2 Features

FDB
VLAN
Spanning Tree
Loopback Detection
Link Aggregation
L2 Multicast Control
LLDP

FDB

Static FDB

Unicast Static FDB

This window is used to view and configure the static unicast forwarding settings on the switch.

To view the following window, click **L2 Features > FDB > Static FDB > Unicast Static FDB**, as shown below:

Figure 4-29 Unicast Static FDB window

The fields that can be configured are described below:

| Parameter | Description |
|--------------------|---|
| Port | Allows the selection of the port number on which the MAC address entered resides. |
| VID | Enter the VLAN ID on which the associated unicast MAC address resides. |
| MAC Address | Enter the MAC address to which packets will be statically forwarded or dropped. This must be a unicast MAC address. |

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to delete all the entries found in the display table.

Click the **Delete** button to remove the specified entry.

Multicast Static FDB

This window is used to view and configure the multicast static FDB settings. To view the following window, click **L2 Features > FDB > Static FDB > Multicast Static FDB**, as shown below:

Figure 4-30 Multicast Static FDB window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| VID | Enter the VLAN ID of the VLAN the corresponding MAC address belongs to. |
| MAC Address | Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address. The format of the destination MAC address is 01-00-5E-XX-XX-XX. |

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries.

Click the **Delete** button to remove the specific entry.

MAC Address Table Settings

This window is used to view and configure the MAC address table's global settings.

To view the following window, click **L2 Features > FDB > MAC Address Table Settings**, as shown below:

Figure 4-31 MAC Address Table Settings (Global Settings) window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------------|--|
| Aging Time (0,10-1000000) | Enter the MAC address table's aging time value here. This value must be between 0 or 10 to 1000000 seconds. By default, this value is 300 seconds. |

Click the **Apply** button to accept the changes made.

After clicking the **MAC Address Learning** tab, at the top of the page, the following page will be available.

| Port | State |
|-------|---------|
| eth1 | Enabled |
| eth2 | Enabled |
| eth3 | Enabled |
| eth4 | Enabled |
| eth5 | Enabled |
| eth6 | Enabled |
| eth7 | Enabled |
| eth8 | Enabled |
| eth9 | Enabled |
| eth10 | Enabled |

Figure 4-32 MAC Address Table Settings (MAC Address Learning) window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|--|
| From Port / To Port | Select the range of ports that will be used for this configuration here. |
| State | Select to enable or disable the MAC address learning function on the ports specified here. |

Click the **Apply** button to accept the changes made.

MAC Address Table

This window is used to view the entries listed in the MAC address table.

To view the following window, click **L2 Features > FDB > MAC Address Table**, as shown below:

| VID | MAC Address | Type | Port |
|-----------|-------------|------|------|
| Clear All | | | |

Figure 4-33 MAC Address Table window

Click the **Clear All** button to clear all dynamic MAC addresses.

VLAN

VLAN Configuration Wizard

This window is the VLAN configuration wizard.

To view the following window, click **L2 Features > VLAN > VLAN Configuration Wizard**, as shown below:

Figure 4-34 VLAN Configuration Wizard window

The fields that can be configured for **VLAN Configuration Wizard** are described below:

| Parameter | Description |
|-----------------------|---|
| Create VLAN | Create VLAN VID here. The range is from 1 to 4094. |
| Configure VLAN | Configure VLAN VID here. The range is from 1 to 4094. |

Click the **Next** button to Configure VLAN.

| Port | Select All | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|--------------------|------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| Tagged | All | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| Untagged | All | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Not Member | All | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Native VLAN (PVID) | All | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| VLAN Mode | | H | H | H | H | H | H | H | H | T | T |

Figure 4-35 VLAN Configuration Wizard window

The fields that can be configured for **VLAN Configuration Wizard** are described below:

| Parameter | Description |
|------------------|---|
| VLAN Name | Set VLAN Name here. |
| Port | Configure port function here: Tagged , Untagged , Not Member and Native VLAN (PVID) . |

Click the **Apply** button to accept the changes made.

Click the **Back** button go back to previous step.

802.1Q VLAN

This window is used to view and configure the VLAN settings on this switch.

To view the following window, click **L2 Features > VLAN > 802.1Q VLAN**, as shown below:

Figure 4-36 802.1Q VLAN window

The fields that can be configured for **802.1Q VLAN** are described below:

| Parameter | Description |
|-----------|---|
| VID List | Enter the VLAN ID list that will be created here. |

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

VLAN Interface

This window is used to view and configure VLAN interface settings.

To view the following window, click **L2 Features > VLAN > VLAN Interface**, as shown below:

Figure 4-37 VLAN Interface window

Click the **VLAN Detail** button to view more detailed information about the VLAN on the specific interface.

Click the **Edit** button to re-configure the specific entry.

After clicking the **VLAN Detail** button, the following page will appear.

Figure 4-38 VLAN Interface Information window

More detailed information about the VLAN of the specific interface is displayed.

Click the **Back** button to return to the previous window.

After click the **Edit** button, the following window will appear. This is a dynamic window that will change when a different **VLAN Mode** was selected. When **Access** was selected as the **VLAN Mode**, the following page will appear.

Figure 4-39 Configure VLAN Interface- Access window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| VLAN Mode | Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk . |
| Acceptable Frame | Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All . |
| Ingress Checking | Select this option to enable or disable the ingress checking function. |
| VID | Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094. |
| From Port / To Port | If Port Clone is enabled, select the appropriate port range used for the Clone configuration here. |

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

When **Hybrid** was selected as the **VLAN Mode**, the following page will appear.

Figure 4-40 Configure VLAN Interface - Hybrid window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| VLAN Mode | Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk . |
| Acceptable Frame | Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All . |
| Ingress Checking | Select the check box to enable or disable the ingress checking function. |
| VID | Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094. |
| Action | Select the action that will be taken here. Options to choose from are Remove , Tagged , and Untagged . |
| Allowed VLAN Range | Enter the allowed VLAN range information here. |
| From Port / To Port | Select the appropriate port range used for the Clone configuration here. |

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

When **Trunk** is selected as the **VLAN Mode**, the following page will appear.

The screenshot shows the 'Configure VLAN Interface' window. The 'Port' is set to 'eth1'. The 'VLAN Mode' is set to 'Trunk'. The 'Acceptable Frame' is set to 'Admit All'. The 'Ingress Checking' is set to 'Enabled'. The 'VID(1-4094)' is set to '1'. The 'Action' is set to 'All'. The 'Allowed VLAN Range' is empty. There are also fields for 'From Port' (eth1) and 'To Port' (eth1) and a 'Clone' checkbox. At the bottom right, there are '<<Back' and 'Apply' buttons.

Figure 4-41 Configure VLAN Interface - Trunk window

The fields that can be configured are described below:

| Parameter | Description |
|-------------------------|--|
| VLAN Mode | Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk . |
| Acceptable Frame | Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All . |
| Ingress Checking | After selecting Trunk as the VLAN Mode the following parameter will be available. Select to enable or disable the ingress checking function. |
| VID | Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094. |
| Action | Select the action that will be taken here. Options to choose from are All , ADD and Remove . |

| | |
|----------------------------|---|
| Allowed VLAN Range | If the Action chosen is Add or Remove, enter the allowed VLAN range information here. |
| From Port / To Port | Select the appropriate port range used for the Clone configuration here. |

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

To view the following window, click **L2 Features > VLAN > VLAN Interface >Port Summary**, as shown below:

| VLAN Interface | | | | |
|-------------------------|-----------|--------------|---------------|-------------|
| VLAN Interface Settings | | Port Summary | | |
| Port | VLAN Mode | Native VLAN | Untagged VLAN | Tagged VLAN |
| eth1 | Hybrid | 5 | 1,5 | |
| eth2 | Hybrid | 5 | 1 | 5 |
| eth3 | Hybrid | 5 | 1,5 | |
| eth4 | Hybrid | 5 | 1 | 5 |
| eth5 | Hybrid | 1 | 1 | |
| eth6 | Hybrid | 1 | 1 | |
| eth7 | Hybrid | 1 | 1 | |
| eth8 | Hybrid | 1 | 1 | |
| eth9 | Hybrid | 1 | 1 | |
| eth10 | Hybrid | 1 | 1 | |
| eth11 | Hybrid | 1 | 1 | |
| eth12 | Hybrid | 1 | 1 | |
| eth13 | Hybrid | 1 | 1 | |
| eth14 | Hybrid | 1 | 1 | |
| eth15 | Hybrid | 1 | 1 | |
| eth16 | Hybrid | 1 | 1 | |
| eth17 | Hybrid | 1 | 1 | |
| eth18 | Hybrid | 1 | 1 | |
| eth19 | Hybrid | 1 | 1 | |
| eth20 | Hybrid | 1 | 1 | |

Figure 4-42 Port Summary window

Port-based VLAN

This window is used to configure the Port-based VLAN function.

To view the following window, click **L2 Features > VLAN > Port-based VLAN**, as shown below:

| Port-based VLAN | | | |
|--|---------|---|---|
| Port-based VLAN Status Settings | | | |
| VLAN State | | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled | <input type="button" value="Apply"/> |
| Note: When Port-Based VLAN is enabled, the 802.1Q VLAN settings and 802.1Q management VLAN settings will be set to Disabled as default, and Surveillance VLAN and Voice VLAN cannot work. The MAC Address Table will be reset to default. | | | |
| Port-based VLAN Settings | | | |
| From Port | To Port | VLAN Index | <input type="button" value="Apply"/> |
| eth1 | eth1 | | |
| Total Entries: 0 | | | <input type="button" value="Delete All"/> |
| VLAN Index | | Egress Ports | |

Figure 4-43 Port-based VLAN window

The fields that can be configured are described below:

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

| | |
|-------------------|---|
| VLAN State | Select this option to enable or disable the Port-based VLAN function. |
|-------------------|---|

Click the **Apply** button to accept the changes made.

When setting the enable the Port-based VLAN:

Figure 4-44 Port-based VLAN window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| VLAN Index | Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094. |

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified vlan.



NOTE:

If you want to delete an existing vlan, you need to delete the member ports first.

If you want to delete the last two or four member ports (uplink port) depending on the model, you need to go to Surveillance mode.

Management VLAN

This window is used to configure the Management VLAN function.

To view the following window, click **L2 Features > VLAN > Management VLAN**, as shown below:

4-45 Management VLAN window

The fields that can be configured are described below:

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

| | |
|------------------------------|---|
| Management VLAN State | Select this option to enable or disable the Management VLAN function. |
| VID | VLAN VID is a unique number (between 1 and 4094) that identifies a particular VLAN. |

Click the **Apply** button to accept the changes made.

Asymmetric VLAN

This window is used to configure the asymmetric VLAN function.

To view the following window, click **L2 Features > VLAN > Asymmetric VLAN**, as shown below:

Figure 4-18 Asymmetric VLAN window

The fields that can be configured are described below:

| Parameter | Description |
|------------------------------|--|
| Asymmetric VLAN State | Select this option to enable or disable the asymmetric VLAN function |

Click the **Apply** button to accept the changes made.

Auto Surveillance VLAN

Auto Surveillance Properties

This window is used to configure the auto surveillance VLAN global settings and display the ports surveillance VLAN information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties**, as shown below:

4-26 Auto Surveillance Properties window

The fields that can be configured for **Global Settings** are described below:

| Parameter | Description |
|------------------------------|---|
| Surveillance VLAN | Select this option to enable or disable the surveillance VLAN state |
| Surveillance VLAN ID | Enter the surveillance VLAN ID. The range is from 2 to 4094. |
| Surveillance VLAN CoS | Select the priority of the surveillance VLAN from 0 to 7. |

| | |
|-------------------|---|
| Aging Time | Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from surveillance VLAN if the port is an automatic surveillance VLAN member. When the last surveillance device stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be reset and stop. |
|-------------------|---|

Click the **Apply** button to accept the changes made.

MAC Settings and Surveillance Device

This window is used to configure the user-defined surveillance device OUI and display the surveillance VLAN information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device**, as shown below:

4-27 MAC Settings and Surveillance Device(User-defined MAC Settings) window

The fields that can be configured are described below:

| Parameter | Description |
|-----------------------|---|
| Component Type | Select the surveillance component type. Options to choose from are Video Management Server , VMS Client/Remote Viewer , Video Encoder , Network Storage , and Other IP Surveillance Device . |
| Description | Enter the description for the user-defined OUI with a maximum of 8 characters. |
| MAC Address | Enter the OUI MAC address. |
| Mask | Enter the OUI MAC address matching bitmask. |

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

After clicking the **Auto Surveillance VLAN Summary** tab, the following page will appear.

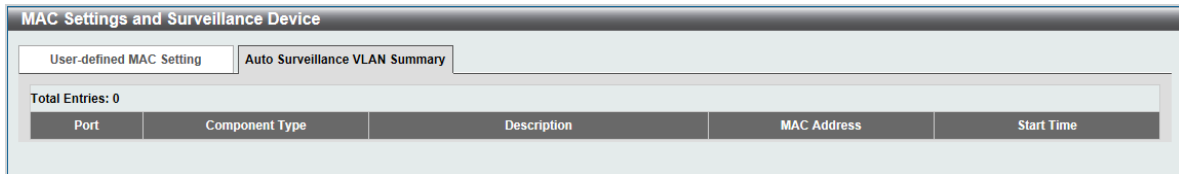


Figure 4-28 MAC Settings and Surveillance Device(Auto Surveillance VLAN Summary) window

Voice VLAN

Voice VLAN Global

Voice VLAN is a VLAN used to carry voice traffic from IP phone. Because the sound quality of an IP phone call will be deteriorated if the data is unevenly sent, the quality of service (QoS) for voice traffic shall be configured to ensure the transmission priority of voice packet is higher than normal traffic.

The switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Global**, as show below:

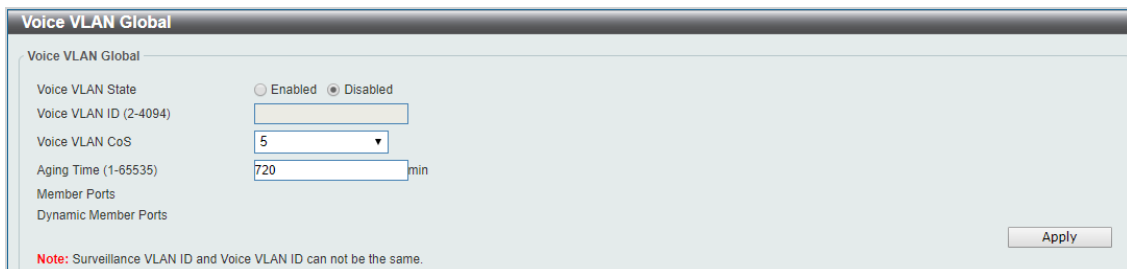


Figure 4-29 Voice VLAN Global window

The fields that can be configured are described below:

| Parameter | Description |
|-------------------------------|---|
| Voice VLAN State | Select this option to enable or disable the voice VLAN. |
| Voice VLAN ID (2-4094) | Enter the voice VLAN ID. The value is range from 2 to 4094. |
| Voice VLAN CoS | Select the priority of the voice VLAN from 0 to 7. |
| Aging Time (1-65535) | Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop. |

Click the **Apply** button to accept the changes made for each individual section.

Voice VLAN Port

This window is used to configure the user-defined voice traffic's port.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI**, as show below:

| Port | State | Mode |
|-------|----------|--------|
| eth1 | Disabled | Manual |
| eth2 | Disabled | Manual |
| eth3 | Disabled | Manual |
| eth4 | Disabled | Manual |
| eth5 | Disabled | Manual |
| eth6 | Disabled | Manual |
| eth7 | Disabled | Manual |
| eth8 | Disabled | Manual |
| eth9 | Disabled | Manual |
| eth10 | Disabled | Manual |

Figure 4-30 Voice VLAN Port window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| From Port / To Port | Select the range of ports that will be used for this configuration here. |
| State | Select this option to enable or disable the Voice VLAN state of the port. |
| Mode | Choose the Voice VLAN mode for the port. This can be Auto untagged , Auto Tagged , or Manual configured. |

Click the **Apply** button to accept the changes made.

Voice VLAN OUI

This window is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI**, as show below:

| OUI Address | Mask | Description | |
|-------------------|-------------------|-------------|--------|
| 00-01-E3-00-00-00 | FF-FF-FF-00-00-00 | Siemens | Delete |
| 00-03-6B-00-00-00 | FF-FF-FF-00-00-00 | Cisco | Delete |
| 00-09-6E-00-00-00 | FF-FF-FF-00-00-00 | Avaya | Delete |
| 00-0F-E2-00-00-00 | FF-FF-FF-00-00-00 | Hua-3COM | Delete |
| 00-60-B9-00-00-00 | FF-FF-FF-00-00-00 | NEC/Phil | Delete |
| 00-D0-1E-00-00-00 | FF-FF-FF-00-00-00 | Pingtel | Delete |
| 00-E0-75-00-00-00 | FF-FF-FF-00-00-00 | Veritel | Delete |
| 00-E0-BB-00-00-00 | FF-FF-FF-00-00-00 | 3com | Delete |

Figure 4-31 Voice VLAN OUI window

The fields that can be configured are described below:

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

| | |
|--------------------|--|
| OUI Address | Enter the OUI MAC address. |
| Mask | Enter the OUI MAC address matching bitmask. |
| Description | Enter the description for the user-defined OUI with a maximum of 8 characters. |

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Voice VLAN Device

This window is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port, the activate time is the latest time saw the device sending the traffic.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Device**, as show below:



The screenshot shows a window titled "Voice VLAN Device". Inside the window, there is a section labeled "Voice VLAN Device Table" containing a table with three columns: "Port", "Voice Device Address", and "Start Time". The table is currently empty.

Figure 4-32 Voice VLAN Device window

Spanning Tree

This switch supports two versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP has been recently introduced to DSS-200G MP/MPP switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D-1998 STP, 802.1D-2004 RSTP.

802.1D-2004 Rapid Spanning Tree

Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however, the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

Note: If Spanning Tree protocol is used, loopback detection will not be available. If Loopback Detection is enabled, the Spanning Tree protocol will not be available. The STP and Loopback Detection cannot be turned on at the same time.

STP Global Settings

This window is used to view and configure the STP global settings.

To view the following window, click **L2 Features > Spanning Tree > STP Global Settings**, as shown below:

Figure 4-34 STP Global Settings window

Note: You cannot configure the STP State and Mode when the Dip Switch on the front panel has been turned on.

The field that can be configured for **Spanning Tree State** is described below:

| Parameter | Description |
|----------------------------|--|
| Spanning Tree State | Select this option to enable or disable the STP global state here. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Spanning Tree Mode** are described below:

| Parameter | Description |
|---------------------------|--|
| Spanning Tree Mode | Select the STP mode used here. Options to choose from are RSTP , and STP . |

Click the **Apply** button to accept the changes made.

The fields that can be configured for **STP Traps** are described below:

| Parameter | Description |
|---------------------------------|---|
| STP New Root Trap | Select this option to enable or disable the STP new root trap option here. |
| STP Topology Change Trap | Select this option to enable or disable the STP topology change trap option here. |

Click the **Apply** button to accept the changes made.

STP Port Settings

This window is used to view and configure the STP port settings.

To view the following window, click **L2 Features > Spanning Tree > STP Port Settings**, as shown below:

| Port | State | Port Fast | Port State |
|------|-------|-----------|------------|
|------|-------|-----------|------------|

Figure 4-35 STP Port Settings window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| State | Select the port state. |
| Port Fast | Select the port fast option here. Options to choose from are Network , Disabled , and Edge . In the Network mode the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. In the Disable mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. In the Edge mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. By default, this option is Edge . |

Click the **Apply** button to accept the changes made.

Loopback Detection

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the switch when a CTP (Configuration Testing Protocol) packet has been looped back to the switch. When the switch detects CTP packets received from a port, this signifies a loop on the network. The switch will automatically block the port and send an alert to the administrator. The Loopback Detection port will restart (change to normal state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

To view the following window, click **L2 Features > Loopback Detection**, as shown below:

Figure 4-36 Loopback Detection window

The fields that can be configured for **Loopback Detection Global Settings** are described below:

| Parameter | Description |
|---------------------------------|--|
| Loopback Detection State | Select to enable or disable loopback detection. The default is Disabled . |
| Trap State | Select to enable or disable the loopback detection trap state. The default is Disabled . |
| Enabled VLAN ID List | This is the range of VLANs that Loopback Detection is enabled on. The range is from 1 to 4094. (Fill in when Mode is set to VLAN-based) |
| Action | The action to perform when a CTP packet is detected on a port. The actions are as follows: Shutdown: shut the port down. None: perform no action. Discarding: blocking port. |
| Function Version | This is the version of Loopback Detection software running on the switch. |
| Mode | This is the Loopback Detection mode running on the switch. The modes are: Port-based: perform port-based Loopback Detection VLAN-based: perform VLAN-based Loopback Detection. |
| Time Interval (5-300) | Set a Loop detection Interval between 5 and 300 seconds. The default is 10 seconds. |
| Recover Time (0, 20-600) | Time allowed (in seconds) for recovery when a Loopback is detected. The Loop Detection Recover Time can be set at 0 seconds, or 20 to 600 seconds. Entering 0 will disable the Loop Detection Recover Time. The default is 60 seconds. |
| Address type | Set a Loop detection packet use multicast or broadcast |

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Loopback Detection Port Settings** are described below:

| Parameter | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration here. |

| | |
|--------------|--|
| State | Select this option to enable or disable the state of the port. |
|--------------|--|

Click the **Apply** button to accept the changes made.

Note: If Spanning Tree protocol is used, loopback detection will not be available. If Loopback Detection is enabled, the Spanning Tree protocol will not be available.

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline.

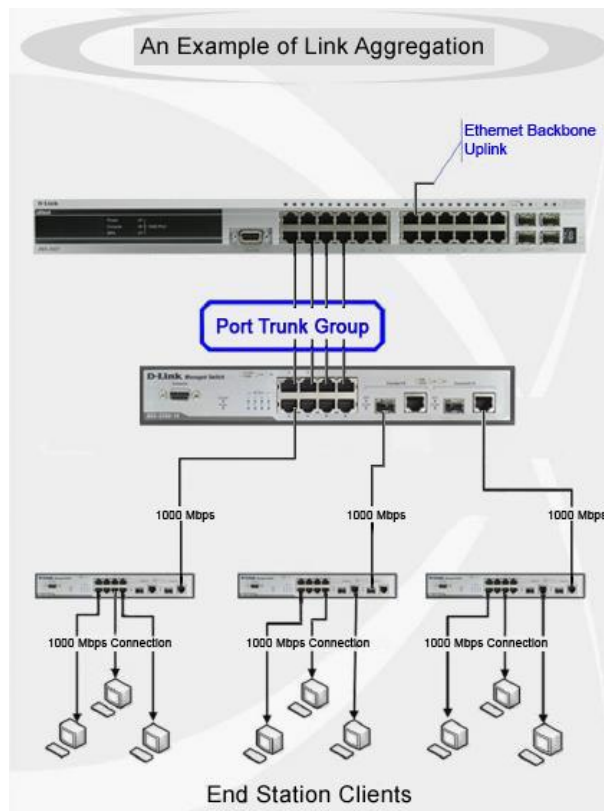


Figure 4-37 Example of Port Trunk Group

The switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

This window is used to view and configure the link aggregation settings.

To view the following window, click **L2 Features > Link Aggregation**, as shown below:

Figure 4-38 Link Aggregation window

The fields that can be configured for **Link Aggregation** are described below:

| Parameter | Description |
|-------------------------------|--|
| System Priority | Select the System Priority, range from 1 to 65535. |
| Load Balance Algorithm | Select the Load Balance Algorithm here. Options to choose from are Source MAC , Destination MAC , Source Destination MAC , Source IP , Destination IP , Source Destination IP , Source L4 Port , Destination L4 Port and Source Destination L4 Port . |
| System ID | Enter the channel System number here. |

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete Member Port** button to remove the specific member port.

Click the **Delete Channel** button to remove the specific entry.

The fields that can be configured for **Channel Group Information** are described below:

| Parameter | Description |
|----------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| Group ID | Enter the channel group number here. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group. |
| Mode | <p>Select the mode option here. Options to choose from are On, Active, and Passive. If the mode On is specified, the channel group type is static. If the mode Active or Passive is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.</p> <p>Active - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.</p> <p>Passive - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports</p> |

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete Member Port** button to remove the specific member port.

Click the **Delete Channel** button to remove the specific entry.

L2 Multicast Control

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host.

IGMP Snooping Settings

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings**, as shown below:

Figure 4-39 IGMP Snooping Settings window

The field that can be configured for **Global Settings** is described below:

| Parameter | Description |
|---------------------|---|
| Global State | Select this option to enable or disable IGMP Snooping global state. |

Click the **Apply** button to accept the changes made.

The field that can be configured for **VLAN Status Settings** is described below:

| Parameter | Description |
|---------------------|---|
| VID (1-4094) | Enter the VLAN ID and enable the VLAN configuration for IGMP. |

The field that can be configured for **VLAN Querier Status Settings** is described below:

| Parameter | Description |
|-----------------------------|---|
| Querier Global State | Select this option to enable or disable IGMP Snooping Querier Global State. |

Click the **Apply** button to accept the changes made.

IGMP Snooping Groups Settings

This window is used to configure and view the IGMP snooping static group, and view IGMP snooping group.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings**, as shown below:

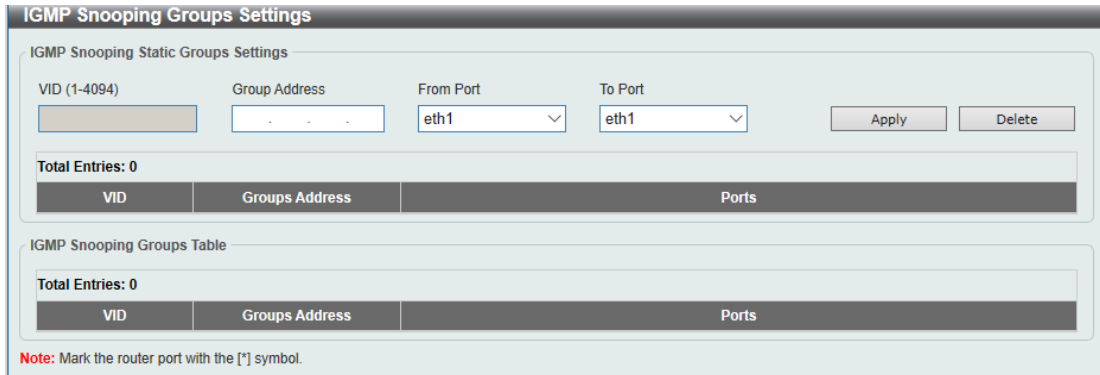


Figure 4-40 IGMP Snooping Groups Settings

The fields that can be configured for **IGMP Snooping Static Groups Settings** are described below:

| Parameter | Description |
|----------------------------|--|
| VID | Enter a VLAN ID of the multicast group. |
| Group Address | Enter an IP multicast group address. |
| From Port / To Port | Select the appropriate port range used for the configuration here. |

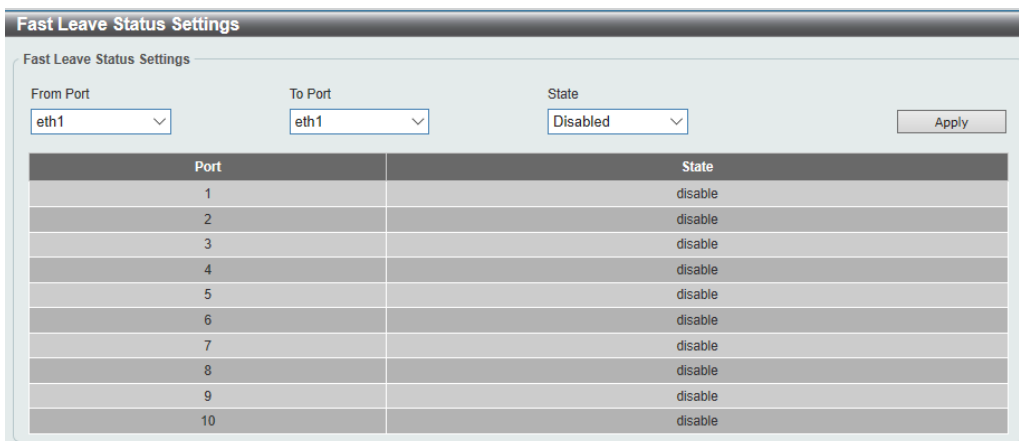
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Fast Leave Status Settings

This window is used to configure and view the Fast Leave Status Settings.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > Fast Leave Status Settings**, as shown below:



| Port | State |
|------|---------|
| 1 | disable |
| 2 | disable |
| 3 | disable |
| 4 | disable |
| 5 | disable |
| 6 | disable |
| 7 | disable |
| 8 | disable |
| 9 | disable |
| 10 | disable |

Figure 4-41 Fast Leave Status Settings

The fields that can be configured for **IGMP Snooping Static Groups Settings** are described below:

| Parameter | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| State | Select this option to enable or disable state. |

Click the **Apply** button to accept the changes made.

IGMP Snooping Mrouter Settings

This window is used to configure and view the IGMP snooping Mrouter, and view IGMP snooping Mrouter.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings**, as shown below:

Figure 4-42 IGMP Mrouter Settings

The fields that can be configured for **IGMP Snooping Mrouter Settings** are described below:

| Parameter | Description |
|----------------------------|--|
| VID | Enter a VLAN ID of the multicast group. |
| From Port / To Port | Select the appropriate port range used for the configuration here. |

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Multicast Filtering

This window is used to view and configure the Layer 2 multicast filtering settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast Filtering**, as shown below:

Figure 4-43 Multicast Filtering window

The fields that can be configured are described below:

| Parameter | Description |
|------------------------------|---|
| Multicast Filter Mode | Select the multicast filter mode here. Options to choose from are Forward Unregistered and Filter Unregistered . When |

| | |
|--|---|
| | selecting the Forward Unregistered option, registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. When selecting the Filter Unregistered option, registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered. |
|--|---|

Click the **Apply** button to accept the changes made.

LLDP

LLDP Global Settings

LLDP (Link Layer Discovery Protocol) provides IEEE 802.1AB standards-based method for switches to advertise themselves to neighbor devices, as well as to learn about neighbor LLDP devices.

This window is used to configure the LLDP global settings.

To view the following window, click **L2 Features > LLDP > LLDP Global Settings**, as shown below:

Figure 4-44 LLDP Global Settings window

The fields that can be configured for **LLDP Global Settings** are described below:

| Parameter | Description |
|------------------------|--|
| LLDP State | Select this option to enable or disable the LLDP feature |
| LLDP Trap State | Select this option to enable or disable the LLDP trap state. |

Click the **Apply** button to accept the changes made.

LLDP Neighbor Port Information

This window is used to display the information learned from the neighbors. The switch receives packets from a remote station but is able to store the information as local.

To view the following window, click **L2 Features > LLDP > LLDP Neighbor Port Information**, as show below:

| Entity | Chassis ID Subtype | Chassis ID | Port ID Subtype | Port ID | Port Description |
|--------|--------------------|-------------------|-----------------|-------------------|------------------|
| 1 | MAC address | 74:da:38:a1:2d:2f | MAC address | 74:da:38:a1:2d:2f | |

Figure 4-45 LLDP Neighbor Port Information window

QoS

802.1p Priority Port Rate Limiting

802.1p Priority

This window is used to view and configure the port's default CoS settings.

To view the following window, click **QoS > 802.1p Priority**, as shown below:

802.1p Priority Settings

Mode
802.1p

Note: The port which has opened port priority DIP switch is forbidden to set mode.

Port Scheduler Method
From Port: eth1 To Port: eth1 Scheduler Method: SP WRR: queue0:queue1:queue2:queue3:queue4:queue5:queue6:q...

Note: The port which has opened port priority DIP switch is forbidden to set Scheduler Method.

802.1p
From Port: eth1 To Port: eth1 Default CoS: 0

Note: The port which has opened port priority DIP switch is forbidden to set COS.

802.1p Priority Table

| Priority | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|-------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Queue Class | queue2 | queue0 | queue1 | queue3 | queue4 | queue5 | queue6 | queue7 |

| Port | Scheduler Method | Default |
|------|------------------|---------|
| eth1 | SP | 0 |
| eth2 | SP | 0 |

Figure 4-46 802.1p Priority Settings (802.1p) window

The fields that can be configured for Port Scheduler Method are described below:

| Parameter | Description |
|----------------------------|---|
| Mode | Select 802.1p or DSCP |
| From Port / To Port | Select the appropriate port range used for configuration here. |
| Scheduler Method | <p>SP - Denoting a Strict Priority scheduling will set the highest queue to be emptied first while the other queues will follow the weighted round-robin scheduling scheme.</p> <p>WRR - Use the weighted round-robin (WRR) algorithm to handle packets in an even distribution in priority classes of service.</p> |

Click the **Apply** button to accept the changes made.

The fields that can be configured **802.1p** are described below:

| Parameter | Description |
|----------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| Default CoS | Select the default CoS option for the port(s) specified here. The priorities are 0-7 . |

Click the **Apply** button to accept the changes made.

When DSCP mode is selected, the following window is displayed:

802.1p Priority Settings

Mode

Note: The port which has opened port priority DIP switch is forbidden to set mode.

Port Scheduler Method

From Port To Port Scheduler Method WRR: queue0.queue1.queue2.queue3.queue4.queue5.queue6.queue7=1:2:3:4:5:6:7:8

Note: The port which has opened port priority DIP switch is forbidden to set Scheduler Method.

802.1p Priority Table

| Priority | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|-------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Queue Class | queue2 | queue0 | queue1 | queue3 | queue4 | queue5 | queue6 | queue7 |

| Port | Scheduler Method | Default |
|------|------------------|---------|
| eth1 | SP | 1 |
| eth2 | SP | 0 |
| eth3 | SP | 0 |
| eth4 | SP | 0 |
| eth5 | SP | 0 |
| eth6 | SP | 0 |
| eth7 | SP | 0 |
| eth8 | SP | 0 |

Figure 4-49 802.1p Priority Settings (DSCP) window

The fields that can be configured DSCP Table are described below:

| Parameter | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| Scheduler Method | Select the scheduler method are SP or WRR. |

Click the **Apply** button to accept the changes.

Port Rate Limiting

This window is used to view and configure the port rate limiting settings.

To view the following window, click **QoS > Port Rate Limiting**, as shown below:

Port Rate Limiting

Port Rate Limiting

From Port To Port Direction Rate Limit

| Port | Input (Rate) | Output (Rate) |
|------|--------------|---------------|
|------|--------------|---------------|

Figure 4-50 Port Rate Limiting window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| Direction | Select the direction option here. Options to choose from are Input and Output . When Input is selected, the rate limit for ingress packets is configured. When Output is selected, the rate limit for egress packets is configured. |
| Rate Limit | Select the rate limit value here. When Direction is Input , this drop-down menu allows you to select data rate from 16Kbps to 512Mbps. |

| | |
|--|---|
| | When Direction is Output , this drop-down menu allows you to select data rate from 16Kbps to 512Mbps. |
|--|---|

Click the **Apply** button to accept the changes made.

Security

Safeguard Engine Settings
Traffic Segmentation
Storm Control
DoS Attack Prevention Settings
Zone Defense Settings
SSL

Safeguard Engine Settings

D-Link's Safeguard Engine is a robust and innovative technology that automatically throttles the impact of packet flooding into the switch's CPU. This function helps protect the Smart switch from being interrupted by malicious viruses or worm attacks.

This window is used to view and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine > Safeguard Engine Settings**, as shown below:

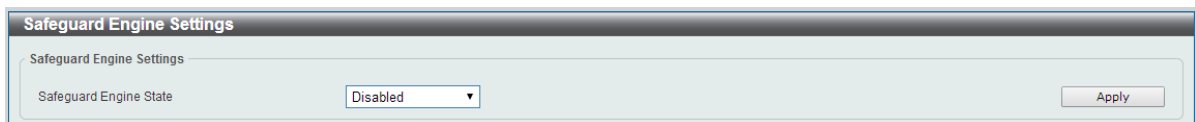


Figure 4-51 Safeguard Engine Settings window

The fields that can be configured for **Safeguard Engine Settings** are described below:

| Parameter | Description |
|-------------------------------|--|
| Safeguard Engine State | Select to enable or disable the safeguard engine feature here. |

Traffic Segmentation

This window is used to view and configure the traffic segmentation settings. When the traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is restricted.

To view the following window, click **Security > Traffic Segmentation**, as shown below:

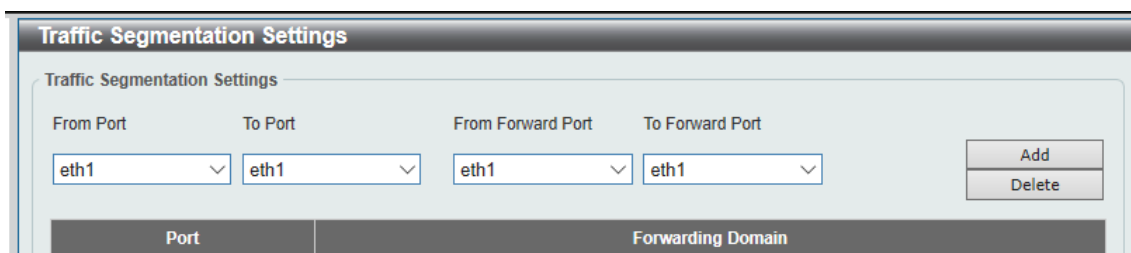


Figure 4-52 Traffic Segmentation Settings window

The fields that can be configured are described below:

| Parameter | Description |
|--|--|
| From Port / To Port | Select the receiving port range used for the configuration here. |
| From Forward Port / To Forward Port | Select the forward port range used for the configuration here. |

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove an entry based on the information entered.

Storm Control

This window is used to view and configure the storm control settings. Once a packet storm has been detected, the switch will drop packets coming into the switch until the storm has subsided.

To view the following window, click **Security > Storm Control**, as shown below:

Figure 4-53 Storm Control window

The fields that can be configured for **Storm Control Port Settings** are described below:

| Parameter | Description |
|----------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| Type | Select the type of storm attack that will be controlled here. Options to choose from are None , Broadcast , Multicast , and Unicast . |
| Rate Limit | Select a data rate from 16Kbps to 512Mbps. |

Click the **Apply** button to accept the changes made.

DoS Attack Prevention Settings

This window is used to view and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types which can be detected by most switches:

- **Land Attack:** This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack:** This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP Null Scan:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and no flags.
- **TCP Xmascan:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets which contain SYN and FIN flags.

- **TCP SYN Src Port Less 1024:** This type of attack involves port scanning by using specific packets which contain source port 0 to 1023 and SYN flag.
- **Ping Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size) which is 65535 bytes. The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.
- **All Types:** All of above types.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:

| DoS Type | State | Action |
|----------------------------|----------|--------|
| Land Attack | Disabled | Drop |
| Blat Attack | Disabled | Drop |
| TCP Null Scan | Disabled | Drop |
| TCP Xmascan | Disabled | Drop |
| TCP SYN-FIN | Disabled | Drop |
| TCP SYN Src Port Less 1024 | Disabled | Drop |
| Ping Death Attack | Disabled | Drop |

Figure 4-47 DoS Attack Prevention Settings window

The fields that can be configured for **DoS Attack Prevention Settings** are described below:

| Parameter | Description |
|---------------------------|---|
| DoS Type Selection | Select the DoS type option that will be prevented here. |
| State | Select to enable or disable the DoS attack prevention feature's global state here. |
| Action | Select the action that will be taken when the DoS attack was detected here. The only option to select here is Drop . |

Click the **Apply** button to accept the changes made.

Zone Defense Settings

This window is used to view and configure the Zone Defense setting.

To view the following window, click **Security > Zone Defense Settings**, as shown below:

Figure 4-55 Zone Defense Settings window

The fields that can be configured for **Zone Defense Settings** are described below:

| Parameter | Description |
|---------------------------|---|
| Zone Defense State | Select to enable or disable the Zone Defense feature's global state here. |

Click the **Apply** button to accept the changes made.

SSL

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption.

SSL Global Settings

This window is used to view and configure the SSL feature's global settings.

To view the following window, click **Security > SSL > Global Settings**, as shown below:

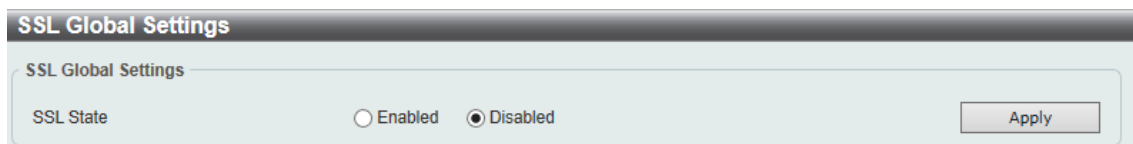


Figure 4-56 SSL Global Settings window

The fields that can be configured for **SSL Global Settings** are described below:

| Parameter | Description |
|------------------|---|
| SSL State | Select to enable or disable the SSL feature's global status here. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Upgrade Certificate and key** are described below:

| Parameter | Description |
|--------------------|--|
| Key | Select to Key file here. |
| Certificate | Select to Upgrade Certificate file here. |

Click the **Apply** button to accept the changes made.

OAM

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view the following window, click **OAM > Cable Diagnostics**, as shown below:

| Port | Type | Link Status | Test Result | Cable Length (M) |
|------|------|-------------|-------------|------------------|
|------|------|-------------|-------------|------------------|

Figure 4-48 Cable Diagnostics window

The fields that can be configured are described below:

| Parameter | Description |
|---------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration here. |

Click the **Test** button to test the specific port.

Click the **Clear** button to clear all the information for the specific port.

Click the **Clear All** button to clear all the information in this table.

Note: The Cable Diagnostics feature is only supported on the copper ports on all DSS-200G MP/MPP Series switches.

Monitoring

Statistics
Mirror Settings

Statistics

Port Counters

This window is used to display port counter statistics.

To view the following window, click **Monitoring > Statistics > Port Counters**, as show below:

| Port | TxOK | TxErr | RxOK | RxErr |
|------|------|-------|------|-------|
|------|------|-------|------|-------|

Figure 4-58 Port Counters window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration here. |

The statistics for the ports are described below:

Tx OK: Number of packets transmitted successfully.

Rx OK: Number of packets received successfully.

Tx Error: Number of transmitted packets resulting in error.

Rx Error: Number of received packets resulting in error.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Refresh** button to refresh the display table.

Click the **Clear** button to clear all the information for the specific port.

Click the **Clear All** button to clear all the information in this table.

Mirror Settings

This window is used to view and configure the mirror feature's settings. The switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a monitoring device to the mirroring port, such as a sniffer, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view the following window, click **Monitoring > Mirror Settings**, as shown below:

Mirror Settings

Mirror Settings

Port

Destination

From Port To Port Frame Type

Source

Apply Delete

Mirror Session Table

| Source Ports | | | Destination port |
|--------------|----|----|------------------|
| Both | RX | TX | |
| | | | |

Figure 4-59 Mirror Settings window

The fields that can be configured for **Mirror Settings** are described below:

| Parameter | Description |
|--------------------|--|
| Destination | Select one destination port for mirroring. |
| Source | Select From Port number and the To Port number as source port for mirroring. Lastly select the Frame Type option. Options to choose from as the Frame Type are Both , RX , and TX . When selecting Both , traffic in both the incoming and outgoing directions will be mirrored. When selecting RX , traffic in only the incoming direction will be mirrored. When selecting TX , traffic in only the outgoing direction will be mirrored. |

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

Green

Power Saving EEE

Power Saving

This window is used to configure the power saving settings of the switch.

To view the following window, click **Green > Power Saving**, as shown below:

Figure 4-60 Power Saving window

The fields that can be configured are described below:

| Parameter | Description |
|---|---|
| Link Detection Power Saving | Select this option to enable or disable the link detection state. When enabled, a port which has a link down status will be turned off to save power to the switch. This will not affect the port's capabilities when the port status is link up. |
| Scheduled Port-shutdown Power Saving | Select this option to enable or disable applying the power saving by scheduled port shutdown. After enabling this option, select a pre-configured Time Profile for the configuration (go to the Power Saving Shutdown Settings tab of the Power Saving menu). |
| Scheduled Hibernation Power Saving | Select this option to enable or disable applying the power saving by scheduled hibernation power (go to the Time Profile Settings section below). |
| Scheduled Dim-LED Power Saving | Select this option to enable or disable applying the power saving by scheduled dimming LEDs (go to the Time Profile Settings section below). |
| Administrative Dim-LED | Select this option to enable or disable the port LED function. |
| Type | Select the type of power saving. Options to choose from are Dim-LED and Hibernation . |
| Time Profile | If a Time Profile was previously created, select the desired profile from the drop-down list. Go to System > Time Range to configure a schedule. |

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete** button to remove the specified entry.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.

Power Saving

Power Saving Global Settings | Power Saving Shutdown Settings

From Port: eth1 | To Port: eth1 | Time Profile: None | Apply

Total Entries: 10

| Port | Time Profile | |
|-------|--------------|--------|
| eth1 | | Delete |
| eth2 | | Delete |
| eth3 | | Delete |
| eth4 | | Delete |
| eth5 | | Delete |
| eth6 | | Delete |
| eth7 | | Delete |
| eth8 | | Delete |
| eth9 | | Delete |
| eth10 | | Delete |

Figure 4-61 Power Saving Shutdown Settings window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| Time Range | If a Time Profile was previously created, select the desired profile from the drop-down list. |

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

EEE

Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

To view the following window, click **Green > EEE**, as shown below:

EEE

EEE Settings

From Port: | To Port: | State: Disabled | Apply

| Port | State |
|------|-------|
| | |

Figure 4-62 EEE window

The fields that can be configured are described below:

| Parameter | Description |
|----------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| State | Select this option to enable or disable the state of this feature here. |

Click the **Apply** button to accept the changes made.

Note: The EEE feature is only supported on the copper ports on all DSS-200G MP/MPP Series switches.

ONVIF

Global Status IP-Camera Information

Global Status

ONVIF is a global standard for improving inter-operability between IP-based security products. It is an effort between various hardware and software vendors to define a specification for the exchange of information between physical security products. The DSS-200G MP/MPP Series support the ONVIF protocol, and its settings can be configured below.

The ONVIF Global Status page enables ONVIF support globally on the switch and allows you to configure ONVIF settings. It also displays global ONVIF statistics for the switch.

To view the following window, click **ONVIF > Global Status**, as shown below:

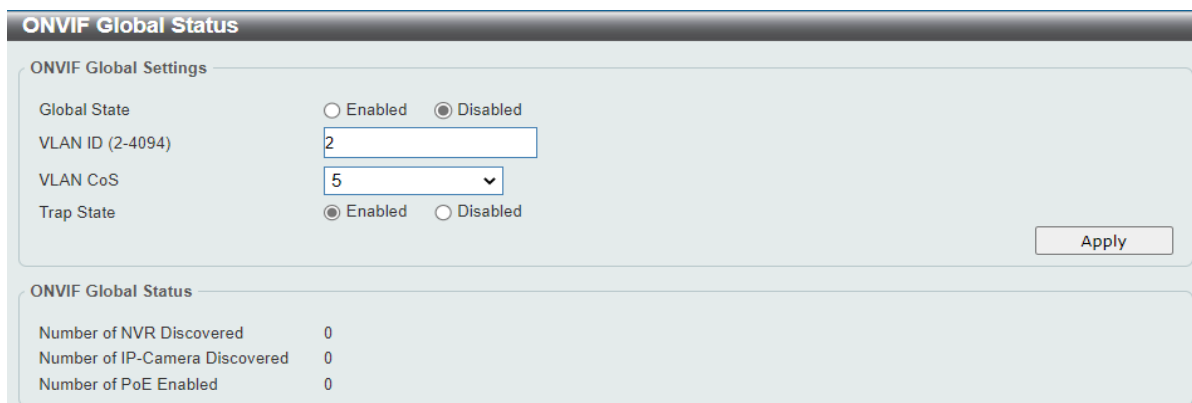


Figure 4-63 ONVIF Global Status window

The fields that can be configured are described below:

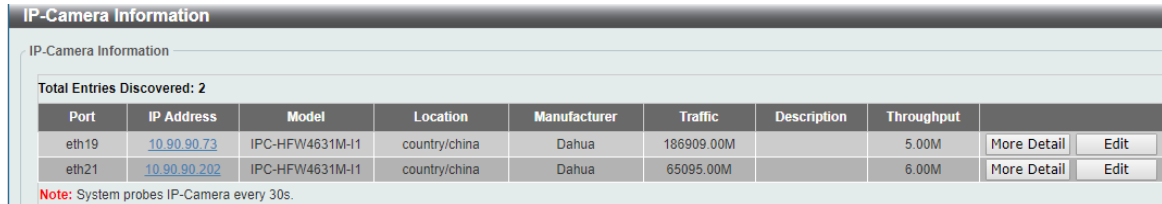
| Parameter | Description |
|-------------------------|--|
| Global State | Select this option to enable or disable ONVIF globally on the switch. This will overwrite Auto Surveillance VLAN and associated QoS settings. |
| VLAN ID (2-4094) | This is the VLAN that is used for surveillance devices on the switch and can be manually configured to be a VLAN created in the VLAN section of this document. |
| VLAN CoS | This is the VLAN Class of Service and can be set to a value between 0 and 7. It uses the IEEE 802.1p Priority Levels to classify traffic. |
| Trap State | Select this option to enable or disable SNMP traps for ONVIF. This SNMP host can be configured in the SNMP Global Settings section of this document. |

Click the **Apply** button to accept the changes made.

IP-Camera Information

The IP-Camera Information page shows the devices that have been discovered through ONVIF. These are ONVIF-compatible devices that have been detected in the VLAN defined in the ONVIF Global Status page. The system probes for new IP cameras every 30 seconds.

To view the following window, click **ONVIF > IP-Camera Information**, as shown below:



The screenshot shows a web interface titled "IP-Camera Information". Below the title, it says "IP-Camera Information" and "Total Entries Discovered: 2". A table lists two entries. The first entry is on port eth19 with IP address 10.90.90.73, model IPC-HFW4631M-I1, location country/china, manufacturer Dahua, traffic 186909.00M, and throughput 5.00M. The second entry is on port eth21 with IP address 10.90.90.202, model IPC-HFW4631M-I1, location country/china, manufacturer Dahua, traffic 65095.00M, and throughput 6.00M. Each entry has "More Detail" and "Edit" buttons. A note at the bottom states: "Note: System probes IP-Camera every 30s."

| Port | IP Address | Model | Location | Manufacturer | Traffic | Description | Throughput | | |
|-------|------------------------------|-----------------|---------------|--------------|------------|-------------|------------|-------------|------|
| eth19 | 10.90.90.73 | IPC-HFW4631M-I1 | country/china | Dahua | 186909.00M | | 5.00M | More Detail | Edit |
| eth21 | 10.90.90.202 | IPC-HFW4631M-I1 | country/china | Dahua | 65095.00M | | 6.00M | More Detail | Edit |

Note: System probes IP-Camera every 30s.

Figure 4-64 IP-Camera Information window

Dip Switch

Dip Status

Extend (250M@10Mbps)

Dip Status

This window is to view the status of the DIP switch located on the front of the device.

To view the following window, click **Dip Switch > Dip Status**, as shown below:

| Dip Status | |
|------------|--------|
| PortPri | Enable |
| Extend | Enable |
| Isolation | Enable |
| PD_Alive | Enable |
| Stp | Enable |

Figure 4-65 Dip Status window

The fields that can be configured are described below:

| Parameter | Description |
|------------------|--|
| PortPri | Check the Port Priority function is enabled or disabled on the switch. When it is enabled, packets entering the ports will be prioritized according to the ingress port number, that is, Port 1 has the highest priority and port 8 (for DSS-200G-10MP/10MPP) and port 24 (for DSS-200G-28MP/28MPP) has the lowest priority. |
| Extend | Check the Extend function is enabled or disabled on the switch. After this function is enabled, the PoE long distance of a controlled port will be able to supply power through a 250-meter network cable (20 watts with Cat 5e cable or above). Note that the ports support this PoE Extend feature are ports 1-4 of DSS-200G-10MP/10MPP and ports 1-8 of DSS-200G-28MP/28MPP. |
| Isolation | Check the Isolation function is enabled or disabled on the switch. After this function is enabled, the port isolation function of the controlled port is enabled. Packets on the controlled port can be forwarded only through the designated uplink port (port 9-10 for DSS-200G-10MP/10MPP and ports 25-28 for the DSS-200G-28MP/28MPP). |
| PD_Alive | Check whether the PD_Alive function is enabled on the switch. After this function is enabled, the PoE PD-alive function of the controlled port is enabled (go to System > PoE > PD Alive). When a PD is disconnected, the PoE will restart the PD for a maximum of three times. If the restart fails for the third time, the switch stops supplying power to the PD. |
| STP | Check whether the STP function is enabled on the switch. After STP is enabled, the STP function on the global and controlled ports is enabled (go to L2 Features > Spanning Tree > STP Global Settings). |

Extend

This window is to view the status of the port Extend State for the PoE function.

To view the following window, click **Dip Switch > Extend**, as shown below:

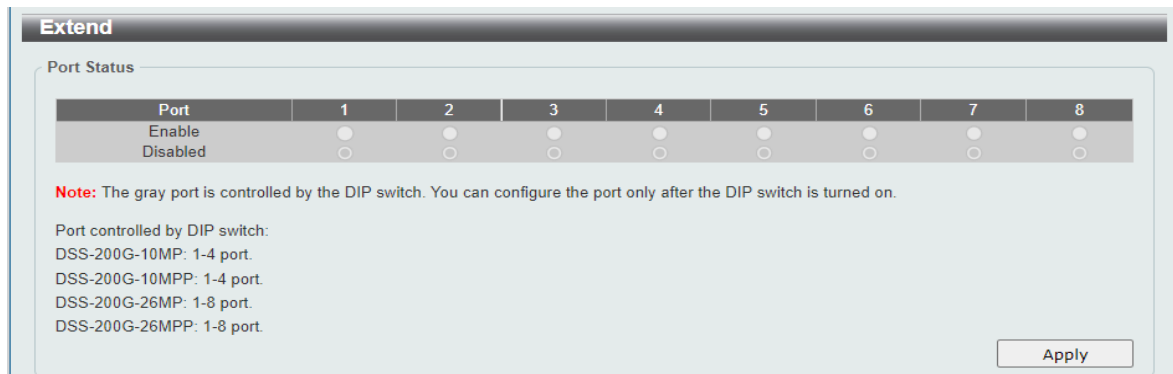


Figure 4-66 Port Extend Status window

The fields that can be configured are described below:

| Parameter | Description |
|-------------|--|
| Port | Enable the DIP switch of the port Extend function on the switch. Ports that can be configured with the PoE Extend functions: DSS-200G-10MP: 1-4 port. DSS-200G-10MPP: 1-4 port. DSS-200G-28MP: 1-8 port. DSS-200G-28MPP: 1-8 port. |

Click **Apply** to save the configuration.

Save and Tools

Save Configuration
Firmware Information
Firmware Upgrade
Configuration Restore & Backup
Ping
Reset
Reboot System
Log Backup

Save Configuration

This window is used to save the running configuration to the start-up configuration of the switch. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:

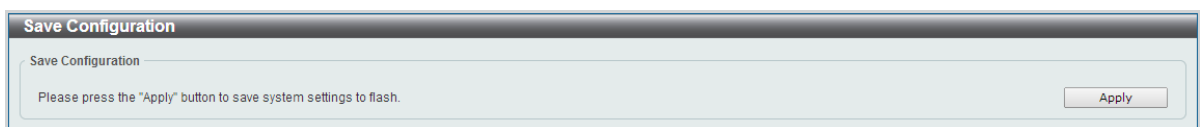


Figure 4-49 Save Configuration window

Click the **Apply** button to save the configuration to the switch's flash memory.

Firmware Information

This window is used to show firmware information.

To view the following window, click **Tools > Firmware Information**, as shown below:

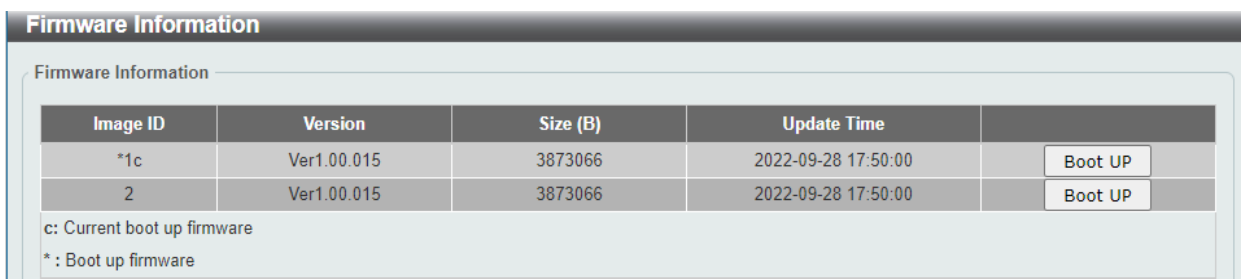


Figure 4-50 Firmware Information window

Boot Up: Clicking the **Boot Up** button will set that firmware image as the active image to use upon the next system start up.

Note: Changing the firmware only happens after the switch has been manually rebooted. In order to boot with the newly selected firmware, make sure that the switch is rebooted.

Firmware Upgrade



Note: When upgrading the firmware on the DSS-200G MP/MPP Series switch, only the image not currently active can be upgraded. All DSS-200G MP/MPP Series switches come with two images, however only one can be active at any time. (e.g. If image 1 is currently in use, only image 2 can be upgraded, and vice versa.)

Note: If the switch is in HTTPS mode, the firmware or configuration cannot be upgraded using regular HTTP.

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade > Firmware Upgrade from HTTP**, as shown below:

Figure 4-69 Firmware Upgrade from HTTP window

The fields that can be configured are described below:

| Parameter | Description |
|-------------|--|
| Source File | Enter the source filename and path of the firmware file located on the local PC. Alternatively click the Choose File button to navigate to the location of the firmware file located on the local PC. |

Click the **Apply** button to initiate the firmware upgrade.

Firmware Upgrade from TFTP

This window is used to initiate a firmware upgrade from a TFTP server.

To view the following window, click **Tools > Firmware Upgrade > firmware Upgrade from TFTP**, as shown below:

Figure 4-70 Firmware Upgrade from TFTP window

The fields that can be configured are described below:

| Parameter | Description |
|----------------|--|
| TFTP Server IP | Enter the TFTP server's IPv4 address here. |
| Source File | Enter the source filename and path of the firmware file located on the TFTP server here. |

Click the **Upgrade** button to initiate the firmware upgrade.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

Note: If the switch is in HTTPS mode, the firmware or configuration cannot be upgraded using regular HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

Figure 4-71 Configuration Restore from HTTP window

The fields that can be configured are described below:

| Parameter | Description |
|-------------|--|
| Source File | Enter the source filename and path of the configuration file located on the local PC. Alternatively click the Choose File button to navigate to the location of the configuration file located on the local PC. |

Click the **Apply** button to initiate the configuration restore.

Click **Effective immediately (running-config)** to have the uploaded configuration loaded immediately.

Click **Take effect after the next boot (startup-config)** to load the configuration after the switch has been rebooted.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:

Figure 4-72 Configuration Restore from TFTP window

The fields that can be configured are described below:

| Parameter | Description |
|----------------|---|
| TFTP Server IP | Enter the TFTP server's IPv4 address here. |
| Source File | Enter the source filename and path of the configuration file located on the TFTP server here. |

Click the **Restore** button to initiate the configuration restore.

Click **Effective immediately (running-config)** to have the uploaded configuration loaded immediately.

Click **Take effect after the next boot (startup-config)** to load the configuration after the switch has been rebooted.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

Figure 4-73 Configuration Backup to HTTP window

Select **Include username password** to save the switch configuration with user accounts and passwords to the backup file.

Select **Exclude username password** to save the switch configuration without user accounts and passwords to the backup file.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to TFTP

This window is used to initiate a configuration file backup to a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:

Figure 4-74 Configuration Backup to TFTP window

The fields that can be configured are described below:

| Parameter | Description |
|-------------------------|---|
| TFTP Server IP | Enter the TFTP server's IPv4 address here. |
| Destination File | Enter the destination path and location where the configuration file should be stored on the TFTP server. |

Select **Include username password** to save the switch configuration with user accounts and passwords to the backup file.

Select **Exclude username password** to save the switch configuration without user accounts and passwords to the backup file.

Click the **Backup** button to initiate the configuration file backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:

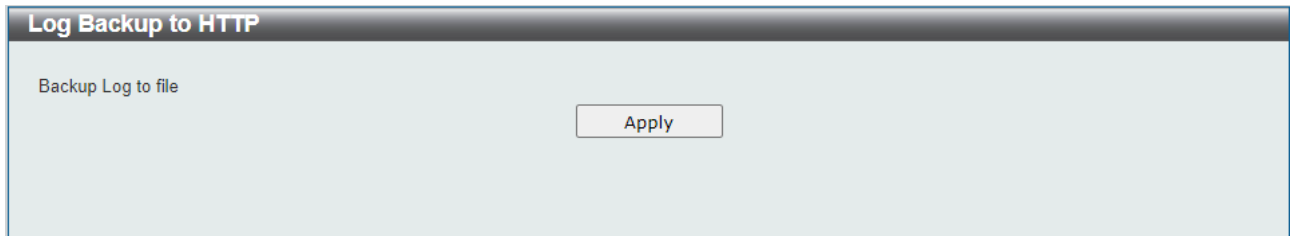


Figure 4-75 Log Backup to HTTP window

Click the **Apply** button to initiate the system log backup.

Log Backup to TFTP

This window is used to initiate a system log backup to a TFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to TFTP**, as shown below:

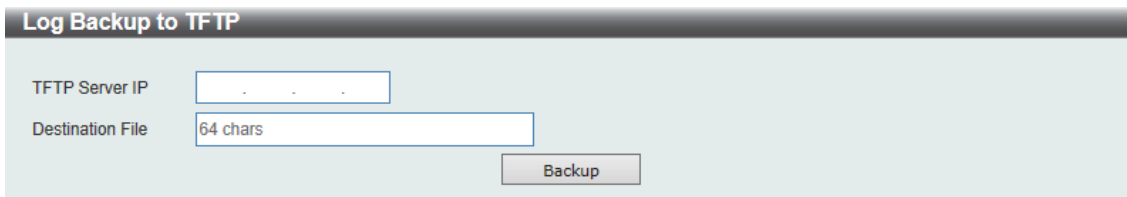


Figure 4-76 Log Backup to TFTP window

The fields that can be configured are described below:

| Parameter | Description |
|-------------------------|--|
| TFTP Server IP | Enter the TFTP server's IPv4 address here. |
| Destination File | Enter the destination path and location where the configuration file should be stored on the TFTP server |

Click the **Backup** button to initiate the system log backup.

Ping

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the switch. This is very useful to verify connectivity between the switch and other nodes on the network.

To view the following window, click **Tools > Ping**, as shown below:

Figure 4-77 Ping window

The fields that can be configured for **IPv4 Ping** are described below:

| Parameter | Description |
|----------------------------|--|
| Target IPv4 Address | Select and enter an IP address to be pinged. |
| Ping Times | Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. Users may enter a number of times between 1 and 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped. |
| Timeout | Select a timeout period between 1 and 60 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped. |

After clicking the **Start** button in **IPv4 Ping** section, the following **IPv4 Ping Result** section will appear:

Figure 4-78 Ping - IPv4 Ping Result window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

Reset

This window is used to reset the switch’s configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:

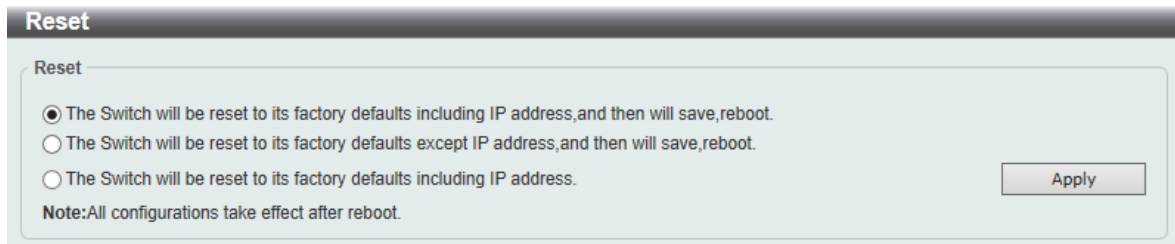


Figure 4-51 Reset window

Select **The Switch will be reset to its factory defaults including IP address and stacking information, and then will save and reboot** option to reset the switch's configuration to its factory default settings.

Select **The Switch will be reset to its factory defaults except IP address, and then will save and reboot** option to reset the switch's configuration to its factory default settings. This option will exclude the IP address from being changed.

Select **The Switch will be reset to its factory defaults including IP address** option to reset the switch's configuration to its factory default settings.

Click the **Apply** button to initiate the factory default reset and reboot the switch.



NOTE: Performing a factory reset in one version of the interface (Standard Mode or Surveillance Mode) will cause settings to be reset in the other version of the interface.

Reboot System

This window is used to reboot the switch and alternatively save the configuration before doing so. To view the following window, click **Tools > Reboot System**, as shown below:

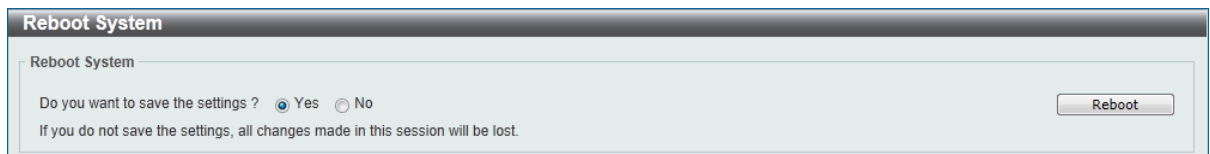


Figure 4-80 Reboot System window

When rebooting the switch, any configuration changes that was made during this session, will be lost unless you select the **Yes** option when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the switch.

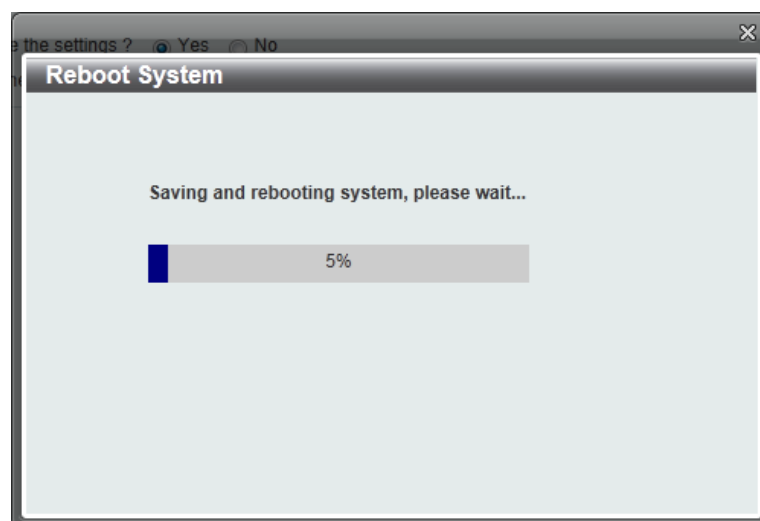


Figure 4-81 Reboot System – Rebooting window

5. Surveillance

Web User Interface – Surveillance Mode

When you complete the Surveillance Mode Smart Wizard you will be presented with the following screen:

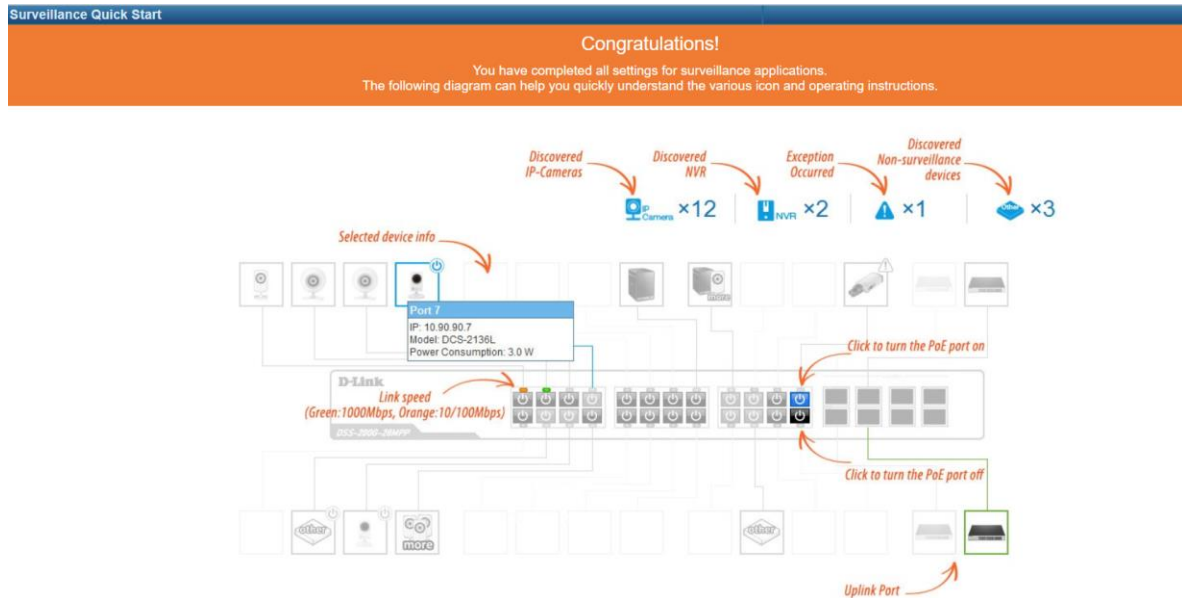


Figure 5-1 Congratulations window

Scroll to the bottom of the page and click the OK button to continue to the Web UI.

Areas of the User Interface

The figure below shows the user interface. Two distinct areas divide the user interface, as described in the table.



Figure 5-2 Main Web UI Window

| Area Number | Description |
|-------------|--|
| AREA 1 | The navigation menu is displayed in this area. Click on the links and navigate the folder structure to display information on the main page. |
| AREA 2 | This is the main page for displaying information and configuration options for the switch. The page displayed here is based on the selection in AREA 1. |
| AREA 3 | This area displays a toolbar used to access Save and Tools menus. It also provides access to the Setup Wizard and selection between Surveillance and Standard Mode . |

The **Surveillance Overview** page loads automatically when you log-in to the switch and contains two tabs; Surveillance Topology and Device Information. To return to the Surveillance Overview page after viewing other pages, click the model number of the switch at the top of the navigation menu.

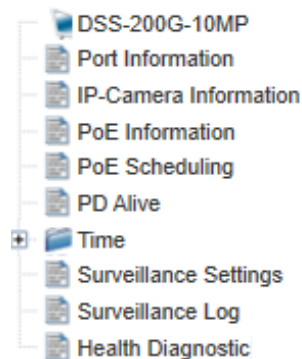


Figure 5-3 Switch Model Number

Surveillance Topology

This is the default tab on the Surveillance Overview page. It contains a diagram of the surveillance topology, including an overview of the devices connected to the switch.

To view the following window, click on the model number of the switch at the top of the navigation menu:

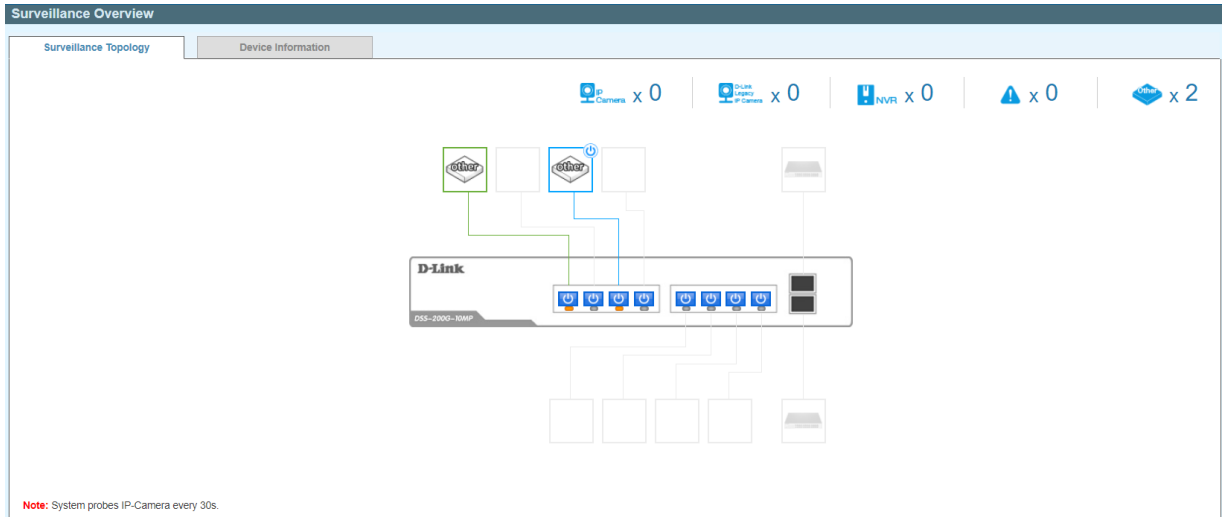







Figure 5-4 Surveillance Topology Window

There is a device count at the top of the page, listing the number of connected IP cameras, Network Video Recorders (NVRs) and unrecognized devices. It also lists the number of warnings on the system.

The icon descriptions are as follows:

| Icon | Description |
|---|--|
|  | The total number of IP cameras detected. |

| | |
|---|--|
|  | D-LINK IPC Discovered by Surveillance VLAN but not support ONVIF protocol. |
|  | The total number of NVRs detected. |
|  | The number of warnings on the system. Consult the Surveillance Log and Health Diagnostic pages for more information. |
|  | The number of ports that have an unknown device connected that does not support ONVIF. |








The Surveillance Topology gives you more information about what is connected to each port. Hover over each device icon to get more information about the recognized devices, such as: the number of devices, device type, IP address, power consumption, link speed and errors. Click on the 'more' link to get more information about the devices connected to a port. Each port can also be powered-on and off using PoE by clicking the power symbol on each port. You can also configure the PD Alive function by clicking on the device icon.







CAUTION: Before connecting the Powered Device (PD) and enabling 60/90 W PoE, make sure it supports IEEE802.3bt, as otherwise it will become damaged.

See below for more information on enabling and disabling PoE.

A breakdown of each device icon is below:

| Icon | Description |
|---|--|
|  | One ONVIF IP camera discovered on this port. |
|  | |
|  | The link is up but no ONVIF IP camera or NVR has been discovered on this port. |
|  | Multiple ONVIF IP cameras discovered on this port. |
|  | One NVR discovered on this port. Any device fetching surveillance stream from IP camera will be recognized as NVR. |
|  | Multiple NVRs discovered on this port. |
|  | One ONVIF IP camera and one NVR discovered on this port. |

| | |
|---|--|
|  | Multiple ONVIF IP cameras and one NVR discovered on this port. |
|  | One ONVIF IP camera and multiple NVRs discovered on this port. |
|  | This port is set as uplink port and it is connected. |
|  | This port is set as uplink port and it is link down. |



NOTE: A breakdown of the device icons can be found by clicking the Help menu at the top of the page.



NOTE: The switch uses ONVIF traffic to monitor the surveillance device status, but some third-party devices do not fully comply with the ONVIF standard. If you are having problems with surveillance devices not being detected, please check the ONVIF compatibility with the original surveillance device manufacturer.







NOTE: The system probes for new IP cameras every 30 seconds.






NOTE: If the switch does not detect any network activity from surveillance devices, it will remove inactive surveillance devices from the Surveillance Topology every 5 minutes.

The icon border indicates the PoE status for the port:



| Icon Border | Description |
|---|--|
|  | The device is operational but not powered by PoE. |
|  | The device is operational and is powered by PoE. |
|  | The device has malfunctioned and there is a problem with the port or device. |

| | |
|---|--|
|  | <p>The device is operational and is powered by PoE and it is activated by PD Alive. Click on the icon to bring up the PD Alive Configuration menu.</p> |
|---|--|

The port status indicators dictate the speed and status of the link:

| Port Status | Description |
|---|---------------------------------------|
|  | The link is down. |
|  | The port is connected at 1 Gbps. |
|  | The port is connected at 10/100 Mbps. |

The PoE status is indicated by the power icon on each port:

| Port Status | Description |
|---|------------------------------|
|  | PoE is enabled on the port. |
|  | PoE is disabled on the port. |

Enabling and Disabling PoE



CAUTION: Before connecting the Powered Device (PD) and enabling 60/90 W PoE, make sure it supports IEEE802.3bt,

The power status of each port can be changed by clicking the power icon on each port. The default setting for PoE is on. To change the PoE type, first disable PoE and then re-enable it using the type of PoE required.

The following dialogue box will be displayed when disabling PoE on a port:

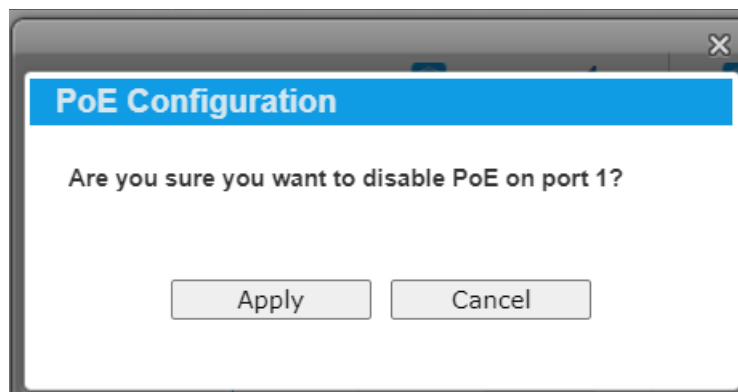


Figure 5-5 PoE Configuration

Click the **Apply** button to accept the changes made.

Device Information

This is the second tab on the Surveillance Overview page and is divided into 7 areas; a device information section, PoE utilization section, bandwidth utilization section, CPU utilization section, Memory utilization section and Rotating speed section.

To view the following window, click on the model number of the switch at the top of the navigation menu and then click the **Device Information** tab:

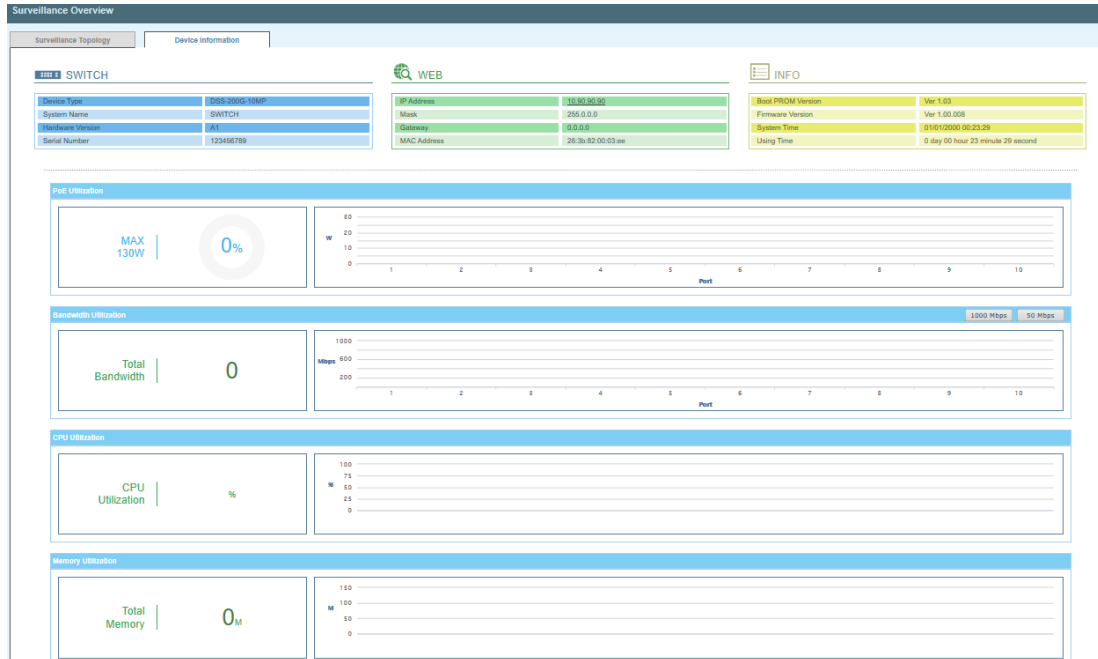


Figure 5-6 Device Information Window

The device information section is sub-divided into 3 sections; switch information, web information and system information. It contains information such as the device type, system name, serial number, IP address settings, MAC address settings, firmware versions and system uptime.

The PoE utilization area contains PoE utilization statistics for the switch. On the left is the total PoE utilization, with the total power budget and overall utilization shown. On the right is a per-port usage graph, showing the PoE utilization for each individual port.

The bandwidth usage section contains bandwidth utilization for the switch. On the left the total bandwidth shows the total inbound traffic on all ports. There is also a per-port bandwidth utilization graph on the right, showing the inbound traffic for each individual port. The scale of the graph can be changed by pressing the 1000 Mbps and 50 Mbps buttons above the graph.

The CPU utilization section contains CPU utilization statistics for the switch. On the left is the current CPU utilization. On the right is CPU usage percentage recorded every 10 seconds.

The memory utilization section shows the memory utilization graph of the switch. On the left is the current memory usage. On the right side shows memory usage records every 10 seconds.

The Temperature section displays the recorded system temperature every 10 seconds.

The Rotating speed section shows the fan speed status.

Note: DSS-200G-10MP does not have fans, the Rotating speed are not shown.

Port Information

The Port Information section provides an overview of the port status for each port. This includes the Throughput, PoE Turn, Loopback Detection Status, Distance, power consumption and the devices connected to each port.

To view the following window, click on the **Port Information** link in the navigation menu:

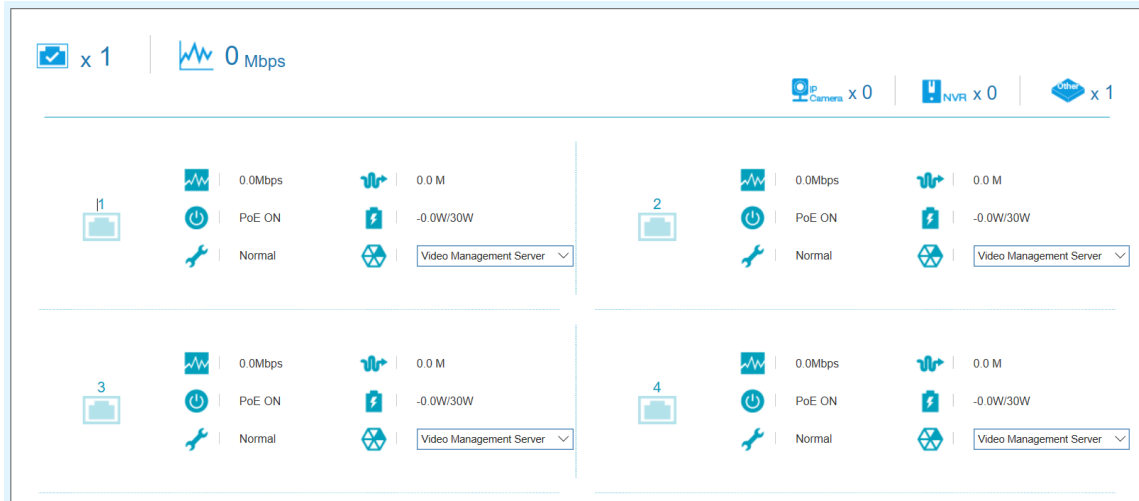














Figure 5-7 Port Information Window

The number of ports in use and the total throughput is listed at the top of the page. The icon descriptions are as follows:

| Icon | Description |
|---|--|
|  | The total number of ports that are being connected. |
|  | The total inbound throughput for all ports on the switch. |
|  | The total number of ONVIF IP Cameras detected. |
|  | The total number of NVRs detected. |
|  | The number of ports that have an unknown device connected that does not support ONVIF. |

Hover-over each field to get more information about each value. A breakdown of each field is below:

| Icon | Description |
|---|--|
|  | The port number of the port. |
|  | The total inbound throughput for the port on the switch (measured in Mbps). |
|  | The cable length (in meters), taken from the Health Diagnostics page. |
|  | The PoE status for the port (PoE on or off). |
|  | The PoE consumption of the port. The first number for PoE means that power is being consumed by the port. The second number is the PoE budget configured for the port (refer to the PoE > PoE Configuration in the Standard Mode). |
|  | The Loopback Detection status. If a loop is detected, the icon will change to include a link to the Health Diagnostics page. |
|  | The Group Details page. If an ONVIF device is detected as being connected to the port, the icon changes to include a link to the Group Details page. If a device is connected that is not ONVIF compatible, a drop-down menu will be available to define the type of device connected. |

Group Details

The Group Details page lists the devices connected to a specific port. Only devices that have been recognized as supporting ONVIF or NVRs will be displayed.

To view the following window, click on the **Port Information** link in the navigation menu and then click on the **Group Details** link for a port that has recognized devices connected to it:

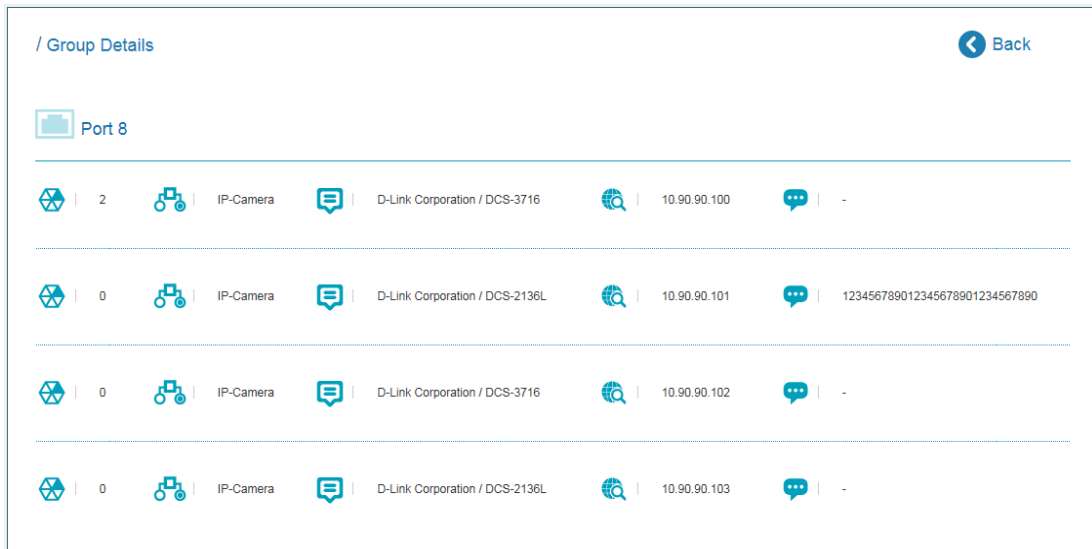









Figure 5-8 Group Details Window

The port number that the Group Details apply to is listed at the top of the page. The icon descriptions are as follows:

| Icon | Description |
|---|--|
|  | The port number that the Group Details apply to. |
|  | Click to go back to the Port Information page. |

Hover-over each field to get more information about each value. A breakdown of each field is below:

| Icon | Description |
|---|--|
|  | The Group Number that the device belongs to. All devices managed by an NVR belong to the same Group Number. These are assigned sequentially, with NVR1 having Group Number 1. If an NVR is removed, the Group Numbers will be updated accordingly (if NVR1 is removed then Group Number 2 will become Group Number 1). |
|  | The device type. This can be an IP camera or NVR. |
|  | The Model name of the IP camera. Nothing is displayed in this field if an NVR is connected. |
|  | The IP address of the IP camera or NVR. |
|  | The device description. This can be edited on the IP camera Information page or NVR Information page. |

IP-Camera Information

The IP-Camera Information section provides information on each camera connected to the switch. It features the port number, device type, throughput, IP address and other information such as port description, power consumption and location.

To view the following window, click on the **IP-Camera Information** link in the navigation menu:

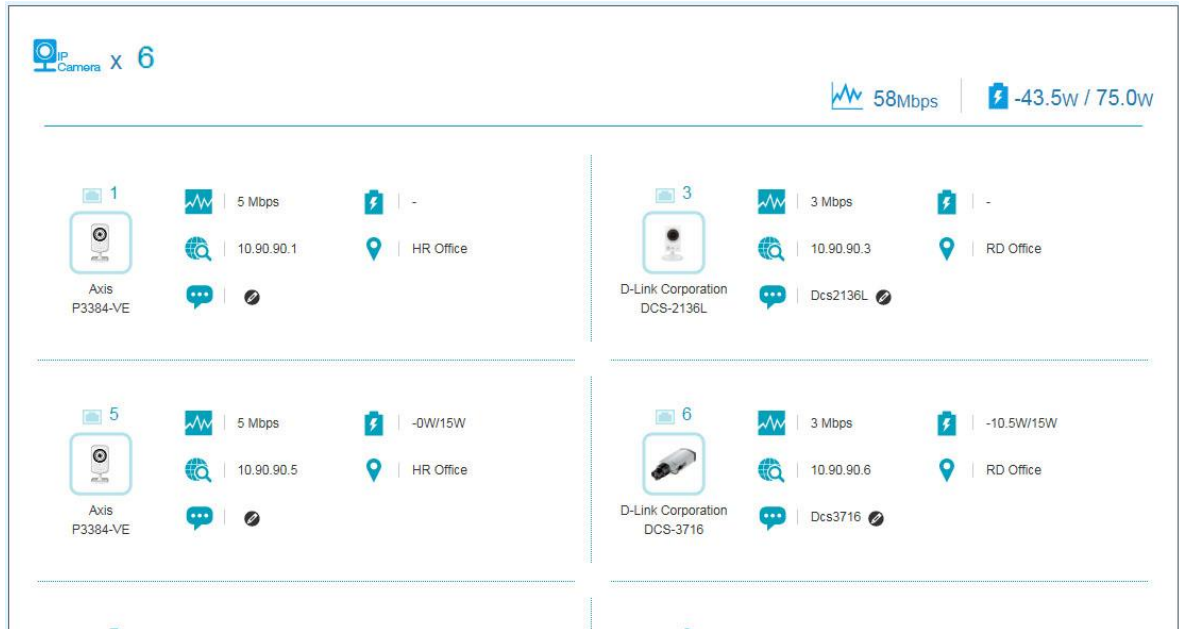








Figure 5-9 IP-Camera Information Window

The total device count, throughput and power consumption is listed at the top of the page. The icon descriptions are as follows:

| Icon | Description |
|------|---|
| | The total number of ONVIF IP cameras detected. |
| | The total inbound throughput for all ports on the switch. |
| | The PoE consumption of the switch. This is listed as one negative integer and one positive integer. The negative integer is the power being consumed by the PoE devices connected to the port. The positive integer is the total PoE budget for the ports currently using PoE, based on the type of PoE in use. |

Hover-over each field to get more information about each value. A breakdown of each field is below:

| Icon | Description |
|------|--|
| | The port number of the port. |
| | The device icon or photo. A generic photo will displayed for a non-D-Link ONVIF camera. A D-Link-specific photo will be displayed for a D-Link ONVIF camera. |
| | The total inbound throughput for the port on the switch (measured in Mbps). |

| | |
|---|---|
|  | The PoE consumption of the port. This is listed as one negative integer and one positive integer. A negative value for PoE means that power is being consumed by the port. The positive integer is the PoE budget for PoE standard in use. |
|  | The IP address of the IP camera. |
|  | The location of the IP camera. |
|  | The description of the IP camera. This can be edited by clicking the black pencil icon next to the field () and then the green pencil icon when the description has been entered () |

Note: System probes IP cameras every 30s.

PoE Information

The PoE Information section provides information on the PoE usage of each port. The port number, PoE status, health status, PoE budget and power consumption is listed for each port. It is possible to click on the health status to be re-directed to the Health Diagnostic page. Hover-over each field to get more information about each value.

To view the following window, click on the **PoE Information** link in the navigation menu:

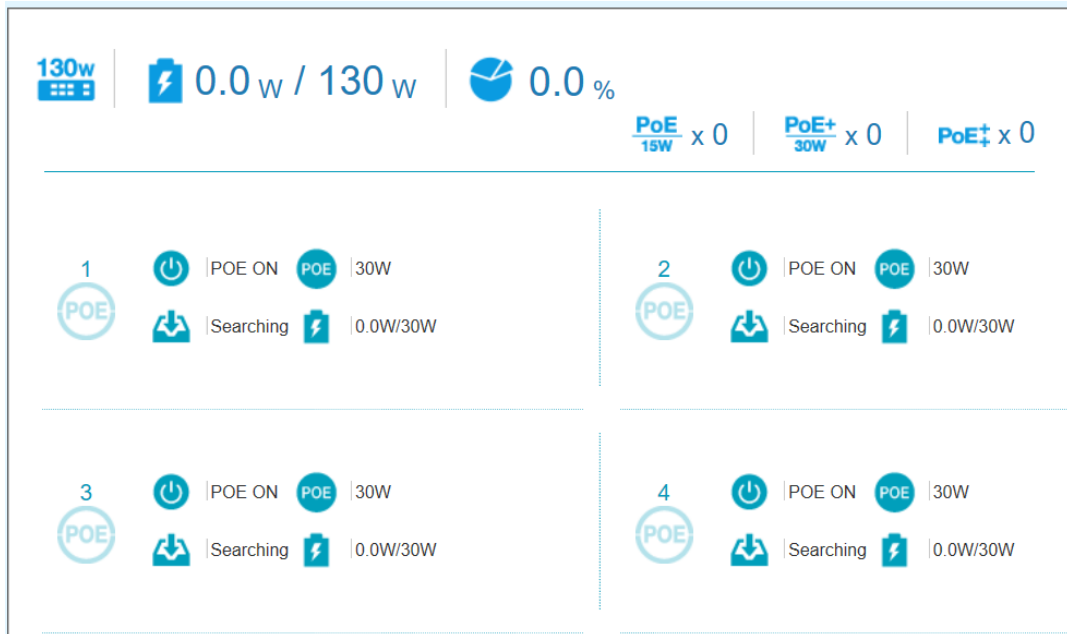







Figure 5-10 PoE Information Window

The total power budget, power consumption, power budget consumption and the types of PoE in use are listed at the top of the page. The icon descriptions are as follows:

| Icon | Description |
|------|---|
| | The total PoE power budget. |
| | The PoE consumption of the switch. The first number is the power being consumed by the PoE devices connected to the switch. The second number is the maximum PoE budget of the entire system. |
| | The current utilization of PoE power budget. |
| | Number of PoE devices rated class 0 to 3 were found |
| | Number of PoE devices rated class 4 were found. |
| | Number of PoE devices rated class 5 to 8 were found |

Hover-over each field to get more information about each value. A breakdown of each field is below:

| Icon | Description |
|------|-------------|
|------|-------------|

| | |
|---|---|
|  | The port number of the port. |
|  | The PoE status for the port (PoE on or off). |
|  | The maximum PoE power budget for this port. This can be 30 W, or 30 W/60 W/90 W if this port supports 4-pair PoE. |
|  | The PoE state. If any fault is detected the icon changes to include a description of the problem and a link to the Health Diagnostic page. |
|  | The PoE consumption of the port. The first number for PoE means that power is being consumed by the port. The second number indicates PoE budget configured for the port (refer to the PoE > PoE Configuration of the Standard Mode). |

PoE Scheduling

PoE Scheduling is a feature which allows you to specify the amount of time that power is delivered to a PoE port. This can be used to save power when devices are not in use, or as a security feature to prevent wireless access from being available outside of business hours, for example. It is possible to set a schedule name, a start time, an end time and which ports the PoE schedule applies to.

To view the following window, click on the **PoE Scheduling** link in the navigation menu:

Figure 5-11 PoE Scheduling Window

The fields that can be configured for the **Time Profile** are described below:

| Parameter | Description |
|-----------------------------|---|
| Range Name | Enter a descriptive name for the PoE schedule. |
| Days | Check this tick-box to enable the schedule daily and gray-out the day-of-week fields in the From Time/To Time sections. |
| From Time (Day/Hour) | The start day and time for the PoE schedule. Click the calendar icon to pick this using a graphic calendar tool. |
| To Time (Day/Hour) | The end day and time for the PoE schedule. Click the calendar icon to pick this using a graphic calendar tool. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **PoE Configuration** are described below:

| Parameter | Description |
|-------------------|---|
| From Port | The start port in the range that the PoE schedule will apply to. |
| To Port | The end port in the range that the PoE schedule will apply to. |
| Time Range | The Time Profile created above. |

Click the **Apply** button to accept the changes made.

PD Alive

This window is used to configure the PD Alive function for PDs connected to the PoE ports. The ping function via ICMP requests is used to check if PDs, connected to the PoE ports, are active or not. When PDs appear to be inactive, the specified action (Reset, Notify, or Both) will be taken.

To view the following window, click on the **PD Alive Configuration** to enter the navigation menu:

| Port | PD Alive State | PD IP Address | Poll Interval | Retry Count | Waiting Time | Action |
|------|----------------|---------------|---------------|-------------|--------------|--------|
| eth1 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth2 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth3 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth4 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth5 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth6 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth7 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |
| eth8 | Enabled | 0.0.0.0 | 30 | 2 | 90 | Both |

Figure 5-11 PD-Alive Window

The fields that can be configured are described below:

| Parameter | Description |
|-------------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration here. |
| PD Alive State | Select to enable or disable the PD Alive function on the specified port(s). Note that a port's PD Alive state cannot be disabled if the DIP Switch on the front panel has been turned on. |
| PD IP Address | Enter the IP address of the PD here. |
| Pool interval (10-300) | Enter the pool interval here. This is the interval between ping messages from the system to PDs connected to the PoE port(s). The range is from 10 to 300 seconds. |
| Retry Count (0-5) | Enter the retry count here. This is the amount of ping messages that will be sent (at each interval) when PDs are not responding. The range is from 1 to 5. |
| Wait Time (30-300) | Enter the waiting time here. This is how long the system will wait before sending ping messages to the PD connected to the PoE port after a 'Reset' action was taken. The range is from 30 to 300 seconds. |
| Action | Select the action that will be taken here. Options to choose from are Reboot , Notify , and Both . Reboot - Specifies to reset the PoE port state (turn PoE off and on). Notify - Specifies to send logs and traps to notify the administrator. Both - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on). |

Click the **Apply** button to accept the changes made.

Time

Clock Settings
SNTP Settings

Clock Settings

This sub-menu is used to configure the time on the switch.

To view the following window, go to: **Time > Clock Settings** in the navigation menu:

Figure 5-12 Clock Settings Window

The fields that can be configured for the **Clock Settings** are described below:

| Parameter | Description |
|-------------------------------|---|
| System Time (HH:MM:SS) | Use this to set the system time in the format (HH:MM:SS). |
| Date (DD / MM / YYYY) | Use this to set the date, in the format (DD / MM / YYYY). |

Click the **Apply** button to accept the changes made.

SNTP Settings

This sub-menu is used to configure an external time source on the switch. Simple Network Time Protocol (SNTP) is a lightweight version of the NTP protocol and can be used to keep the system clock in sync with a network-based time source.

To view the following window, go to: **Time > SNTP Settings** in the navigation menu:

Figure 5-13 SNTP Settings Window

The fields that can be configured for the **SNTP Global Settings** are described below:

| Parameter | Description |
|---------------------------------|---|
| Current Time Source | Displays the current time source for the switch. |
| SNTP State | Set the SNTP state. Options are Enabled or Disabled . |
| Pool Interval (30-99999) | Set the synchronization interval for SNTP. The default is 1000 seconds and the range is 30 – 99999 seconds. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **SNTP Server Settings** are described below:

| Parameter | Description |
|---------------------|---|
| Server | Select major server or standby server |
| IPv4 Address | Enter the IP address of the SNTP server you would like to synchronize with. |

Click the **Apply** button to accept the changes made.

Surveillance Settings

The Surveillance Settings page is used to configure the settings for the Surveillance VLAN. This is a VLAN dedicated for IP camera and surveillance traffic and can be used to manage surveillance devices on the network.

To view the following window, click on the **Surveillance Settings** link in the navigation menu:

Figure 5-14 Surveillance Settings Window

The fields that can be configured for the **Surveillance VLAN Settings** are described below:

| Parameter | Description |
|-------------------------|--|
| VLAN ID (2-4094) | Enter a VLAN number for the surveillance VLAN in the range (2-4094). |

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **IP Settings** are described below:

| Parameter | Description |
|--------------------|--|
| Get IP From | Choose how the management IP for this VLAN is assigned to the switch. Options are: DHCP or Static . If Static is chosen, the following fields become available: |
| IP Address | Enter the IP address for the surveillance VLAN management IP. |
| Mask | Enter the net mask for the surveillance VLAN management IP. |
| Gateway | Enter the gateway for the surveillance VLAN. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **SNMP Host Settings** are described below:

| Parameter | Description |
|--------------------------|--|
| Host IPv4 Address | Enter the IP address of the SNMP Network Management Server (NMS) which will receive SNMP Traps from this device. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **Log Server** are described below:

| Parameter | Description |
|--------------------------|---|
| Host IPv4 Address | Enter the IP address of the Sys log NMS which will receive Sys log messages from this device. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **Password Settings** are described below:

| Parameter | Description |
|-------------------------|--|
| Password | Configure the password that will be used to restrict access to the device via the Web UI. The password must contain 8 to 30 characters and include both letters and numbers. |
| Confirm Password | Confirm the password that will be used to restrict access to the device via the Web UI. The password must contain 8 to 30 characters and include both letters and numbers. |

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **Uplink Port Settings** are described below:

| Parameter | Description |
|------------------|---|
| From Port | Enter the start port in the range for Uplink Ports. These are used for connecting the surveillance VLAN with other switches. |
| To Port | Enter the end port in the range for Uplink Ports. These are used for connecting the surveillance VLAN with other switches. |

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete any entries in the list of uplink ports.



NOTE: It is highly recommended that only uplink ports are connected to other switches, as the IP camera discovery process is disabled on these ports. Use the **Uplink Port Settings** section of the interface to define which ports connect to other switches.

NOTE: The default uplink ports of the DSS-200G-10MP/10MPP are port 9 and port 10. The default uplink ports of DSS-200G-28MP/28MPP are port 25 to port 28.

Surveillance Log

The Surveillance Log consists of a list of Sys log messages that have been generated by the switch. Depending on whether a Sys log server has been defined in the Surveillance Settings section, these may be local to the switch or copied to an external logging server. The messages are ordered in date order with the latest message at the top of the list. Please consult an external source for more information on Sys log logging levels.

To view the following window, click on the **Surveillance Log** link in the navigation menu:



| Index | Time | Level | Log Description |
|-------|---------------------|---------|---|
| 14 | 2023/10/27 14:11:57 | INFO(6) | ONVIF: Remove IPC(IP:192.168.0.168 MAC:00-0e-ae-a5-d4-8f) |
| 13 | 2023/10/27 14:05:58 | INFO(6) | ONVIF: Add IPC(IP:192.168.0.168 MAC:00-0e-ae-a5-d4-8f) |
| 12 | 2023/10/27 14:05:57 | INFO(6) | ONVIF: Remove IPC(IP:192.168.0.168 MAC:00-0e-ae-a5-d4-8f) |
| 11 | 2023/10/27 13:39:18 | INFO(6) | ONVIF: Add IPC(IP:192.168.0.168 MAC:00-0e-ae-a5-d4-8f) |
| 10 | 2023/10/27 11:37:28 | INFO(6) | ONVIF: Remove IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |
| 9 | 2023/10/27 11:32:24 | INFO(6) | ONVIF: Add IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |
| 8 | 2023/10/27 11:10:39 | INFO(6) | ONVIF: Remove IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |
| 7 | 2023/10/27 11:05:35 | INFO(6) | ONVIF: Add IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |
| 6 | 2023/10/27 10:06:35 | INFO(6) | ONVIF: Remove IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |
| 5 | 2023/10/27 10:03:00 | INFO(6) | ONVIF: Add IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |
| 4 | 2000/01/02 02:50:22 | INFO(6) | ONVIF: Remove IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |
| 3 | 2000/01/02 02:45:17 | INFO(6) | ONVIF: Add IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |
| 2 | 2000/01/01 02:41:28 | INFO(6) | ONVIF: Remove IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |
| 1 | 2000/01/01 02:36:24 | INFO(6) | ONVIF: Add IPC(IP:192.168.0.20 MAC:00-0e-ae-a5-d4-8f) |

Figure 5-15 Surveillance Log Window

Refresh: This will refresh the page.

Backup: This will allow you to save a local copy of the Sys log messages as a text file.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Health Diagnostic

The Health Diagnostic page is linked-to by the Port Information and PoE Information pages and displays an overview of the port status. It contains the port number, Loopback Detection status, Cable Link status, PoE Status, Tx/Rx Error Counter, DDM (Digital Diagnostic Monitoring), and number of Discovered Surveillance Devices on the port (which links to the Group Details page) and the detected cable length. The page automatically refreshes every 30 seconds.

To view the following window, click on the **Health Diagnostic** link in the navigation menu:

| Health Diagnostic | | | | | | | |
|-------------------|---------------------------|------------|------------|-------------------|-----|---------------------------------|-----------------|
| Port | Loopback Detection Status | Cable Link | PoE Status | Tx/Rx CRC Counter | DDM | Discovered Surveillance Devices | Detect Distance |
| 1 | Normal | - | Searching | - | - | ┆ | Detect |
| 2 | Normal | - | Disable | - | - | ┆ | Detect |
| 3 | Normal | - | Searching | - | - | ┆ | Detect |
| 4 | Normal | - | Searching | - | - | ┆ | Detect |
| 5 | Normal | - | Disable | - | - | ┆ | Detect |
| 6 | Normal | - | Searching | - | - | ┆ | Detect |
| 7 | Normal | - | Searching | - | - | ┆ | Detect |
| 8 | Normal | - | Searching | - | - | ┆ | Detect |
| 9 | Normal | 1000M/Full | Searching | Pass | - | 0 | Detect |
| 10 | Normal | - | Searching | - | - | ┆ | Detect |
| 11 | Normal | - | Searching | - | - | ┆ | Detect |
| 12 | Normal | - | Searching | - | - | ┆ | Detect |
| 13 | Normal | - | Searching | - | - | ┆ | Detect |
| 14 | Normal | - | Searching | - | - | ┆ | Detect |
| 15 | Normal | - | Searching | - | - | ┆ | Detect |
| 16 | Normal | - | Searching | - | - | ┆ | Detect |

Figure 5-16 Health Diagnostic Window

Detect: Detect the cable length of the listed port.

Detect All: Detect the cable length of all ports.

Save and Tools

Firmware Information
Firmware Upgrade
Configuration Restore & Backup
Reset
Reboot System

Firmware Information

This window is used to show firmware information.

To view the following window, click **Tools > Firmware Information**, as shown below:

| Firmware Information | | | | |
|----------------------|--------------|----------|---------------------|--|
| Image ID | Version | Size (B) | Update Time | |
| *1c | Ver1.00.020 | 3825949 | 2000-01-01 00:04:40 | <input type="button" value="Boot UP"/> |
| 2 | Ver1.00.019b | 3882133 | 2000-01-01 00:06:34 | <input type="button" value="Boot UP"/> |

c: Current boot up firmware
 *: Boot up firmware

Figure 5-17 Firmware Information window

Boot Up: Clicking the **Boot Up** button will set that firmware image as the active image to use upon the next system start up.



NOTE: Changing the firmware only takes effect after the switch has been manually rebooted. In order to boot with the newly selected firmware, make sure that the switch is rebooted.

Firmware Upgrade



NOTE: When upgrading the firmware on the DSS-200G MP/MPP series switch, only the image not currently active can be upgraded. All DSS-200G MP/MPP series switches come with two images, however only one can be active at any time. (e.g. If image 1 is currently in use, only image 2 can be upgraded, and vice versa.)

NOTE: If the switch is in HTTPS mode, the firmware or configuration cannot be upgraded using regular HTTP.

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

| Firmware Upgrade from HTTP | |
|--------------------------------------|---|
| Source File | <input type="button" value="Choose File"/> No file chosen |
| Destination | Image 2 |
| <input type="button" value="Apply"/> | |

Figure 5-18 Firmware Upgrade from HTTP window

The fields that can be configured are described below:

| Parameter | Description |
|--------------------|---|
| Source File | Enter the source filename and path of the firmware file located on the local PC. Alternatively click the Browse button to navigate to the location of the firmware file located on the local PC. |

Click the **Apply** button to initiate the firmware upgrade.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

NOTE: If the switch is in HTTPS mode, the firmware or configuration cannot be upgraded using regular HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

Figure 5-19 Configuration Restore from HTTP window

The fields that can be configured are described below:

| Parameter | Description |
|-------------|---|
| Source File | Enter the source filename and path of the configuration file located on the local PC. Alternatively click the Browse button to navigate to the location of the configuration file located on the local PC. |

Click the **Apply** button to initiate the configuration restore.

Click **Effective immediately (running-config)** to have the uploaded configuration loaded immediately.

Click **Take effect after the next boot (startup-config)** to load the configuration after the switch has been rebooted.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

Figure 5-20 Configuration Backup to HTTP window

Select **Include username password** to save the switch user accounts and passwords to the backup file.

Select **Exclude username password** to save the switch user accounts and passwords to the backup file.

Click the **Apply** button to initiate the configuration file backup.

Reset

This window is used to reset the switch's configuration to the factory default settings.

To view the following window, click **Tools >Reset**, as shown below:



Figure 5-21 Reset window

Select **The Switch will be reset to its factory defaults including IP address, and then will save and reboot.** to reset the switch's configuration to its factory default settings.

Select **The Switch will be reset to its factory default except IP address, and then will save and reboot.** to reset the switch's configuration to its factory default settings. This option will exclude the IP address from being changed.

Select **The Switch will be reset to its factory defaults including IP address.** to reset the switch's configuration to its factory default settings.

Click the **Apply** button to initiate the factory default reset and reboot the switch.



NOTE: Performing a factory reset in one version of the interface (Standard Mode or Surveillance Mode) will cause settings to be reset in the other version of the interface.

Reboot System

This window is used to reboot the switch and alternatively save the configuration before doing so. To view the following window, click **Tools >Reboot System**, as shown below:



Figure 5-22 Reboot System window

When rebooting the switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the switch.

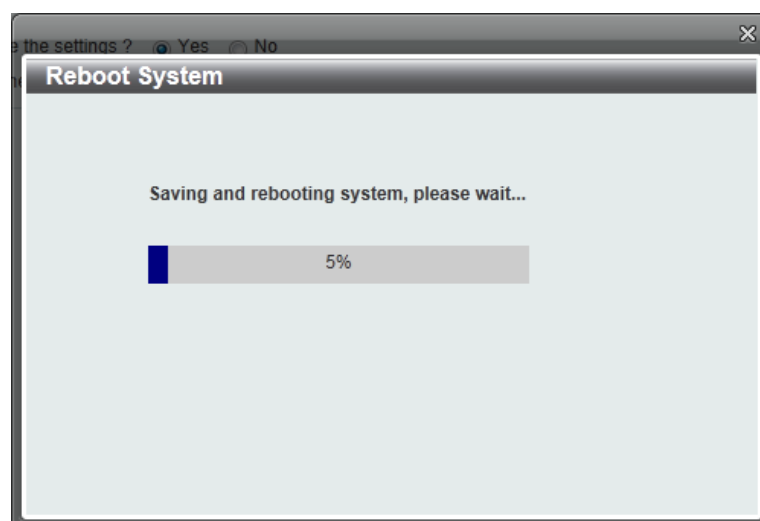


Figure 5-23 Reboot System – Rebooting window

Help

Help

Click the Help button on the page for Help information.

Surveillance Help

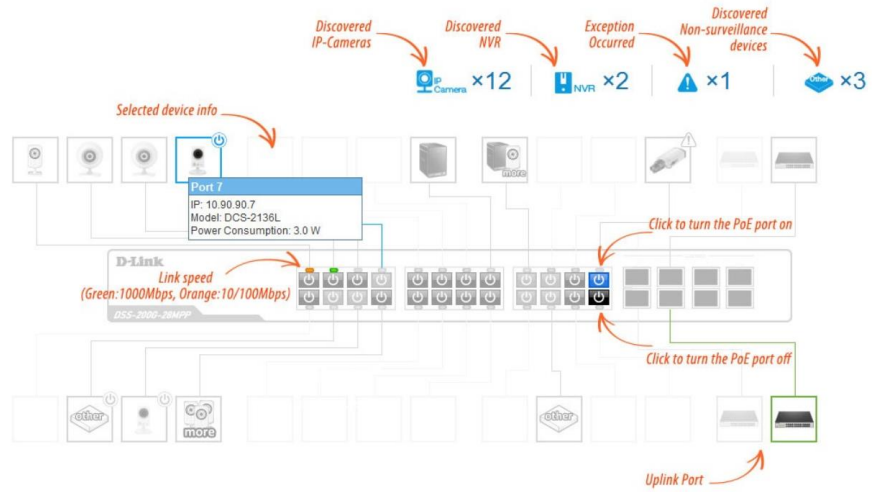


Figure 5-24 Help Window

6. Appendix A - Ethernet Technology

This chapter will describe the features of the D-Link DSS-200G MP/MPP series switch and provide some background information about Ethernet/Fast Ethernet/Gigabit Ethernet switching technology.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, and management objects, but with a tenfold increase in theoretical throughput of over 100-Mbps Fast Ethernet and a hundredfold increase over 10-Mbps Ethernet. Since it is compatible with all 10-Mbps and 100-Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting existing investments in hardware, software, or trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential to help solving network bottlenecks that frequently develop as more advanced computer users and newer applications continue to demand greater network resources. Upgrading key components, such as backbone connections and servers to Gigabit Ethernet technology can greatly improve network response times as well as significantly speed up the traffic between subnets.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internet working technologies. And with expected advances in the coming years in silicon technology and digital signal processing that will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, outfitting your network with a powerful 1000-Mbps-capable backbone/server connection which will create a flexible foundation for the next generation of network technology products.

Fast Ethernet Technology

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies have been proposed to provide greater bandwidth and improve client/server response times. Among them, 100BASE-T (Fast Ethernet) provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The non-disruptive and smooth evolution nature, and the dominating potential market base, virtually guarantees cost-effective and high performance Fast Ethernet solutions.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the CSMA/CD Ethernet protocol. Since the 100Mbps Fast Ethernet is compatible with all other 10Mbps Ethernet environments, it provides a straightforward upgrade and utilizes existing investments in hardware, software, and personnel training.

Switching Technology

Another approach to push beyond the limits of Ethernet technology is the development of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by dividing a local area network into different segments which won't compete with each other for network transmission capacity.

The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another. By doing this the total network capacity is multiplied, while still maintaining the same network cabling and adapter cards.

7. Appendix B - Technical Specifications

Hardware Specifications

Key Components / Performance

- Switching Capacity:
 - DSS-200G-10MP: 20Gbps
 - DSS-200G-10MPP: 20Gbps
 - DSS-200G-28MP: 56Gbps
 - DSS-200G-28MPP: 56Gbps
- Max. Forwarding Rate:
 - DSS-200G-10MP: 14.88Mpps
 - DSS-200G-10MPP: 14.88Mpps
 - DSS-200G-28MP: 41.67Mpps
 - DSS-200G-28MPP: 41.67Mpps
- Forwarding Mode: Store and Forward
- Packet Buffer memory:
 - DSS-200G-10MP: 4.1Mbits
 - DSS-200G-10MPP: 4.1Mbits
 - DSS-200G-28MP: 4.1Mbits
 - DSS-200G-28MPP: 4.1Mbits
- Flash Memory: 32M Byte

Port Functions

- 10/100/1000BaseTX ports compliant with the following standards:
 - IEEE 802.3
 - IEEE 802.3u
 - IEEE 802.3ab
 - IEEE802.3at
 - IEEE 802.3af
 - IEEE 802.3bt (DSS-200G MPP Series only)
 - Supports Full/half-Duplex operations at 10/100Mbps
 - Supports Full-Duplex operation at 1000Mbps
 - Supports IEEE 802.3x Flow Control
 - Support Auto-Negotiation
 - Compliant to IEEE 802.3az Energy Efficiency Ethernet.
- SFP ports compliant with the following standards:
 - IEEE 802.3u compliance
 - IEEE 802.3z compliance

Physical & Environment

- Maximum Power Consumption
 - DSS-200G-10MP: 9.63 W (POE OFF) 160.2 W (POE ON)
 - DSS-200G-10MPP: 15.4 W (POE OFF) 267.5 W (POE ON)
 - DSS-200G-28MP: 25.5 W (POE OFF) 425.9 W (POE ON)
 - DSS-200G-28MPP: 23.52 W (POE OFF) 579.3 W (POE ON)
- Standby Power Consumption
 - DSS-200G-10MP: 9.53 W
 - DSS-200G-10MPP: 15.4 W
 - DSS-200G-28MP: 25.2 W
 - DSS-200G-28MPP: 23.12 W
- Power input:100~240 VAC, 50/60Hz, internal universal power supply
- Acoustic Value:
 - DSS-200G-10MP: 0dB (fanless)
 - DSS-200G-10MPP PoE input 210-242W, 8571RPM: 49.9dB
 - DSS-200G-10MPP PoE input 180-210W, 6483RPM: 43.5dB
 - DSS-200G-10MPP PoE input 150-180W, 5777RPM: 40.1dB
 - DSS-200G-10MPP PoE input 120-150W, 4834RPM: 36.4dB
 - DSS-200G-10MPP PoE input 90-120W, 3892RPM: 33.2dB
 - DSS-200G-10MPP PoE input 60-90W, 2976RPM: 30.8dB
 - DSS-200G-10MPP PoE input 30-60W, 2374RPM: 28.5dB
 - DSS-200G-10MPP PoE input 0-30W, 1678RPM: 26.1dB
 - DSS-200G-28MP PoE input 322.8-370W, 7533RPM: 43.2dB
 - DSS-200G-28MP PoE input 282.3-322.8W, 6510RPM: 41.1dB
 - DSS-200G-28MP PoE input 241.7-282.3W, 5836RPM: 38.8dB
 - DSS-200G-28MP PoE input 201.9-241.7W, 4905RPM: 36.5dB
 - DSS-200G-28MP PoE input 161.3-201.9W, 4008RPM: 34.8dB
 - DSS-200G-28MP PoE input 121.2-161.3W, 3050RPM: 33.2dB
 - DSS-200G-28MP PoE input 80.5-121.2W, 2448RPM: 32.6dB
 - DSS-200G-28MP PoE input 0-80.5W, 1692RPM: 32.4dB
 - DSS-200G-28MPP PoE input 313-518W, 10226RPM: 50.6dB
 - DSS-200G-28MPP PoE input 274-313W, 7774RPM: 44.3dB
 - DSS-200G-28MPP PoE input 243-274W, 6734RPM: 41.8dB
 - DSS-200G-28MPP PoE input 196-243W, 5833RPM: 38.1dB
 - DSS-200G-28MPP PoE input 155-196W, 4874RPM: 34.6dB
 - DSS-200G-28MPP PoE input 115-155W, 3775RPM: 31.7dB
 - DSS-200G-28MPP PoE input 77-115W, 2875RPM: 29.2dB
 - DSS-200G-28MPP PoE input 0-77W, 1936RPM: 26.1dB

- ›
- › Operation Temperature: -5~50°C
- › Storage Temperature: -40~70°C
- › Operation Humidity: 0%~95% RH
- › Storage Humidity: 0%~95% RH

Emission (EMI)

Certifications

- › FCC class A
- › CE Class A
- › VCCI Class A
- › BSMI

Safety Certifications

- › CUL, LVD, CB, BSMI

Features

L2 Features

- › 8K MAC address
- › Loopback Detection
- › Port Mirroring
- › Link Aggregation
- › Cable Diagnostics
- › Spanning Tree
- › Ethernet Ring Protection Switching (ERPS)

L2 Multicasting

- › IGMP Snooping

VLAN

- › 802.1Q VLAN standard
- › Port-Based VLAN
- › Auto Surveillance VLAN
- › Voice VLAN:
- › Asymmetric VLAN

Quality of Service (QoS)

- › 802.1p priority
- › 8 queues
- › Bandwidth Control

Security

- › Storm Control
- › Traffic Segmentation
- › DoS Attack Prevention
- › SSL
- › D-Link Safeguard

Management

- › Web-based GUI or D-Link Network Assistant
- › Configuration backup/restoration via Web-based management
- › Firmware upgrade via Web-based management
- › System Reset & Reboot,
- › Factory reset by pressing the reset button
- › SNMP, LLDP, Dual Image, 2 level user account (admin/user), SNTTP

Power Saving

- › IEEE 802.3az Compliant (Energy Efficient Ethernet)
- › D-Link Green Technologies
 - Power saving by link status
 - Power Saving by LED Shut-Off
 - Power Saving by Port Shut-Off
 - Power Saving by System Hibernation

Surge Protection

- › All PoE ports support 6 KV surge protection

8. Appendix C –Rack Mount Instructions

Safety Instructions - Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)

9. Appendix D – Surveillance Mode Defaults

Enabling Surveillance Mode activates the following settings:

- Enables the Auto Surveillance VLAN
- PD Alive disabled on all ports
- Disables QoS
- Enables D-Link Safeguard
- Sets Loopback Detection
- Enables SNMP and SNMP traps
- Enables Syslog
- VLAN member ports configured as untagged
- Disables Spanning Tree