GSW-1676
GSW-2476
User Manual

COMPLIANCES

FCC - Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

You may use unshielded twisted-pair (UTP) for RJ-45 connections - Category 3 or better for 10 Mbps connections, Category 5 or better for 100 Mbps connections, Category 5, 5e, or 6 for 1000 Mbps connections. For fiber optic connections, you may use 50/125 or 62.5/125 micron multimode fiber or 9/125 micron single-mode fiber.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This information technology equipment complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

RFI Emission:

- Limit class A according to EN 55022:1998
- Limit class A for harmonic current emission according to EN 61000-3-2/1995
- Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995

Immunity:

- Product family standard according to EN 55024:1998
- Electrostatic Discharge according to EN 61000-4-2:1995 (Contact Discharge: ±4 kV, Air Discharge: ±8 kV)
- Radio-frequency electromagnetic field according to EN 61000-4-3:1996 (80 - 1000 MHz with 1 kHz AM 80% Modulation: 3 V/m)
- Electrical fast transient/burst according to EN 61000-4-4:1995 (AC/DC power supply: ±1 kV, Data/Signal lines: ±0.5 kV)
- Surge immunity test according to EN 61000-4-5:1995 (AC/DC Line to Line: ±1 kV, AC/DC Line to Earth: ±2 kV)
- Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996 (0.15 - 80 MHz with 1 kHz AM 80% Modulation: 3 V/m)
- Power frequency magnetic field immunity test according to EN 61000-4-8:1993 (1 A/m at frequency 50 Hz)
- Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994 (>95% Reduction @10 ms, 30% Reduction @500 ms, >95% Reduction @5000 ms)

LVD:

- EN 60950-1:2001

Warning: Do not plug a phone jack connector in the RJ-45 port. This may damage this device.

Safety Compliance

Warning: Fiber Optic Port Safety

CLASS I
LASER DEVICE

When using a fiber optic port, never look at the transmit laser while it is powered on. Also, never look directly at the fiber TX port and fiber cable ends when they are powered on.

Avertissment: Ports pour fibres optiques - sécurité sur le plan optique

DISPOSITIF LASER
DE CLASSE I

Ne regardez jamais le laser tant qu'il est sous tension. Ne regardez jamais directement le port TX (Transmission) à fibres optiques et les embouts de câbles à fibres optiques tant qu'ils sont sous tension.

Warnhinweis: Faseroptikanschlüsse - Optische Sicherheit

LASERGERÄT
DER KLASSE I

Niemals ein Übertragungslaser betrachten, während dieses eingeschaltet ist. Niemals direkt auf den Faser-TX-Anschluß und auf die Faserkabelenden schauen, während diese eingeschaltet sind.

Power Cord Safety

Please read the following safety information carefully before installing this switch:

Warning: Installation and removal of the unit must be carried out by qualified personnel only.

- The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.
- Do not connect the unit to an A.C. outlet (power supply) without an earth (ground) connection.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC 320 appliance inlet.
- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.
- This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the following:

Power Cord Set	
U.S.A. and Canada	The cord set must be UL-approved and CSA certified.
	The minimum specifications for the flexible cord are: - No. 18 AWG - not longer than 2 meters, or 16 AWG. - Type SV or SJ - 3-conductor
	The cord set must have a rated current capacity of at least 10 A
	The attachment plug must be an earth-grounding type with NEMA 5-15P (15 A, 125 V) or NEMA 6-15P (15 A, 250 V) configuration.
Denmark	The supply plug must comply with Section 107-2-D1, Standard DK2-1a or DK2-5a.
Switzerland	The supply plug must comply with SEV/ASE 1011.
U.K.	The supply plug must comply with BS1363 (3-pin 13 A) and be fitted with a 5 A fuse which complies with BS1362.
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
Europe	The supply plug must comply with CEE7/7 (“SCHUKO”).
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
	IEC-320 receptacle.

Warnings and Cautionary Messages

Warning: This product does not contain any serviceable user parts.

Warning: Installation and removal of the unit must be carried out by qualified personnel only.

Warning: When connecting this device to a power outlet, connect the field ground lead on the tri-pole power plug to a valid earth ground line to prevent electrical hazards.

Warning: This switch uses lasers to transmit signals over fiber optic cable. The lasers are compliant with the requirements of a Class 1 Laser Product and are inherently eye safe in normal operation. However, you should never look directly at a transmit port when it is powered on.

Caution: Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge when handling this equipment.

Caution: Do not plug a phone jack connector in the RJ-45 port. This may damage this device. Les raccordeurs ne sont pas utilisé pour le système téléphonique!

Caution: Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Environmental Statement

The manufacturer of this product endeavours to sustain an environmentally-friendly policy throughout the entire production process. This is achieved though the following means:

- Adherence to national legislation and regulations on environmental production standards.
- Conservation of operational resources.
- Waste reduction and safe disposal of all harmful un-recyclable by-products.
- Recycling of all reusable waste content.
- Design of products to maximize recyclables at the end of the product's life span.
- Continual monitoring of safety standards.

End of Product Life Span

This product is manufactured in such a way as to allow for the recovery and disposal of all included electrical components once the product has reached the end of its life.

Manufacturing Materials

There are no hazardous nor ozone-depleting materials in this product.

Documentation

All printed documentation for this product uses biodegradable paper that originates from sustained and managed forests. The inks used in the printing process are non-toxic.

Purpose

This guide details the hardware features of this switch, including Its physical and performance-related characteristics, and how to install the switch.

Audience

This guide is for system administrators with a working knowledge of network management. You should be familiar with switching and networking concepts.

Related Publications

As part of the switch firmware, there is an online web-based help that describes all management related features.

Table of Contents

TABLES

FIGURES

Chapter 1 About the Switch

Overview

The LevelOne GSW-1676 and GSW-2476 are intelligent Layer 2 WebSmart Switches with 16 or 24 10/100/1000BASE-T ports, four of which are combination ports* that are shared with four SFP transceiver slots (see Figure 1-1, Ports 21-24 on the GSW-2476 and Ports 13-16 on the GSW-1676).

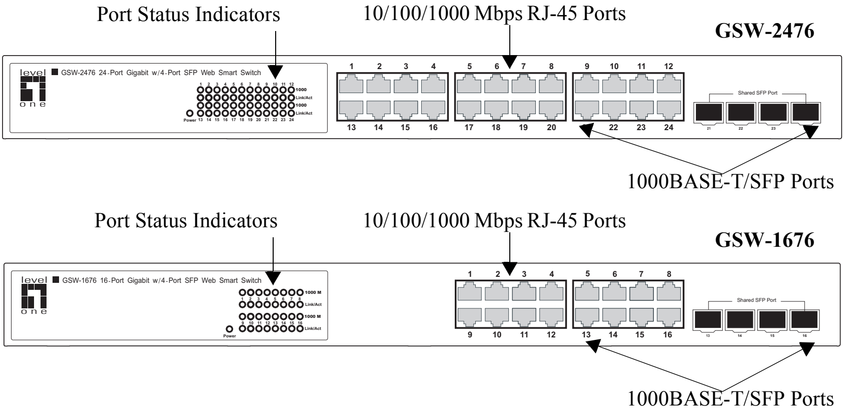


Figure 1-1 Front Panels

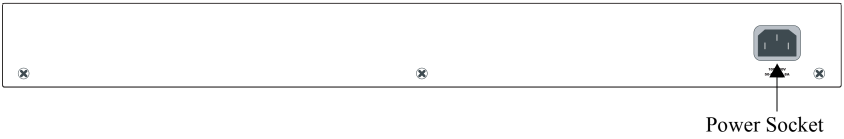


Figure 1-2 Rear Panel (both switches)

* If an SFP transceiver is plugged in, the corresponding RJ-45 port is disabled for ports 21-24 on the GSW-2476 and ports 13-16 on the GSW-1676.

Switch Architecture

The switches employ a wire-speed, non-blocking switching fabric. This permits simultaneous wire-speed transport of multiple packets at low latency on all ports. The switches also feature full-duplex capability on all ports, which effectively doubles the bandwidth of each connection.

The switches use store-and-forward switching to ensure maximum data integrity. With store-and-forward switching, the entire packet must be received into a buffer and checked for validity before being forwarded. This prevents errors from being propagated throughout the network.

Network Management Options

The switches contain a comprehensive array of LEDs for "at-a-glance" monitoring of network and port status. They also include a management agent that allows you to configure or monitor the switches using their embedded management software.

Description of Hardware

10/100/1000BASE-T Ports

The switch contains 16 or 24 RJ-45 ports that operate at 10 Mbps or 100 Mbps, half or full duplex, or at 1000 Mbps, full duplex. Because all ports on the switch support automatic MDI/MDI-X operation, you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. (See “1000BASE-T Pin Assignments” on page B-5.)

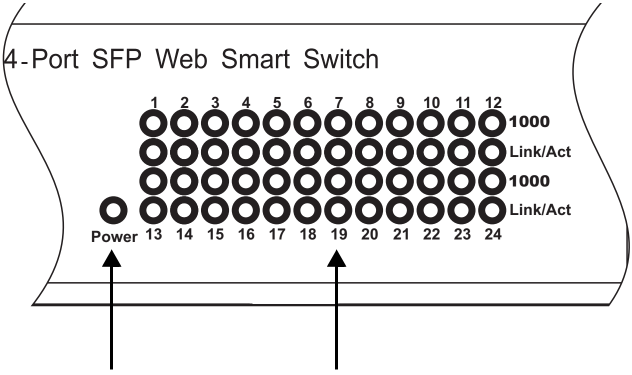
Each of these ports support auto-negotiation, so the optimum transmission mode (half or full duplex), and data rate (10, 100, or 1000 Mbps) can be selected automatically. If a device connected to one of these ports does not support auto-negotiation, the communication mode of that port can be configured manually.

SFP Slots

The Small Form Factor Pluggable (SFP) transceiver slots are shared with four of the RJ-45 ports (ports 21-24 on the GSW-2476, and ports 13-16 on the GSW-1676). In its default configuration, if an SFP transceiver (purchased separately) is installed in a slot and has a valid link on its port, the associated RJ-45 port is disabled and cannot be used. The switch can also be configured to force the use of an RJ-45 port or SFP slot, as required.

Port and Power Status LEDs

The switch includes a display panel for key system and port indications that simplify installation and network troubleshooting. The LEDs, which are located on the front panel for easy viewing, are shown below and described in the following tables.



Power Status LED   Port Status LEDs

Figure 1-3 Port LEDs and Power LED

Table 1-1 Port Status LEDs

LED	Condition	Status
Fast Ethernet Ports (Ports 1-16/24)		
Link/Act (Link/Activity)	On/Flashing Green	Port has established a valid network connection. Flashing indicates activity.
	Off	There is no valid link on the port.
1000 Mbps	On Green	Port is operating at 1000 Mbps.
	Off	Port is operating at 10 or 100 Mbps.

Table 1-2 Power Status LED

LED	Condition	Status
Power	Green	Internal power is operating normally.
	Off	Power off.

Power Supply Socket

The power socket is located on the rear panel of the switch. The standard power socket is for the AC power cord.

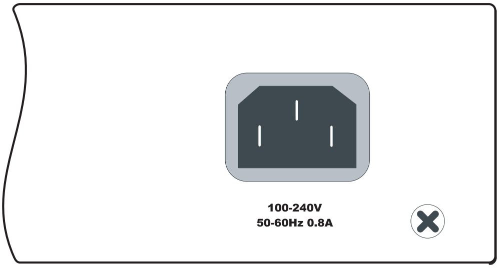


Figure 1-4 Power Supply Socket

Features and Benefits

Connectivity

- 16 or 24 10/100/1000 Mbps ports for easy Gigabit Ethernet integration and for protection of your investment in legacy LAN equipment.
- Auto-negotiation enables each RJ-45 port to automatically select the optimum communication mode (half or full duplex) if this feature is supported by the attached device; otherwise the port can be configured manually.
- RJ-45 10/100/1000BASE-T ports support auto MDI/MDI-X pinout selection.
- Unshielded (UTP) cable supported on all RJ-45 ports: Category 3 or better for 10 Mbps connections, Category 5 or better for 100 Mbps connections, and Category 5, 5e, 6 or better for 1000 Mbps connections.

- IEEE 802.3-2005 Ethernet, Fast Ethernet, and Gigabit Ethernet.

Expandability

- 4 Small Form Factor Pluggable (SFP) transceiver slots (shared with 1000BASE-T ports).
- Supports 1000BASE-SX, 1000BASE-LX and 1000BASE-ZX SFP transceivers.

Performance

- Transparent bridging.
- Provides store-and-forward switching.
- Supports Jumbo frames up to 9.6 Kbytes.
- Supports flow control.
- Broadcast storm control.

Management

- "At-a-glance" LEDs for easy troubleshooting.
- Network management agent.
  - Manages switch in-band or out-of-band.
  - Supports web-based interface.

CHAPTER 2
NETWORK PLANNING

Introduction to Switching

A network switch allows simultaneous transmission of multiple packets via non-crossbar switching. This means that it can partition a network more efficiently than bridges or routers. Switches have, therefore, been recognized as one of the most important building blocks for today's networking technology.

When performance bottlenecks are caused by congestion at the network access point (such as the network card for a high-volume file server), the device experiencing congestion (server, power user or hub) can be attached directly to a switched port. And, by using full-duplex mode, the bandwidth of the dedicated segment can be doubled to maximize throughput.

When networks are based on repeater (hub) technology, the distance between end stations is limited by a maximum hop count. However, a switch turns the hop count back to zero. So subdividing the network into smaller and more manageable segments, and linking them to the larger network by means of a switch, removes this limitation.

A switch can be easily configured in any Ethernet, Fast Ethernet, or Gigabit Ethernet, network to significantly boost bandwidth while using conventional cabling and network cards.

Application Examples

The GSW-1676 and GSW-2476 are not only designed to segment your network, but also to provide a wide range of options in setting up network connections. Some typical applications are described below.

Collapsed Backbone

The GSW-1676 and GSW-2476 are an excellent choice for mixed Ethernet, Fast Ethernet, and Gigabit Ethernet installations where significant growth is expected in the near future. In a basic stand-alone configuration, the switches can provide direct full-duplex connections for up to 16 or 24 workstations or servers. You can easily build on this basic configuration, adding direct full-duplex connections to workstations or servers. When the time comes for further expansion, just connect to another hub or switch using one of the Gigabit Ethernet ports built into the front panel, or a Gigabit Ethernet port on a plug-in SFP transceiver.

In the figure below, the GSW-2476 is operating as a collapsed backbone for a small LAN. It is providing dedicated 10 Mbps full-duplex connections to workstations, 100 Mbps full-duplex connections to power users, and 1 Gbps full-duplex connections to servers.

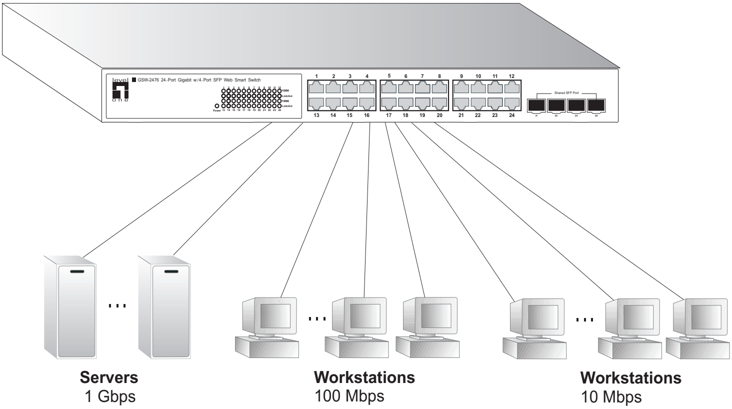


Figure 2-1 Collapsed Backbone

Central Wiring Closet

With 16 or 24 parallel bridging ports (i.e., 16 or 24 distinct collision domains), the switch can collapse a complex network down into a single efficient bridged node, increasing overall bandwidth and throughput.

In the figure below, the 1000BASE-T RJ-45 ports on the GSW-2476 are providing 1 Gbps full-duplex connections for up to 24 local segments. In addition, the switch is also connecting remote servers over fiber optic cable at 1 Gbps.

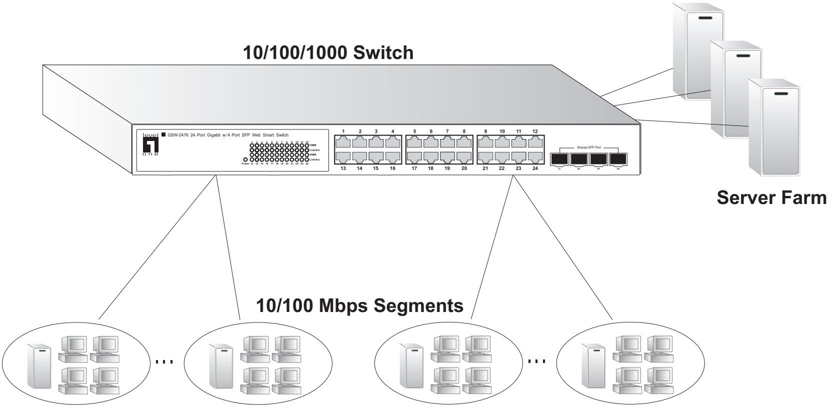


Figure 2-2 Central Wiring Closet

Remote Connections with Fiber Cable

Fiber optic technology allows for longer cabling than any other media type. A 1000BASE-SX (MMF) link can connect to a site up to 550 meters away, a 1000BASE-LX (SMF) link up to 10 km, and a 1000BASE-ZX link up to 70 km. This allows a switch stack to serve as a collapsed backbone, providing direct connectivity for a widespread LAN.

A 1000BASE-SX SFP transceiver can be used for a high-speed connection between floors in the same building, and a 1000BASE-LX transceiver can be used for high-bandwidth core connections between buildings in a campus setting. For long-haul connections, a 1000BASE-ZX SFP transceiver can be used to reach another site up to 100 kilometers away.

The figure below illustrates three GSW-2476 switches interconnecting multiple segments with fiber cable.

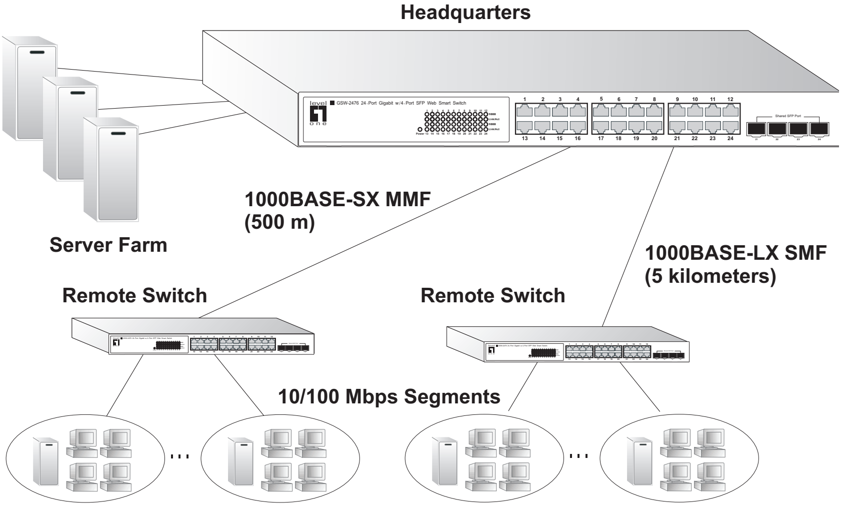


Figure 2-3 Remote Connections with Fiber Cable

Making VLAN Connections

The switch supports VLANs that can be used to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This provides a more secure and cleaner network environment.

VLANs can be based on untagged port groups, or traffic can be explicitly tagged to identify the VLAN group to which it belongs. Untagged VLANs can be used for small networks attached to a single switch. However, tagged VLANs should be used for larger networks, and all the VLANs assigned to the inter-switch links.

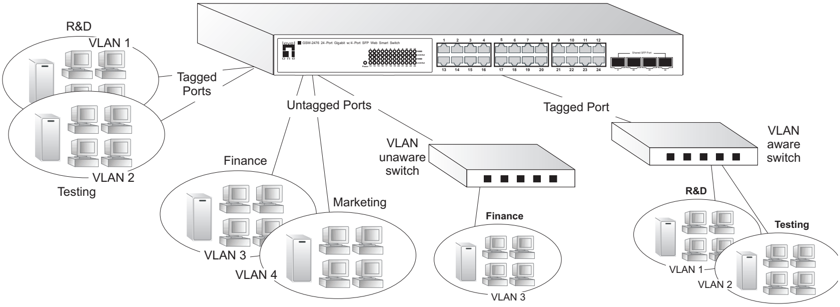


Figure 2-4 Making VLAN Connections

Note: When connecting to a switch that does not support IEEE 802.1Q VLAN tags, use untagged ports.

Application Notes

1. Full-duplex operation only applies to point-to-point access (such as when a switch is attached to a workstation, server or another switch). When the switch is connected to a hub, both devices must operate in half-duplex mode.

2. For network applications that require routing between dissimilar network types, you can attach the switch directly to a multi-protocol router.

3. As a general rule, the length of fiber optic cable for a single switched link should not exceed:

   - 1000BASE-SX: 550 m (1805 ft) for multimode fiber
   - 1000BASE-LX: 10 km (6.2 miles) for single-mode fiber
   - 1000BASE-ZX: 70 km (43.5 miles) for single-mode fiber

   However, power budget constraints must also be considered when calculating the maximum cable length for your specific environment.

Chapter 3 Installing the Switch

Selecting a Site

The GSW-1676 and GSW-2476 can be mounted in a standard 19-inch equipment rack or on a flat surface. Be sure to follow the guidelines below when choosing a location.

- The site should:
  - be at the center of all the devices you want to link and near a power outlet.
  - be able to maintain its temperature within 0 to 40 °C (32 to 104 °F) and its humidity within 10% to 90%, non-condensing
  - provide adequate space (approximately five centimeters or two inches) on all sides for proper air flow
  - be accessible for installing, cabling and maintaining the devices
  - allow the status LEDs to be clearly visible
- Make sure twisted-pair cable is always routed away from power lines, fluorescent lighting fixtures and other sources of electrical interference, such as radios and transmitters.
- Make sure that the unit is connected to a separate grounded power outlet that provides 100 to 240 VAC, 50 to 60 Hz, is within 2 m (6.6 feet) of each device and is powered from an independent circuit breaker. As with any equipment, using a filter or surge suppressor is recommended.

Ethernet Cabling

To ensure proper operation when installing the switches into a network, make sure that the current cables are suitable for 10BASE-T, 100BASE-TX or 1000BASE-T operation. Check the following criteria against the current installation of your network:

- Cable type: Unshielded twisted pair (UTP) or shielded twisted pair (STP) cables with RJ-45 connectors; Category 3 or better for 10BASE-T, Category 5 or better for 100BASE-TX, and Category 5, 5e or 6 for 1000BASE-T.
- Protection from radio frequency interference emissions
- Electrical surge suppression
- Separation of electrical wires (switch related or other) and electromagnetic fields from data based network wiring
- Safe connections with no damaged cables, connectors or shields

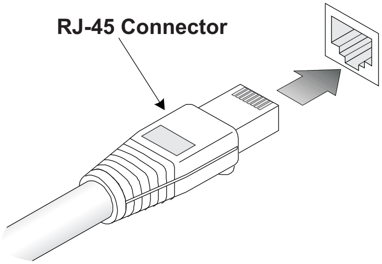


Figure 3-1 RJ-45 Connections

Equipment Checklist

After unpacking the switch, check the contents to be sure you have received all the components. Then, before beginning the installation, be sure you have all other necessary installation equipment.

Package Contents

- GSW-1676 or GSW-2476
- Four adhesive foot pads
- Bracket Mounting Kit containing two brackets and eight screws for attaching the brackets to the switch
- Power cord
- CD User Guide

Optional Rack-Mounting Equipment

If you plan to rack-mount the switches, be sure to have the following equipment available:

- Four mounting screws for each device you plan to install in a rack—these are not included
- A screwdriver

Mounting

The GSW-1676 and GSW-2476 can be mounted in a standard 19-inch equipment rack or on a desktop or shelf. Mounting instructions for each type of site follow.

Rack Mounting

Before rack mounting the switch, pay particular attention to the following factors:

- Temperature: Since the temperature within a rack assembly may be higher than the ambient room temperature, check that the rack-environment temperature is within the specified operating temperature range (see page C-2).
- Mechanical Loading: Do not place any equipment on top of a rack-mounted unit.
- Circuit Overloading: Be sure that the supply circuit to the rack assembly is not overloaded.
- Grounding: Rack-mounted equipment should be properly grounded. Particular attention should be given to supply connections other than direct connections to the mains.

To rack-mount devices:

1. Attach the brackets to the device using the screws provided in the Bracket Mounting Kit.

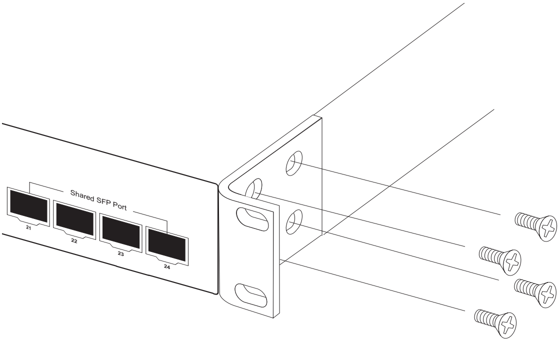


Figure 3-2 Attaching the Brackets

2. Mount the device in the rack, using four rack-mounting screws (not provided).

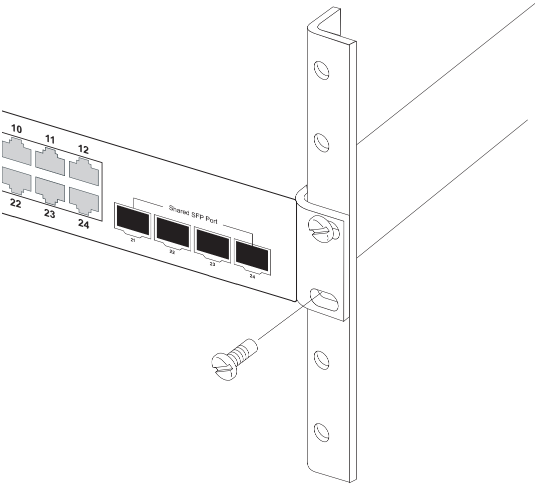


Figure 3-3 Installing the Switch in a Rack

3. If installing a single switch only, turn to “Connecting to a Power Source” at the end of this chapter.

4. If installing multiple switches, mount them in the rack, one below the other, in any order.

Desktop or Shelf Mounting

1. Attach the four adhesive feet to the bottom of the first switch.

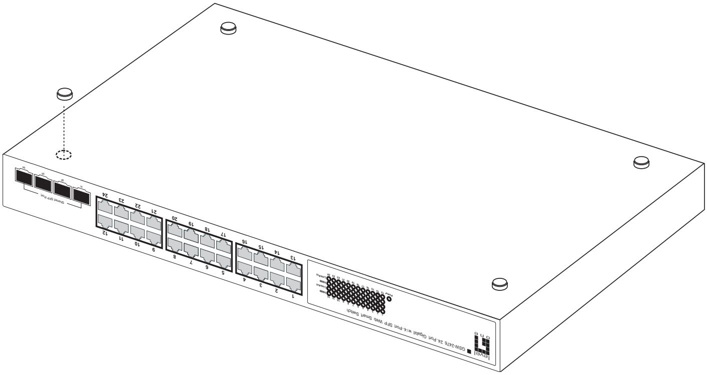


Figure 3-4 Attaching the Adhesive Feet

2. Set the device on a flat surface near an AC power source, making sure there are at least two inches of space on all sides for proper air flow.

3. If installing a single switch only, go to “Connecting to a Power Source” at the end of this chapter.

4. If installing multiple switches, attach four adhesive feet to each one. Place each device squarely on top of the one below, in any order.

Installing an SFP Transceiver

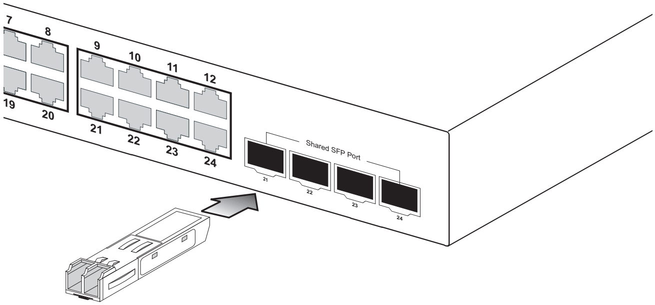


Figure 3-5 Inserting an SFP Transceiver into a Slot

The switch supports the following optional transceivers:

- 1000BASE-SX (SGVT-0300)
- 1000BASE-LX (SGVT-0301
- 1000BASE-ZX (SGVT-0302)

To install an SFP transceiver, do the following:

1. Consider network and cabling requirements to select an appropriate transceiver type. Refer to “Connectivity Rules” on page 4-6.
2. Insert the transceiver with the optical connector facing outward and the slot connector facing down. Note that SFP transceivers are keyed so they can only be installed in one orientation.
3. Slide the transceiver into the slot until it clicks into place.

Note: SFP transceivers are hot-swappable. The switch does not need to be powered off before installing or removing a transceiver. However, always first disconnect the network cable before removing a transceiver.

Note: SFP transceivers are not provided in the switch package.

Connecting to a Power Source

To connect a device to a power source:

1. Insert the power cable plug directly into the socket located at the back of the device.

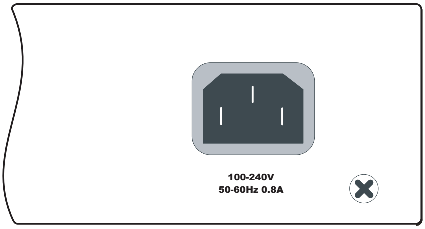


Figure 3-6 Power Socket

2. Plug the other end of the cable into a grounded, 3-pin, AC power source.

   Note: For international use, you may need to change the AC line cord. You must use a line cord set that has been approved for the socket type in your country.

3. Check the front-panel LEDs as the device is powered on to be sure the Power LED is on. If not, check that the power cable is correctly plugged in.

CHAPTER 4
MAKING NETWORK CONNECTIONS

Connecting Network Devices

The GSW-1676 and GSW-2476 are designed to interconnect multiple segments (or collision domains). They can be connected to network cards in PCs and servers, as well as to hubs, switches or routers. They may also be connected to devices using optional SFP transceivers.

Twisted-Pair Devices

Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category 5, 5e or 6 cable for 1000BASE-T connections, Category 5 or better for 100BASE-TX connections, and Category 3 or better for 10BASE-T connections.

Cabling Guidelines

The RJ-45 ports on the switch support automatic MDI/MDI-X pinout configuration, so you can use standard straight-through twisted-pair cables to connect to any other network device (PCs, servers, switches, routers, or hubs).

See Appendix B “Cables” for further information on cabling.

Caution: Do not plug a phone jack connector into an RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Connecting to PCs, Servers, Hubs and Switches

1. Attach one end of a twisted-pair cable segment to the device's RJ-45 connector.

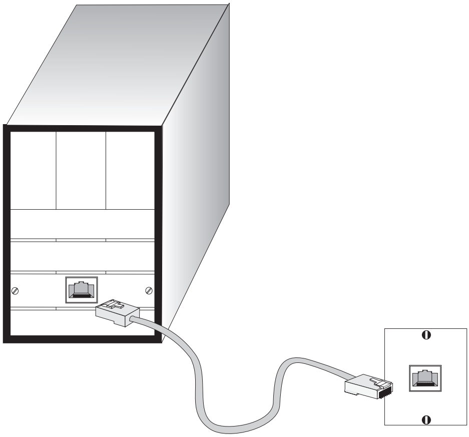


Figure 4-1 Making Twisted-Pair Connections

2. If the device is a PC card and the switch is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet. (See "Network Wiring Connections" on page 4-3.) Otherwise, attach the other end to an available port on the switch.

   Make sure each twisted pair cable does not exceed 100 meters (328 ft) in length.

3. As each connection is made, the Link LED (on the switch) corresponding to each port turns on to indicate that the connection is valid.

Network Wiring Connections

Today, the punch-down block is an integral part of many of the newer equipment racks. It is actually part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment follows.

1. Attach one end of a patch cable to an available port on the switch, and the other end to the patch panel.

2. If not already in place, attach one end of a cable segment to the back of the patch panel where the punch-down block is located, and the other end to a modular wall outlet.

3. Label the cables to simplify future troubleshooting. See "Cable Labeling and Connection Records" on page 4-8.

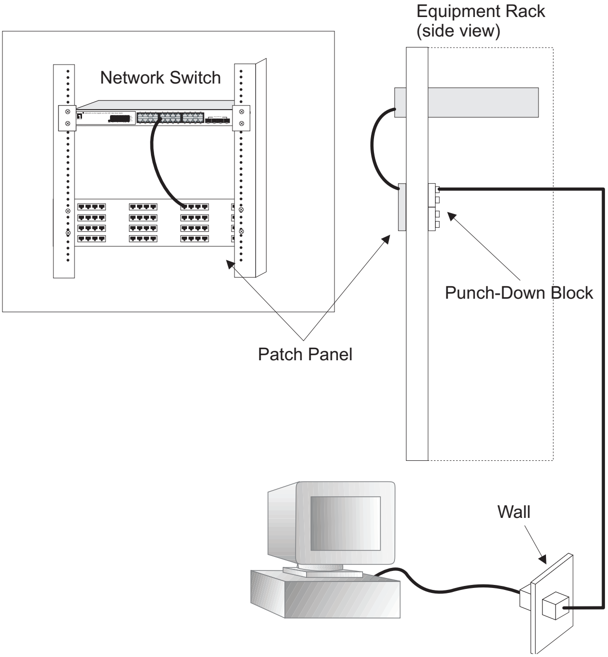


Figure 4-2 Wiring Closet Connections

Fiber Optic SFP Devices

An optional Gigabit SFP transceiver (1000BASE-SX, 1000BASE-LX or 1000BASE-ZX) can be used for a backbone connection between switches, or for connecting to a high-speed server.

Each single-mode fiber port requires 9/125 micron single-mode fiber optic cable with an LC connector at both ends. Each multimode fiber optic port requires 50/125 or 62.5/125 micron multimode fiber optic cabling with an LC connector at both ends.

Warning: the switch use lasers to transmit signals over fiber optic cable. The lasers are compliant with the requirements of a Class 1 Laser Product and are inherently eye safe in normal operation. However, you should never look directly at a transmit port when it is powered on.

Note: When selecting a fiber SFP device, considering safety, please make sure that it can function at a temperature that is not less than the recommended maximum operational temperature of the product. You must also use an approved Laser Class 1 SFP transceiver.

1. Remove and keep the LC port’s rubber cover. When not connected to a fiber cable, the rubber cover should be replaced to protect the optics.

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

3. Connect one end of the cable to the LC port on the switch and the other end to the LC port on the other device. Since LC connectors are keyed, the cable can be attached in only one orientation.

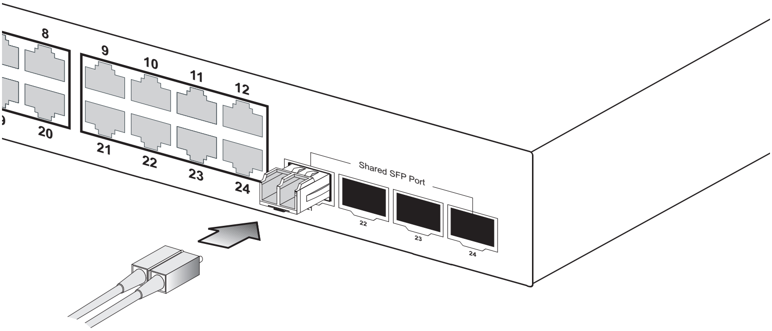


Figure 4-3 Making Connections to SFP Transceivers

4. As a connection is made, check the Link LED on the switch corresponding to the port to be sure that the connection is valid.

The 1000BASE-SX, 1000BASE-LX and 1000BASE-ZX fiber optic ports operate at 1 Gbps full duplex. The maximum length for fiber optic cable operating at Gigabit speed will depend on the fiber type as listed under “1000 Mbps Gigabit Ethernet Collision Domain” on page 4-6.

Connectivity Rules

When adding hubs (repeaters) to your network, please follow the connectivity rules listed in the manuals for these products. However, note that because switches break up the path for connected devices into separate collision domains, you should not include the switch or connected cabling in your calculations for cascade length involving other devices.

1000BASE-T Cable Requirements

All Category 5 UTP cables that are used for 100BASE-TX connections should also work for 1000BASE-T, providing that all four wire pairs are connected. However, it is recommended that for all critical connections, or any new cable installations, Category 5e (enhanced Category 5) or Category 6 cable should be used. The Category 5e specification includes test parameters that are only recommendations for Category 5. Therefore, the first step in preparing existing Category 5 cabling for running 1000BASE-T is a simple test of the cable installation to be sure that it complies with the IEEE 802.3-2005 standards.

1000 Mbps Gigabit Ethernet Collision Domain

Table 4-1 Maximum 1000BASE-T Gigabit Ethernet Cable Length

Cable Type	Maximum Cable Length	Connector
Category 5, 5e, 6 100-ohm UTP or STP	100 m (328 ft)	RJ-45

Table 4-2 Maximum 1000BASE-SX Fiber Optic Cable Length

Fiber Diameter	Fiber Bandwidth	Cable Length Range	Connector
62.5/125 micron multimode fiber (MMF)	160 MHz/km	2-220 m (7-722 ft)	LC
	200 MHz/km	2-275 m (7-902 ft)	LC
50/125 micron multimode fiber (MMF)	400 MHz/km	2-500 m (7-1641 ft)	LC
	500 MHz/km	2-550 m (7-1805 ft)	LC

Table 4-3 Maximum 1000BASE-LX Fiber Optic Cable Length

Fiber Diameter	Fiber Bandwidth	Cable Length Range	Connector
9/125 micron single-mode fiber	N/A	2 m - 10km (7 ft - 6.4 miles)	LC

Table 4-4 Maximum 1000BASE-ZX Fiber Optic Cable Length

Fiber Diameter	Fiber Bandwidth	Cable Length Range	Connector
9/125 micron single-mode fiber	N/A	2 m - 70 km (7 ft - 43.5 miles)	LC

100 Mbps Fast Ethernet Collision Domain

Table 4-5 Maximum Fast Ethernet Cable Length

Type	Cable Type	Maximum Cable Length	Connector
100BASE-TX	Category 5 or better 100-ohm UTP or STP	100 m (328 ft)	RJ-45

10 Mbps Ethernet Collision Domain

Table 4-6 Maximum Ethernet Cable Length

Type	Cable Type	Maximum Length	Connector
10BASE-T	Categories 3, 4, 5 or better 100-ohm UTP	100 m (328 ft)	RJ-45

Cable Labeling and Connection Records

When planning a network installation, it is essential to label the opposing ends of cables and to record where each cable is connected. Doing so will enable you to easily locate inter-connected devices, isolate faults and change your topology without need for unnecessary time consumption.

To best manage the physical implementations of your network, follow these guidelines:

- Clearly label the opposing ends of each cable.
- Using your building's floor plans, draw a map of the location of all network-connected equipment. For each piece of equipment, identify the devices to which it is connected.
- Note the length of each cable and the maximum cable length supported by the switch ports.
- For ease of understanding, use a location-based key when assigning prefixes to your cable labeling.
- Use sequential numbers for cables that originate from the same equipment.
- Differentiate between racks by naming accordingly.
- Label each separate piece of equipment.
- Display a copy of your equipment map, including keys to all abbreviations at each equipment rack.

CHAPTER 5
INITIAL CONFIGURATION

To make use of the management features of your switch, you must first configure it with an IP address that is compatible with the network it is being installed in. This should be done before you permanently install the switch in the network.

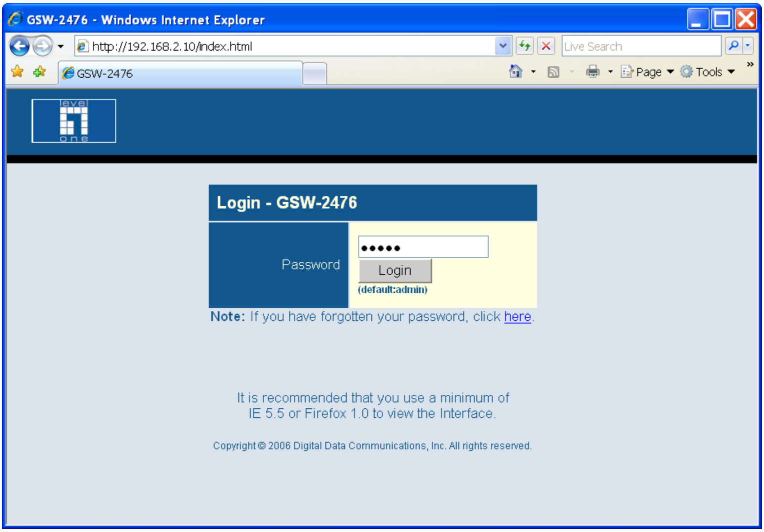
Follow this procedure:

1. Place your switch close to the PC that you intend to use for configuration. It helps if you can see the front panel of the switch while working on your PC.

2. Connect the Ethernet port of your PC to any port on the front panel of your switch. Connect power to the switch and verify that you have a link by checking the front-panel LEDs.

3. Check that your PC has an IP address on the same subnet as the switch. The default IP address of the switch is 192.168.2.10 and the subnet mask is 255.255.255.0, so the PC and switch are on the same subnet if they both have addresses that start 192.168.2.x. If the PC and switch are not on the same subnet, you must manually set the PC's IP address to 192.168.2.x (where "x" is any number from 1 to 255, except 10). If you are unfamiliar with this process, see "Changing a PC's IP Address" on page 5-3.

4. Open your web browser and enter the address http://192.168.2.10. If your PC is properly configured, you will see the login page of your switch. If you do not see the login page, repeat step 3.


GSW-2476 - Windows Internet Explorer
http://192.168.2.10/index.html
Live Search
GSW-2476
Page
Tools
level one

Login - GSW-2476

Password •••••

Login

(default:admin)

Note: If you have forgotten your password, click here.

It is recommended that you use a minimum of IE 5.5 or Firefox 1.0 to view the Interface.

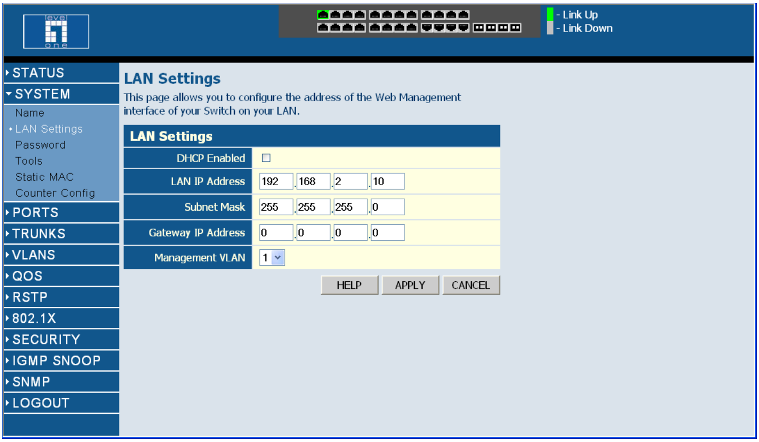
Copyright © 2006 Digital Data Communications, Inc. All rights reserved.

Figure 5-1 Login Page

Note: The web interface examples in this guide are based on the GSW-2476. Other than the number of ports, there are no other differences between the GSW-2476 and GSW-1676.

5. Enter the default password "admin" and click on the Login button.

6. From the menu, click on SYSTEM, then click on LAN Settings. On the LAN Settings page, enter the new IP address, Subnet Mask and Gateway IP Address for the switch, then click on the APPLY button.



LAN Settings

This page allows you to configure the address of the Web Management interface of your Switch on your LAN.

LAN Settings	
DHCP Enabled	□
LAN IP Address	192 . 168 . 2 . 10
Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	0 . 0 . 0 . 0
Management VLAN	1

Figure 5-2 LAN Settings Page

No other configuration changes are required at this stage, but it is recommended that you change the administrator's password before logging out. To change the password, click SYSTEM, Password, and then fill in all the fields on the Password Settings page before clicking on the APPLY button.

Changing a PC's IP Address

To change the IP address of a Windows 2000 PC:

1. Click Start, Settings, then Network and Dial-up Connections.

2. For the IP address you want to change, right-click the network connection icon, and then click Properties.

3. In the list of components used by this connection on General tab, select Internet Protocol (TCP/IP), and then click the Properties button.

4. In the Internet Protocol (TCP/IP) Properties dialog box, click to select Use the following IP address. Then type your intended IP address, Subnet mask, and Default gateway in the provided text boxes.

5. Click OK to save the changes.

To change the IP address of a Windows XP PC:

1. Click Start, Control Panel, then Network Connections.

2. For the IP address you want to change, right-click the network connection icon, and then click Properties.

3. In the list of components used by this connection on General tab, select Internet Protocol (TCP/IP), and then click the Properties button.

4. In the Internet Protocol (TCP/IP) Properties dialog box, click to select Use the following IP address. Then type your intended IP address, Subnet mask, and Default gateway in the provided text boxes

5. Click OK to save the changes.

Note: For users of systems other than Windows 2000 or Windows XP, refer to your system documentation for information on changing the PC's IP address.

CHAPTER 6
CONFIGURING THE SWITCH

Using the Web Interface

This switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 5.0 or above, or Firefox v1.5 or above).

Prior to accessing the switch from a Web browser, be sure you have performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway. (Defaults: IP address 192.168.2.10; Subnet mask 255.255.255.0; Gateway 0.0.0.0)

2. Set a new password using the web interface. (Default: "admin"). Access to the web interface is controlled by the password. See "Configuring the Logon Password" on page 6-17.

Note: If you cannot remember the switch's IP address, you can restore the original settings by following the procedure described in the "Troubleshooting" section.

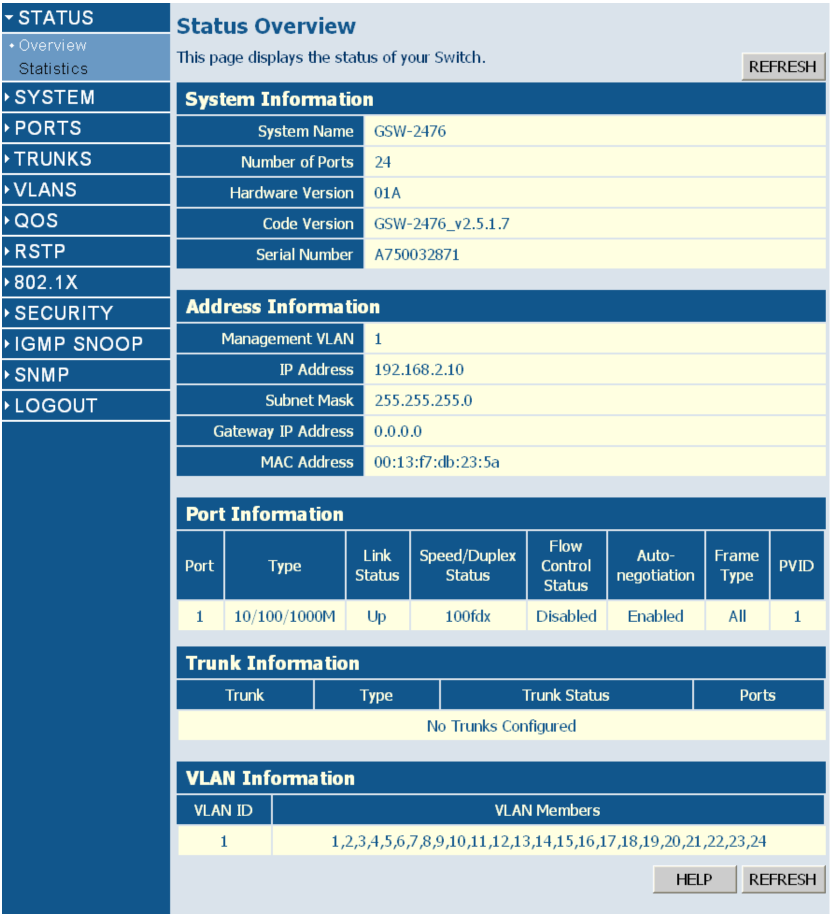
Navigating the Web Browser Interface

To access the web-browser interface you must first enter a password. The administrator has read/write access to all configuration parameters and statistics. The default password for the administrator is "admin."

Note: If user input is not detected within five minutes, the current session is terminated.

Home Page

When your web browser connects with the switch's web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and Status Overview on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.



Status Overview

This page displays the status of your Switch.

System Information

System Name	GSW-2476
Number of Ports	24
Hardware Version	01A
Code Version	GSW-2476_v2.5.1.7
Serial Number	A750032871

Address Information

Management VLAN	1
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:13:f7:db:23:5a

Port Information

Port	Type	Link Status	Speed/Duplex Status	Flow Control Status	Auto-negotiation	Frame Type	PVID
1	10/100/1000M	Up	100fdx	Disabled	Enabled	All	1

Trunk Information

Trunk	Type	Trunk Status	Ports
No Trunks Configured			

VLAN Information

VLAN ID	VLAN Members
1	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 6-1 Home Page

Note: The web interface examples in this guide are based on the GSW-2476. Other than the number of ports, there are no other differences between the GSW-2476 and GSW-1676.

Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes the web page configuration buttons.

Configuration Options

Button	Action
Apply	Sets specified values to the system.
Cancel	Cancels specified values and restores current values prior to pressing Apply.
Help	Links directly to web help.

Notes: 1. To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

Panel Display

The web agent displays an image of the switch's ports. The switch ports display green when they have a valid link to another device. To show the port number, place mouse pointer onto the intended port.

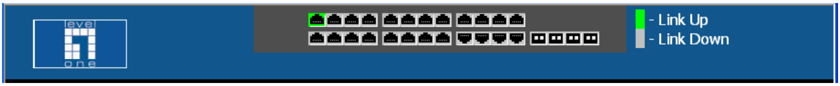


Figure 6-2 Panel Display

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from the web-browser interface.

Main Menu

Menu	Description	Page
STATUS		6-8
Overview	Provides a basic system description, including system name, IP address, port, trunk, and VLAN information.	6-8
Statistics	Shows interface and RMON statistics for the selected port.	6-11
SYSTEM		6-15
Name	Shows the name of the switch.	6-15
LAN Settings	Sets the LAN IP address, subnet mask, and gateway IP address.	6-15
Password	Changes the password.	6-17
Tools		6-18
Restore to Factory Defaults	Forces the switch to perform a power reset and restores the original factory settings.	6-18
Upgrade Firmware	Upgrades the switch system firmware using a file provided by LevelOne.	6-19
Upload/Download Configuration	Uploads or downloads the configuration file.	6-19
Restart	Restarts the switch.	6-20
Static MAC	Adds static MAC addresses to the switch MAC address table.	6-21
Counter Config	Selects traffic statistics you want to monitor.	6-22
PORTS		6-24
Settings	Configure the speed and duplex mode of ports.	6-24

Main Menu (Continued)

Menu	Description	Page
Rate Limiting	Sets the rate limiting parameters for ports.	6-25
Storm Control	Sets the broadcast storm control parameters.	6-27
Port Mirroring	Sets up the port mirroring features of the switch to enable traffic monitoring.	6-28
Cable Diagnostic	Diagnoses cable faults.	6-30
TRUNKS		6-30
Membership	Selects ports to group into static trunks.	6-33
Settings	Configures trunk connection settings.	6-33
Rate Limiting	Sets the rate limiting parameters for trunks.	6-33
LACP Setup	Configures Link Aggregation Control Protocol (LACP) on the switch.	6-35
LACP Status	Shows the LACP group status.	6-36
VLANS		6-38
VLAN Membership	Configure VLAN port groups.	6-39
VLAN Port Config	Configures VLAN behavior for individual ports and trunks.	6-38
QOS		6-45
Settings	Sets the priority of packets forwarded through the switch.	6-45
RSTP		6-50
Settings	Configures Spanning Tree parameters.	6-51
Status	Shows Spanning Tree bridge and port status.	6-55
802.1X		6-57
Settings	Sets up 802.1X port authentication.	6-59
Statistics	Displays the 802.1X statistics collected by the switch.	6-62
Security		6-66
IP Filter	Sets up port IP control filters.	6-66
Port Security	Sets security policy for ports.	6-67

Main Menu (Continued)

Menu	**Description**	**Page**
Management Access Filter	Sets up management access filter.	6-69
IGMP Snooping		6-71
Settings	Sets up IGMP Snooping configuration.	6-73
Status	Shows IGMP Snooping status.	6-73
SNMP		6-75
Settings	Configures community strings and related trap functions.	6-75
LOGOUT	Quits to the Login page.	NA

Basic Information

Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

Field Attributes

System Information

- **System Name** – Name assigned to the switch system.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.
- **Code Version** – Version number of the code.
- **Serial Number** – The serial number of the switch.

Address Information

- **Management VLAN** – ID of the configured VLAN (this is set to 1 and cannot be changed) all ports on the unit are members of VLAN 1. The management station must always be attached to a port on VLAN 1.
- **IP Address** – Address of the VLAN to which the management station is attached. (Note that the management station must always be on VLAN 1.) Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
- **Gateway IP Address** – IP address of the gateway router between the switch and management stations that exist on other network segments. (Default: 0.0.0.0)
- **MAC Address** – The physical layer address of the switch.

Port Information

- **Type** – Indicates the port type.
- **Link Status** – Indicates if the link is Up or Down.
- **Speed/Duplex Status** – Shows the current speed and duplex mode.
  - **Auto**: Not currently connected, will auto-negotiate these settings.

  - **10hdx**: 10 Mbps half duplex.
  - **10fdx**: 10 Mbps full duplex.
  - **100hdx**: 100 Mbps half duplex.
  - **100fdx**: 100 Mbps full duplex.
  - **1000fdx**: 1000 Mbps full duplex.
- **Flow Control Status** – Indicates whether flow control is enabled or disabled. (IEEE 802.3x, or Back-Pressure)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Frame Type** – Either "Tagged" or "All." "Tagged" means that the port will only receive VLAN-tagged packets. When set to "All," the port will also receive untagged packets.
- **PVID** - The VLAN ID assigned to untagged frames received on the interface. Outgoing frames are tagged unless the frame's VLAN ID is the same as the PVID. When the PVID is set to "None," all outgoing frames are tagged. (Default: 1)

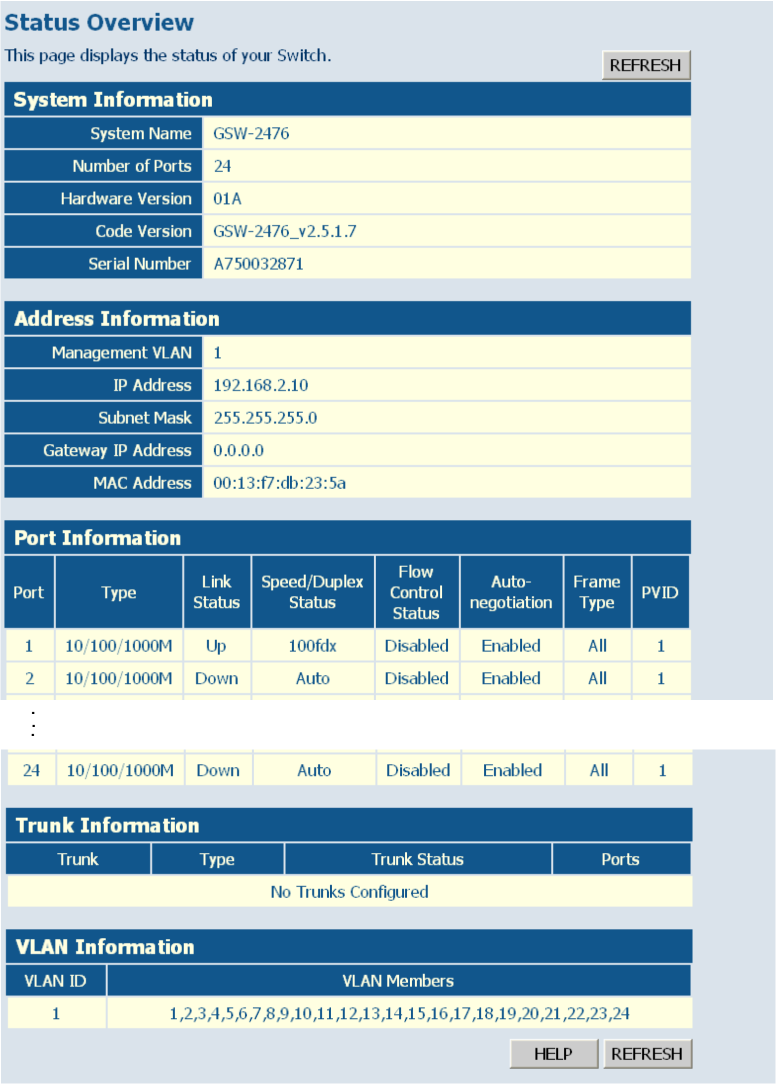
Trunk Information

- **Trunk** – The trunk label. "T1" through "T8" are used as trunk labels.
- **Type** – All trunks and ports on this switch are 10/100/1000Mbps
- **Trunk Status** – Indicates the speed and duplex setting of the trunk. This can be changed on the TRUNKS > Settings page.
  - **Auto**: Not currently connected, will auto-negotiate these settings.
  - **10hdx**: 10 Mbps half duplex.
  - **10fdx**: 10 Mbps full duplex.
  - **100hdx**: 100 Mbps half duplex.
  - **100fdx**: 100 Mbps full duplex.
  - **1000fdx**: 1000 Mbps full duplex.
- **Ports** – The ports that are members of the trunk.

VLAN Information

- **VLAN ID** – A number in the range 1 - 4094 which identifies the VLAN.
- **VLAN Members** – A list of the ports that are members of the VLAN. By default, all ports are members of VLAN 1.

Web – Click STATUS, Overview.



Status Overview

This page displays the status of your Switch.

System Information

System Name	GSW-2476
Number of Ports	24
Hardware Version	01A
Code Version	GSW-2476_v2.5.1.7
Serial Number	A750032871

Address Information

Management VLAN	1
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:13:f7:db:23:5a

Port Information

Port	Type	Link Status	Speed/Duplex Status	Flow Control Status	Auto-negotiation	Frame Type	PVID
1	10/100/1000M	Up	100fdx	Disabled	Enabled	All	1
2	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
⋮							
24	10/100/1000M	Down	Auto	Disabled	Enabled	All	1

Trunk Information

Trunk	Type	Trunk Status	Ports
No Trunks Configured			

VLAN Information

VLAN ID	VLAN Members
1	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 6-3 Status Overview

Showing Port Statistics

You can display statistics on network traffic from the ports. These statistics can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). All values displayed have been accumulated since the last system reboot, but can be reset to zero by clicking the CLEAR button. The current statistics are not displayed until you click the REFRESH button.

Port Statistics

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmitted Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmitted Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Received High Priority Packets	The total number of received packets that are set as High Priority in the QoS settings.
Received Normal Priority Packets	The total number of received packets that are set as High Priority in the QoS settings.
Transmitted High Priority Packets	The total number of transmitted packets that are set as High Priority in the QoS settings.
Transmitted Normal Priority Packets	The total number of transmitted packets that are set as High Priority in the QoS settings.

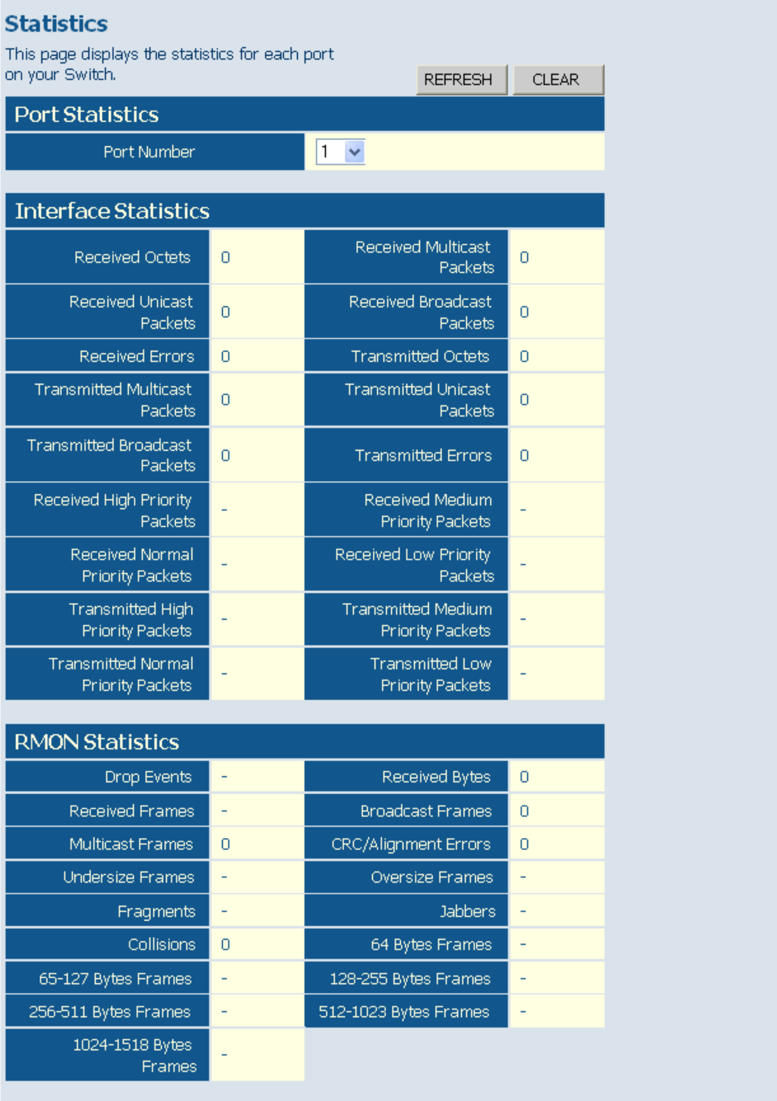
Port Statistics (Continued)

Parameter	Description
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmitted Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmitted Errors	The number of outbound packets that could not be transmitted because of errors.
Received Medium Priority Packets	The total number of received packets that are set as Medium Priority in the QoS settings.
Received Low Priority Packets	The total number of received packets that are set as Low Priority in the QoS settings.
Transmitted Medium Priority Packets	The total number of transmitted packets that are set as Medium Priority in the QoS settings.
Transmitted Low Priority Packets	The total number of transmitted packets that are set as Low Priority in the QoS settings.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.

Port Statistics (Continued)

Parameter	Description
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Web – Click STATUS, Statistics.



Statistics

This page displays the statistics for each port on your Switch.

Port Statistics

Port Number	1

Interface Statistics

Received Octets	0	Received Multicast Packets	0
Received Unicast Packets	0	Received Broadcast Packets	0
Received Errors	0	Transmitted Octets	0
Transmitted Multicast Packets	0	Transmitted Unicast Packets	0
Transmitted Broadcast Packets	0	Transmitted Errors	0
Received High Priority Packets	-	Received Medium Priority Packets	-
Received Normal Priority Packets	-	Received Low Priority Packets	-
Transmitted High Priority Packets	-	Transmitted Medium Priority Packets	-
Transmitted Normal Priority Packets	-	Transmitted Low Priority Packets	-

RMON Statistics

Drop Events	-	Received Bytes	0
Received Frames	-	Broadcast Frames	0
Multicast Frames	0	CRC/Alignment Errors	0
Undersize Frames	-	Oversize Frames	-
Fragments	-	Jabbers	-
Collisions	0	64 Bytes Frames	-
65-127 Bytes Frames	-	128-255 Bytes Frames	-
256-511 Bytes Frames	-	512-1023 Bytes Frames	-
1024-1518 Bytes Frames	-		

Figure 6-4 Port Statistics

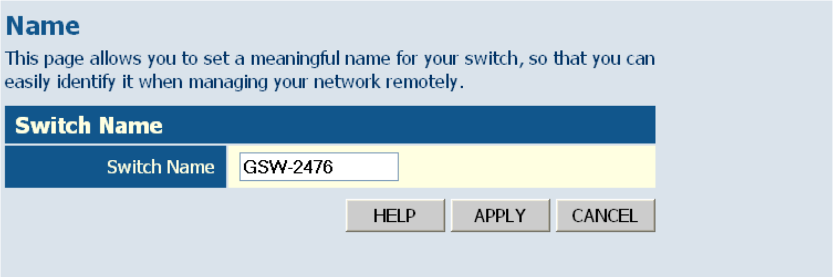
Displaying the System Name

You can identify the system by displaying the device name.

Field Attributes

- **Switch Name** – A name assigned to the switch system.

Web – Click System, Name.



Name

This page allows you to set a meaningful name for your switch, so that you can easily identify it when managing your network remotely.

Switch Name

Switch Name	GSW-2476

Figure 6-5 System Name

Setting the Switch's IP Address

This section describes how to configure an IP interface for management access over the network. The IP address for this switch is 192.168.2.10 by default. To manually configure an address, you need to change the switch's default settings (IP address 192.168.2.10 and netmask 255.255.255.0) to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

Field Attributes

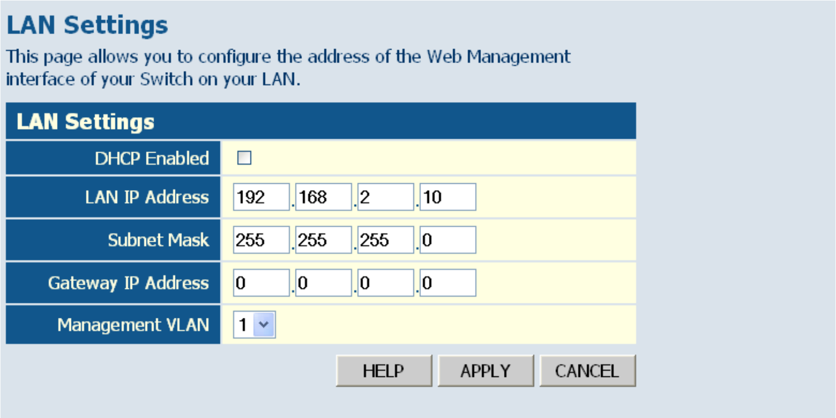
- **DHCP Enabled** – Check the box to enable DHCP. (Default: enabled)
- **LAN IP Address** – Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.2.10)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)

- **Gateway IP Address** – IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)
- **Management VLAN** – ID of the configured VLAN (1-4093, no leading zeroes). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.

Note: If you cannot remember the switch's IP address, you can restore the original settings by following the procedure described in "Troubleshooting" on page A-1.

Manual Configuration

Web – Click System, LAN Settings. Enter the IP address, subnet mask, gateway, and select the management VLAN, then click APPLY. Note that if you change the switch's IP address, you must close the web interface and start a new session using the new IP address.



LAN Settings

This page allows you to configure the address of the Web Management interface of your Switch on your LAN.

LAN Settings	
DHCP Enabled	□
LAN IP Address	192 . 168 . 2 . 10
Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	0 . 0 . 0 . 0
Management VLAN	1

Figure 6-6 LAN Settings

Configuring the Logon Password

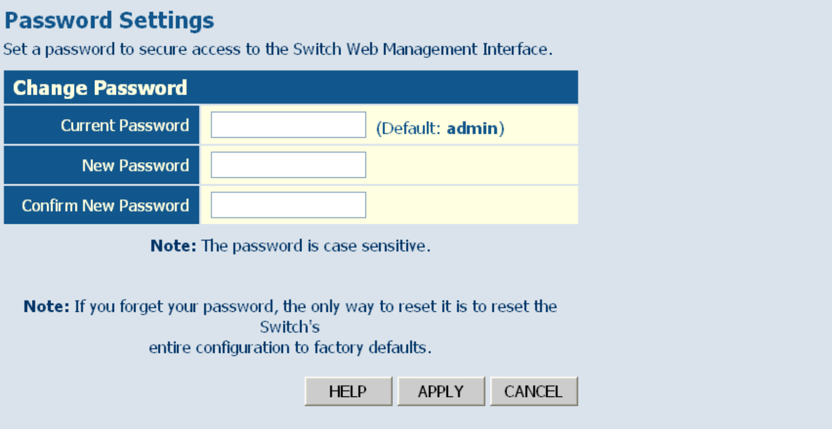
The administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

Field Attributes

- **Current Password** – Input the current password. (Default is "admin")
- **New Password** – Specifies the new user password. (Range: 1-16 characters plain text, case sensitive)
- **Confirm New Password** – Re-enter in the new password for confirmation.

Note: If you cannot remember the password, you can restore the original settings by following the procedure described in "Troubleshooting" on page A-1.

Web – Click System, Password. To change the password for the administrator, enter the current password, the new password, and confirm it by entering it again, then click APPLY.



Password Settings

Set a password to secure access to the Switch Web Management Interface.

Change Password

Current Password	(Default: **admin**)
New Password	
Confirm New Password	

Note: The password is case sensitive.

Note: If you forget your password, the only way to reset it is to reset the Switch's entire configuration to factory defaults.

Figure 6-7 Password Settings

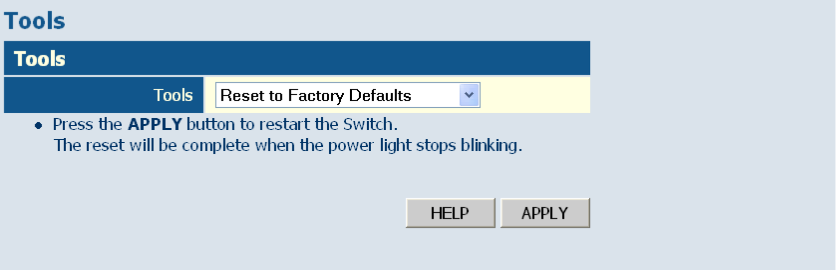
Tools

On the Tools page, you can restore the switch to its default settings, upgrade the firmware of the switch, or restart the switch.

Restore to Factory Defaults

Forces the switch to restore the original factory settings. To reset the switch, select "Reset to Factory Defaults" from the drop-down list and click APPLY. The LAN IP Address, Subnet Mask and Gateway IP Address will not be reset.

Web – Click System, Tools, Reset to Factory Defaults.



Tools

Tools

Tools: Reset to Factory Defaults

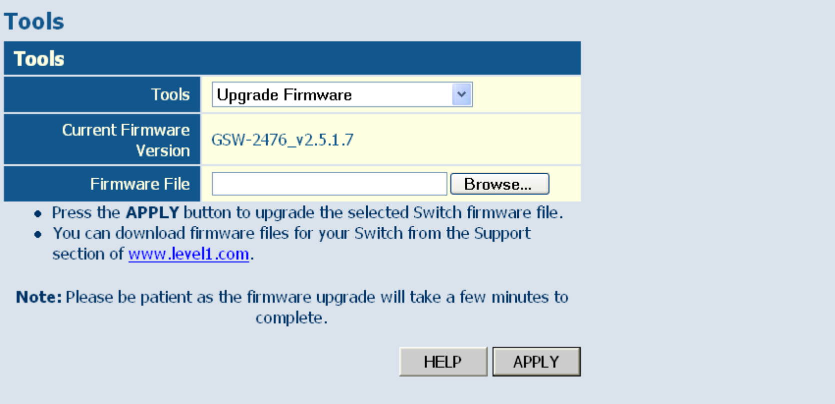
- Press the **APPLY** button to restart the Switch.
  The reset will be complete when the power light stops blinking.

Figure 6-8 Reset to Factory Defaults

Upgrade Firmware

Upgrades the switch system firmware using a file provided by LevelOne. Select "Upgrade Firmware" from the Tools drop-down list, then click the "Browse" button to select the firmware file. Click the APPLY button to upgrade the selected switch firmware file. You can download firmware files for your switch from the Support section of the LevelOne web site at www.level1.com.

Web – Click System, Tools, Reset to Factory Defaults.



Tools

Tools	
Tools	Upgrade Firmware
Current Firmware Version	GSW-2476_v2.5.1.7
Firmware File	

- Press the **APPLY** button to upgrade the selected Switch firmware file.
- You can download firmware files for your Switch from the Support section of www.level1.com.

Note: Please be patient as the firmware upgrade will take a few minutes to complete.

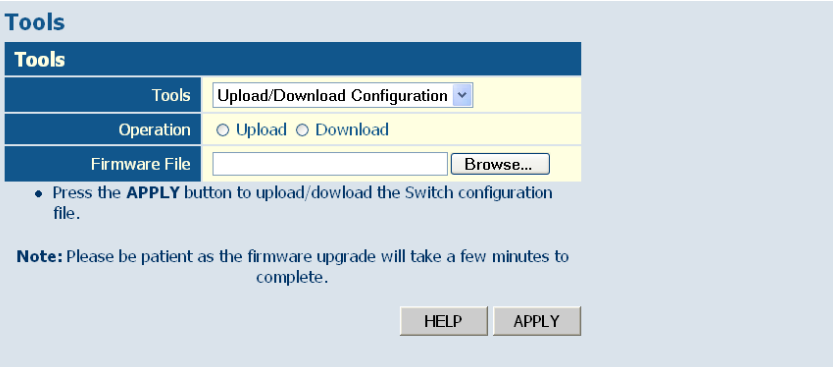
Figure 6-9 Upgrade Firmware

Upload/Download Configuration

The Upload/Download Configuration feature allows you to save the switch's current configuration or restore a previously saved configuration back to the device. Configuration files can be saved to any location on the web management station.

Web – Click SYSTEM, Tools, Upload/Download Configuration. To upload or download the configuration file, select "Upload/Download Configuration" from the Tools drop-down list, then select "Upload" to save a configuration or "Download" to restore a configuration. Use the

Browse button to choose a file location on the web management station, or to find a saved configuration file.



Tools

Tools	
Tools	Upload/Download Configuration
Operation	○ Upload ○ Download
Firmware File	

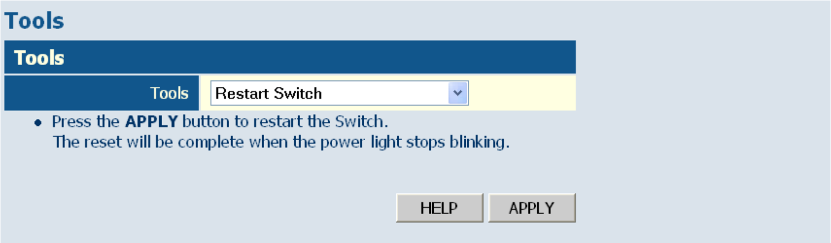
- Press the **APPLY** button to upload/dowload the Switch configuration file.

Note: Please be patient as the firmware upgrade will take a few minutes to complete.

Figure 6-10 Upload/Download Configuration

Restart Switch

Web – Click SYSTEM, Tools, Restart Switch. To restart the switch, click APPLY. The reset will be complete when the user interface displays the login page.



Tools

Tools	
Tools	Restart Switch

- Press the **APPLY** button to restart the Switch.
  The reset will be complete when the power light stops blinking.

Figure 6-11 Restart Switch

Static MAC

Switches store the MAC addresses for all known devices in the attached network. This information is used to forward traffic directly between the inbound and outbound ports. All the MAC addresses learned by monitoring traffic are stored in a dynamic address table, which removes (ages out) any addresses that are not "seen" for a specified time period.

You can also manually configure static MAC addresses that are assigned to specific ports on the switch. A static MAC address is bound to a specific port and will not be moved or aged out. You can define up to 24 static MAC addresses on the switch.

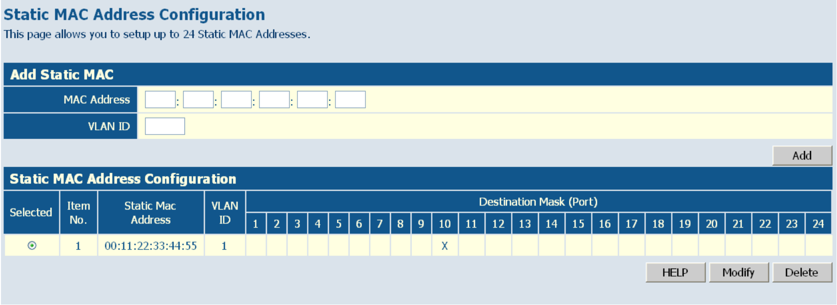
Add Static MAC

Type the static MAC address and associated VLAN ID (1-4095) into corresponding fields in the Add Static MAC table. After clicking the ADD button, a new page opens to configure the Destination Mask for this MAC entry. Only one static MAC address can be added at a time.

Static MAC Address Configuration

This table shows the stored static MAC entries in MAC table.

Web – Click System, Static MAC. Enter the MAC address, VLAN ID, and click ADD to add a new static MAC address. Then mark the port to which this MAC address is bound, and click Apply.



Static MAC Address Configuration

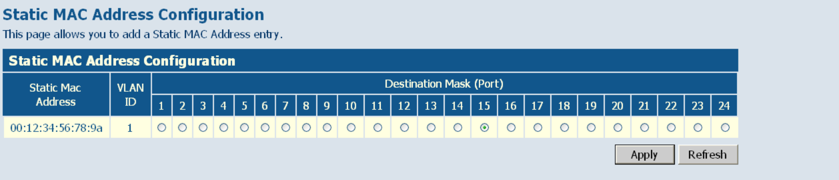
This page allows you to setup up to 24 Static MAC Addresses.

Add Static MAC

MAC Address	__ : __ : __ : __ : __ : __
VLAN ID	__

Static MAC Address Configuration

Selected	Item No.	Static Mac Address	VLAN ID	Destination Mask (Port)																							
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
⦿	1	00:11:22:33:44:55	1										X														



Static MAC Address Configuration

This page allows you to add a Static MAC Address entry.

Static MAC Address Configuration

Static Mac Address	VLAN ID	Destination Mask (Port)																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
00:12:34:56:78:9a	1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	⦿	○	○	○	○	○	○	○	○	○

Figure 6-12 Static MAC Address Configuration

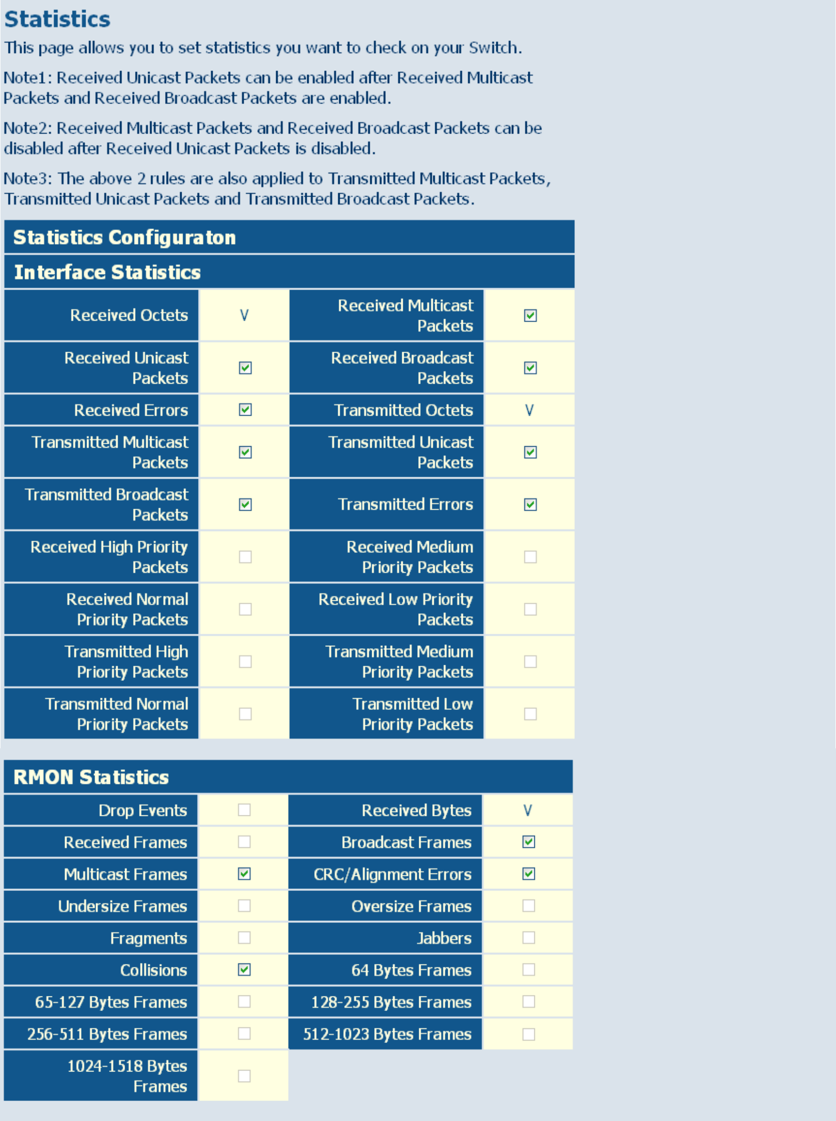
Counter Configuration

This page allows specific statistics to be selected for monitoring. It is possible to monitor up to five transmit counters and five receive counters, as well as 1 transmit byte counter and receive byte counter.

Please also note the following restrictions.

- Received Unicast Packets can be enabled after Received Multicast Packets and Received Broadcast Packets are enabled.
- Received Multicast Packets and Received Broadcast Packets can be disabled after Received Unicast Packets is disabled.
- The above 2 rules are also applied to Transmitted Multicast Packets, Transmitted Unicast Packets and Transmitted Broadcast Packets.

Web – Click SYSTEM, Counter Config.



Statistics

This page allows you to set statistics you want to check on your Switch.

Note1: Received Unicast Packets can be enabled after Received Multicast Packets and Received Broadcast Packets are enabled.

Note2: Received Multicast Packets and Received Broadcast Packets can be disabled after Received Unicast Packets is disabled.

Note3: The above 2 rules are also applied to Transmitted Multicast Packets, Transmitted Unicast Packets and Transmitted Broadcast Packets.

Statistics Configuraton

Interface Statistics

Received Octets	V	Received Multicast Packets	☑
Received Unicast Packets	☑	Received Broadcast Packets	☑
Received Errors	☑	Transmitted Octets	V
Transmitted Multicast Packets	☑	Transmitted Unicast Packets	☑
Transmitted Broadcast Packets	☑	Transmitted Errors	☑
Received High Priority Packets	□	Received Medium Priority Packets	□
Received Normal Priority Packets	□	Received Low Priority Packets	□
Transmitted High Priority Packets	□	Transmitted Medium Priority Packets	□
Transmitted Normal Priority Packets	□	Transmitted Low Priority Packets	□

RMON Statistics

Drop Events	□	Received Bytes	V
Received Frames	□	Broadcast Frames	☑
Multicast Frames	☑	CRC/Alignment Errors	☑
Undersize Frames	□	Oversize Frames	□
Fragments	□	Jabbers	□
Collisions	☑	64 Bytes Frames	□
65-127 Bytes Frames	□	128-255 Bytes Frames	□
256-511 Bytes Frames	□	512-1023 Bytes Frames	□
1024-1518 Bytes Frames	□		

Figure 6-13 Counter Configuration

Port Configuration

Ports Settings

You can use the Port Configuration page to manually set the speed, duplex mode, and flow control.

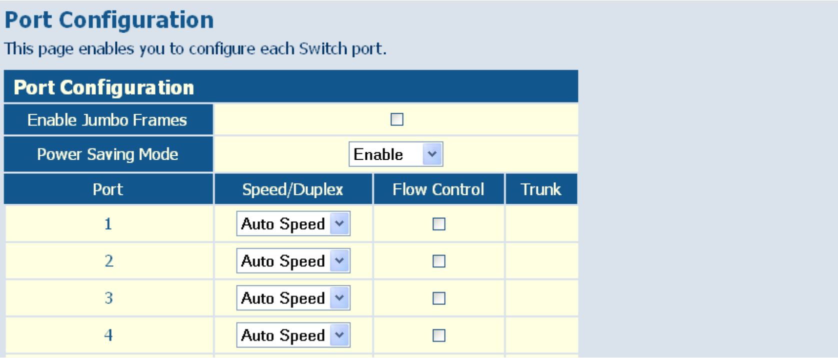
Field Attributes

- **Enable Jumbo Frames** – This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- **Power Saving Mode** – Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements.

  IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can significantly reduce power used for cable lengths of 20 meters or less, and continue to ensure signal integrity.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode.
- **Flow Control** – Allows flow control to be enabled or disabled. When the box is checked, flow control is enabled.
- **Trunk** – Indicates if a port is a member of a trunk.

Note: Ports within a trunk cannot be configured individually. However, you can use the “Trunk Configuration” page to manually set the same speed, duplex mode, and flow control for every port in a trunk.

Web – Click PORTS, Settings. Enable or disable jumbo frames, select the required settings for any port, and then click APPLY.



Port Configuration

This page enables you to configure each Switch port.

Port Configuration			
Enable Jumbo Frames	□		
Power Saving Mode	Enable		
Port	Speed/Duplex	Flow Control	Trunk
1	Auto Speed	□	
2	Auto Speed	□	
3	Auto Speed	□	
4	Auto Speed	□	

Figure 6-14 Port Configuration

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the switch. Traffic that falls within the rate limit is transmitted or received, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

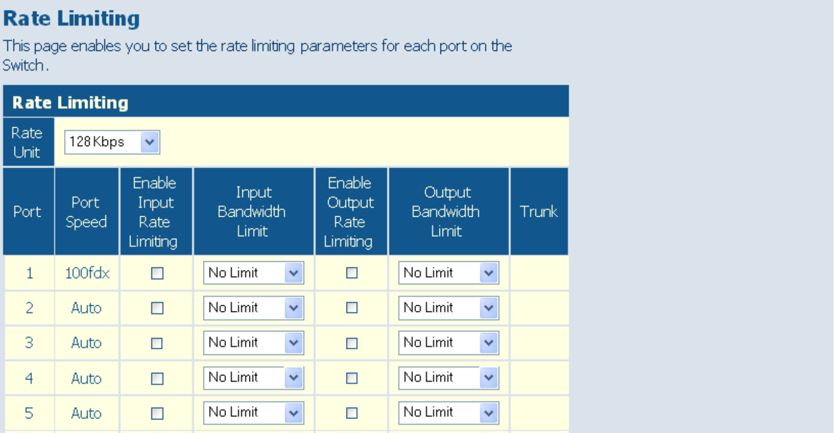
The Input/Output Bandwidth Limit field is a type-in box which accepts an integer number in the range 1 to 100. The number specifies the percentage of the total bandwidth of the port that can be used before packets are dropped or flow-control starts.

Field Attributes

- **Rate Unit** – This field sets the granularity of the bandwidth limit which can be set for individual ports. To change the granularity, first choose an option from this list, click APPLY, and then view the options in the Input/Output Bandwidth Limit drop-down box for any of the ports. (Options: 128 kbps, 1 Mbps, 10 Mbps, 30 Mbps, 100 Mbps)

- **Enable Rate Limiting** – Enables input or output rate limiting for the selected interface. (Default: Disabled)
- **Bandwidth Limit** – Sets the rate limit for ingress or egress traffic. When this limit is exceeded, packets are dropped, until the rate falls back beneath the configured limit. (The options displayed depend on the selection for Rate Unit.)

Web – Click PORTS, Rate Limiting. This page enables you to set the rate limiting parameters for each port on the switch.



Rate Limiting

This page enables you to set the rate limiting parameters for each port on the Switch.

Rate Limiting

Rate Unit: 128 Kbps

Port	Port Speed	Enable Input Rate Limiting	Input Bandwidth Limit	Enable Output Rate Limiting	Output Bandwidth Limit	Trunk
1	100fdx	□	No Limit	□	No Limit	
2	Auto	□	No Limit	□	No Limit	
3	Auto	□	No Limit	□	No Limit	
4	Auto	□	No Limit	□	No Limit	
5	Auto	□	No Limit	□	No Limit	

Figure 6-15 Rate Limiting

Storm Control

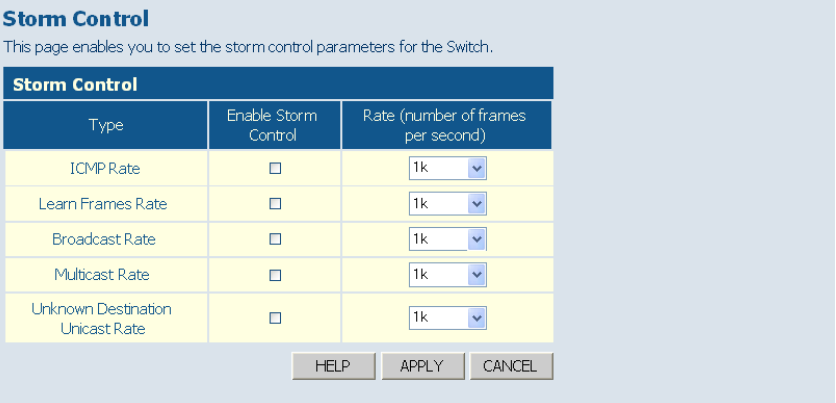
Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

Field Attributes

- **Type** – List the type of traffic which can be rate limited, including ICMP, learn frames, broadcast, multicast and flooded unicast frames.
- **Enable Storm Control** – Click the check box to enable storm control for the specific frame type.
- **Rate** (number of frames per second) – The Rate field is set by a single drop-down list. The same threshold is applied to every port on the switch. When the threshold is exceeded, packets are dropped, irrespective of the flow-control settings. (Options: 1k - 32768k, in steps of 2^n)

Web – Click PORTS, Storm Control. This page enables you to set the broadcast storm control parameters for every port on the switch.



Storm Control

This page enables you to set the storm control parameters for the Switch.

Storm Control

Type	Enable Storm Control	Rate (number of frames per second)
ICMP Rate	□	1k
Learn Frames Rate	□	1k
Broadcast Rate	□	1k
Multicast Rate	□	1k
Unknown Destination Unicast Rate	□	1k

Figure 6-16 Port Broadcast Control

Port Mirroring

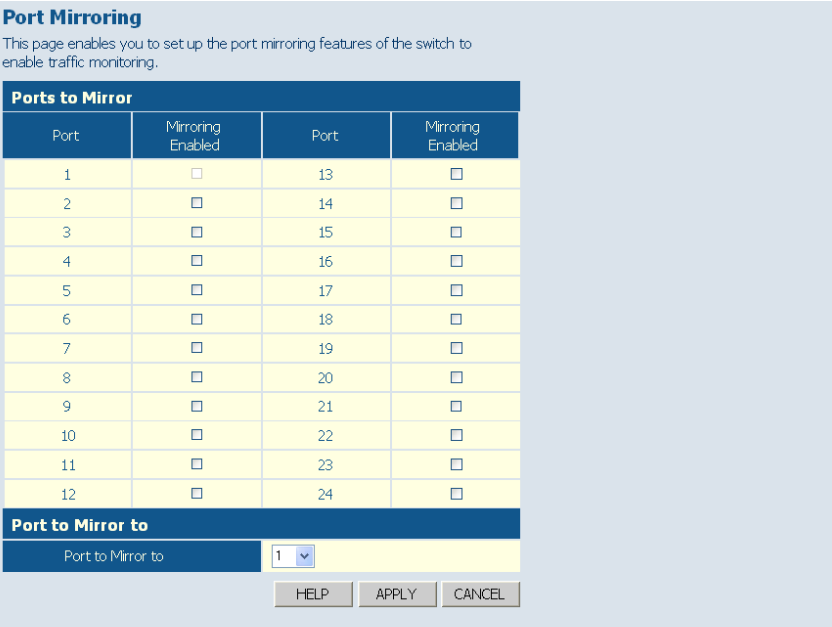
You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Field Attributes

- **Ports to Mirror** - Select the ports that you want to mirror from this section of the page. A port will be mirrored when the “Mirroring Enabled” check-box is checked.
- **Port to Mirror to** – The port that will “duplicate” or “mirror” the traffic on the source port. Only incoming packets can be mirrored. Packets will be dropped when the available egress bandwidth is less than ingress bandwidth.

Note: If the total ingress bandwidth exceeds the mirror port's egress bandwidth, packets will eventually be dropped on ingress to the switch, which means they will not reach the mirror port or their intended destination port. Input rate-limiting in conjunction with port flow-control should be used to ensure that the total ingress bandwidth never exceeds the egress bandwidth.

Web – Click PORTS, Port Mirroring.



Port Mirroring

This page enables you to set up the port mirroring features of the switch to enable traffic monitoring.

Ports to Mirror

Port	Mirroring Enabled	Port	Mirroring Enabled
1	□	13	□
2	□	14	□
3	□	15	□
4	□	16	□
5	□	17	□
6	□	18	□
7	□	19	□
8	□	20	□
9	□	21	□
10	□	22	□
11	□	23	□
12	□	24	□

Port to Mirror to

Port to Mirror to	1

Figure 6-17 Port Mirroring

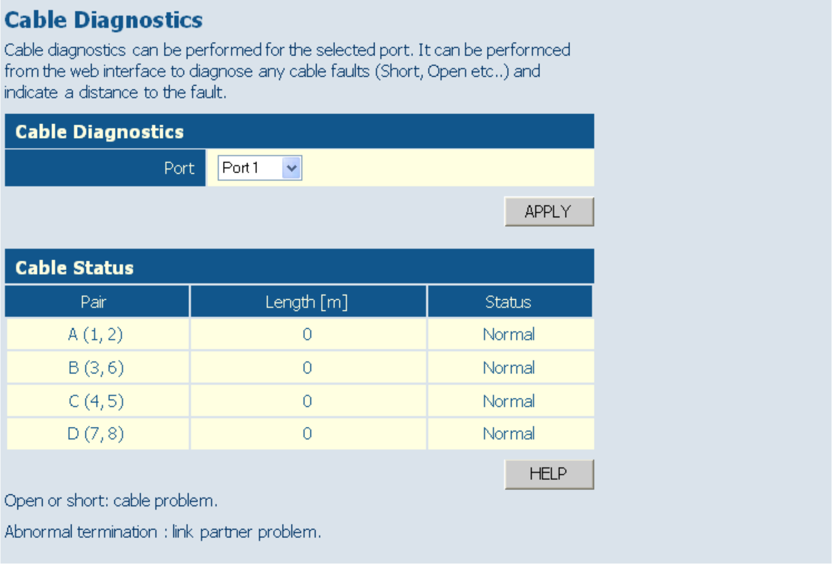
Cable Diagnostics

You can perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open, etc.) and feedback a distance to the fault.

Field Attributes

- **Cable Diagnostics** – Cable diagnostics is performed on a per-port basis. Select the port number from the drop-down list.
- **Cable Status** – Shows the cable length, operating conditions and isolates a variety of common faults that can occur on Category 5 twisted pair cabling.

Web – Click PORTS, Cable Diagnostics.



Cable Diagnostics

Cable diagnostics can be performed for the selected port. It can be performced from the web interface to diagnose any cable faults (Short, Open etc..) and indicate a distance to the fault.

Cable Diagnostics

Port: Port 1

Cable Status

Pair	Length [m]	Status
A (1, 2)	0	Normal
B (3, 6)	0	Normal
C (4, 5)	0	Normal
D (7, 8)	0	Normal

Open or short: cable problem.

Abnormal termination : link partner problem.

Figure 6-18 Cable Diagnostics

Trunk Membership

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices.

This page allows you to create a maximum of eight trunks of up to eight ports each. The Membership Table has one row for each port and a column for each trunk. Each row contains nine radio buttons which are used to indicate which trunk (if any) to which the port belongs.

When a trunk is first created it is given the following default configuration:

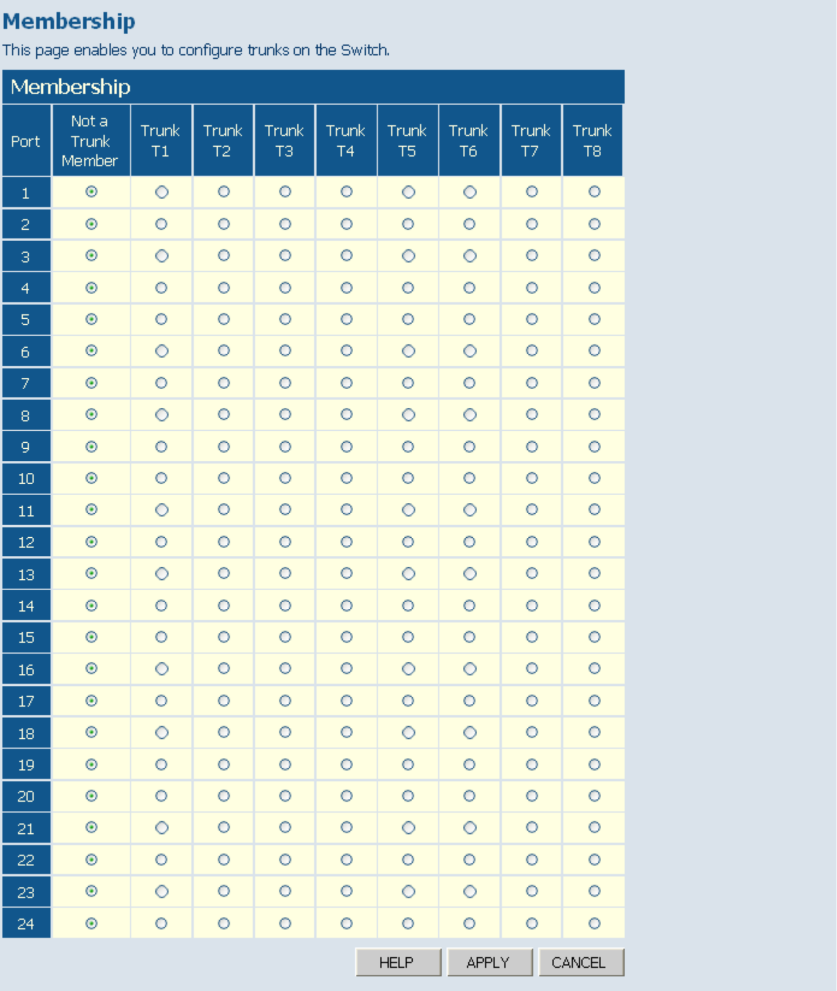
- Speed/Duplex is set to Auto Speed (TRUNKS > Settings).
- Flow Control is turned off (TRUNKS > Settings).
- Rate Limiting is turned off (TRUNKS > Rate Limiting).
- The trunk is a member of VLAN 1 (VLANS > VLAN Membership) with a PVID of 1. The trunk will accept both tagged and untagged packets.

Ports that are removed from the trunk, retain the configuration that they had when members of the trunk. Ports that are added to the trunk after its creation, inherit the current configuration of the trunk.

Field Attributes

- **Port** – The front panel port number.
- **Not a Trunk Member** – If the radio button in this column is selected, the port is not a member of any trunk. (This is the default state.)
- **Trunk T1-T8** – These columns correspond to the eight trunks that are supported by the switch. To assign a port to a trunk, click on the radio button in the corresponding column, then click APPLY.

Web – Click TRUNKS, Membership. To assign a port to a trunk, click the required trunk number, then click APPLY.



Membership

This page enables you to configure trunks on the Switch.

Membership

Port	Not a Trunk Member	Trunk T1	Trunk T2	Trunk T3	Trunk T4	Trunk T5	Trunk T6	Trunk T7	Trunk T8
1	●	○	○	○	○	○	○	○	○
2	●	○	○	○	○	○	○	○	○
3	●	○	○	○	○	○	○	○	○
4	●	○	○	○	○	○	○	○	○
5	●	○	○	○	○	○	○	○	○
6	●	○	○	○	○	○	○	○	○
7	●	○	○	○	○	○	○	○	○
8	●	○	○	○	○	○	○	○	○
9	●	○	○	○	○	○	○	○	○
10	●	○	○	○	○	○	○	○	○
11	●	○	○	○	○	○	○	○	○
12	●	○	○	○	○	○	○	○	○
13	●	○	○	○	○	○	○	○	○
14	●	○	○	○	○	○	○	○	○
15	●	○	○	○	○	○	○	○	○
16	●	○	○	○	○	○	○	○	○
17	●	○	○	○	○	○	○	○	○
18	●	○	○	○	○	○	○	○	○
19	●	○	○	○	○	○	○	○	○
20	●	○	○	○	○	○	○	○	○
21	●	○	○	○	○	○	○	○	○
22	●	○	○	○	○	○	○	○	○
23	●	○	○	○	○	○	○	○	○
24	●	○	○	○	○	○	○	○	○

Figure 6-19 Trunk Membership

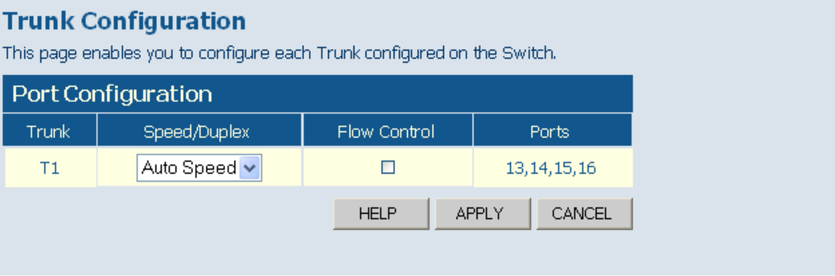
Trunk Configuration

This page allows you to configure the speed, duplex mode, and flow control for a trunk.

Field Attributes

- **Trunk** – Indicates trunk identifier.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode for all ports in the trunk. (Default: Auto speed)
- **Flow Control** – Allows flow control to be enabled or disabled. When the box is checked, flow control is enabled.
- **Ports** – Indicates which ports belong to the trunk.

Web – Click TRUNKS, Settings.



Trunk Configuration

This page enables you to configure each Trunk configured on the Switch.

Port Configuration

Trunk	Speed/Duplex	Flow Control	Ports
T1	Auto Speed	□	13,14,15,16

Figure 6-20 Trunk Configuration

Trunk Rate Limit

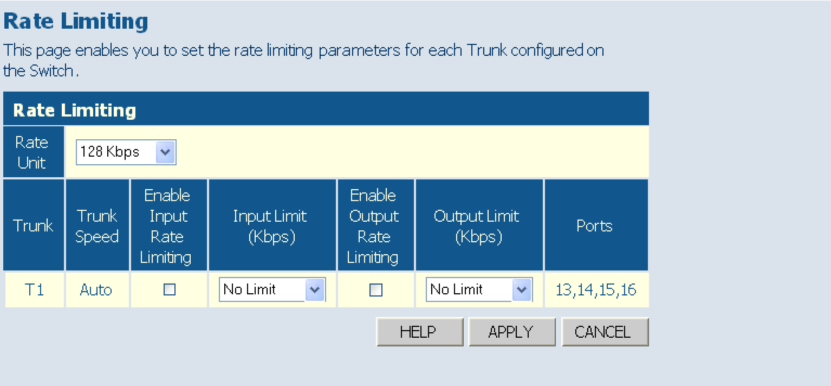
This page allows you to change the maximum input and output data rate for each each trunk on the switch.

Field Attributes

- **Rate Unit** – This field sets the granularity of the bandwidth limit which can be set for individual trunks. To change the granularity, first choose an option from this list, click APPLY, and then view the options in the Input/Output Bandwidth Limit drop-down box for any of the trunks. (Options: 128 kbps, 1 Mbps, 10 Mbps, 30 Mbps, 100 Mbps)

- **Trunk** – Indicates trunk identifier.
- **Trunk Speed** – Indicates the trunk speed.
- **Enable Input/Output Rate Limiting** - Mark the box to enable Input/ Output Rate Limiting.
- **Input/Output Limit** – Sets the threshold for trunk bandwidth measured in number of frames per second. When this limit is exceeded, packets are dropped, until the rate falls back beneath the configured limit. (Options: 1k - 32768k, in steps of 2^n)
- **Ports** – Indicates which ports belong to the trunk.

Web – Click TRUNKS, Rate Limiting.



Rate Limiting

This page enables you to set the rate limiting parameters for each Trunk configured on the Switch.

Rate Limiting

Rate Unit: 128 Kbps

Trunk	Trunk Speed	Enable Input Rate Limiting	Input Limit (Kbps)	Enable Output Rate Limiting	Output Limit (Kbps)	Ports
T1	Auto	□	No Limit	□	No Limit	13,14,15,16

Figure 6-21 Trunk Rate Limiting

LACP Setup

This page allows you to enable 802.3ad Link Aggregation Control Protocol (LACP) for the selected port.

You can configure any number of ports on the switch to use LACP. If ports on another device are also configured for LACP, the switch and the other device will negotiate a trunk link between them. However, before making any physical connections, consider the following points:

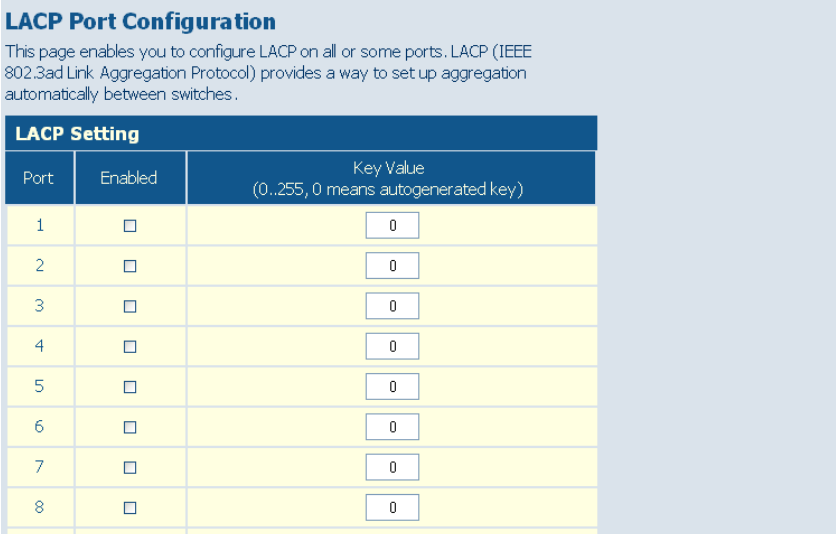
- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.

Field Attributes

- **Port** – A front panel port number.
- **Enabled** – Enables LACP for the selected port.
- **Key Value** – Configures a port's LACP administration key.

  The port administrative key must be set to the same value for ports that belong to the same link aggregation group (LAG). If this administrative key is not set when an LAG is formed (i.e., it has the null value of 0), this key will automatically be set to the same value as that used by the LAG.

Web – Click TRUNKS, LACP Setup. Enable LACP on each port to be configured as a member of an LAG. Leave the administrative key set to a null value to allow the switch to automatically configure this attribute, or set it a specific value to maintain more precise control over the ports which will be connected to another device. Click APPLY.



LACP Port Configuration

This page enables you to configure LACP on all or some ports. LACP (IEEE 802.3ad Link Aggregation Protocol) provides a way to set up aggregation automatically between switches.

LACP Setting

Port	Enabled	Key Value (0..255, 0 means autogenerated key)
1	□	0
2	□	0
3	□	0
4	□	0
5	□	0
6	□	0
7	□	0
8	□	0

Figure 6-22 LACP Port Configuration

Displaying LACP Status

This page allows you display the operational state for the local and remote side of an link aggregation.

Field Attributes

LACP Aggregation

Displays the LACP status for each port. For active link aggregation groups, the ports attached at the other end of the link are also displayed.

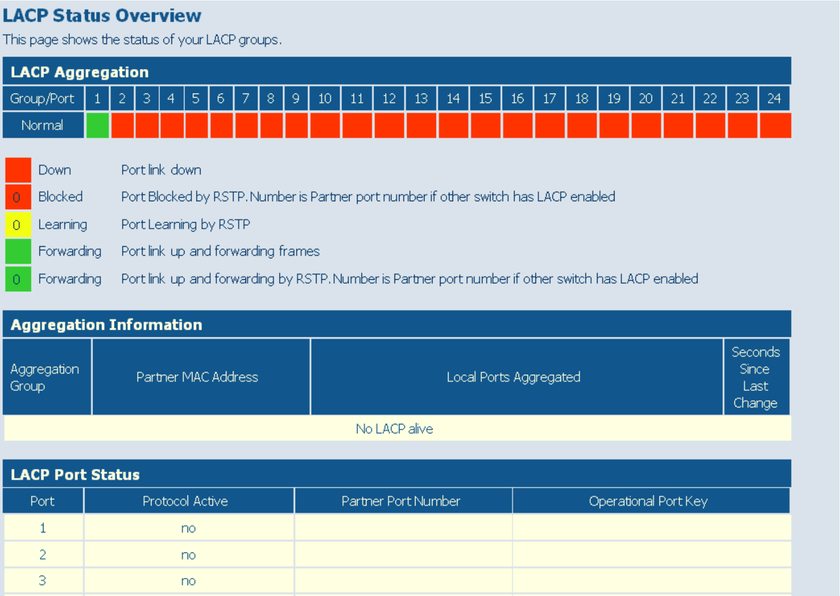
Aggregation Information

- **Aggregation Group** – Identifier for a local link aggregation group.
- **Partner MAC Address** – Physical address of device at other end of link.
- **Local Ports Aggregated** – Local ports participating in this LAG.
- **Seconds Since Last Change** – Time since the last LACP packet was received.

LACP Port Status

- **Port** – A front panel port number.
- **Protocol Active** – Indicates whether or not LACP is active on this port.
- **Partner Port Number** – A list of the ports attached at the remote end of this LAG link member.
- **Operational Port Key** – Current operational value of the key used by this LAG.

Web – Click TRUNKS, LACP Status.



LACP Status Overview

This page shows the status of your LACP groups.

LACP Aggregation

Group/Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

🟥	Down	Port link down
🟥 0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
🟨 0	Learning	Port Learning by RSTP
🟩	Forwarding	Port link up and forwarding frames
🟩 0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

Aggregation Information

Aggregation Group	Partner MAC Address	Local Ports Aggregated	Seconds Since Last Change
No LACP alive			

LACP Port Status

Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		

Figure 6-23 LACP Status Overview

Configuring VLAN Groups

The 802.1Q VLAN Configuration page allows you to create and delete VLANs (Virtual LANs), and set up or modify VLAN group members.

Introduction to VLANs

VLANs are logical partitions of the physical LAN. You can use VLANs to increase network performance or improve internal network security.

If the network has adequate performance and security for your current needs, it is recommended that you leave the VLAN settings in the default configuration. The default configuration is as follows:

- All ports are members of VLAN 1
- The switch management interface is on VLAN 1
- All ports have a Port VLAN ID (PVID) of 1
- All ports can send and receive both VLAN-tagged and untagged packets (that is, they are hybrid ports)

In the default configuration, any port is able to send traffic to any other port and a PC connected to any port will be able to access the management interface. Broadcast traffic, for example, will be flooded to all ports on the switch.

The VLAN parameters that can be configured for each port on the switch include VLAN Aware Enabled, Ingress Filtering Enabled, QinQ Enabled, Packet Type, and PVID. Note that the ports within a trunk cannot be configured individually; configure the static trunk instead (trunks are labelled T1 to T8). Also, note that the VLAN parameters of a dynamic link aggregation group formed through LACP cannot be configured. The port members of a dynamic link aggregation group must be configured prior to setting up the group.

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network. QinQ tunneling expands VLAN space by using this VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging). Ports on the switch can be set to support QinQ when providing a direct link to a service provider's network.

Creating VLANs and Assigning Port Members

To create a new VLAN, enter an identifier in the Add VLAN Group table, click the Add button, and then configure the port or static trunk members on the 802.1Q VLAN Group page. To modify the membership settings for an existing VLAN, select a VLAN from the VLAN Group List, and click Modify. Each row in the VLAN membership table corresponds to one port or static trunk. Trunked ports cannot be configured individually. Also, note that the VLAN membership of dynamically configured LACP trunks cannot be modified.

Field Attributes

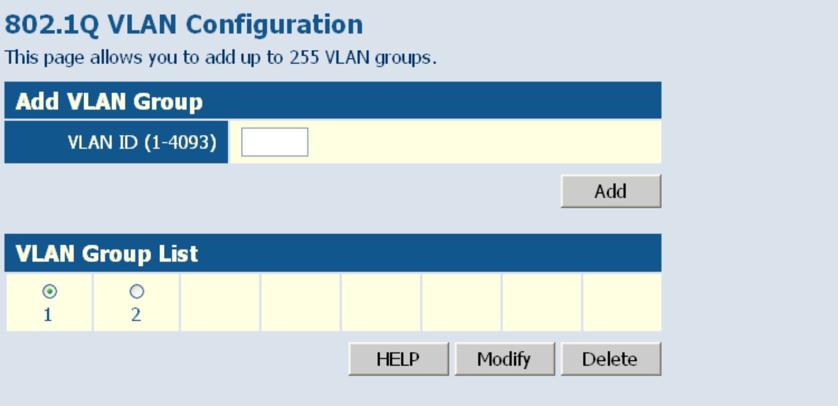
Add VLAN Group

- **VLAN ID** – Input a VLAN ID and click APPLY to create a new VLAN.

VLAN Group List

- **VLAN List** – The list of up to 64 VLANs. You can modify or delete these VLANs.

Web – Click VLANS, VLAN Membership.



802.1Q VLAN Configuration

This page allows you to add up to 255 VLAN groups.

Add VLAN Group

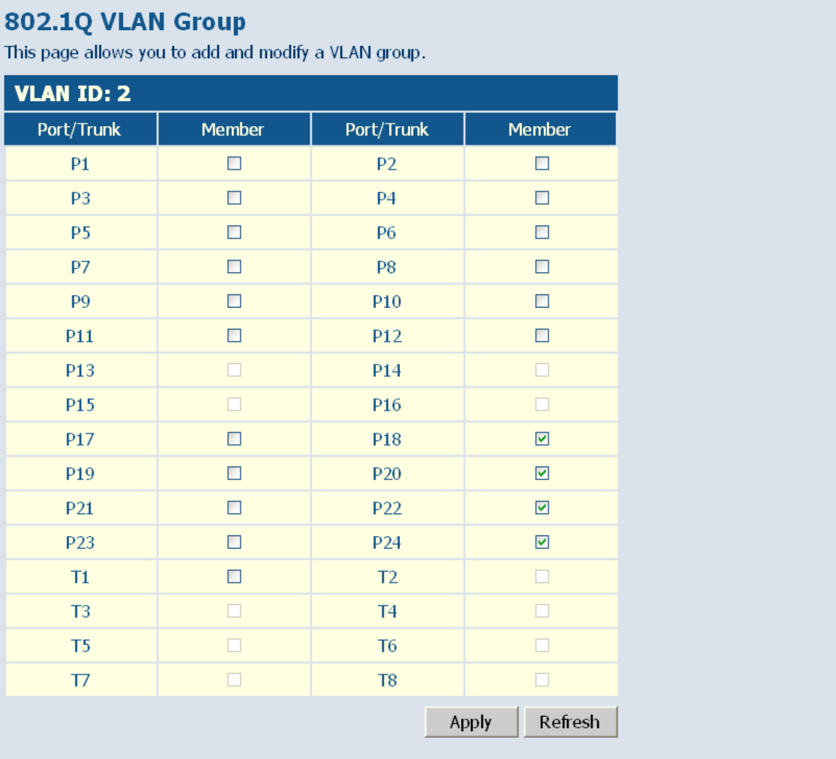
VLAN ID (1-4093)

VLAN Group List

● 1 ○ 2

Figure 6-24 802.1Q VLAN Configuration

Web – After creating a new VLAN, the following screen displays. Assign the ports and trunks associated with the VLAN, and click Apply.



802.1Q VLAN Group

This page allows you to add and modify a VLAN group.

VLAN ID: 2

Port/Trunk	Member	Port/Trunk	Member
P1	□	P2	□
P3	□	P4	□
P5	□	P6	□
P7	□	P8	□
P9	□	P10	□
P11	□	P12	□
P13	□	P14	□
P15	□	P16	□
P17	□	P18	☑
P19	□	P20	☑
P21	□	P22	☑
P23	□	P24	☑
T1	□	T2	□
T3	□	T4	□
T5	□	T6	□
T7	□	T8	□

Figure 6-25 VLAN Group Settings

Configuring VLAN Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID) and accepted frame types. The 802.1Q Per Port Configuration page allows you to change the VLAN parameters for individual ports. Each row of the table corresponds to one port or static trunk; trunked ports cannot be configured individually. Also, note that the VLAN attributes of dynamically configured LACP trunks cannot be modified.

Field Attributes

- **Port/Trunk** – The port-number of the port or the ID of a trunk.
- **VLAN Aware Enabled** – VLAN aware ports are able to use VLAN tagged frames to determine the destination VLAN of a frame. (Default: Enabled)

  VLAN aware ports will strip the VLAN tag from received frames and insert the tag in transmitted frames (except for the PVID). VLAN unaware ports will not strip the tag from received frames or insert the tag in transmitted frames.

  For QinQ operation, a customer port should be set to VLAN unaware and a provider port (trunk port) should be set to VLAN aware.
- **Ingress Filtering Enabled** – If enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded. (Default: Disabled)
- **QinQ** – A QinQ enabled port will accept packets up to 1526 bytes in length, which means double tag header frames can be accepted. QinQ should be enabled for provider ports but not for customer ports.

  QinQ “customer” ports are those ports that are connected to normal VLAN aware switches in the customer’s network. QinQ “network” ports are those which are connected to the service provider's network. To tunnel packets through a service provider’s metro network, QinQ needs to be enabled on the network port.
- **Packet Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. (Default: All)

  If the Packet Type is set to “All,” the port can accept incoming tagged and untagged packets. Any received packets that are untagged are assigned to the default VLAN. Any tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. Outgoing packets will be tagged unless the packet's VLAN ID is the same as the PVID. PCs should be connected to ports with Packet Type set to "All." PCs cannot, in general, send or receive tagged packets.

If the Packet Type is set to "Tagged Only," the port will drop untagged packets and will only receive tagged packets. Tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet.

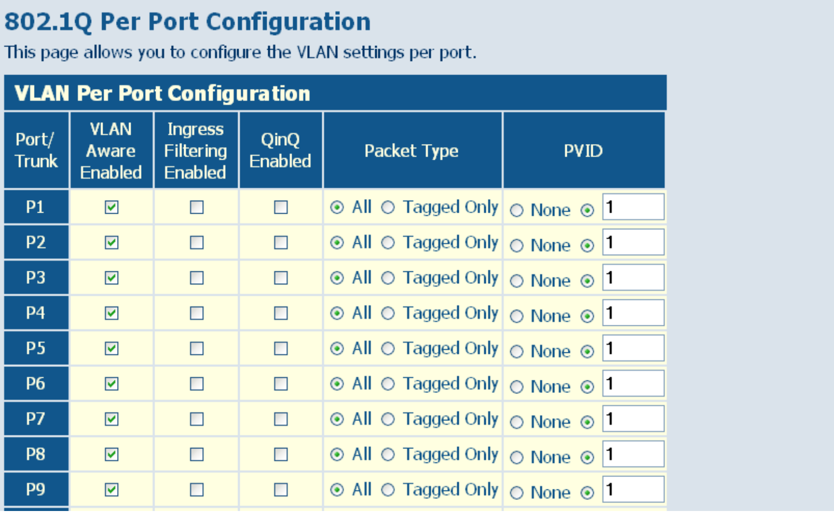
- **PVID** – The port VLAN ID (PVID) is associated with untagged, ingress packets. It is assigned to untagged frames received on the specified interface. The PVID has no effect on ports that have Packet Type set to "Tagged Only." (Default PVID: 1)

  It is not possible to remove a port from VLAN 1 unless its PVID has been changed to something other than 1.

  Outgoing packets are tagged unless the packet's VLAN ID is the same as the PVID. When the PVID is set to "None," all outgoing packets are tagged.

Note: If you select "Tagged Only" mode for a port, we recommend setting the PVID to "None" as the standard configuration.

Web – Click VLANS, VLAN Port Configuration. Fill in the required settings for each interface, and click Apply.



802.1Q Per Port Configuration

This page allows you to configure the VLAN settings per port.

VLAN Per Port Configuration

Port/ Trunk	VLAN Aware Enabled	Ingress Filtering Enabled	QinQ Enabled	Packet Type	PVID
P1	☑	□	□	● All ○ Tagged Only	○ None ● 1
P2	☑	□	□	● All ○ Tagged Only	○ None ● 1
P3	☑	□	□	● All ○ Tagged Only	○ None ● 1
P4	☑	□	□	● All ○ Tagged Only	○ None ● 1
P5	☑	□	□	● All ○ Tagged Only	○ None ● 1
P6	☑	□	□	● All ○ Tagged Only	○ None ● 1
P7	☑	□	□	● All ○ Tagged Only	○ None ● 1
P8	☑	□	□	● All ○ Tagged Only	○ None ● 1
P9	☑	□	□	● All ○ Tagged Only	○ None ● 1

Figure 6-26 VLAN Settings

QoS Settings

QoS (Quality of Service) is a mechanism which is used to prioritize certain traffic as it is forwarded through the switch. Both the queue service mode (strict or weighted round robin), and the method of classifying the priority of ingress traffic can be configured on this page.

Traffic can be classified as High, Medium, Normal or Low priority. When the switch is heavily loaded, lower priority traffic is dropped first. You can select how to prioritize traffic by using one of the QoS modes (none, 802.1p, or DSCP).

Selecting the Queue Mode

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue.

Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.

WRR uses a relative weighting for each queue which determines the amount of packets the switch transmits every time it services each queue before moving on to the next queue. Thus, a queue weighted 8 will be allowed to transmit up to 8 packets, after which the next lower priority queue will be serviced according to it’s weighting. This prevents the head-of-line blocking that can occur with strict priority queuing.

Selecting the Method of Priority Processing

This switch supports several common methods of prioritizing traffic to meet application requirements. It can process traffic priorities specified by the IEEE 802.1p priority bits in Layer 2 traffic, or the Differentiated Services Code Point (DSCP) service priority bits found in Layer 3/4 traffic. When either of these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

If the QoS mode is set to 802.1p, and the ingress packet type is IPv4, then priority processing will be based on the 802.1p value in the ingress packet. For an untagged packet, the default port priority is used for priority processing (i.e., CoS value 0, which maps to the Normal Queue).

If the QoS mode is set to DSCP, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.

Field Attributes

Queue Mode

- **Strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **WRR** – Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights with default values of 1, 2, 4, 8 for queues 0 through 7, respectively. (This is the default selection.)
  Note that WRR can only be selected if Jumbo Frame mode is disabled on the Port Configuration page (see “Port Configuration” on page 6-24).

QoS Mode

- **QoS Disabled** – QoS is turned off and all packets have equal priority.
- **802.1p** – Packets are prioritized using the 802.1p field in the VLAN tag. This field is three bits long, representing the values 0 - 7. When the QoS Mode is set to 802.1p, the 802.1p Configuration table appears, allowing you to map each of the eight 802.1p values to a local priority queue (low, normal, medium or high). The default settings are shown below.

Mapping CoS Values to Egress Queues

Egress Queue	low	normal	medium	high
802.1-p Priority	1,2	0,3	4,5	6,7

You can use the Prioritize Traffic drop-down list to quickly map the values in the 802.1p Configuration table to the same priority queue. Use

Custom if you want to set each value individually.

Note that end-stations, like PCs, are not usually VLAN aware, so they do not create VLAN-tagged frames. As a result, 802.1p is not an ideal method to use when there are a lot of PCs connected to the switch.

- **DSCP** – Packets are prioritized using the DSCP (Differentiated Services Code Point) value.

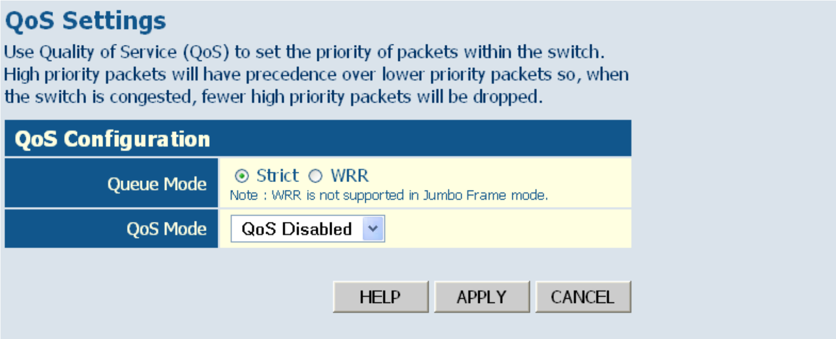
  The Differentiated Services Code Point (DSCP) is a six-bit field that is contained within an IP (TCP or UDP) header. The six bits allow the DSCP field to take any value in the range 0 - 63. When QoS Mode is set to DSCP, the DSCP Configuration table is displayed, allowing you to map each of the DSCP values to a hardware output queue (low, normal, medium or high). The default settings are shown below. Note that all the DSCP values not specified are mapped to the normal egress queue.

Mapping DSCP Priorities to Egress Queues

IP DSCP Value	**Egress Queue**
8, 10, 12, 14, 16	low
0, 18, 20, 22, 24	normal
26, 28, 30, 32, 34, 36, 38, 40, 42	medium
46, 48, 56	high

You can use the Prioritize Traffic drop-down list to quickly set the values in the DSCP Configuration table to a common priority queue. Use Custom if you want to set each value individually.

Web – Click QOS, Settings. In QoS Mode, select QoS Disabled, 802.1p, or DSCP to configure the related parameters.



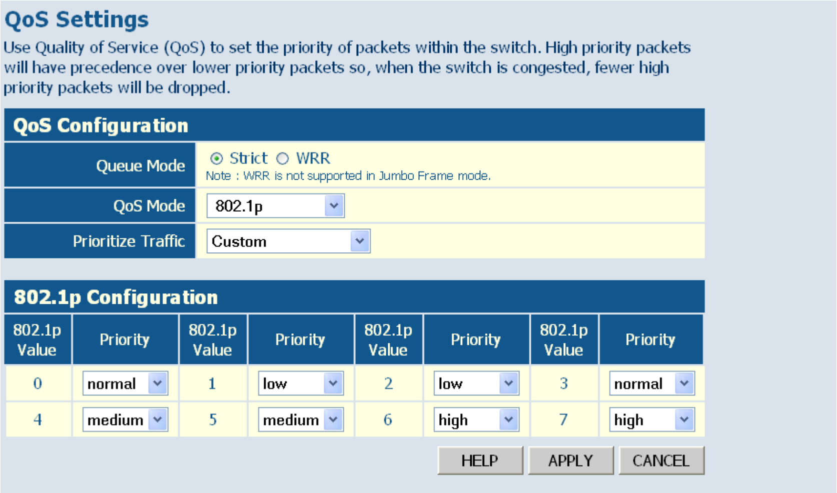
QoS Settings

Use Quality of Service (QoS) to set the priority of packets within the switch. High priority packets will have precedence over lower priority packets so, when the switch is congested, fewer high priority packets will be dropped.

QoS Configuration	
Queue Mode	● Strict ○ WRR Note : WRR is not supported in Jumbo Frame mode.
QoS Mode	QoS Disabled

Figure 6-27 QoS Settings

When the QoS Mode is set to 802.1p, the 802.p Configuration table is displayed as shown below.



QoS Settings

Use Quality of Service (QoS) to set the priority of packets within the switch. High priority packets will have precedence over lower priority packets so, when the switch is congested, fewer high priority packets will be dropped.

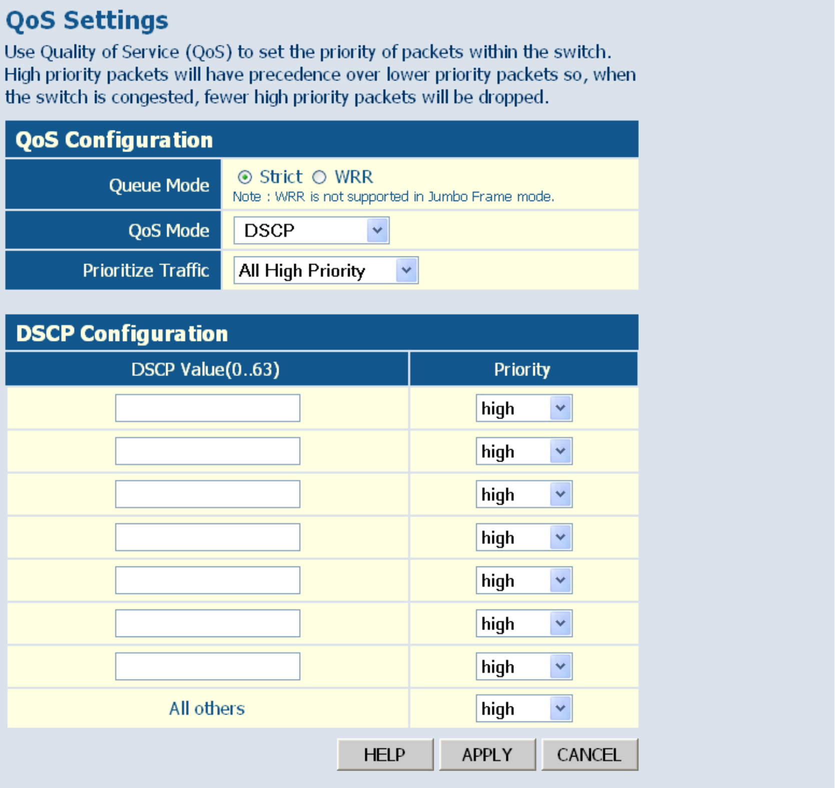
QoS Configuration	
Queue Mode	● Strict ○ WRR Note : WRR is not supported in Jumbo Frame mode.
QoS Mode	802.1p
Prioritize Traffic	Custom

802.1p Configuration

802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal	1	low	2	low	3	normal
4	medium	5	medium	6	high	7	high

Figure 6-28 802.1p Configuration

When the QoS Mode is set to DSCP, the DSCP Configuration table is displayed as shown below.



QoS Settings

Use Quality of Service (QoS) to set the priority of packets within the switch. High priority packets will have precedence over lower priority packets so, when the switch is congested, fewer high priority packets will be dropped.

QoS Configuration

Queue Mode	◉ Strict ○ WRR Note : WRR is not supported in Jumbo Frame mode.
QoS Mode	DSCP
Prioritize Traffic	All High Priority

DSCP Configuration

DSCP Value(0..63)	Priority
	high
	high
	high
	high
	high
	high
	high
All others	high

Figure 6-29 DSCP Configuration

RSTP

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP (Rapid Spanning Tree Protocol, IEEE 802.1w) is designed as a general replacement for the slower, legacy Spanning Tree Protocol (STP, IEEE 802.1D). RSTP achieves much faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Configuring RSTP

Use the RSTP Configuration page to specify global or port-specific parameters for the Rapid Spanning Tree Protocol.

Field Attributes

RSTP System Configuration

- **System Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.) (Default: 32768; Range: 0-61440, in steps of 4096)
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message (BPDU frame).
  (Default: 2;
  Minimum: 1,
  Maximum: The lower of 10 or [(Max. Message Age / 2) - 1])
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. That also means the maximum life time for a BPDU frame. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.
  (Default: 20,
  Minimum: The higher of 6 or [2 x (Hello Time + 1)],
  Maximum: The lower of 40 or [2 x (Forward Delay - 1)])
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding).

This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
(Default: 15;
Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
Maximum: 30)

- **Force Version** – RSTP supports connections to either RSTP or STP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
  - **Normal** (RSTP Mode) – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.
  - **Compatible** (STP Mode) – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

RSTP Port Configuration

Field Attributes

- **Port** - The number of a port or all aggregations (i.e., static trunks). Note that the spanning tree attributes for dynamically configured LACP trunks cannot be modified.
- **Enabled** - Enables/disables RSTP on an interface. (Default: Disabled).
- **Edge** Port (Fast Forwarding) - You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables

during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Enabled)

- **Path Cost** - This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)

  (Range: 0 for auto-configuration, 1-65535 for the short path cost method, 1-200,000,000 for the long path cost method)

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode.

  Note that when Force Version is set to Compatible mode (STP) and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

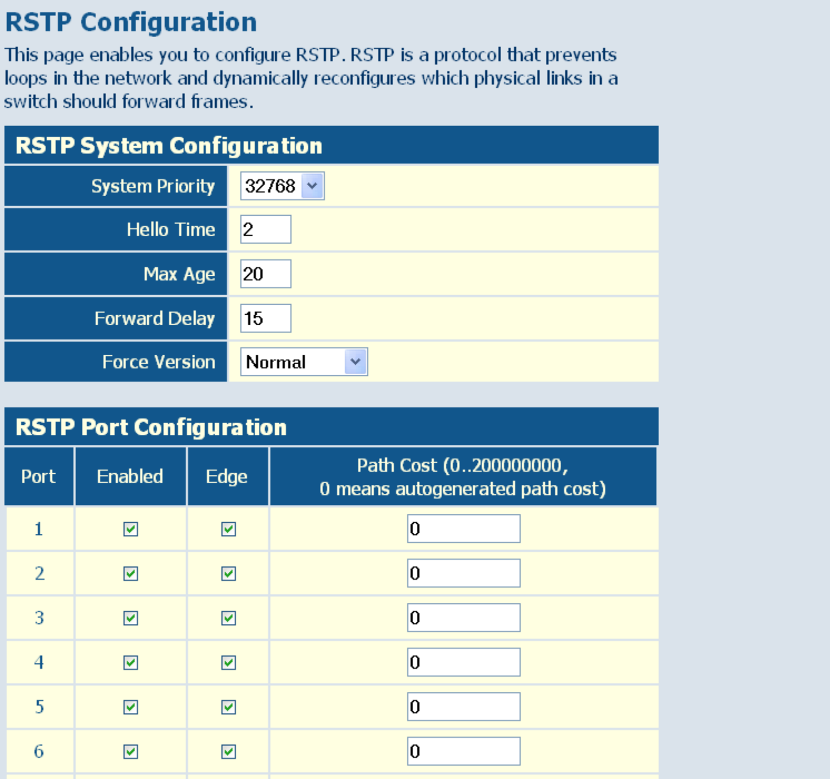
Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Default STA Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	2,000,000 1,000,000 500,000
Fast Ethernet	Half Duplex Full Duplex Trunk	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	10,000 5,000

Web – Click RSTP, Settings. Set any required system or port-specific attributes for RSTP, and click APPLY.



RSTP Configuration

This page enables you to configure RSTP. RSTP is a protocol that prevents loops in the network and dynamically reconfigures which physical links in a switch should forward frames.

RSTP System Configuration	
System Priority	32768
Hello Time	2
Max Age	20
Forward Delay	15
Force Version	Normal

RSTP Port Configuration

Port	Enabled	Edge	Path Cost (0..200000000, 0 means autogenerated path cost)
1	☑	☑	0
2	☑	☑	0
3	☑	☑	0
4	☑	☑	0
5	☑	☑	0
6	☑	☑	0

Figure 6-30 RSTP Configuration

Displaying RSTP Status

Use the RSTP Status page to display global and port-specific status and attribute settings for the Rapid Spanning Tree Protocol.

Field Attributes

RSTP Bridge Overview

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.
- **Fwd Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Topology** – Shows if STP topology is stable or undergoing changes.
- **Root ID** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device, and the port connected to the root device.

RSTP Port Status

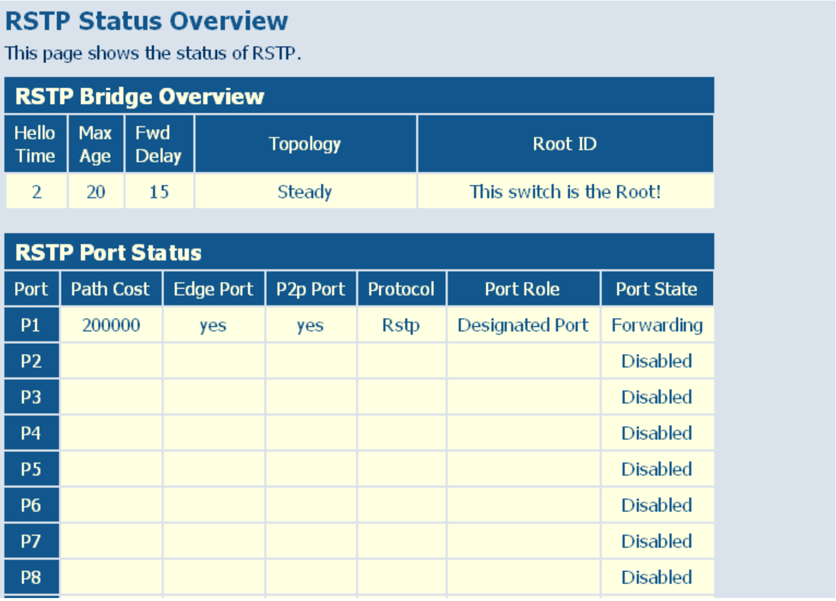
- **Port/Trunk** - The number of a port or the ID of a static trunk.
- **Path Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Edge Port** – Shows if this port is functioning as an edge port, either through manual selection (see the RSTP Port Configuration table) or auto-detection. Note that if the switch detects another bridge connected

to this port, the manual setting for Edge Port will be overridden, and the port will instead function as a point-to-point connection.

- **P2P Port** – Shows if this port is functioning as a Point-to-Point connection to exactly one other bridge.

  The switch can automatically determine if the interface is attached to a point-to-point link or to shared media. If shared media is detected, the switch will assume that it is connected to two or more bridges.
- **Protocol** – Shows the spanning tree protocol functioning on this port, either RSTP or STP (that is, STP-compatible mode).
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port); or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.
- **Port State** – Displays current state of this port within the Spanning Tree:
  - Discarding – Port receives STA configuration messages, but does not forward packets.
  - Learning – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - Forwarding – Port forwards packets, and continues learning addresses.
  - Disabled – Spanning tree is enabled on this port, but it has no role within the spanning tree.
  - Non-STP – Spanning tree is not enabled on this port.

Web – Click RSTP, Status.



RSTP Status Overview

This page shows the status of RSTP.

RSTP Bridge Overview				
Hello Time	Max Age	Fwd Delay	Topology	Root ID
2	20	15	Steady	This switch is the Root!

RSTP Port Status						
Port	Path Cost	Edge Port	P2p Port	Protocol	Port Role	Port State
P1	200000	yes	yes	Rstp	Designated Port	Forwarding
P2						Disabled
P3						Disabled
P4						Disabled
P5						Disabled
P6						Disabled
P7						Disabled
P8						Disabled

Figure 6-31 RSTP Status Overview

802.1X

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The encryption method used to pass authentication messages can be MD5 (Message-Digest 5), TLS (Transport Layer Security), or TTLS (Tunneled Transport Layer Security). TLS, TTLS, and PEAP will be supported in future releases. The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

The operation of dot1x on the switch requires the following:

- The switch must have an IP address assigned.
- The IP address of the RADIUS server must be specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to dot1x “Auto” mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and client also have to support the same EAP authentication type – MD5. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

Configuring 802.1X

Use the 802.1X Configuration page to specify global or port-specific parameters for the IEEE 802.1X Port Authentication Protocol.

Field Attributes

System Settings

- **Mode** - Enables or disables 802.1X globally for all ports on the switch. The 802.1X protocol must be enabled globally for the switch before the port settings are active. (Default: Disabled)
- **RADIUS IP** - Address of authentication server.
- **RADIUS UDP Port** - Network port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
- **RADIUS Secret Key**- Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
- **Reauthentication Enabled** - Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)
- **Reauthentication Period** - Sets the time period after which a connected client must be re-authenticated. (Range: 1-3600 seconds; Default: 3600 seconds)
- **EAP Timeout** - Sets the time period during an authentication session that the switch waits for a supplicant response before re-transmitting an EAP packet. (Range: 1-255; Default: 30 seconds)

Port Settings

- **Port** - The port number.
- **Admin State** - Sets the authentication mode to one of the following options:
  - **Auto** - Requires a 802.1X-aware client to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access.
  - **Force-Authorized** - Forces the port to grant access to all clients,

either 802.1X-aware or otherwise. (This is the default setting.)

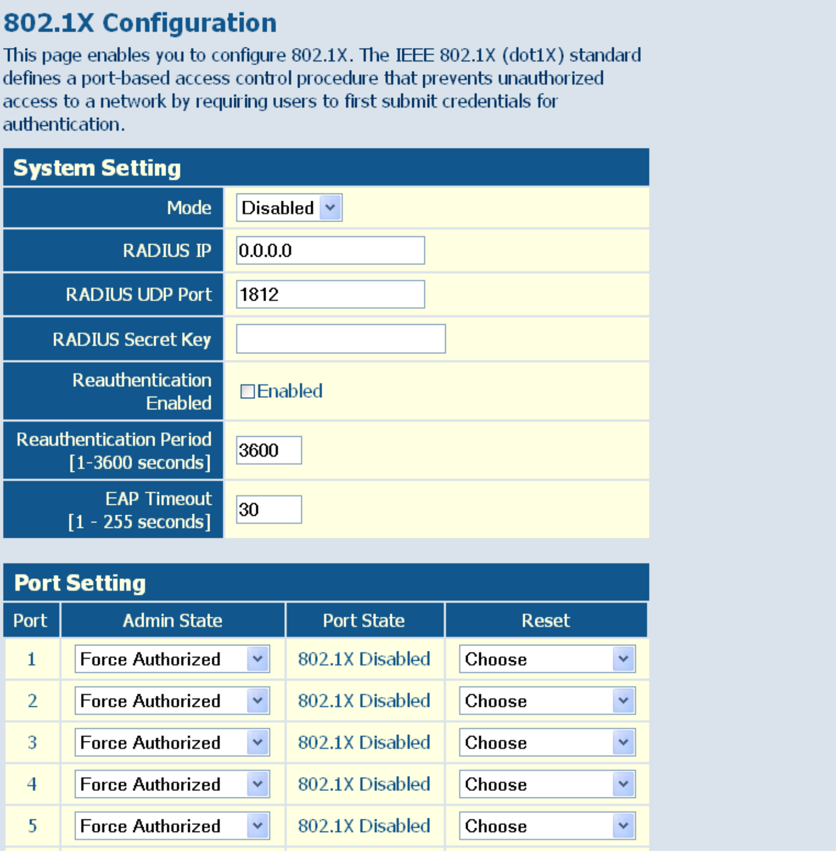
  - **Force-Unauthorized** - Forces the port to deny access to all clients, either 802.1X-aware or otherwise.

- **Port State** - Administrative state for port access control.
- **Reset** - The two available options include:
  - **Re-Authenticate** - Schedules a re-authentication to whenever the quiet-period of the port runs out.
  - **Force-Reinitialize** - Bypasses the quiet-period of the port and enables immediate re-authentication regardless of the status for the quiet-period.

The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

If a re-authentication fails, the IEEE802.1X standard enforces a so-called "quiet-period" in which the authenticator (switch) shall be quiet and not re-try another authentication – also packets from the supplicant are discarded during this quiet period – this way 'brute-force' attacks are prevented.

Web – Click 802.1X, Settings. Enable 802.1X globally for the switch, modify the global and port-specific parameters required, and click APPLY.



802.1X Configuration

This page enables you to configure 802.1X. The IEEE 802.1X (dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication.

System Setting

Mode	Disabled
RADIUS IP	0.0.0.0
RADIUS UDP Port	1812
RADIUS Secret Key	
Reauthentication Enabled	□Enabled
Reauthentication Period [1-3600 seconds]	3600
EAP Timeout [1 - 255 seconds]	30

Port Setting

Port	Admin State	Port State	Reset
1	Force Authorized	802.1X Disabled	Choose
2	Force Authorized	802.1X Disabled	Choose
3	Force Authorized	802.1X Disabled	Choose
4	Force Authorized	802.1X Disabled	Choose
5	Force Authorized	802.1X Disabled	Choose

Figure 6-32 802.1X Configuration

802.1X Statistics

Use the 802.1X Statistics page to display statistics for dot1x protocol exchanges for any port.

Field Attributes

- **Port Statistics** - Statistics can be viewed on a per-port basis. Select the port that you want to view here.

Authenticator Counters

- EntersConnecting – The number of times that the state machine transitions to the CONNECTING state from any other state.
- EntersWhileAuthenticating – he number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
- AuthTimeoutsWhileAuthenticating – The number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
- AuthEapStartsWhileAuthenticating – the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
- AuthReauthsWhileAuthenticated – The number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request.
- AuthEapLogoffWhileAuthenticated – The number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
- EapLogoffsWhileConnecting – The number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
- AuthSuccessesWhileAuthenticating – the number of times that the state machine transitions from AUTHENTICATING to

AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.

- AuthFailWhileAuthenticating – The number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
- AuthEapLogoffWhileAuthenticating – The number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
- AuthEapStartsWhileAuthenticated – The number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.

Backend Authenticator Counters

- backendResponses – The number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server.
- backendOtherRequestsToSupplicant – The number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure or Success message) to the Supplicant (i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method.
- backendAuthFails – The number of times that the state machine receives an EAP-Failure message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.
- backendAccessChallenges – The number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.

- backendAuthSuccesses – The number of times that the state machine receives an EAP-Success message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.

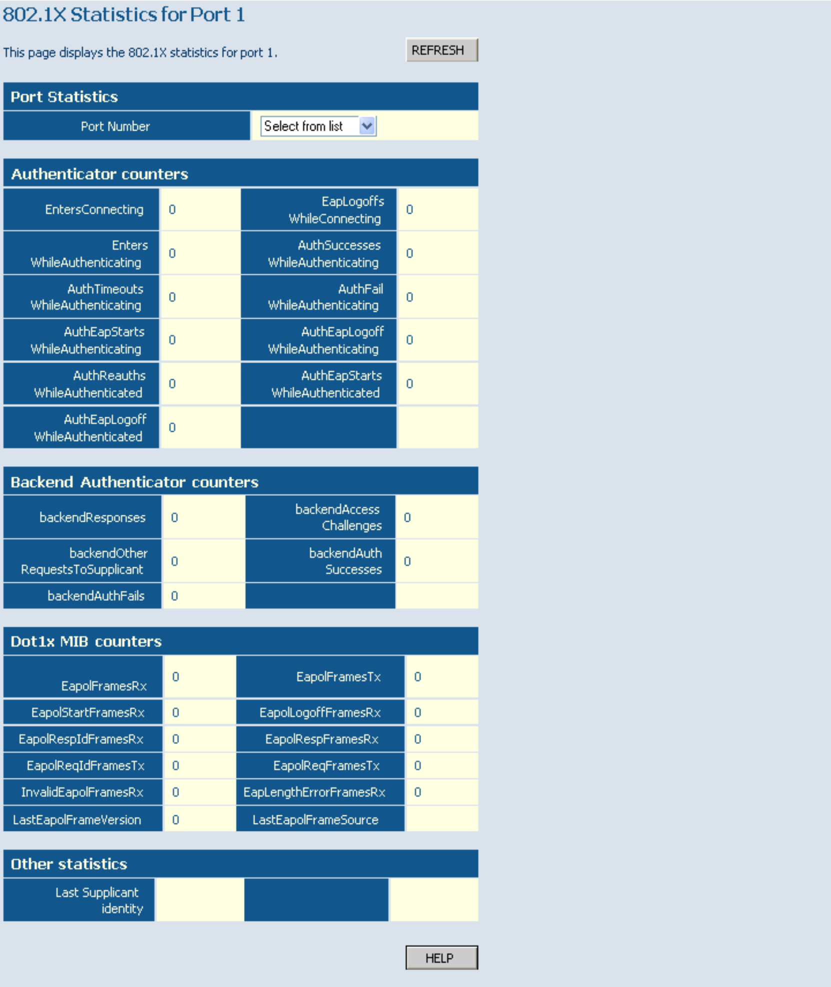
Dot1x MIB Counters

- EapolFramesRx – The number of valid EAPOL frames of any type that have been received by this Authenticator.
- EapolStartFramesRx – The number of EAPOL Start frames that have been received by this Authenticator.
- EapolRespIdFramesRx – The number of EAP Resp/Id frames that have been received by this Authenticator.
- EapolReqIdFramesTx – The number of EAP Req/Id frames that have been transmitted by this Authenticator.
- InvalidEapolFramesRx – The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
- LastEapolFrameVersion – The protocol version number carried in the most recently received EAPOL frame.
- EapolFramesTx – The number of EAPOL frames of any type that have been transmitted by this Authenticator.
- EapolLogoffFramesRx – The number of EAPOL Logoff frames that have been received by this Authenticator.
- EapolRespFramesRx – The number of EAP Resp/Id frames that have been received by this Authenticator.
- EapolReqFramesTx – The number of EAP Req/Id frames that have been transmitted by this Authenticator.
- EapLengthErrorFramesRx – The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
- LastEapolFrameSource – The source MAC address carried in the most recently received EAPOL frame.

Other Statistics

- Last Supplicant identity – MAC address of last authorized client.

Web – Click 802.1X, Statistics.



802.1X Statistics for Port 1

This page displays the 802.1X statistics for port 1.

Port Statistics

Port Number	Select from list

Authenticator counters

EntersConnecting	0	EapLogoffs WhileConnecting	0
Enters WhileAuthenticating	0	AuthSuccesses WhileAuthenticating	0
AuthTimeouts WhileAuthenticating	0	AuthFail WhileAuthenticating	0
AuthEapStarts WhileAuthenticating	0	AuthEapLogoff WhileAuthenticating	0
AuthReauths WhileAuthenticated	0	AuthEapStarts WhileAuthenticated	0
AuthEapLogoff WhileAuthenticated	0		

Backend Authenticator counters

backendResponses	0	backendAccess Challenges	0
backendOther RequestsToSupplicant	0	backendAuth Successes	0
backendAuthFails	0		

Dot1x MIB counters

EapolFramesRx	0	EapolFramesTx	0
EapolStartFramesRx	0	EapolLogoffFramesRx	0
EapolRespIdFramesRx	0	EapolRespFramesRx	0
EapolReqIdFramesTx	0	EapolReqFramesTx	0
InvalidEapolFramesRx	0	EapLengthErrorFramesRx	0
LastEapolFrameVersion	0	LastEapolFrameSource	

Other statistics

Last Supplicant identity			

Figure 6-33 802.1X Statistics

Security

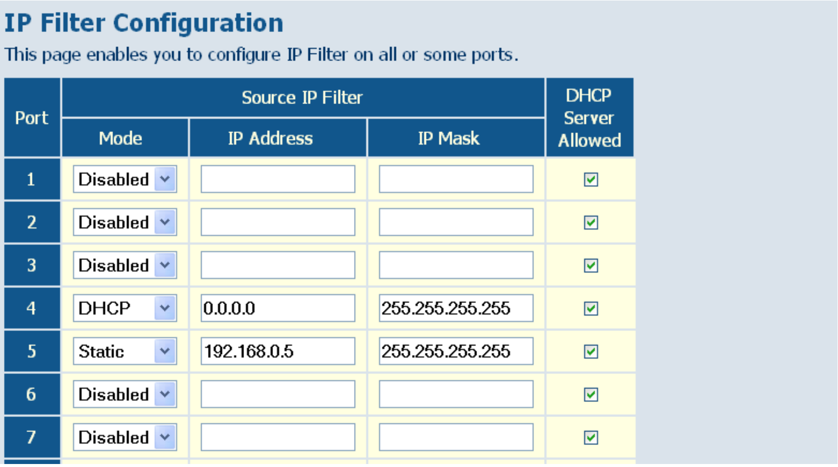
IP Filter

On this page, you can set up a source IP Filter on all or some ports. It is used to block unwanted access and provide access to the network for either a specific source IP address or a specific subnet.

Field Attributes

- **Port** - The number of the port.
- **Mode** - Select the IP filter mode for this port.
  - **Disabled** - Disable the source IP filter.
  - **Static** - Enable the IP filter with configured values in the IP Address and IP Mask fields.
  - **DHCP** - The IP address for the device connected to this port will be automatically assigned by DHCP server and only frames with the assigned IP address are allowed to access the network. The IP Address and IP Mask fields will be filled with the assigned IP address and 255.255.255.255 individually by software.
- **IP Address** - Set up IP addresses to allow access. Frames with IP address outside the allowed range will be dropped.
- **IP Mask** - Sets an IP mask to allow access for a specific subnet. To allow frames with a specific IP address, set the mask to 255.255.255.255.
- **DHCP Sever Allowed** - Enables or disables access to a DHCP server on a port. When DHCP Server Allowed is selected on a port, the port is allowed to be linked to a DHCP server. This can prevent the access of unwanted or unsolicited DHCP servers.

Web – Click Security, IP Filter. Set the security mode, any required static addresses, and specify whether or not a DHCP server may be attached. Then click APPLY.



IP Filter Configuration

This page enables you to configure IP Filter on all or some ports.

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled			☑
2	Disabled			☑
3	Disabled			☑
4	DHCP	0.0.0.0	255.255.255.255	☑
5	Static	192.168.0.5	255.255.255.255	☑
6	Disabled			☑
7	Disabled			☑

Figure 6-34 IP Filter Configuration

Port Security

Port security is a feature that allows you to configure a port with one or more MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action as specified by the Intrusion Action attribute.

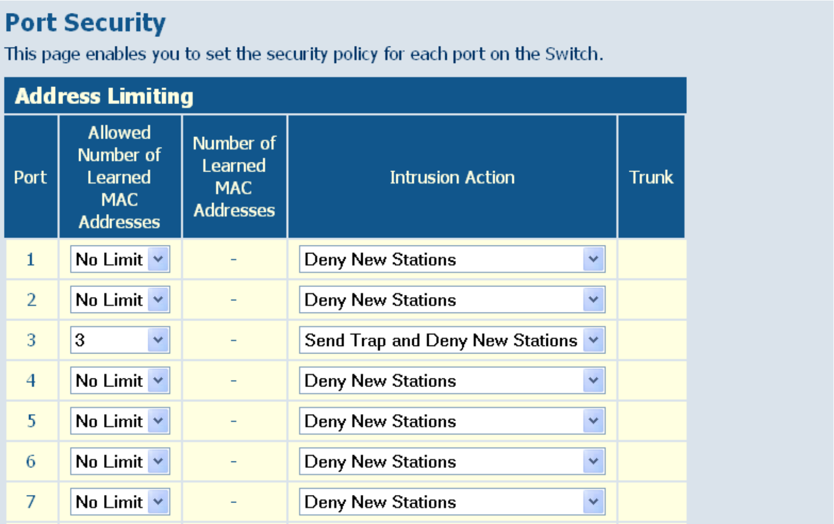
Note: Port security only addresses dynamically learned MAC addresses and has no limitations on static MAC addresses. On this switch, 24 static MAC address can be configured by System > Static MAC configuration page

Field Attributes

- **Port** - The number of the port.
- **Allowed Number of Learned MAC Addresses** - Set the maximum of MAC addresses that can be learned by this port. The options are shown below.
    - **No Limit** - No limit is set on the number of dynamically learned MAC address. This means port security is disabled.
    - **0** - No dynamically learned MAC address is allowed on this port. This does not affect any static MAC addresses that are configured for the port.
    - **1~8** - The maximum number of dynamically learned MAC address.

  The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.
- **Number of Learned MAC Addresses** - Displays the number of currently learned MAC addresses. The string '-' is displayed if a port is set to "No Limit" in the Allowed Number of Learned MAC Addresses field.
- **Intrusion Action** - Action to be carried out if unauthorized MAC addresses are detected.
    - **Deny New Stations** - A station with an unauthorized MAC address will be denied to access the port.
    - **Send Trap and Deny New Stations** - Besides denying the new station, a trap message is sent by the switch to report an intrusion action. The SNMP host to which this trap message is sent must be defined in the SNMP Trap Destination field on the SNMP Configuration page (see page page 75)
- **Trunk** - Display the trunk ID if the port is member of a trunk group.

Web – Click Security, Port Security. Set the number of allowed MAC addresses and the response to a detected intrusion, then click APPLY.



Port Security

This page enables you to set the security policy for each port on the Switch.

Address Limiting

Port	Allowed Number of Learned MAC Addresses	Number of Learned MAC Addresses	Intrusion Action	Trunk
1	No Limit	-	Deny New Stations	
2	No Limit	-	Deny New Stations	
3	3	-	Send Trap and Deny New Stations	
4	No Limit	-	Deny New Stations	
5	No Limit	-	Deny New Stations	
6	No Limit	-	Deny New Stations	
7	No Limit	-	Deny New Stations	

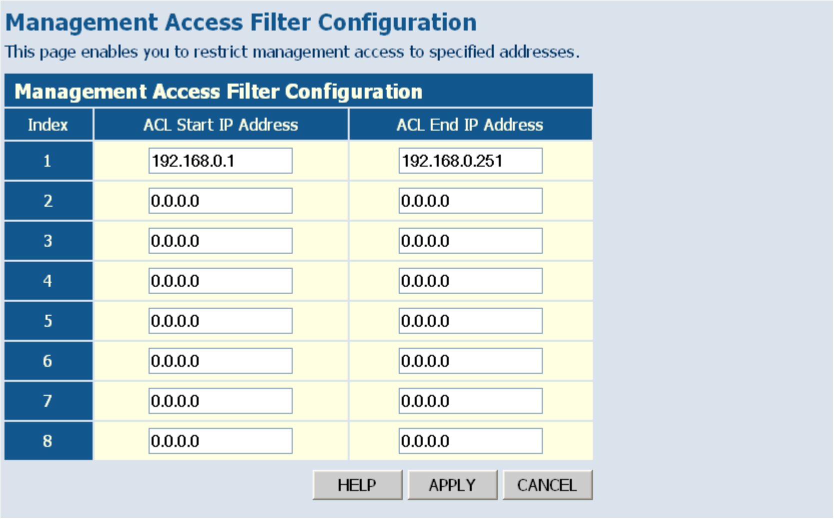
Figure 6-35 Port Security

Management Access Filter

This page enables you to set up a management access filter on the switch. With the Management Access Filter Configuration table, you can create a list of up to 8 IP addresses or IP address groups that are allowed management access to the switch through the web interface or SNMP. The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses. If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection.

Note: Invalid frames will not be able to access management interface, but normal forwarding is not impacted.

Web – Click Security, Management Access Filter. Enter a specific IP address or an address range, and click APPLY.



Management Access Filter Configuration

This page enables you to restrict management access to specified addresses.

Management Access Filter Configuration

Index	ACL Start IP Address	ACL End IP Address
1	192.168.0.1	192.168.0.251
2	0.0.0.0	0.0.0.0
3	0.0.0.0	0.0.0.0
4	0.0.0.0	0.0.0.0
5	0.0.0.0	0.0.0.0
6	0.0.0.0	0.0.0.0
7	0.0.0.0	0.0.0.0
8	0.0.0.0	0.0.0.0

Figure 6-36 Management Access Filter Configuration

IGMP Snooping

The switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping monitors IGMP service requests passing between multicast clients and servers, and dynamically configures the ports which need to receive the multicast traffic.

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

This switch can passively snoop on IGMP query and report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

Note: For IGMPV3, the switch incudes basic support for reports only, Source Multicast is not supported.

Configuring IGMP Snooping and Query Parameters

Use the IGMP Snooping Configuration page to enable or disable IGMP snooping, to designate the ports attached to multicast routers, and to enable or disable flooding of unknown multicast traffic.

Field Attributes

IGMP Snooping Configuration

- **IGMP Enabled** - When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. (Default: Disabled)
- **Router Ports** - Set if ports are connecting to the IGMP administrative routers.

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to a port on this switch, you can manually configure the port (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

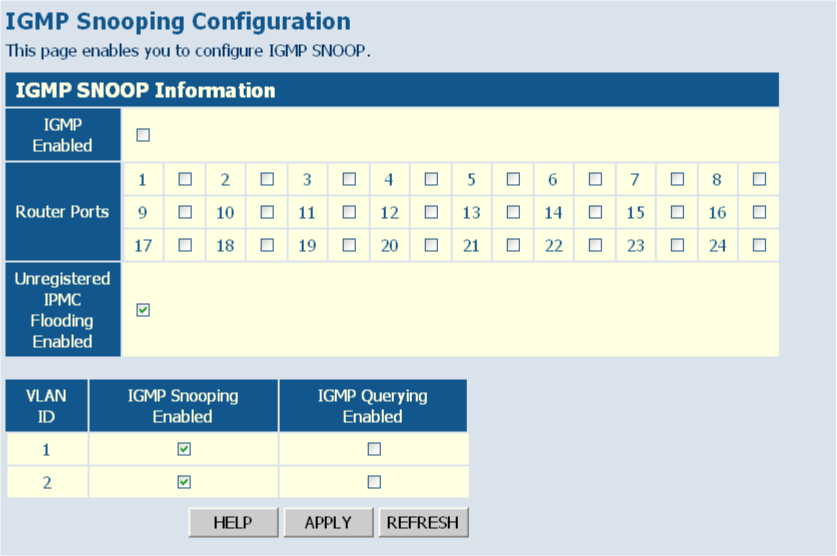
- **Unregistered IPMC Flooding Enabled** - Set the forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will be flooded to the attached VLAN when enabled, or forwarded only to multicast router ports when disabled. (Default: Enabled)

IGMP Snooping VLAN Configuration

- **VLAN ID** - The VLAN ID.
- **IGMP Snooping Enabled** - When enabled both globally (as described in the preceding section) and on a selected VLAN, the switch will monitor network traffic on that interface to determine which hosts want to receive multicast traffic. (Default: Enabled)
- **IGMP Querying Enabled** - When enabled, the port can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)

  A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/ switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Web – Click IGMP Snoop, Settings. Modify the required global or VLAN-specific attributes, and click APPLY.



IGMP Snooping Configuration

This page enables you to configure IGMP SNOOP.

IGMP SNOOP Information																
IGMP Enabled	□															
Router Ports	1	□	2	□	3	□	4	□	5	□	6	□	7	□	8	□
	9	□	10	□	11	□	12	□	13	□	14	□	15	□	16	□
	17	□	18	□	19	□	20	□	21	□	22	□	23	□	24	□
Unregistered IPMC Flooding Enabled	☑															

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	☑	□
2	☑	□

Figure 6-37 IGMP Snooping Configuration

Displaying IGMP Statistics

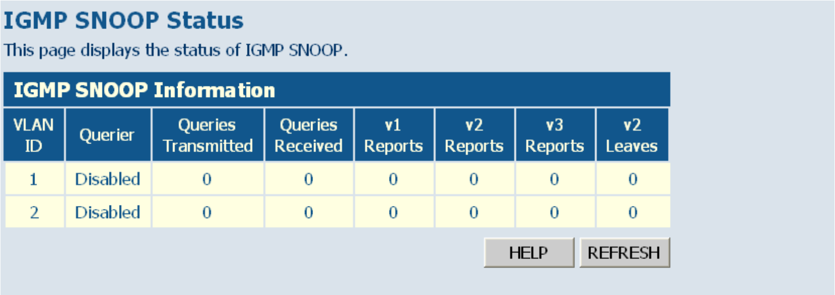
Use the IGMP Snooping Statistics page to show IGMP Snooping statistics for each VLAN.

Field Attributes

- **VLAN ID** - VLAN ID number.
- **Querier** - Shows whether Querying is enabled.
- **Queries Transmitted** - The number of transmitted Query packets. A general query is sent by a multicast router (or querier) to learn the complete multicast reception state of its neighboring interfaces.
- **Queries Received** - The number of received Query packets.
- **v1 Reports** - The number of received v1 Report packets.

- **v2 Reports** - The number of received v2 Report packets.
- **v3 Reports** - The number of received v3 Report packets.
- **v3 Leave** - The number of v3 leave packets received.

Web – Click IGMP Snoop, Status.



IGMP SNOOP Status

This page displays the status of IGMP SNOOP.

IGMP SNOOP Information

VLAN ID	Querier	Queries Transmitted	Queries Received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Disabled	0	0	0	0	0	0
2	Disabled	0	0	0	0	0	0

Figure 6-38 IGMP Snooping Status

SNMP

Use the SNMP Settings page to configure the Simple Network Management Protocol (SNMP), including enabling the local SNMP agent on this switch, specifying a trap manager, and setting the access strings.

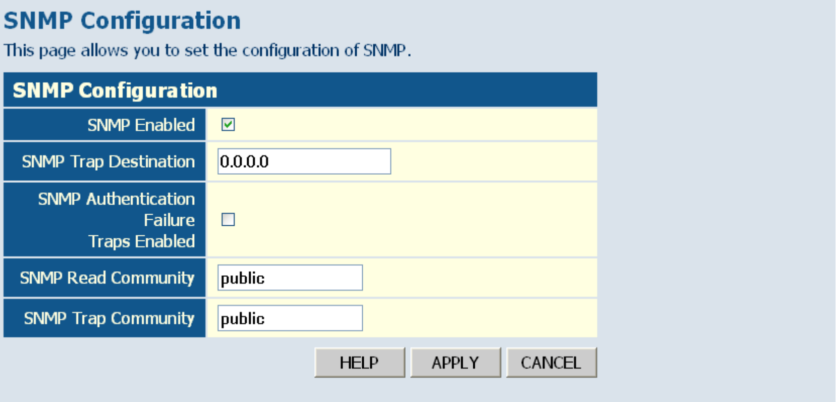
Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems. The switch includes an onboard SNMP agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports. A network management station can access this information using network management software. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Field Attributes

- **SNMP Enabled** - Enables or disables SNMP on the switch. Supports SNMP version 1 and 2c management clients.
- **SNMP Trap Destination** - IP address of the trap manager to receive notification messages from this switch. Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station.
- **SNMP Authentication Failure Traps Enabled** – Issues a notification message to specified IP trap managers whenever authentication of an SNMP request fails. This can occur if an incorrect community string is supplied for SNMP authentication. (Default: Disabled)
- **SNMP Read Community** - A community string that acts like a password and permits read access to the SNMP database on this switch. Authorized management stations are only able to retrieve MIB objects.

- **SNMP Trap Community** - Community string sent with the notification operation.

Web – Click SNMP, Settings. Set the local SNMP agent status, specify a trap manager, set the community access stings, and click APPLY.



SNMP Configuration

This page allows you to set the configuration of SNMP.

SNMP Configuration

SNMP Enabled	☑
SNMP Trap Destination	0.0.0.0
SNMP Authentication Failure Traps Enabled	□
SNMP Read Community	public
SNMP Trap Community	public

Figure 6-39 SNMP Configuration

Appendix A
Troubleshooting

Diagnosing Switch Indicators

Table A-1 Troubleshooting Chart

Symptom	**Action**
Power LED is Off	• Check connections between the switch, the power cord, and the wall outlet. • Contact your dealer for assistance. • Contact LevelOne Technical Support.
Link LED is Off	• Verify that the switch and attached device are powered on. • Be sure the cable is plugged into both the switch and corresponding device. • If the switch is installed in a rack, check the connections to the punch-down block and patch panel. • Verify that the proper cable type is used and its length does not exceed specified limits. • Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.

Power and Cooling Problems

If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or internal power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses or surges at the power outlet, and verify that the fans on the unit are unobstructed and running prior to shutdown. If you still cannot isolate the problem, then the internal power supply may be defective.

Installation

Verify that all system components have been properly installed. If one or more components appear to be malfunctioning (such as the power cord or network cabling), test them in an alternate environment where you are sure that all the other components are functioning properly.

In-Band Access

You can access the management agent in the switch from anywhere within the attached network using a Web browser, or other network management software tools. However, you must first configure the switch with a valid IP address, subnet mask, and default gateway. If you have trouble establishing a link to the management agent, check to see if you have a valid network connection. Then verify that you entered the correct IP address. Also, be sure the port through which you are connecting to the switch has not been disabled. If it has not been disabled, then check the network cabling that runs between your remote location and the switch.

Reset the Switch

As situation requires, you might want to reset the switch and to restore to the default settings. To reset the switch:

1. Unplug the power cord from the power socket.
2. Unplug all cables from the ports.
3. Use an Ethernet cable to connect port 1 to port 2.
4. Plug the power cord back to the power socket
5. Wait at least 40 seconds before unplugging cables from port 1 and port 2.

Note: After resetting the switch, every setting, including password and IP address, will restore to the default value.

APPENDIX B
CABLES

Twisted-Pair Cable and Pin Assignments

For 10BASE-T/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. For 1000BASE-T connections the twisted-pair cable must have four pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Caution: Each wire pair must be attached to the RJ-45 connectors in a specific orientation.

Caution: DO NOT plug a phone jack connector into any RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

Figure B-1 illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

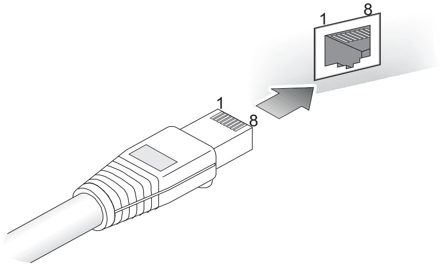


Figure B-1 RJ-45 Connector Pin Numbers

10BASE-T/100BASE-TX Pin Assignments

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections, or 100-ohm Category 5 or better cable for 100 Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 ports on the switch base unit support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3, and 6 at the other end of the cable. When using any RJ-45 port on the switch, you can use either straight-through or crossover cable.

Table B-1 10/100BASE-TX MDI and MDI-X Port Pinouts

Pin	MDI Signal Name	MDI-X Signal Name
1	Transmit Data plus (TD+)	Receive Data plus (RD+)
2	Transmit Data minus (TD-)	Receive Data minus (RD-)
3	Receive Data plus (RD+)	Transmit Data plus (TD+)
6	Receive Data minus (RD-)	Transmit Data minus (TD-)
4,5,7,8	Not used	Not used

Note: The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Straight-Through Wiring

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through. (When auto-negotiation is enabled for any RJ-45 port on the switch, you can use either straight-through or crossover cable to connect to any device type.)

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet connections.

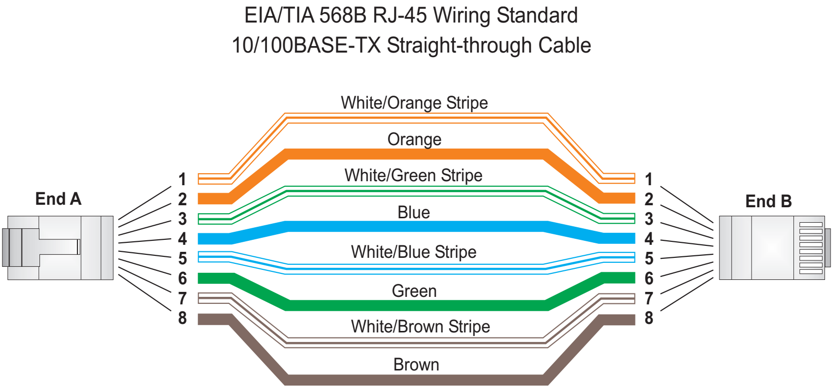


Figure B-2 Straight-through Wiring

Crossover Wiring

If the twisted-pair cable is to join two ports and either both ports are labeled with an "X" (indicating MDI-X) or neither port is labeled with an "X" (which indicates MDI), a crossover must be implemented in the wiring. (When auto-negotiation is enabled for any RJ-45 port on the switch, you can use either straight-through or crossover cable to connect to any device type.)

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet connections.

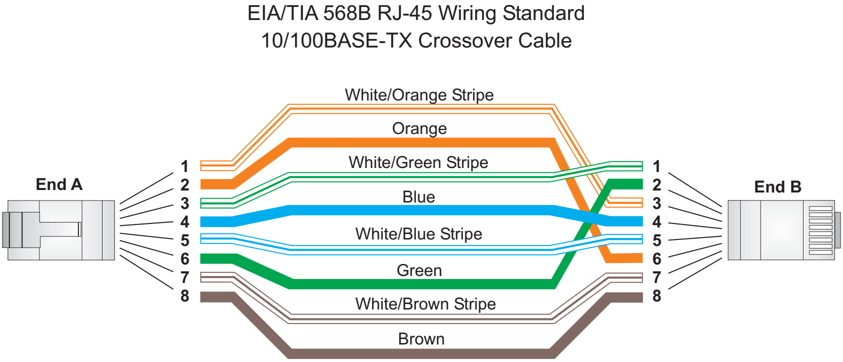


Figure B-3 Crossover Wiring

1000BASE-T Pin Assignments

All 1000BASE-T ports support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs.

The table below shows the 1000BASE-T MDI and MDI-X port pinouts. These ports require that all four pairs of wires be connected. Note that for 1000BASE-T operation, all four pairs of wires are used for both transmit and receive.

Use 100-ohm Category 5, 5e or 6 unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for 1000BASE-T connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

Table B-2 1000BASE-T MDI and MDI-X Port Pinouts

Pin	MDI Signal Name	MDI-X Signal Name
1	Bi-directional Data One Plus (BI_D1+)	Bi-directional Data Two Plus (BI_D2+)
2	Bi-directional Data One Minus (BI_D1-)	Bi-directional Data Two Minus (BI_D2-)
3	Bi-directional Data Two Plus (BI_D2+)	Bi-directional Data One Plus (BI_D1+)
4	Bi-directional Data Three Plus (BI_D3+)	Bi-directional Data Four Plus (BI_D4+)
5	Bi-directional Data Three Minus (BI_D3-)	Bi-directional Data Four Minus (BI_D4-)
6	Bi-directional Data Two Minus (BI_D2-)	Bi-directional Data One Minus (BI_D1-)
7	Bi-directional Data Four Plus (BI_D4+)	Bi-directional Data Three Plus (BI_D3+)
8	Bi-directional Data Four Minus (BI_D4-)	Bi-directional Data Three Minus (BI_D3-)

Cable Testing for Existing Category 5 Cable

Installed Category 5 cabling must pass tests for Attenuation, Near-End Crosstalk (NEXT), and Far-End Crosstalk (FEXT). This cable testing information is specified in the ANSI/TIA/EIA-TSB-67 standard. Additionally, cables must also pass test parameters for Return Loss and Equal-Level Far-End Crosstalk (ELFEXT). These tests are specified in the ANSI/TIA/EIA-TSB-95 Bulletin, "The Additional Transmission Performance Guidelines for 100 Ohm 4-Pair Category 5 Cabling."

Note that when testing your cable installation, be sure to include all patch cables between switches and end devices.

Adjusting Existing Category 5 Cabling to Run 1000BASE-T

If your existing Category 5 installation does not meet one of the test parameters for 1000BASE-T, there are basically three measures that can be applied to try and correct the problem:

1. Replace any Category 5 patch cables with high-performance Category 5e or Category 6 cables.
2. Reduce the number of connectors used in the link.
3. Reconnect some of the connectors in the link.

Fiber Standards

The current TIA (Telecommunications Industry Association) 568-A specification on optical fiber cabling consists of one recognized cable type for horizontal subsystems and two cable types for backbone subsystems.

Horizontal 62.5/125 micron multimode (two fibers per outlet).
Backbone 62.5/125 micron multimode or single mode.

TIA 568-B will allow the use of 50/125 micron multimode optical fiber in both the horizontal and backbone in addition to the types listed above. All optical fiber components and installation practices must meet applicable building and safety codes.

Appendix C Specifications

Physical Characteristics

Ports

GSW-1676:

12 10/100/1000BASE-T, with auto-negotiation

4 10/100/1000BASE-T shared with 4 SFP transceiver slots.

GSW-2476:

20 10/100/1000BASE-T, with auto-negotiation

4 10/100/1000BASE-T shared with 4 SFP transceiver slots.

Network Interface

Ports 1-16/24: RJ-45 connector, auto MDI/X

10BASE-T: RJ-45 (100-ohm, UTP cable; Category 3 or better)

100BASE-TX: RJ-45 (100-ohm, UTP cable; Category 5 or better)

1000BASE-T: RJ-45 (100-ohm, UTP or STP cable; Category 5, 5e, or 6)

*Maximum Cable Length - 100 m (328 ft)

Buffer Architecture

400 Kbytes

Aggregate Bandwidth

48 Gbps

Switching Database

8K MAC address entries, 1K static MAC addresses;

LEDs

System: Power

Port: Link/Act, 1000

Weight
3.72 kg (8.44 lbs)

Size
44.0 x 17.1 x 4.3 cm (17.0 x 6.7 x 1.7 in.)

Temperature
Operating: 0 to 40 °C (32 to 104 °F)
Storage: -40 to 70 °C (-40 to 158 °F)

Humidity
Operating: 10% to 90% (non-condensing)

AC Input
100 to 240 V, 50-60 Hz, 0.8 A

Power Supply
Internal, auto-ranging transformer: 100 to 240 VAC, 50 to 60 Hz

Power Consumption
28 Watts

Maximum Current
0.25 A @ 115 VAC
0.12 A @ 230 VAC

Switch Features

Forwarding Mode
Store-and-forward

Throughput
Wire speed

Management Features

In-Band Management

Web manager

Software Loading

HTTP in-band

Standards

IEEE 802.3-2005
  Ethernet, Fast Ethernet, Gigabit Ethernet
IEEE 802.1Q Virtual LAN
IEEE 802.1X, Port-Based Network Access Control, 2001
ISO/IEC 8802-3

Compliances

CE Mark

Emissions

FCC Class A

GLOSSARY

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

1000BASE-LX

IEEE 802.3z specification for Gigabit Ethernet over two strands of 50/125, 62.5/125 or 9/125 micron core fiber cable.

1000BASE-SX

IEEE 802.3z specification for Gigabit Ethernet over two strands of 50/125 or 62.5/125 micron core fiber cable.

1000BASE-T

IEEE 802.3ab specification for Gigabit Ethernet over 100-ohm Category 5 or 5e twisted-pair cable (using all four wire pairs).

1000BASE-ZX

Specification for long-haul Gigabit Ethernet over two strands of 9/125 micron core fiber cable.

Auto-Negotiation

Signalling method allowing each node to select its optimum operational mode (e.g., speed and duplex mode) based on the capabilities of the node to which it is connected.

Bandwidth

The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.

Collision

A condition in which packets transmitted over the cable interfere with each other. Their interference makes both signals unintelligible.

Collision Domain

Single CSMA/CD LAN segment.

CSMA/CD

CSMA/CD (Carrier Sense Multiple Access/Collision Detect) is the communication method employed by Ethernet, Fast Ethernet, or Gigabit Ethernet.

End Station

A workstation, server, or other device that does not forward traffic.

Ethernet

A network communication system developed and standardized by DEC, Intel, and Xerox, using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, thin coax and twisted-pair cable.

Fast Ethernet

A 100 Mbps network communication system based on Ethernet and the CSMA/CD access method.

Full Duplex

Transmission method that allows two network devices to transmit and receive concurrently, effectively doubling the bandwidth of that link.

Gigabit Ethernet

A 1000 Mbps network communication system based on Ethernet and the CSMA/CD access method.

IEEE

Institute of Electrical and Electronic Engineers.

IEEE 802.3

Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE 802.3ab

Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Gigabit Ethernet. (Now incorporated in IEEE 802.3-2002.)

IEEE 802.3u

Defines CSMA/CD access method and physical layer specifications for 100BASE-TX Fast Ethernet. (Now incorporated in IEEE 802.3-2002.)

IEEE 802.3x

Defines Ethernet frame start and stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002.)

IEEE 802.3z

Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet. (Now incorporated in IEEE 802.3-2005.)

LAN Segment

Separate LAN or collision domain.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

LED

Light emitting diode used for monitoring a device or network condition.

Link Segment

Length of twisted-pair or fiber cable joining a pair of repeaters or a repeater and a PC.

Local Area Network (LAN)

A group of interconnected computers and support devices.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about the device.

Media Access Control (MAC)

A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

Modal Bandwidth

Bandwidth for multimode fiber is referred to as modal bandwidth because it varies with the modal field (or core diameter) of the fiber. Modal bandwidth is specified in units of MHz per km, which indicates the amount of bandwidth supported by the fiber for a one km distance.

Network Diameter

Wire distance between two end stations in the same collision domain.

Redundant Power Supply (RPS)

A backup power supply unit that automatically takes over in case the primary power supply should fail.

RJ-45 Connector

A connector for twisted-pair wiring.

Switched Ports

Ports that are on separate collision domains or LAN segments.

TIA

Telecommunications Industry Association

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

UTP

Unshielded twisted-pair cable.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, allowing users to share information and resources as though located on the same LAN.

INDEX