Intel® Express 460T Standalone Switch

User Guide

Intel Corporation, 5200 NE Elam Young Parkway, Hillsboro OR 97124-6497

Fifth Edition **June 2001** **746438-003**

Contents

1 Setting Up the Intel® Express 460T Standalone Switch

Overview

This guide provides information on configuring and managing the Intel® Express 460T Standalone Switch and is organized into these chapters:

- Chapter 1 - Information on the switch hardware and optional modules
- Chapter 2 - Information on using the switch in a LAN and advanced features like link aggregation and virtual LANs (VLANs)
- Chapter 3 - How to use Intel Device View
- Chapter 4 - How to use Web Device Manager
- Chapter 5 - How to use Local Management

Management

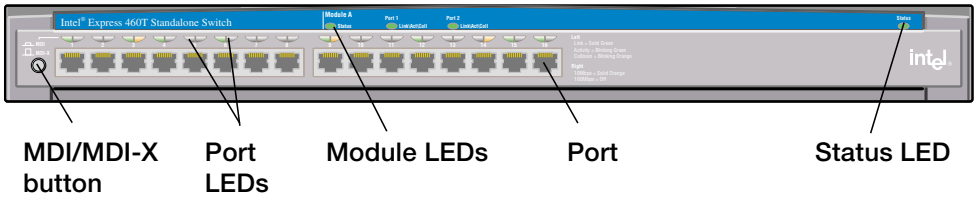
Through the switch's built-in management you can configure the device and monitor network health. There are several methods for managing this switch; you can use one method or any combination.

- **SNMP management applications** like Intel Device View, LANDesk® Network Manager, or Hewlett Packard OpenView* are tailored for Intel products and show a graphical representation of the device (with the use of the proper MIB).
- **Onboard management** allows control over the device without using an SNMP application. The Web Device Manager provides a graphical interface while Local Management is a menu-driven interface.
- **Other SNMP-compliant applications** can manage 460T switches if you compile the switch's MIB files into that application.

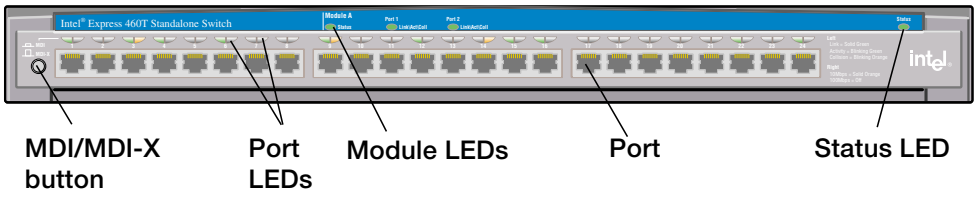
Switch Features

The following diagrams show the major features of the 16-port and 24-port versions of the 460T Standalone Switches.

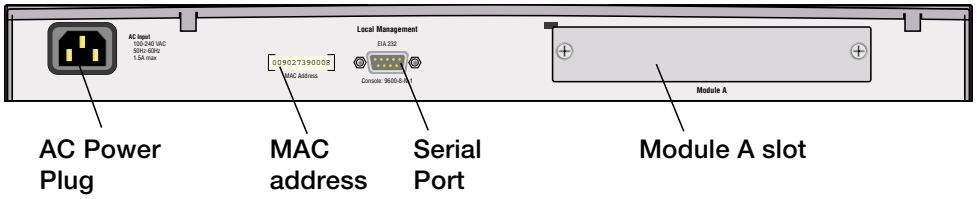
16-port 460T Switch (Product Code ES460T16)



24-port 460T Switch (Product Code ES460T24)



Back of 16-port and 24-port 460T Switch

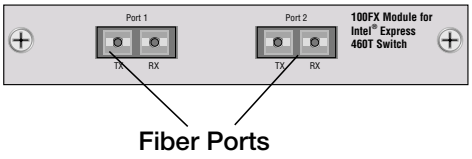


- Auto-negotiates speed, duplex, and flow control—10 Mbps or 100 Mbps *per port.*
- Half-duplex and full-duplex flow control.
- One expansion slot for the optional 100FX, 1000SX, 1000LX, or 1000T module.
- Configure port settings manually through management.
- Access menu-driven Local Management through the serial port or a Telnet session.
- Access the graphic, Web-based, Web Device Manager through a Web browser.

Module Features

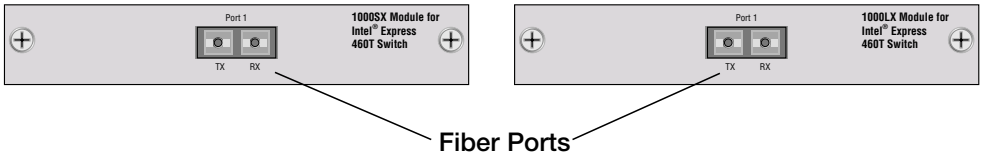
Both the 16-port and 24-port versions of the 460T Standalone Switches can accept a module to provide additional functionality.

100Base-FX Fiber Module (Product Code ES460MFX)



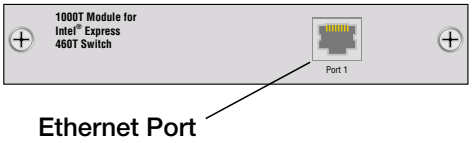
- Connects to 100Base-FX devices (such as a switch or server) at full- or half-duplex.
- Extends network diameter up to 400 m (half-duplex) or 2000 m (full-duplex).

1000Base-SX Gigabit Module (Product Code ES460MSX)
1000Base-LX Gigabit Module (Product Code ES460MLX)



- Connects to 1000Base-SX or 1000Base-LX devices at full-duplex.
- SX module extends network diameter 260 m to 550 m (depending on type of fiber).
- LX module extends network diameter 550 m to 5000 m (depending on type of fiber).

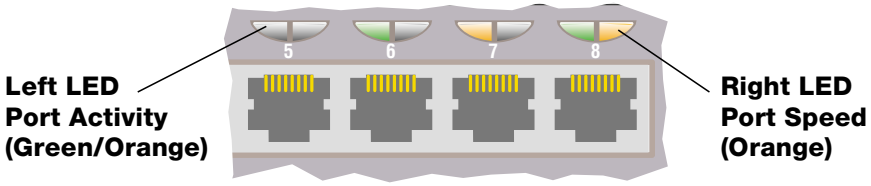
1000Base-T Gigabit Module (Product Code ES460MT)



- Connects at 100 Mbps at full-duplex or half-duplex, or 1000 Mbps at full-duplex.
- Extends network diameter up to 100 m.

Port LEDs

The LEDs above each port indicate port status, individual port speed, and port activity.



LED	Status	Meaning
Left	Solid green[1]	Device linked.
	Blinking green	Receiving activity on that port.
	Blinking orange	A collision was detected on this segment.
	Off	No link detected.
Right	Solid orange	Device connected at 10 Mbps.
	Off	Device connected at 100 Mbps.

Status LEDs

The switch status LED is located above the port LEDs. This LED indicates the condition of the switch.

LED	Status	Meaning
Status	Orange	Switch is performing diagnostics.
	Green	Diagnostics have passed, the switch is ready.
	Red[2]	Diagnostics have failed.

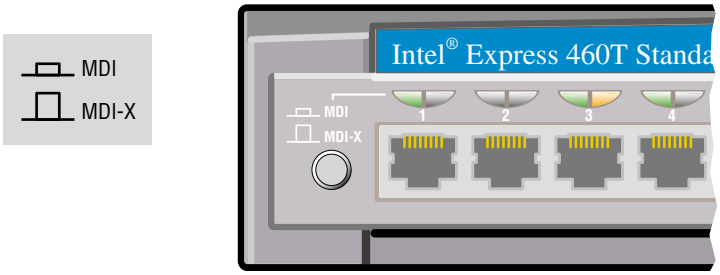
---

1 If the left LED is solid green, but there is no activity when you try to ping a device connected to that port, the port is probably disabled through management. Re-enable the port and try again.

2 When the switch is first powered on, the Status LED is red for a couple of seconds before the diagnostic mode starts, then it turns orange.

Crossover Button

The 460T switch has a button that toggles port 1 from MDI-X to MDI. With the button depressed (MDI) you can to connect to another switch or a hub without using a crossover cable. For more information, see pages 9-10.



Connection Guidelines

General

- The 460T switch can auto-negotiate port speed and can operate at 10 Mbps or 100 Mbps per port. The switch matches the highest possible speed of an attached device.
- The 460T switch can auto-negotiate port duplex and can operate at half-duplex or full-duplex.

Cabling

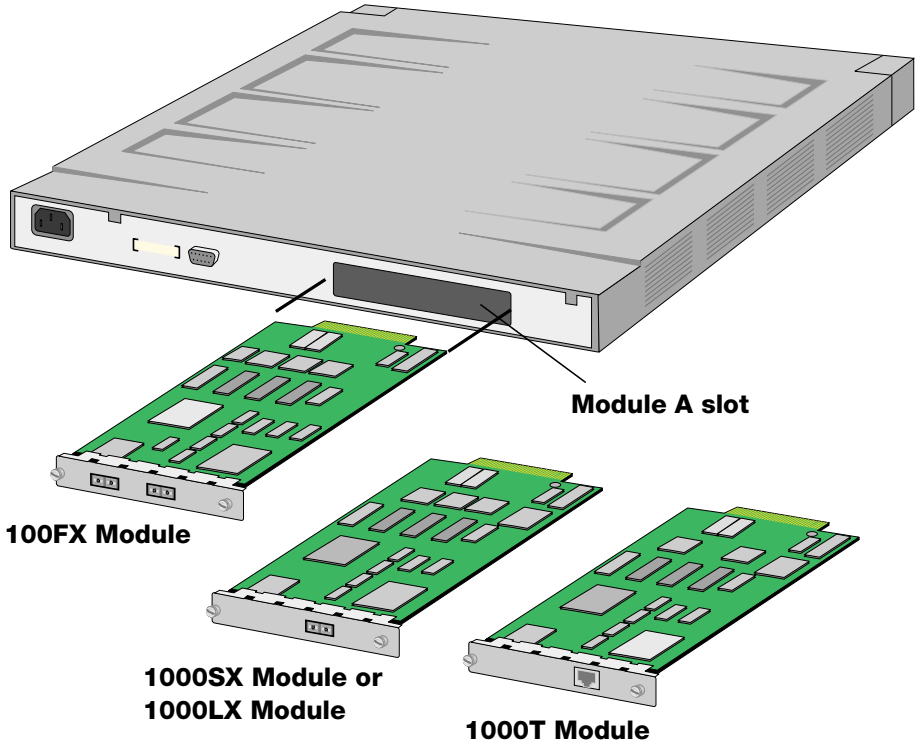
- Use Category 5 unshielded twisted-pair (CAT 5 UTP) cable when connecting 100 Mbps devices to the switch.
- Use Category 3, 4, or 5 unshielded twisted-pair (CAT 3, 4, or 5 UTP) cable when connecting 10 Mbps devices to the switch.
- Limit the cable length between devices to 100 meters (330 feet).
- Use a straight-through cable to connect the switch to a server or workstation. For more information on cabling, see pages 9 and 10.
- To connect to another switch or hub use a crossover cable on any port, or set port 1 to MDI and use a straight-through cable.

Installing a Module

You can install optional modules only in the Module A slot located at the back of the switch. Use the LEDs on the front of the switch to check the module's status.

To install the module in the switch

1. Unplug the power cord from the switch. Remove the panel from the expansion slot labeled Module A.
2. Align the module with the card guides inside the switch and slide the module into the slot. Press firmly to connect the module and secure it with the retaining screws.
3. Plug in the power cord.



Module A LEDs

The LEDs are located on the front of the switch above ports 9-16. These LEDs provide information about the 100FX, 1000SX, or 1000LX module such as the module's status, link, port activity, and collisions.

LED	Status	Meaning
Status	Solid green	Module is present and functioning.
	Off	No module present.
Link\Act\Coll	Solid green	Device linked.
	Blinking green	Receiving activity on that port.
	Blinking orange	A collision was detected on this segment.
	Off	No link detected.

When you are using the 1000SX, 1000LX, or 1000T module, only the port 1 LED will blink and show activity because the module has only one port.

Configuring Modules

Generally, you do not need to make any changes to the optional modules because they are designed to configure themselves automatically for the attached device. However, you might need to configure the modules in order to communicate with older devices. You can use the Local Management or Web Device Manager to configure the 100FX, 1000SX, 1000LX, or 1000T modules. See Chapter 4 for more information about the Web Device Manager, and Chapter 5 for more information about Local Management.

Media Requirements

Incorrect cabling is often the cause of network performance problems. The next two pages provide information about how to make sure your cabling is correct.

100Base-TX

The 100Base-TX Fast Ethernet specification requires that you use CAT 5 UTP cabling to operate at 100 Mbps. If you use lower-grade cabling (CAT 3 or CAT 4), you may get a connection, but also experience data loss or slow performance. The limit is 100 meters between any two devices.

10Base-T

The 10Base-T Ethernet specification lets you use CAT 3, CAT 4, or CAT 5 UTP cabling. The limit is 100 meters between any two devices.

NOTE:

100 meters = 330 feet

200 meters = 660 feet

500 meters = 1,650 feet

2 km = 2000 meters = 6,600 feet

5 km = 5000 meters = 16,500 feet

100Base-FX

The optional Fiber Module lets you connect to a switch at distances up to 400 meters (hubs up to 160 m) at half-duplex or 2 km at full-duplex. Use 62.5/125 µm multimode fiber optic cable with an SC-type fiber optic connector.

1000Base-T

The 1000Base-T Gigabit specification requires that you use CAT 5 UTP cabling to operate at 1000 Mbps. If you use a lower grade cabling you will experience either no connection or extreme data loss. The maximum distance between any two devices is 100 meters.

1000Base-SX/1000Base-LX

The optional 1000Base-SX and 1000Base-LX Gigabit Modules provide a high-speed connection to another device at distances up to 5 km. The maximum distance depends on the type of cable used. Refer to the following table for a list of cable types and maximum distances. Use cables with an SC-type fiber optic connector.

Selecting the right cable

Media Type	Cabling Used	Maximum distance
100Base-FX Module (full-duplex)	62.5/125 µm multimode	2,000 m
100Base-FX Module (half-duplex)	62.5/125 µm multimode	(160 m to hub, 400 m to router, switch, or PC)
1000Base-T\100Base-TX (Gigabit) Module	Category 5 (CAT 5) unshielded twisted pair cable	100 m
1000Base-SX (Gigabit) Module	50/125 µm multimode 62.5/125 µm multimode	550 m 260 m
1000Base-LX (Gigabit) Module	50/125 µm multimode 62.5/125 µm multimode 9/125 µm singlemode	550 m 550 m 5,000 m

Testing a Cable

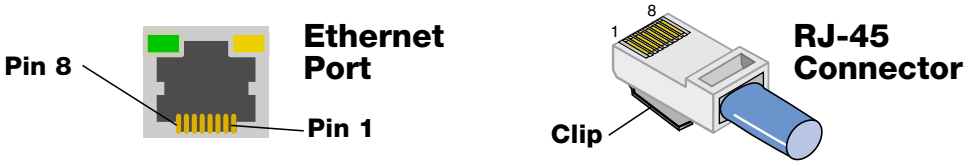
When using a 100Base-TX module, you can quickly check the cable's link integrity by plugging one end into port 1 and the other end into port 2. Make sure the crossover (MDI/MDI-X) button is out. Check the Activity LEDs for ports 1 and 2. If the LEDs are on, you have a functioning crossover cable.

If the LEDs are off, push the MDI/MDI-X button in. If the Activity LEDs for ports 1 and 2 turn on, you have a functioning straight-through cable. However, if the LEDs remain off, you probably have a bad cable.

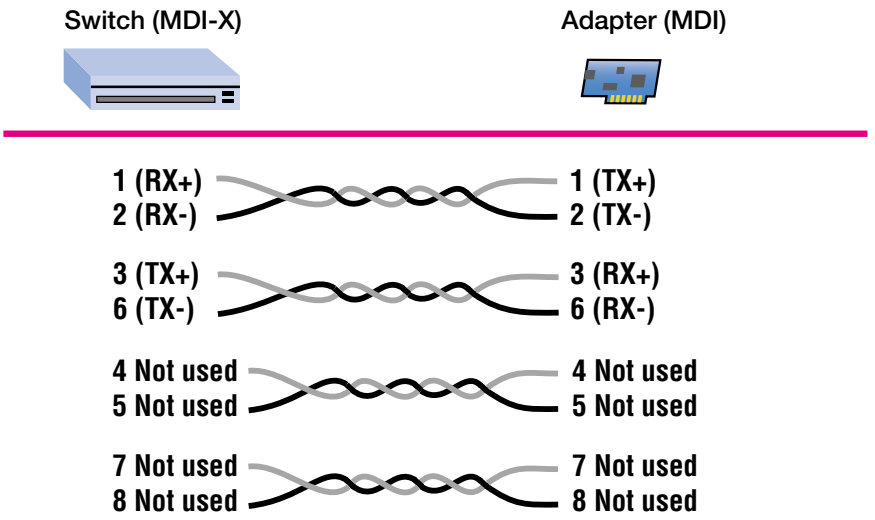
If a cable passes these tests, but the network connection is slow, verify that wires 1, 2 and 3, 6 on the cable are twisted pairs, as shown in the following diagrams.

Straight-through vs. Crossover Cables

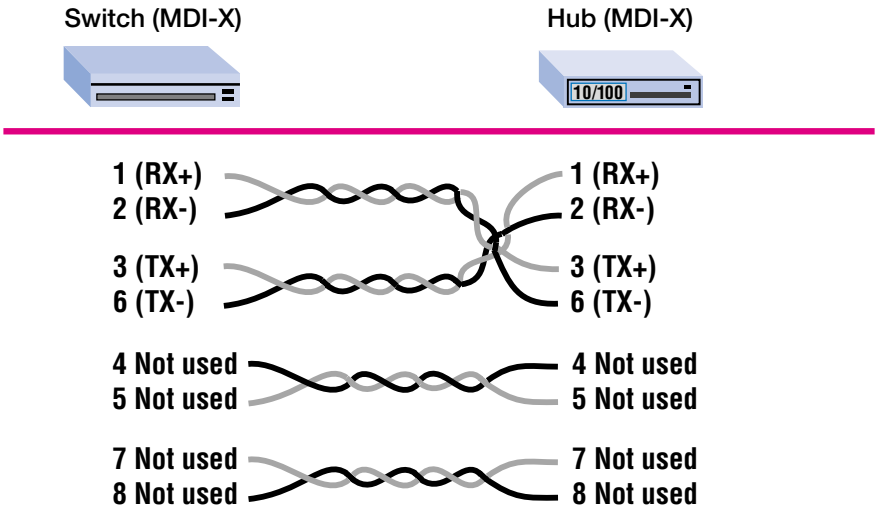
Switch ports are wired for MDI-X. Use a straight-through cable to connect to a workstation or server (network adapter cards are wired MDI). To connect to another MDI-X port, use a crossover cable. Following are the pin arrangements for the switch's Ethernet port and the typical RJ-45 connector.



Straight-through UTP cable (for 100Base-TX)



Crossover UTP cable (for 100Base-TX)



2 Using the Intel® Express 460T Standalone Switch

Overview

This section provides an overview for using the Express 460T standalone switch within a network. The chapter covers the basic differences between a switch and hub, basic switching features like flow control and Spanning Tree, and a discussion of more advanced features such as link aggregation and the types of VLANs available on the switch.

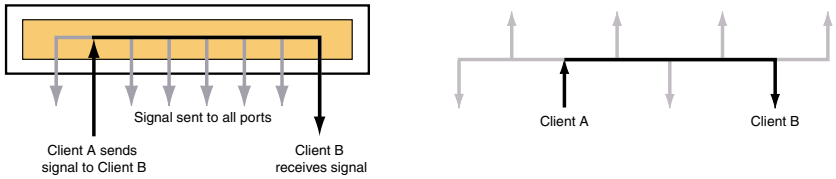
If you are already familiar with switching technology you can skip ahead to a particular section within the chapter. The following list shows where you can find a particular topic.

What is a Switch?

A switch segments traffic, providing each port its own collision domain. This is different from a hub where all ports belong to the same collision domain.

Segments and Hubs

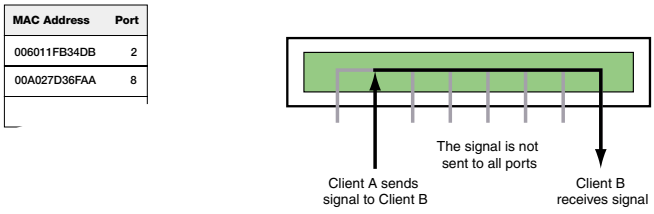
Hubs combine multiple wires so all attached devices behave like they are on the same wire. Because the devices share the same segment, data sent by one device is retransmitted to all devices on the same hub. This is equivalent to having all devices connected in a bus topology as illustrated below.



The disadvantage is all devices must share the total available bandwidth. The more devices that are attached to the hub the less bandwidth for each user. Also, network performance suffers because all devices receive traffic and collisions from other users as the hub retransmits data across all ports.

Switches

Switches send traffic only to specific ports, rather than transmitting data across all ports. This means that each device attached to the switch receives fewer collisions and the entire bandwidth is available to the device.



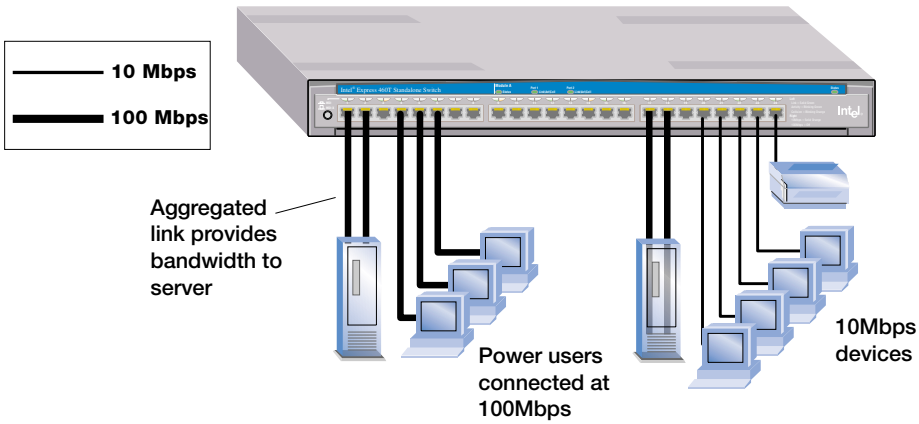
The switch maintains a table that associates a device's MAC address to a port on the switch. When Client A communicates with Client B, the switch checks the table to determine which port Client B is attached to and then forwards the traffic to that port. If a device sends traffic to an address that is not in the table (or sends broadcast or multicast traffic) the switch sends the traffic out to all ports on the switch. When the switch receives a response it updates the table with the new address.

Sample Configurations

The following examples illustrate how the 460T switch can be used in a network.

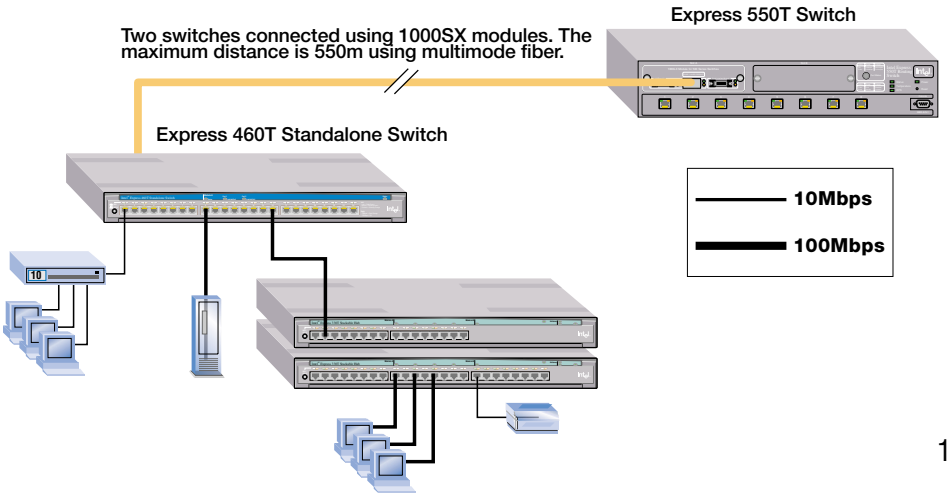
Desktop PC Bandwidth

In this example, desktop PC users are connected directly to the 460T switch. Power users are connected at 100 Mbps while regular users can be connected at 10 Mbps. Aggregated links provide additional bandwidth to the servers.



Small Office Backbone

In this example, the 460T switch serves as the backbone for a small network. The switch can provide high-bandwidth support to the clients (servers and power users) that require it while providing connections for 10 Mbps devices. Use the optional modules available for the 460T to extend the reach of the network beyond 100 meters (330 feet). For example, to connect different buildings or remote campuses to an Intel® Express 550T Switch located at a central office.



Flow Control

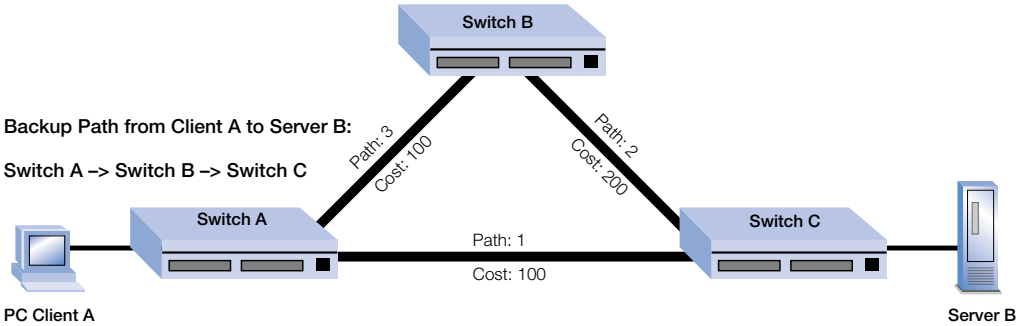
When network traffic is heavy, the switch's port buffers fill up faster than the switch can send the information. In cases like this, the switch tells the transmitting device to wait until the information in the buffer can be sent. This traffic control mechanism is called flow control.

The method of flow control depends on whether the port is set to full-duplex or half-duplex. If a port operates at half-duplex, the switch sends a collision (also called backpressure) which causes the transmitting device to wait. If the port operates at full-duplex, the switch sends out an IEEE 802.3x PAUSE frame. You can enable or disable flow control for each port on the 460T switch.

Spanning Tree Protocol

Spanning Tree is a protocol that prevents loops within the network topology. A loop can occur if there is more than one path for information to travel between devices. The Spanning Tree Protocol works by determining the "cost" of a connection. For example, if two devices are connected by two links, Spanning Tree uses the connection with the lowest cost and blocks the second connection.

Spanning Tree prevents loops by allowing only one active path between any two network devices at a time. However, you can also use this behavior to establish redundant links between devices that can take over if the primary link fails.



Primary Path from Client A to Server B: Switch A –> Switch C

In this example, Client A can communicate with Server B over two different paths. The primary path is Path 1 because the cost of the connection between switches A and C is lower than the cost between switches A, B and C. If the primary path fails, then traffic is automatically sent over the backup path.

Tagged Frames

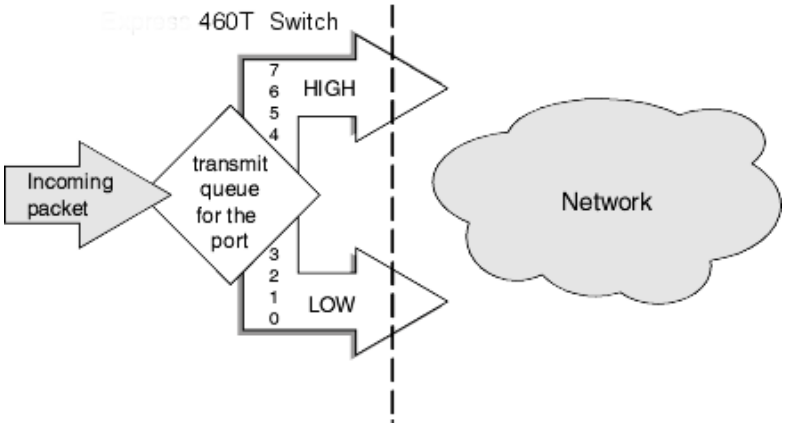
The 802.1D (1998 Edition) and 802.1Q specifications published by the IEEE (Institute of Electrical and Electronic Engineers) extended Ethernet functionality to add tag information to Ethernet frames and propagate these tagged frames between bridges (for example, a switch). The tag can carry priority information, VLAN information, or both and enables bridges to intelligently direct traffic across the network.

Priority

The IEEE 802.1D (1998 Edition) specification incorporates IEEE 802.1p and defines information in the frame tag to indicate a priority level. When these tagged packets are sent out on the network, the higher priority packets are transferred first. Priority packet tagging (also known as Traffic Class Expediting) is usually set on the LAN adapter in a PC and works with other elements of the network (switches, routers) to deliver priority packets first. The priority level can range from 0 (low) to 7 (high).

The 460T switch can read the priority tags and forward traffic on a per port basis. The switch uses two priority queues per port and routes traffic to a queue depending on the packet's tag. For example, when a packet comes into the switch with a high-priority tag, the switch routes the packet to its high-priority queue.

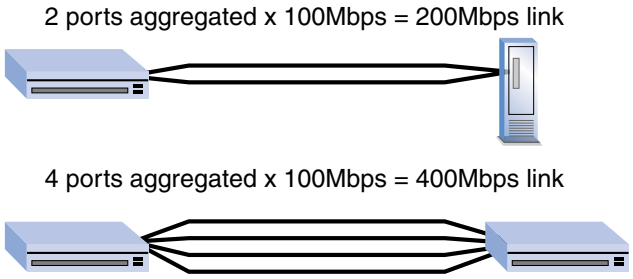
Although there are eight priority levels, the 460T switch can only route a packet into one of the two queues. The switch maps levels 0-3 to the low queue (which is the default) and levels 4-7 to the high queue. If a packet is untagged, the switch determines the best way to send the packet.



Link Aggregation

You can use link aggregation (sometimes known as port trunking) to combine from 2 to 8 (adjacent) ports so that they function as a single high-speed link. For example, link aggregation is useful when making connections between switches or to connect servers to the switch.

You can also use link aggregation to increase the bandwidth to some devices. Link aggregation can also provide a redundant link for fault tolerance. If one link in the aggregation fails, the switch balances the traffic among the remaining links.



To aggregate ports, you must link an “anchor” port to an adjacent port. The 460T Switch supports up to four link aggregation groups (anchor ports 1, 9, 17) for a 24-port switch and up to three link aggregation groups (anchor ports 1, 9) on a 16-port switch. This includes one link aggregation group for the two 100FX module ports.

Guidelines

When setting up link aggregation, remember these guidelines:

- The switch treats aggregated links as a single port. This includes Spanning Tree and VLANs.
- All ports share the same settings as the anchor port. You can change anchor port settings, but you cannot configure other ports in the link.
- When a port is configured as a member of an aggregated link, it immediately adopts the characteristics of the anchor port. When a port is no longer a member of an aggregated link, the characteristics are reset to the default settings (autonegotiate speed/duplex, flow control enabled).
- If a port is part of an aggregated link, it cannot be configured as the target port for a port mirror. However, a port in an aggregated link can serve as the source port for a port mirror.

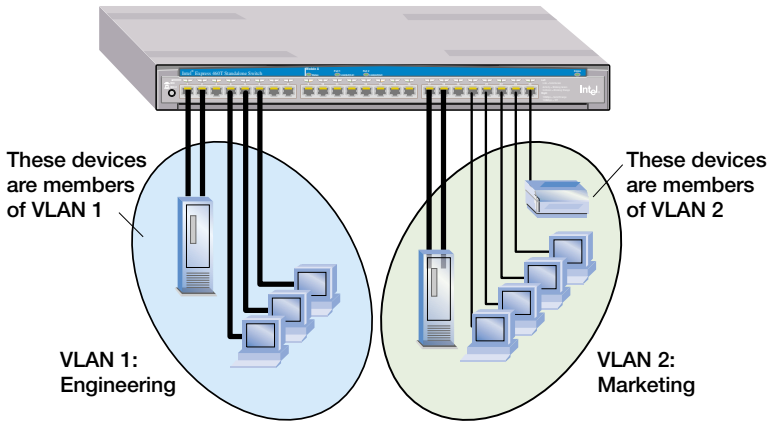
Virtual LANs (VLANs)

A Virtual LAN is a logical network grouping you can use to isolate network traffic so members of the VLAN receive traffic only from other members. Creating a VLAN is the equivalent of physically moving a group of devices to a separate switch (creating a Layer 2 broadcast domain). The advantage of a VLAN is that you can reduce broadcast traffic for the entire switch, and increase security, without changing the wiring of your network.

The 460T switch supports three types of VLANs: port-based, MAC-based, and tag-based. See Chapter 5 for more information about creating and configuring VLANs.

Port-Based VLANs

This is the simplest and most common form of VLAN. In a port-based VLAN, the system administrator assigns the switch's ports to a specific VLAN. For example, the system administrator can designate ports 2, 4, 6, and 9 as part of the engineering VLAN and ports 17, 19, 21, and 23 as part of the marketing VLAN. The advantage of port-based VLANs is that they are easy to configure and, because all changes occur at the switch, they are transparent to the users. The 460T supports up to 12 port-based VLANs. A port can belong to only one VLAN at a time.

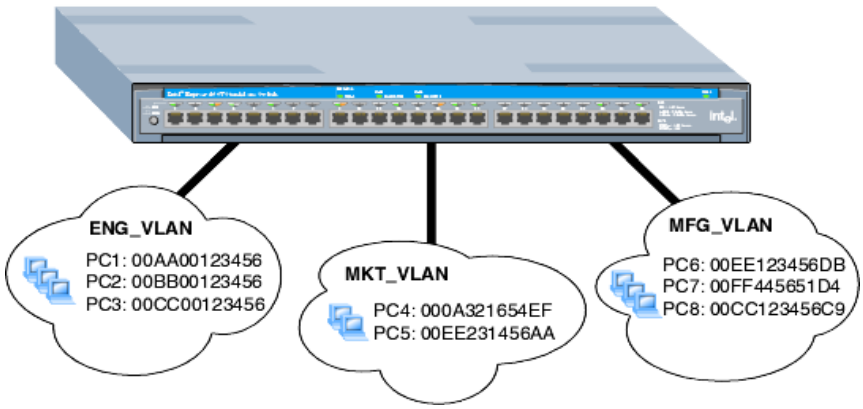


If a user relocates, the system administrator reassigns the port to the new VLAN. Another advantage is if a hub is connected to a port that is part of a VLAN, all devices connected to the hub are also part of the VLAN. The disadvantage is that there is no way to exclude an individual device on that hub from becoming part of the VLAN.

MAC-Based VLANs

Membership in this type of VLAN is based on assigning the MAC address of a device to a VLAN. The advantage to this type of VLAN is that even if users relocate, they remain on the same VLAN as long as they stay connected to the same switch. The 460T switch supports up to 12 MAC-based VLANs.

The disadvantage is that the initial configuration and subsequent administration of a MAC-based VLAN can be challenging because the system administrator needs to maintain lists of MAC addresses and enter those addresses into the switch. Another disadvantage is that MAC-based VLANs cannot span switches.



MAC-based VLANs, as designed on the 460T Switch, are intended to limit broadcast and multicast traffic over the network. The switch relies on limiting broadcast traffic to constrain network visibility of network applications (such as TCP/IP) that rely on broadcasts (such as ARP) for station discovery.

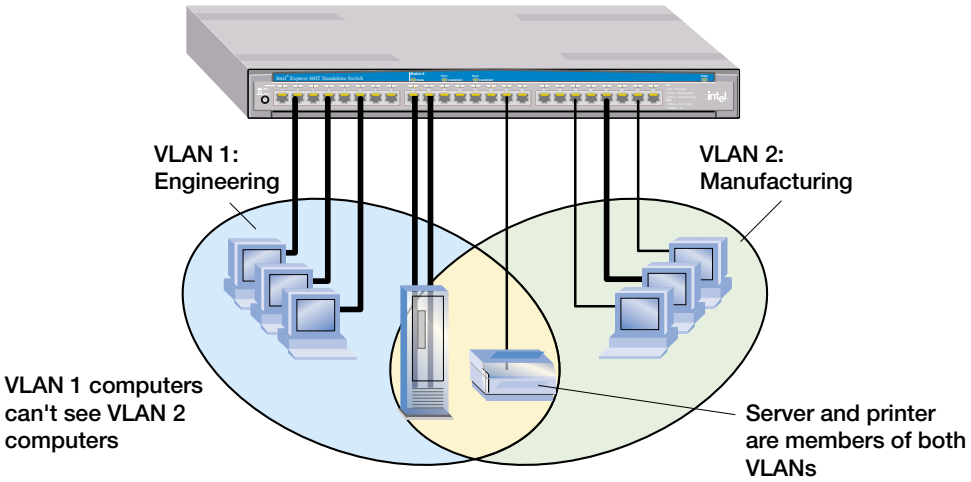
The 460T MAC-based VLANs are not intended to be a secure solution. For secure VLANs use either port-based or IEEE 802.1Q-based VLANs.

IEEE 802.1Q (Tag-Based) VLANs

The third type of VLAN supported by the 460T switch is based on the IEEE 802.1Q specification. The specification provides a uniform way to create VLANs within a network and enables you to create a VLAN that can also span across the network. Previously, VLAN implementation was vendor-specific so it was not possible to create a VLAN across devices from different vendors.

The 802.1Q VLAN works by using a tag added to the Ethernet frames. The tag contains a VLAN Identifier (VID) that identifies the frame as belonging to a specific VLAN. These tags allow switches that support the 802.1Q specification to segregate traffic between devices and communicate a device's VLAN association across switches.

There are multiple advantages to implementing 802.1Q VLANs. First, it improves performance by helping to contain broadcast and multicast traffic across the switch. Second, ports can belong to more than one VLAN. Third, VLANs can span multiple switches that support the 802.1Q specification. Finally, it provides security and improves performance by logically isolating users and grouping them together. The 460T switch supports up to 256 tag-based VLANs.



A logical grouping can be mapped to a work group. For example, you can create a VLAN that groups all the users from the engineering department into one VLAN. This logical grouping improves performance by cutting down traffic that belongs to a different logical group (for example, marketing), improves security (engineering can't see marketing), and eases moves because the user doesn't have to be physically located in the same group to participate in the VLAN.

On the 460T switch, overlapping VLANs can be supported by using 802.1Q-capable devices. However, for non-802.1Q-capable devices, overlapping VLANs can be supported by implementing an asymmetric VLAN on the switch. An asymmetric VLAN is a type of 802.1Q configuration where endstations send traffic on one VLAN and receive traffic on another VLAN. The 460T switch supports asymmetric VLANs.

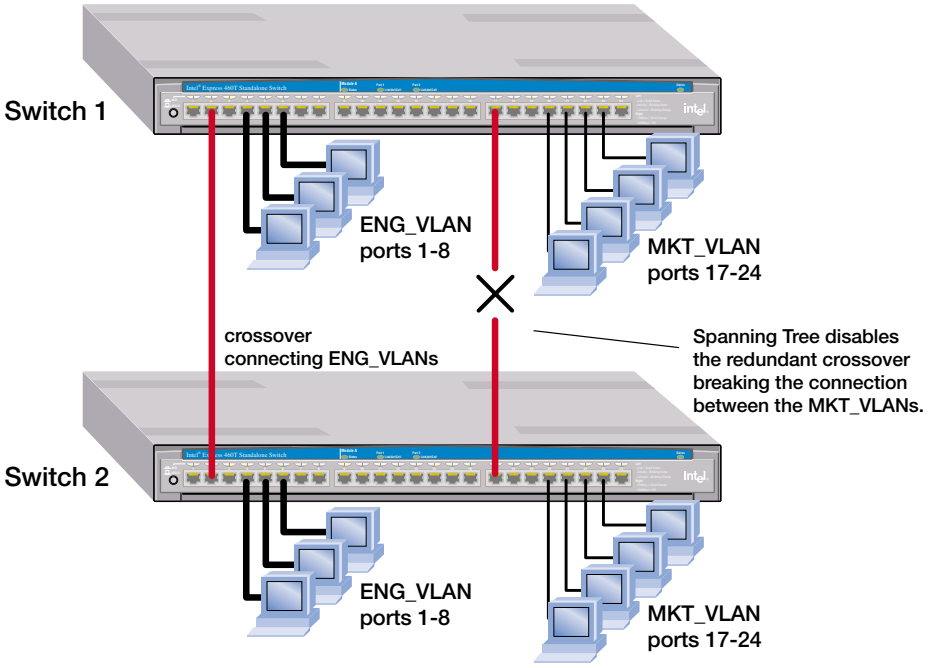
For more information about asymmetric VLANs, see *http://support.intel.com /support* or see IEEE 802.1Q Specification Annex B.1.3.

Spanning Tree and VLANs

The 460T supports the Spanning Tree Protocol across the entire switch, not per VLAN. If a loop occurs in a VLAN the port is disabled and all VLAN traffic over that port is blocked.

The following diagram shows an example. Both Switch 1 and Switch 2 have two port-based VLANs configured. Crossover cables connect the ENG_VLAN on Switch 1 to ENG_VLAN on and Switch 2. Crossover cables also connect the MRKT_VLAN on Switch 1 to the MRKT_VLAN on Switch 2. When Spanning Tree is enabled, the redundant link between the MRKT_VLANs is blocked and those VLANs can no longer communicate.

When the switch is running 802.1Q VLANs, Spanning Tree is required for GVRP (GARP VLAN Registration Protocol) to work properly.



GARP VLAN Registration Protocol (GVRP)

Because IEEE 802.1Q VLANs can span networks, managing changes to the VLAN poses a challenge for network administrators. The GARP VLAN Registration Protocol (GVRP) provides a dynamic mechanism for switches to share topology information and manage changes with other switches. The network administrator does not have to manually propagate VLAN configuration information across switches.

GARP (Generic Attribute Registration Protocol) is defined by the IEEE 802.1D (1998 Edition) specification and is the mechanism used by switches and end nodes to propagate VLAN configurations across the network domain. GVRP uses GARP as a foundation to propagate VLAN configurations to other switches. Devices that support GVRP transmit their updates to a known multicast address that all GVRP-capable devices monitor for information updates.

Sending GVRP messages between switches accomplishes the following tasks:

- Dynamically adds or removes a port from participating in a VLAN.
- Sends updates about the switch's own VLAN configuration to neighboring GVRP-capable devices.
- Integrates dynamic and static VLAN configurations within the same switch. Static VLAN configurations are created by the user on the switch for devices that don't support GVRP.

Note: dynamically created VLANs are not saved in the switch's memory. When the device sending out the GVRP updates is disabled or rebooted, the dynamic VLAN is removed.

Internet Group Multicast Protocol (IGMP)

Generally, the switch broadcasts multicast traffic to all ports. For multicast traffic based on the TCP/IP using the IGMP protocol, the switch can optimize the broadcasting of multicast traffic by forwarding multicast traffic only to ports that require it.

IGMP Snooping is a feature that allows the switch to forward multicast traffic intelligently. The switch “snoops” the IGMP query and report messages and forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

IGMP requires a router that detects multicast groups on its subnets and keeps track of group membership. Note that multicasting is not connection oriented, so data is delivered to the requesting hosts on a best-effort level of service.

3 Using Intel® Device View

Overview

You can use Intel® Device View to manage Intel Express 460T Standalone Switches and other supported Intel networking devices on your network.

Intel Device View provides these features:

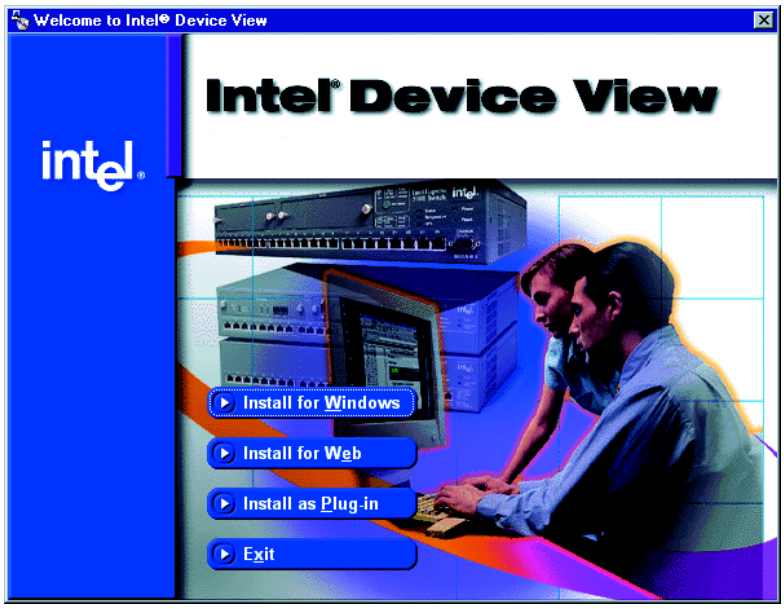
- The ability to configure new network devices
- A graphical device manager for Intel switches, hubs, and routers
- Autodiscovery, which finds supported Intel devices on the network
- The Device Tree, which shows all the supported devices detected on your network
- Remote Network Monitoring (RMON)
- Web or Windows* platform
- Plug-in to Hewlett Packard OpenView*, IBM Tivoli NetView*, and Intel LANDesk® Network Manager
- Other useful tools such as a TFTP server

Installing Intel Device View

Before you install Intel Device View, make sure your PC meets the system requirements in the *Intel Device View User Guide*, which is included on the Intel Device View CD-ROM.

To install Intel Device View

1 Insert the Intel Device View CD-ROM in your computer's CD-ROM drive. The Intel Device View installation screen appears. If it doesn't appear, run `autoplay.exe` from the CD-ROM.



2 Choose the version of Intel Device View you want to install.

- Click **Install for Windows** to install Intel Device View for use on this PC only.
- Click **Install for Web** to install Intel Device View on a Web server. Access the Device View server from any PC on your network with Microsoft Internet Explorer* 4.0x or later.
- Click **Install as Plug-in** to install Intel network device support for Hewlett Packard OpenView, IBM Tivoli NetView, or Intel LANDesk Network Manager. This option is available when you have OpenView, Net View, or LANDesk Network Manager installed on the PC.

3 Follow the on-screen instructions in the installation program.

Starting Intel Device View

Install either the Windows or Web version of Intel Device View.

Windows version

From your desktop, click Start and then click Programs > Intel Device View > Intel Device View - Windows. The main screen appears.

Web version

- From your desktop, click Start and then click Programs > Intel Device View > Intel Device View - Web. The main screen appears.
- To view Intel Device View from another PC on your network, type the following URL.

  http://*servername*/devview/main.htm

  where ***servername*** is the IP address or name of the server where Intel Device View is installed. The main screen appears.

NOTE
These are the requirements if you want to use the Web version of Intel Device View:

Web browser

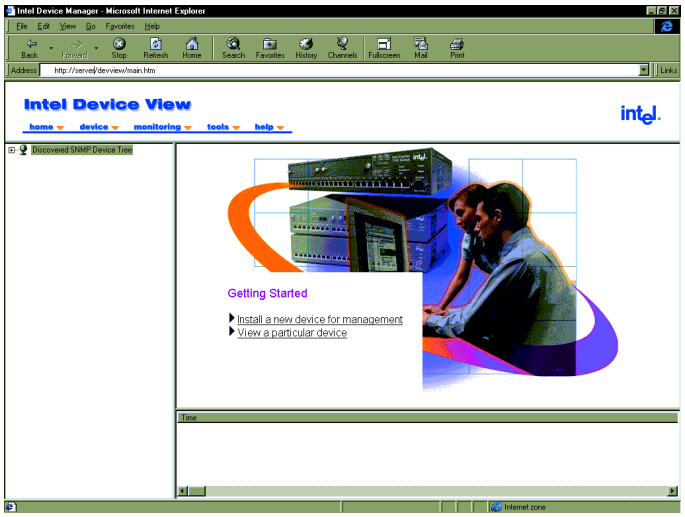
Internet Explorer 4.0 or later

Web Server

IIS 2.0 or later

Peer Web Services*

Netscape Enterprise* Web Server 3.01 or later



Installing a New Device

After you've installed a new switch on your network, you can use the Intel Device View Device Install Wizard to configure it for management.

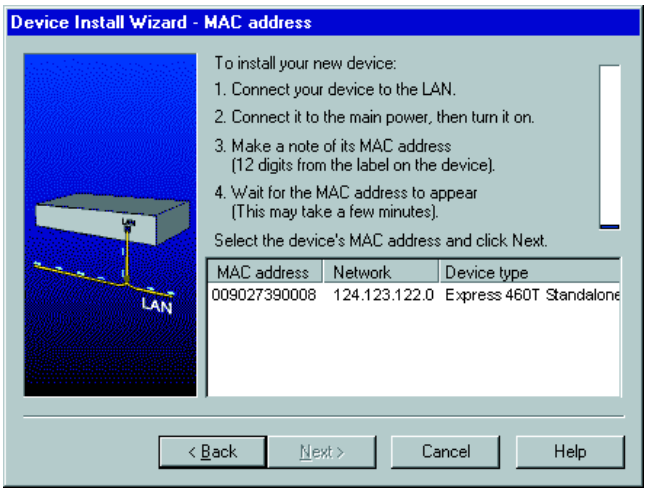
To install and configure a new switch for management

1 Start Intel Device View. The Device Install Wizard appears. If it doesn't appear, click Install from the Device menu or double-click the appropriate MAC address in the Device Tree under Unconfigured Devices. (The MAC address is located on the rear of the switch.)

2 On the Device Install Wizard - Start screen, click Next.

3 On the Device Install Wizard - MAC Address screen, click the MAC address of the new switch and then click Next.

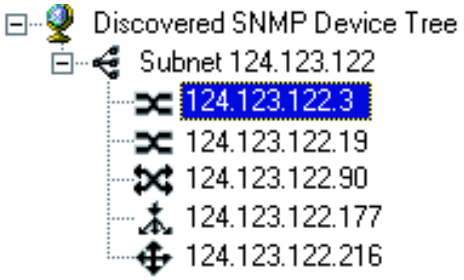
NOTE
The 460T sends BootP requests for several minutes; after that time, if no IP has been entered, the switch stops sending the request and continues to boot.



4 Follow the instructions in the wizard to assign an IP address and a name to the switch.

Using the Device Tree

When you start Intel Device View, the Device Discovery service begins searching for supported Intel network devices on your network. As it discovers devices, the Device Discovery service adds an icon for each device to the Device Tree on the left side of the screen.



Different states of the 460T switch are represented by icons in the Device Tree.

Device Tree icons

 Device Tree root

 Subnet

 Intel Express Switch (if non-responding the icon is red)

 Unconfigured Intel Express Switch

 Group of Intel Express Switches

 Intel Express Router

 Intel Express Switch (Layer 3 capable)

 Intel Express Stackable Hub

The Device Tree works much like Windows Explorer. To expand the root or a subnet, click the (+) next to the icon. To collapse the view, click the (-) next to the icon. Double-click a device icon to view the device image.

To add a device to the Device Tree

Use this procedure if the device does not automatically appear after installation.

1. Right-click anywhere on the Device Tree.
2. Click Add Device on the menu that appears.
3. In the Add Device dialog box, type the IP address of the switch you want to add.
4. Fill in the other fields, as appropriate.
5. Click OK.

The icon for the new switch appears in the Device Tree.

To refresh the Device Tree

Refreshing the Device Tree updates it to show any newly discovered devices and changes in device status.

1. Right-click anywhere on the Device Tree.
2. Click Refresh on the menu that appears.

To delete a device from the Device Tree

1. Right-click the device you want to remove from the Device Tree.
2. Click Delete on the menu that appears.

Deleting a device from the Device Tree does not affect the actual device.

To find a device in the Device Tree

1. Right-click anywhere on the Device Tree.
2. Click Find on the menu that appears.
3. In the Find Device dialog box, type the IP address of the device you want to find in the tree.
4. Click OK.

The device's icon is highlighted in the Device Tree.

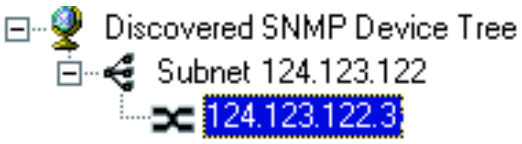
Losing contact with a device

If Intel Device View loses contact with a switch, it replaces the switch icon with the non-responding switch icon, which is red.

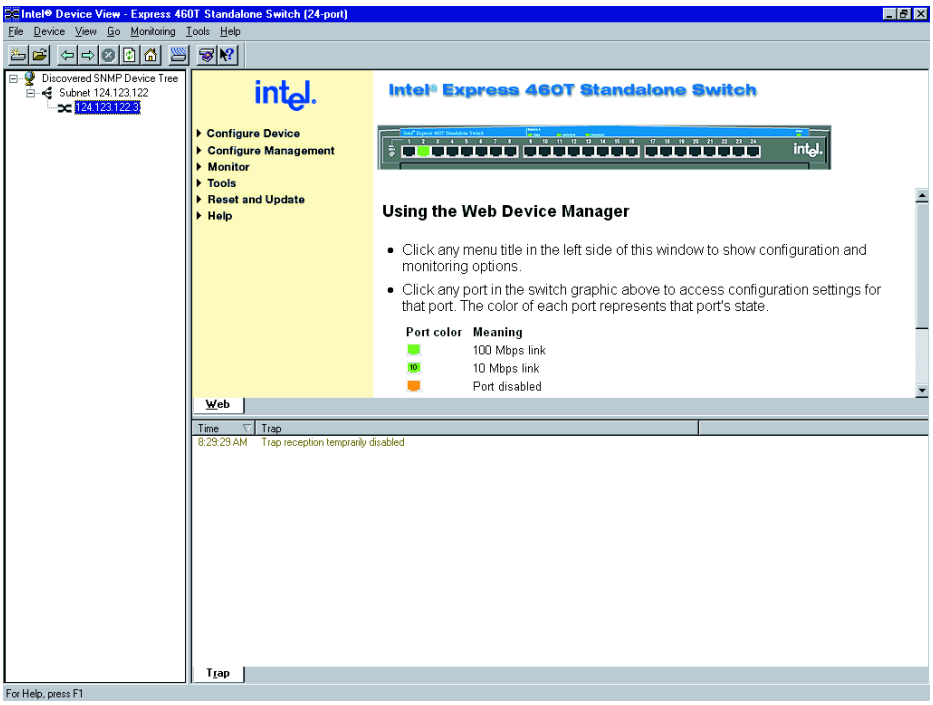
If the non-responding switch icon appears, you cannot manage the device in Intel Device View. If you cannot ping the device or start a Telnet session, try accessing the switch's Local Management.

Managing a Switch

To manage an Intel Express 460T Standalone Switch, double-click the switch icon in the Device Tree. In the example shown below, the switch has been assigned an IP address of 124.123.122.3.



The Web Device Manager appears in the Intel Device View window.



For information about using Intel Device View,see the program's Help or see the *Intel Device View User Guide* on the Intel Device View installation CD-ROM.

Viewing RMON information

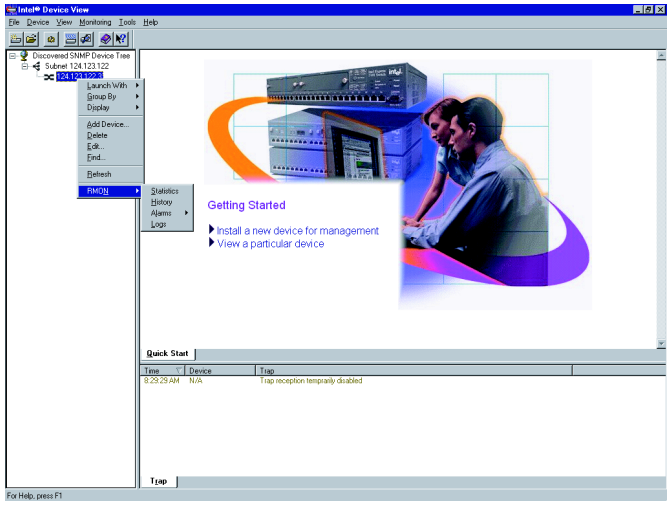
The remote monitoring (RMON) specification extends SNMP functionality to look at traffic patterns on the network instead of merely looking at the traffic for an individual device. The following RMON groups are supported:

- **Group 1 (Statistics):** Monitors utilization and error statistics for each network segment (10 Mbps or 100 Mbps).
- **Group 2 (History):** Records periodic statistical samples from variables available in the statistics group.
- **Group 3 (Alarms):** Enabless you to set a sampling interval and alarm thresholds for statistics. When a threshold is passed, the switch creates an event. For example, you might set an alarm to create an event if switch utilization exceeds 30%.
- **Group 9 (Events):** Provides notification and tells the switch what to do when an event occurs on the network. Events can send a trap to a receiving station or place an entry in the log table, or both. For example, when the switch experiences an RMON Event, it sends out an Alarm.

The switch also keeps a log that shows a list of the RMON Events and RMON Alarms that have occurred on the switch.

To view RMON statistics

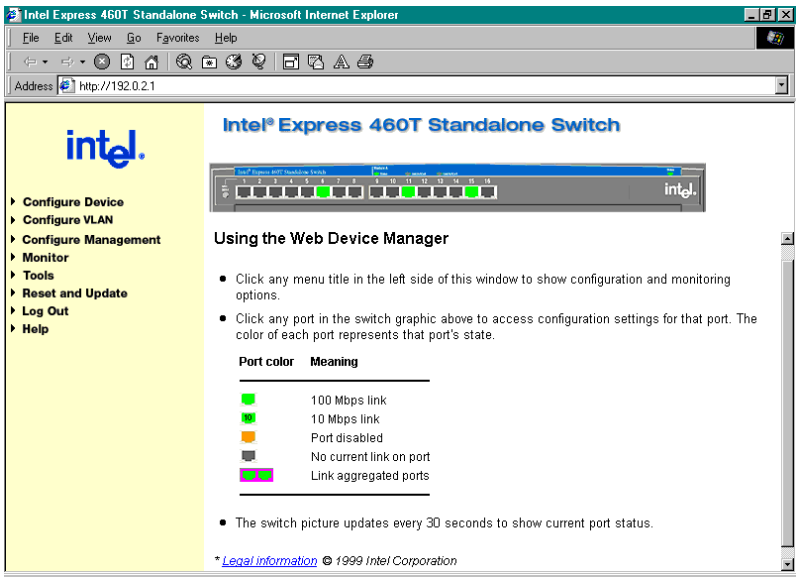
1. Right-click the icon for the switch in the Device Tree and then point to RMON.
2. Click the RMON option you want to view.



To access RMON features, you can use LANDesk Network Manager or an SNMP application that supports RMON such as OpenView. For more information about using RMON to monitor the switch, see the Intel Device View Help.

4 Using the Web Device Manager

You can use the Web Device Manager, which is built into the Intel® Express 460T Standalone Switch, to manage and monitor the switch using a Web browser. For example, you can use the Web Device Manager to configure the switch or individual ports, or to monitor traffic statistics and utilization.



For more information about using this interface, see the Web Device Manager Help.

Accessing the Web Device Manager

1 In the Location or Address field of your Web browser type the IP address of the switch. For example, to use the default IP address of the switch, type 192.0.2.1 in the Location or Address field and then press Enter.

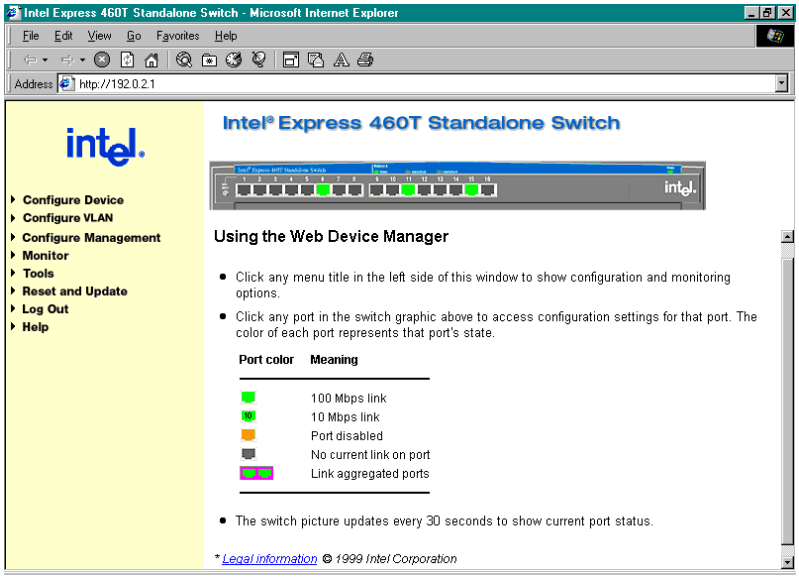
2 When prompted, type your user name and password. By default, no user name or password is assigned. If you previously set a user name and password using Local Management, enter those here.

3 Click OK. The Web Device Manager screen appears in your Web browser.

Note

The default IP address assigned to the switch is 192.0.2.1. To access the switch with the default IP address, your workstation must be on the 192.0.2.0 subnet.

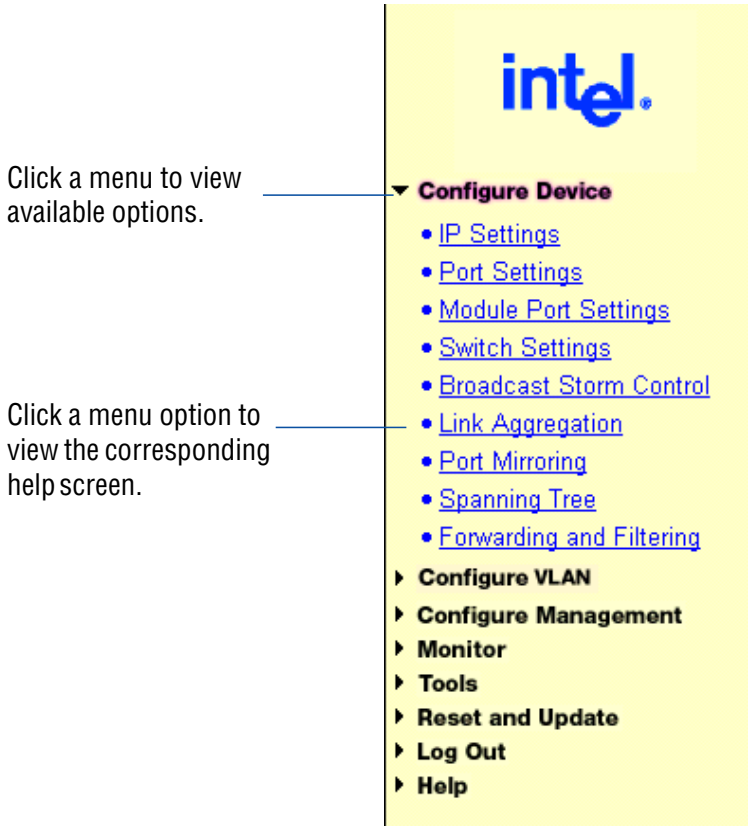
Or you can connect to the switch using Local Management and set an IP address that is on your network. Then you can access the Web Device Manager using the new IP address.



Navigating the Web Device Manager

1 On the left side of the Web Device Manager window, click a menu item (such as Configure Device) to show the available options.

2 Click an option on the menu. The corresponding screen appears on the right side of your Web browser window.



3 To hide the options, click the menu item again.

Using Management Screens

After you select an option from the navigation menu, the corresponding screen appears in the right side of your Web browser window.

Switch faceplate graphic

A graphical representation of the switch faceplate appears at the top of the screen. The following example shows a 24-port switch.

If the option you're working with allows you to configure or monitor a specific port, you can change to that port by clicking it on the faceplate graphic.

Port color on the faceplate graphic indicates the status of the port.

Port Color	Meaning
Green	Port has a link at 100 Mbps.
Green with "10"	Port has a link at 10 Mbps.
Magenta outline	Ports are in a link aggregation.
Orange	Port is disabled.
Gray	No link.

Buttons

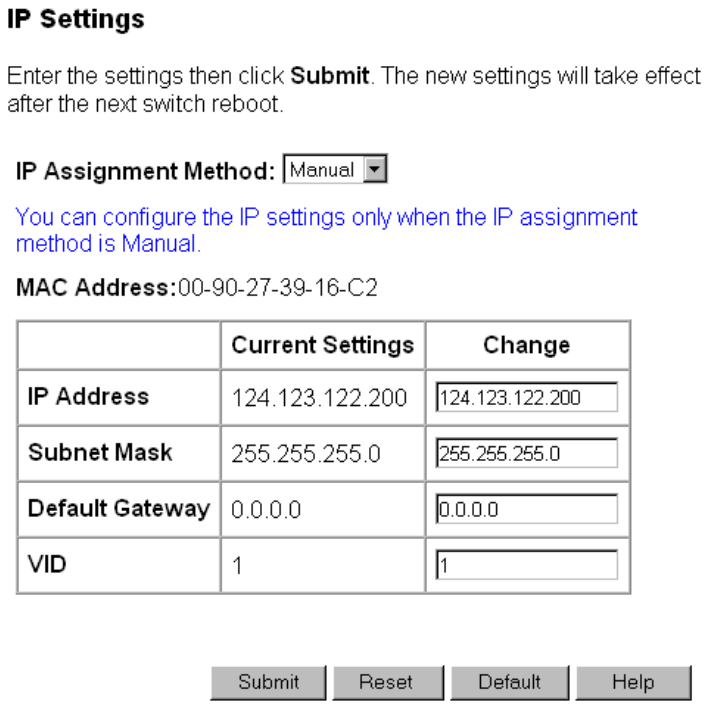
Each configuration screen includes four buttons on the bottom of the screen.

Button	Function
Submit	Applies the configuration settings on the current screen. **Note:** If you do not save the settings to the switch's flash memory your changes will be lost when the switch is rebooted.
Reset	Clears any changes you made on the current screen and restores the currently applied settings.
Default	Applies factory defaults for this screen's settings. When you log out, you can permanently save the new settings to the switch. Otherwise, they are lost upon the next reboot.
Help	Displays Help for the current screen.

Configuring the Switch's IP Settings

Note: You must select Manual in the IP Assignment Method box before you can change the IP settings.

1 Click the Configure Device menu and then click IP Settings. The IP Settings screen appears on the right side of the Web Device Manager window.



2 To manually configure the IP settings, select Manual in the IP Assignment Method box. Under Change, type the new IP address, subnet mask, and default gateway. If you have set up tag-based VLANs on the switch, you can specify the VID of the VLAN where the switch's SNMP management agent will reside.

3 Click Submit.

4 The new IP settings do not take effect until the switch reboots. Do one of the following:

To have the changes take effect now, click Save and Reboot. Rebooting the switch temporarily interrupts network connectivity to the switch.

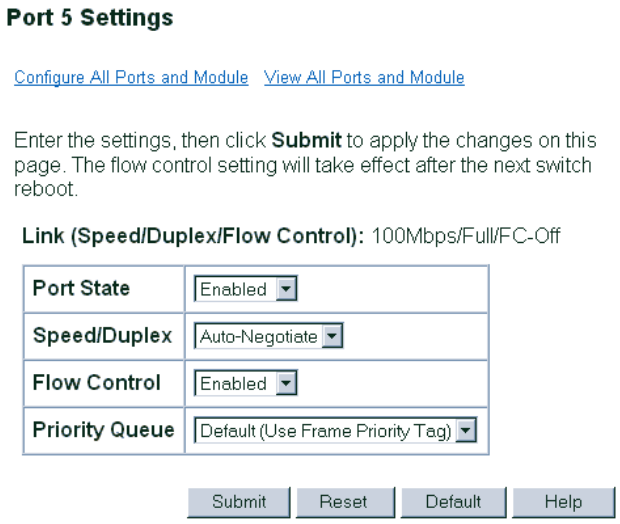
To have the changes take effect later, click Reboot Later.

Configuring a Port

You can use the Web Device Manager to enable or disable a port, and to change its speed, duplex, flow control, and priority settings.

To change port settings

1 Click the Configure Device menu and then click Port Settings. To access the Port Settings screen, click the port you want to configure on the faceplate graphic.



Note

If you change the flow control or IP settings, you must reboot the switch before the new settings can take effect.

2 Click the options you want to change.

- **Port State** to enable or disable the port.
- **Speed/Duplex** to set port speed to Auto-Negotiate, 10 Mbps, or 100 Mbps.
- **Flow Control** to enable or disable flow control.
- **Priority Queue** to set the priority queue for packets sent or received on this port.

3 Click Submit.

Managing User Accounts

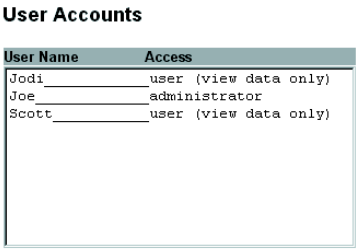
Create user accounts to give specific users read or write access to the switch through the Web Device Manager and Local Management. You can create up to three accounts on the switch.

To create a user account

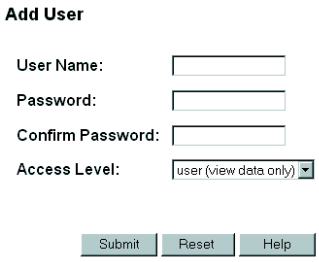
Note

The accounts and passwords you create with the Web Device Manager are the same accounts and passwords used to access Local Management.

1 Click the Configure Management menu and then click User Accounts. The first account you create must be an administrator.



2 Click Add.



3 In the User Name box, type a username. The username can be up to fifteen characters long and is case-sensitive.

4 In the Password box, type a password. The password can be up to fifteen characters long and is case-sensitive. Asterisks (*) appear on the screen as you type the password.

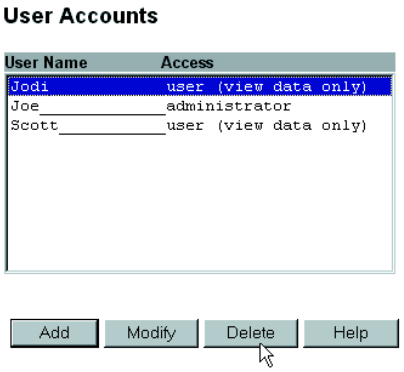
5 In the Confirm Password box, type the same password.

6 In the Access Level box click an access level. An administrator can view all settings and make configuration changes. A user can only view settings and cannot change the configuration.

7 Click Submit.

To delete a user account

1. Click the Configure Management menu and then click User Accounts.
2. In the User Accounts screen, click the account you want to delete.
3. Click Delete.



If you delete the account you used to log in for this session, you can continue to use that account until you log out. If you delete the only user account on the switch, you can log in again using the default of no username and no password.

Configuring VLANs

Virtual LANs, or VLANs, provide a way to create a logical network grouping without regard to physical location of the network nodes.

For more information about VLANs, see "Virtual LANs" in Chapter 2.

The two main steps to set up a VLAN with the Web Device Manager are:

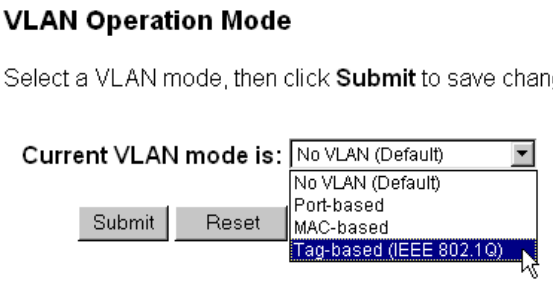
- Set the switch's VLAN operation mode.
- Configure the type of VLAN you selected.

To set the switch's VLAN operation mode

NOTE

You can have only one operation mode active on the switch at a time. Choose port-based, tag-based or MAC-based.

1 Click the Configure VLAN menu and then click VLAN Operation Mode.



2 In the Current VLAN Mode Is box, click the type of VLAN to set up. You can set the 460T switch to use port-based, MAC-based, or tag-based VLANs. See "Virtual LANs" in Chapter 2 for more information about VLAN types.

3 Click Submit.

4 The switch automatically reboots. The switch must be rebooted whenever you change its VLAN operation mode.

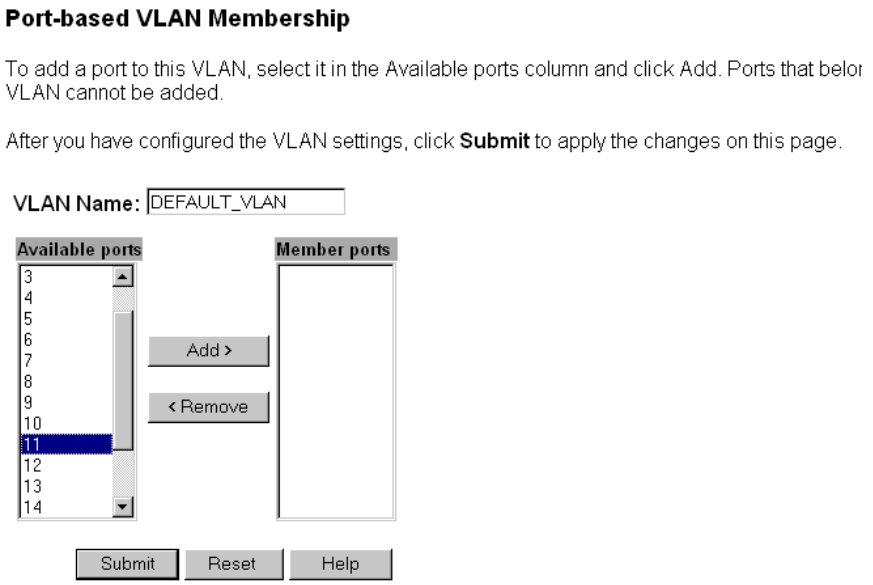
After the switch reboots, you can configure the type of VLAN that you selected.

Port-based VLAN

You configure a port-based VLAN by creating the VLAN and then adding participating ports. The switch can support up to 12 port-based VLANs. However a port can be a member of only one VLAN; port-based VLANs cannot overlap.

To configure a port-based VLAN

1 Click the Configure VLAN menu and then click Port-based VLAN.



2 Click Add to create a new VLAN, or select a VLAN and click Edit to change its configuration.

3 If you are creating a new VLAN, type a name in the VLAN Name box.

4 In the Available ports box, select a port to add to the VLAN and click Add.

5 Click Submit.

MAC-based VLAN

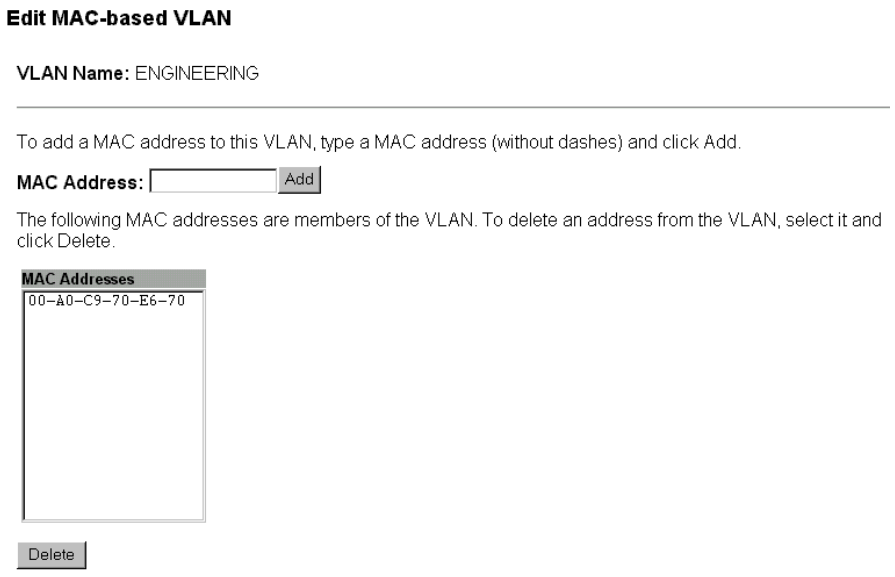
You configure a MAC-based VLAN by creating the VLAN and then adding the MAC addresses of member devices.

To create a MAC-based VLAN

1. Click the Configure VLAN menu and then click MAC-based VLAN.
2. Click Add VLAN.
3. In the VLAN Name box, type a name for the VLAN.
4. Click Submit.

To add or delete addresses from a MAC-based VLAN

1. In the list of MAC-based VLANs, click a VLAN and then click Edit MAC Addresses.
2. In the MAC Address field, type a MAC address (without the hyphens) and click Add. All MAC addresses in the VLAN are listed in the MAC Addresses box.



3. To delete an address from the member list, click the address and click Delete.
4. When the list of addresses is complete, click Submit.

Tag-based VLAN

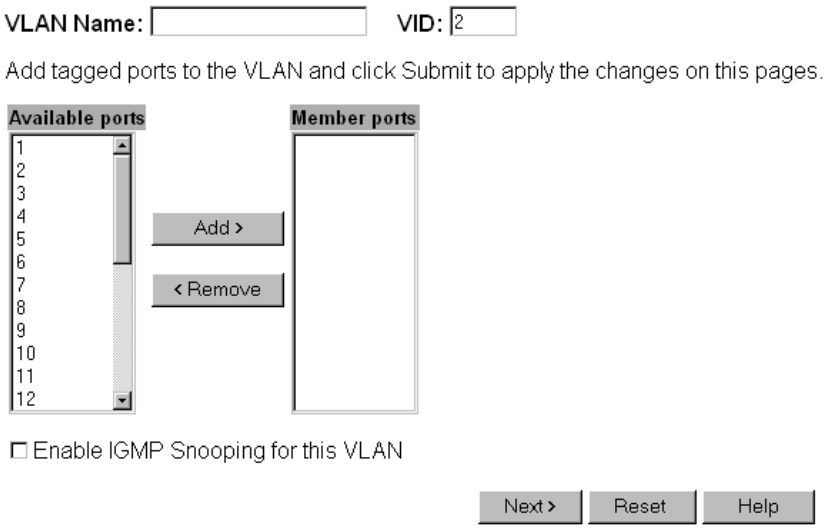
You configure a tag-based VLAN by configuring port membership and ingress/egress rules. If any of your devices don't support 802.1Q VLAN tags, additional configuration may be necessary.

To configure a tag-based (IEEE 802.1Q) VLAN

1 Create a VLAN and assign member ports.

a Click the Configure VLAN menu and then click Tag-based (IEEE 802.1Q) VLAN.

b On the main Tag-based VLAN page, click Add to create a new VLAN. To modify an existing VLAN, click the VLAN name and click Edit.



c If you are creating a new VLAN, type a name and VID (from 2 to 4094) to identify it.

d To add a port to the VLAN, click the port in the Available ports box and click Add. To remove a port, click the port in the Member ports box and click Remove.

e The switch supports up to 12 IGMP Snooping sessions to manage broadcast traffic. To make the VLAN be part of an IGMP Snooping session, select the Enable IGMP Snooping check box.

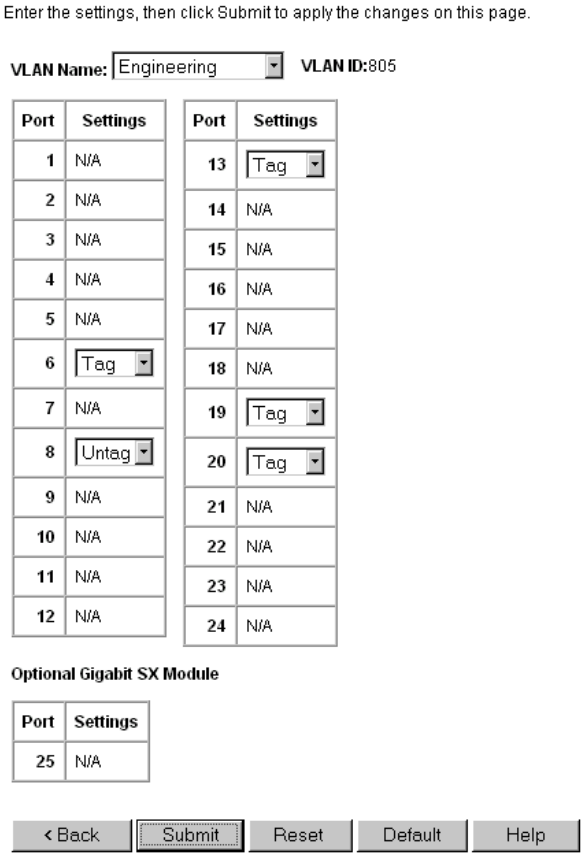
f When you finish adding ports, click Next.

2 Configure ports for egress (outbound) tagging.

a Ensure that the VLAN Name field displays the name of the VLAN you are configuring.

b To determine whether or not the switch will remove (untag) tags before sending traffic out of each port, select Tag or Untag for each of the VLAN's ports.

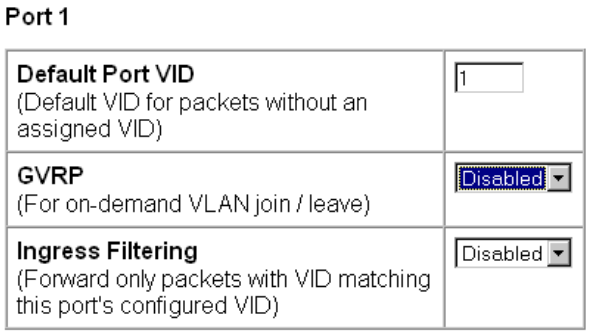
c Click Submit.



3 Configure ports for handling untagged traffic.

a From the main Tag-based VLAN page, click Port Settings.

b On the Port Settings screen, you can set port-specific behaviors for processing VLAN traffic. To configure a specific port, click it in the faceplate graphic. To configure the same setting across all ports, click Configure All Ports and Module.



Options include:

- **Default Port VID**: Sets the port VID (PVID) that will be assigned to untagged traffic on a given port. For example, if port 10's default PVID is 100, all untagged packets on port 10 will belong to VLAN 100. The default setting for all ports is VID 1.
- **GVRP**: Allows automatic VLAN configuration between the switch and nodes.
- **Ingress filtering**: Allows incoming frames belonging to a specific VLAN to be forwarded if the port belongs to the same VLAN. Disabling this setting causes all frames to be forwarded, regardless of the port's VLAN membership.

4 Click Submit.

NOTE

When configuring link aggregation between two 460T switches, you must connect anchor port to anchor port, and member port to member port.

Link Aggregation

Use link aggregation to group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth between devices on the network, such as another switch or a server.

The anchor port is the base port in a link aggregation, and it is the only port in the aggregation with configurable settings. All member ports in an aggregation take on the settings of the anchor port.

Only consecutive ports, starting from the anchor port, can be grouped in a link aggregation. For example, ports 1, 2, and 3 are a valid link aggregation; ports 2, 4, and 7 are not.

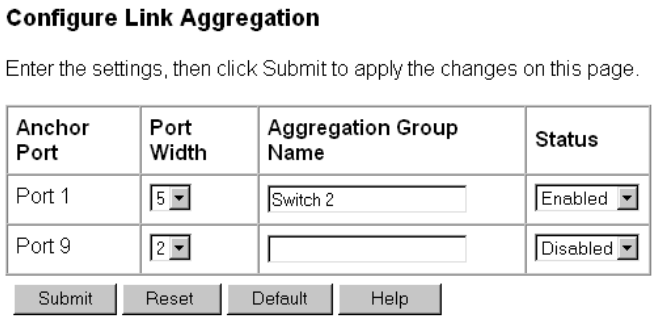
On the Web Device Manager switch faceplate graphic, a link aggregation is shown with its ports outlined in magenta.

To create a link aggregation

NOTE

Connectivity is momentarily interrupted when you apply changes.

1 Click the Configure Device menu and then click Link Aggregation.



2 Choose the anchor port. Anchor ports are listed by number in the left column.

3 In the Port Width box, click the total number of ports (including the anchor port) to include in the link aggregation.

4 In the Aggregation Group Name box, ype a name for the aggregation group.

5 To make the group active, click Enable.

6 Click Submit.

Static MAC Addresses

The MAC address table stores all the MAC addresses known by the switch. The switch uses this table for forwarding traffic to specific devices to avoid broadcasting traffic to every port for communication.

There are two ways to add addresses to the MAC address table:

- The switch can learn addresses and add them dynamically. Dynamic entries remain in the table only while the associated node is active. They are deleted if the node is inactive for longer than a specified period of time, known as the age-out time; the default is 300 seconds.
- You can manually add MAC addresses to the table. These are called static addresses, because they remain in the table until you remove them, even if the associated node is inactive or taken off the network.

To add a static MAC address to the address table

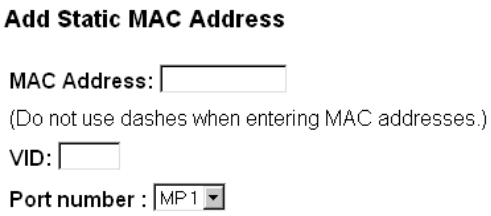
1 Click the Configure Device menu, then click Forwarding and Filtering.

2 Click Static MAC Addresses.

3 Click Add.

Note

To view the switch's address table, click the Monitor menu, click Advanced, then click MAC Address Table.



4 In the MAC Address box, type the MAC address of a device on the network. Do not include hyphens.

5 If port-based or tag-based (IEEE 802.1Q) VLANs are set up on the switch, static MAC addresses are associated with specific VLANs. Type the VLAN name (port-based VLANs) or VID (tag-based VLANs) to associate with the MAC address.

6 In the Port number box, click a port number. The port number for the optional LX and SX modules is MP1; the port numbers for the FX module are MP1 and MP2.

7 Click Add.

Configuring Community Strings and Trap Receivers

A trap receiver is a computer on the network that is running an SNMP management application and receives messages sent by the switch. For example, the switch can send a trap to the trap receiver when it detects a change in port speed.

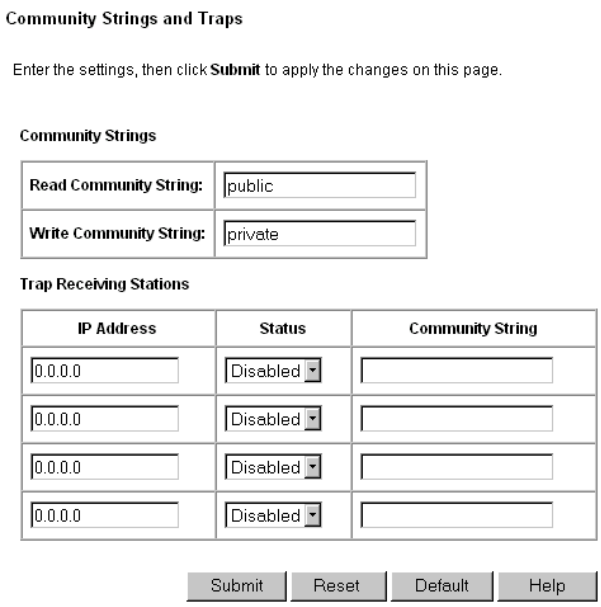
NOTE

The following traps are supported by the switch:

- Power to the switch was cycled or reset.
- Link, speed, or other status changes on a port.
- A port is partitioned.
- Authentication failure.

To specify a trap receiver

1 Click the Configure Management menu and then click Community Strings and Traps.



2 In the IP Address box, type the IP address of the computer you want to use as a trap receiver. You can specify up to four trap receivers.

3 In the Status box, click Enabled.

4 In the Community String box, type the trap receiver's SNMP application community string.

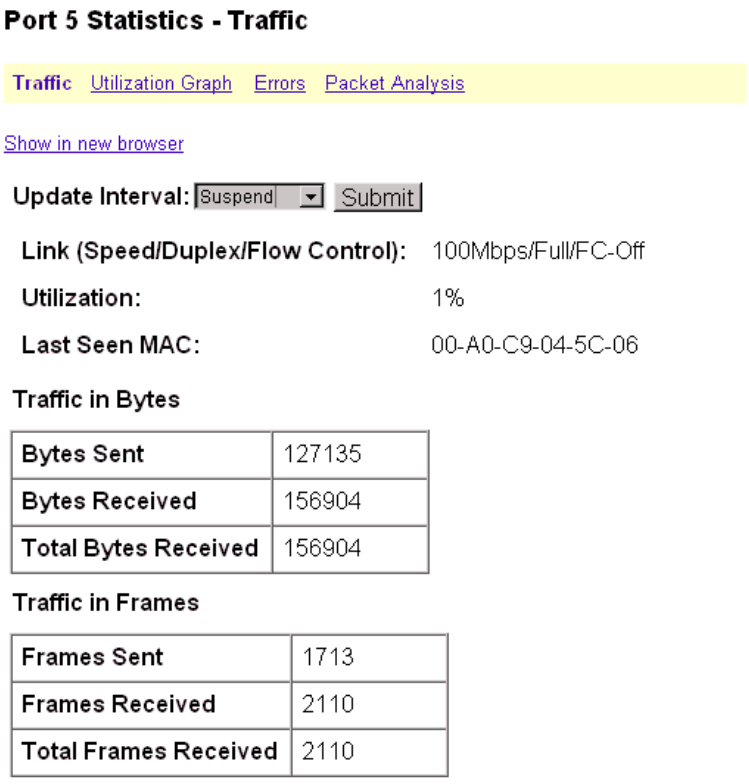
5 Click Submit.

Monitoring Switch Activity

The Web Device Manager lets you view traffic, utilization, and error statistics for the switch and for individual ports. For more information on statistics, see “Port Traffic Statistics,” “Port Error Statistics,” and “Packet Analysis” in Chapter 5.

To view port statistics

1. Click the Monitor menu and then click Port Statistics.
2. From the row of options under the page heading, click the option you want to view:
   - Traffic
   - Utilization Graph
   - Errors
   - Packet Analysis

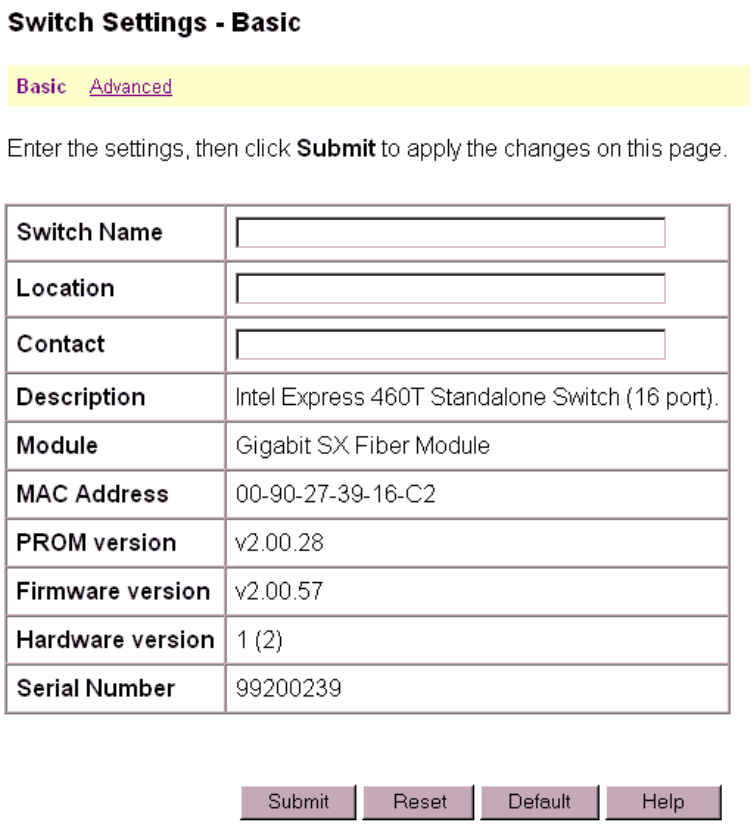


Viewing/Changing Switch Information

You can view information about the switch, such as its MAC address, firmware version, name, location, and contact person. Some of the fields can be updated, others are read-only.

To view and configure switch settings

1 Click the Configure Device menu and then click Switch Settings.



2 In the Switch Name, Location, and Contact fields you can provide additional information about the switch. You can type up to 40 characters in each field.

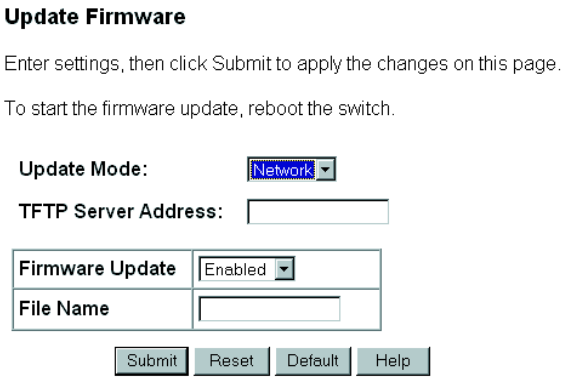
3 When you finish, click Submit.

Updating Switch Firmware

Use the Update Firmware screen to set the switch up to update its firmware from a TFTP server. The actual firmware update occurs while the switch is rebooting.

To update the switch's firmware

1 Click the Reset and Update menu and then click Update Firmware.



2 In the Update Mode box, select a mode:

- If the switch will use a network connection for downloading the new firmware file, click Network.
- If the switch will use a SLIP out-of-band connection (for example, a serial port) for downloading the new firmware file, click SLIP.

3 In the TFTP Server Address box, type the IP address of the server that hosts the file.

4 In the Firmware Update box, click Enabled.

5 In the File Name box, type the name of the firmware file.

6 Click Submit.

The next time the switch reboots it downloads and installs the new firmware during the boot process. If you want to view this process, you must use a terminal program and be connected to the switch though the console port.

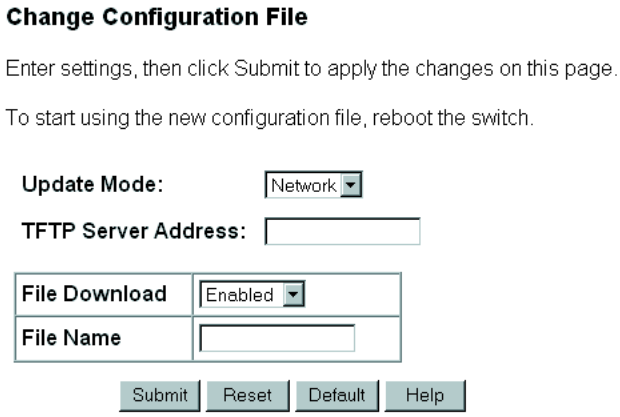
Note

If you don't have a TFTP server application, one is provided with Intel Device View (for Windows*) and LANDesk® Network Manager.

To update the switch's configuration file

The configuration file contains information and configuration settings specified by the network administrator. For more information on using configuration files, see "Upload Configuration Image File" in Chapter 5.

1 Click the Reset and Update menu and then click Change Configuration File.



2 Select a mode from the Update Mode box.

- If the switch will use a network connection for downloading the new configuration file, click Network.
- If the switch will use a SLIP out-of-band connection (for example, a serial port) for downloading the new configuration file, click SLIP.

3 In the TFTP Server Address box, type the IP address of the server that hosts the file.

4 In the File Download box, click Enabled.

5 In the File Name box, type the name of the configuration file.

6 Click Submit.

The new configuration settings will be applied to the switch upon the next reboot.

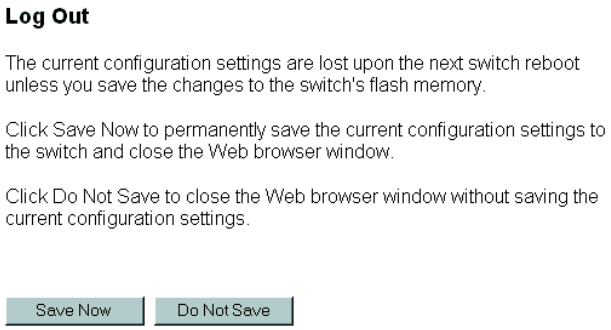
Saving Configuration Changes and Logging Out

Each time you make configuration changes using the Web Device Manager, the switch immediately uses the new settings.

However, unless you permanently save the configuration changes when you log out of the Web Device Manager, they are lost upon the next switch reboot.

To save changes and log out

1 On the menu, click Log Out.



2 Click Save Now to save the current configuration settings. The Web browser window closes and you are successfully logged off of the Web Device Manager.

If you click Do Not Save, all current configuration settings are lost the next time the switch is rebooted.

5 Using Local Management

Overview

Another way to configure the switch is through the Local Management interface. Local Management provides the same functionality as the Web Device Manager using a text-based interface.

Accessing Local Management

You can access Local Management in two different ways: by connecting directly to the switch's serial port, or through a Telnet session (using either an IP address you assign or the default IP address of 192.0.2.1).

Using the serial port

1. Use the null modem cable included with the switch to connect the serial port of your PC to the serial port of the switch.
2. Start a terminal emulation program (such as HyperTerminal* in Windows* 98). Use these communication parameters:
   - 9600 baud
   - 8 data bits
   - No parity
   - 1 stop bit
   - No flow control
3. Press Enter to connect to the Local Management.
4. Log on to Local Management. By default, no password or username is assigned. To assign them, see "User Accounts" in this chapter.

NOTE

You use the same user name and password to log onto Web Device Manager and Local Management.

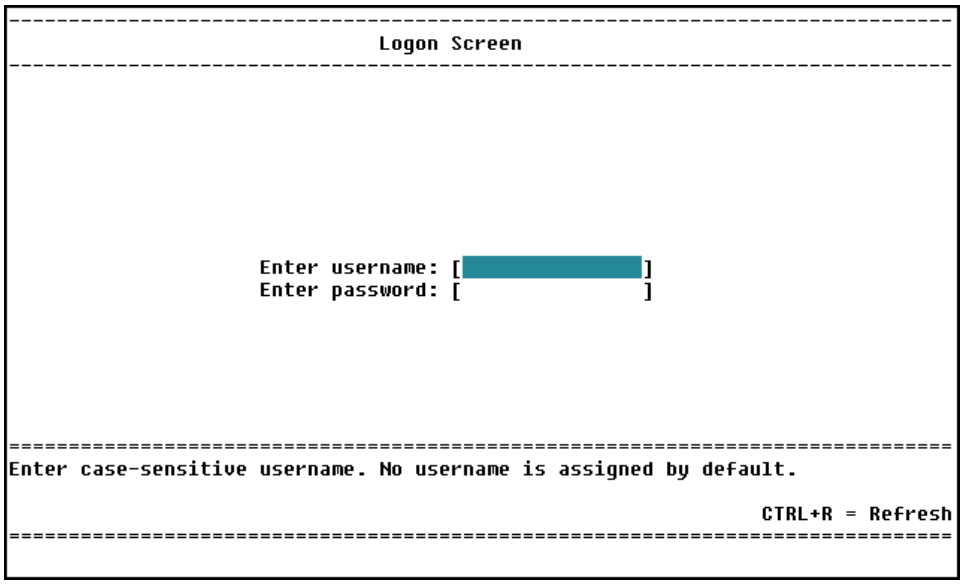
Using Telnet

NOTE

To access the switch using Telnet, your workstation must be in the same subnet as the switch.

1. Open a Telnet application. In Windows 98 or Windows NT*, select Run from the Start Menu and then type: **telnet** ↵Enter.
2. On the Terminal menu, select Preferences. Make sure the emulation type is VT-100/ANSI and that VT100 arrows are enabled.
3. On the Connect menu, select Remote System. Enter the IP address of the switch and click Connect. (The default IP address is 192.0.2.1.)
4. Log on to Local Management. By default, no password or username is assigned.

Logon Screen

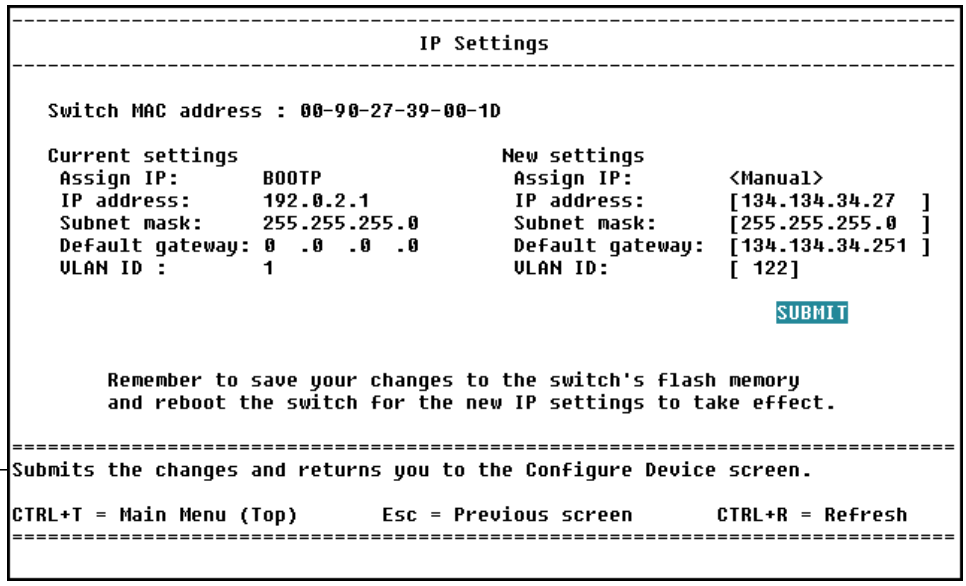


Description

By default, no username or password is assigned to the switch. Press ↵Enter twice to log on to the Local Manager. Usernames and passwords can consist of any characters and can be up to fifteen characters in length. Remember that usernames and passwords are case-sensitive.

Navigation

The console menus provide a basic interface for configuring switch options. For navigation tips, see the text below the graphic.



Help at the bottom of the screen provides information about the selected item.

Screen Legend

Use the ↑ ↓ ← → keys or the Tab and Bksp keys to move between screen fields.

<Manual> Angle brackets indicate a toggle field. Use the Spacebar to toggle selections within the field. In this example, the options change between Manual, BOOTP 10 Mins, BOOTP Continuous, and DHCP.

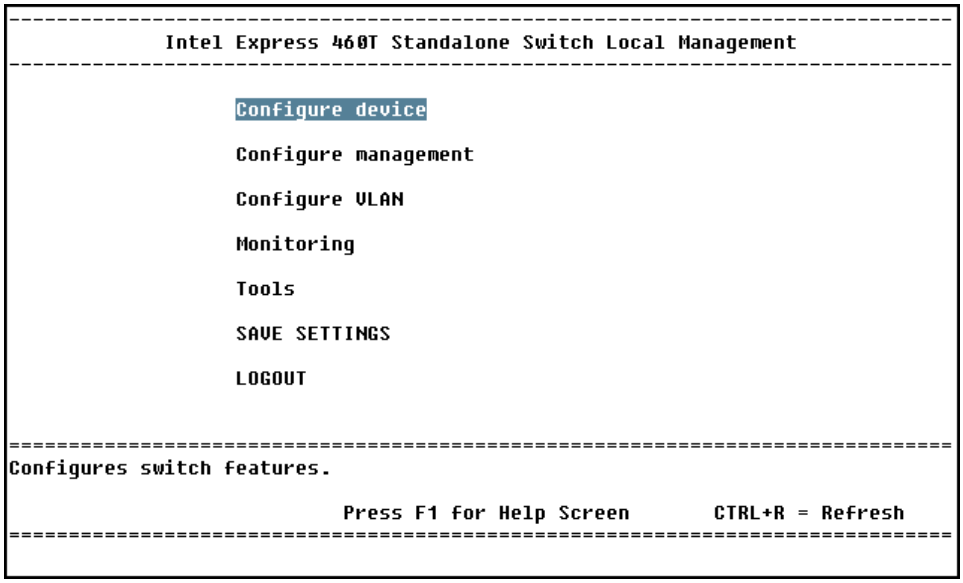
[255.255.255.0] Brackets indicate an input field.Use the arrow keys to select the field and then type the required information. By default, Local Management is in overstrike mode, which means it replaces existing characters as you type.

SUBMIT Any word in all caps is a button. Use the Tab key or the ↑ ↓ ← → keys to select it and press Enter to activate it.

NOTE

If you are using the Windows* 2000 operating system, the arrow keys and F1 key do not work. Use the Tab and Bksp keys to move from field to field on the screen.

Main Menu (Top Screen)



LOCATION

To return to the Main Menu at any time, press Ctrl T.

Description

The Main Menu is the starting point for all other Local Management screens. Use the ↑ ↓ arrow keys to choose an option and press ↵ Enter to display the screen.

Configure device: Access menus to assign an IP address to the switch, change port settings, or configure advanced switch settings.

Configure management: Set SNMP traps and trap monitoring stations, administer user accounts, or update the switch's firmware.

Configure VLAN: Set up and administer VLANs on the switch.

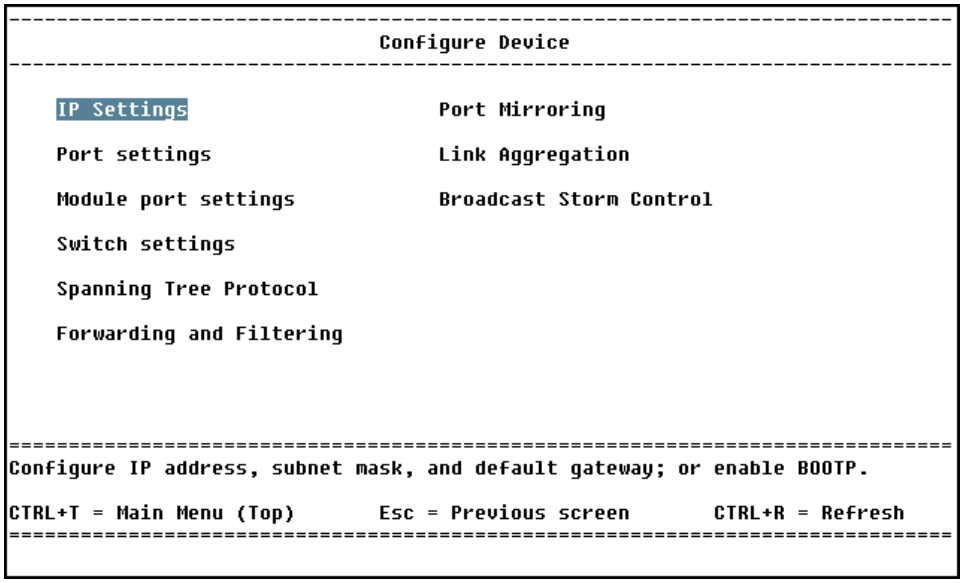
Monitoring: Access menus to monitor traffic and activity at the port or switch level. These menus also provide information on network errors and collisions.

Tools: View the switch Trap/Event log, ping devices to check connectivity, save the current switch configuration to an image file on a server.

SAVE SETTINGS: Save configuration changes to the switch's flash memory. Any changes not saved to memory are lost on the next reboot.

LOGOUT: Return to the logon screen.

Configure Device



LOCATION

Main Menu

Configure Device

Description

IP settings: Configures the switch's IP address.

Port settings: Configures port speed, enables and disables ports, and displays link status.

Module port settings: Configures the module's speed and duplex settings, enables and disables ports, and displays link status.

Switch settings: Sets switch identification, displays detailed information about the switch hardware and firmware, and configures some advanced switch settings.

Spanning Tree Protocol: Configures Spanning Tree for the entire switch or individual ports.

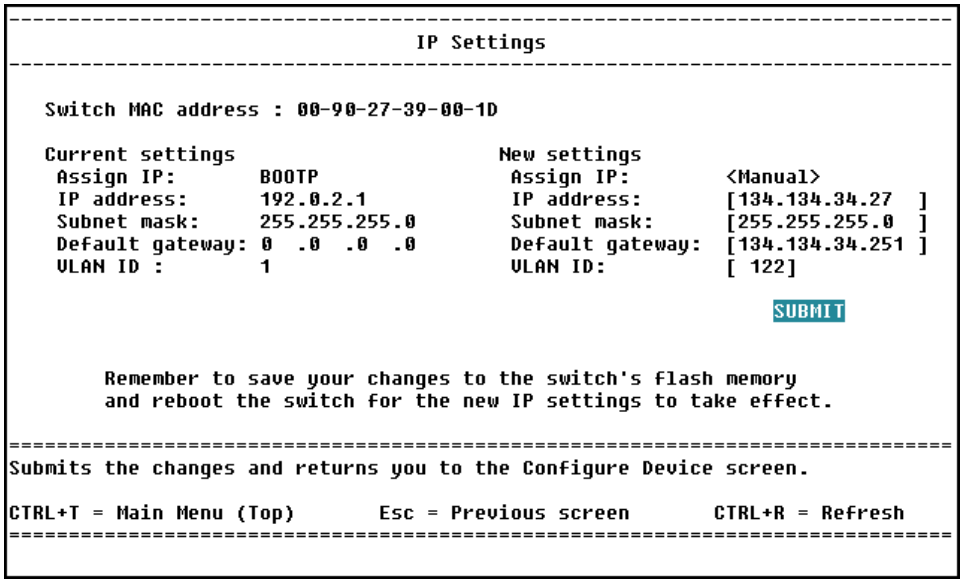
Forwarding and Filtering: Adds, removes, or locks the switch's address table, enables IGMP snooping, and sets filters for specific MAC addresses.

Port Mirroring: Sends a copy of data from one port to another for monitoring and troubleshooting purposes.

Link Aggregation: Combines ports on the switch to increase bandwidth.

Broadcast Storm Control: Configures ports to drop excessive broadcast traffic before it floods the network.

Configure IP Address



LOCATION

Main Menu

Configure Device

IP Settings

Description

Switch MAC address: The unique hardware address assigned by Intel.

Current settings: The switch's current IP configuration.

New settings: Assign a new IP configuration to the switch.

Assign IP: Indicates if the switch obtains an IP address dynamically, or if you assign an address manually. The options are BOOTP 10 Mins, which looks for a BOOTP server for 10 minutes; BOOTP Continuous; DHCP, which looks for a DHCP server; and Manual.

IP address: The IP configuration used by the switch. Use the IP address shown here to access the switch through Telnet or a ping test.

Subnet mask: Should match the mask for other devices on the network.

Default gateway: The IP address of the device that routes to different networks—typically, a router or routing server. Set this option to manage the switch remotely.

VLAN or VLAN ID (port-based or tag-based VLANs only): Specify a VLAN where the switch's SNMP management agent will reside. This option appears only when port-based and IEEE 802.1Q VLANs are active on the switch.

SUBMIT: Submits the changes and returns you to the Configure Device screen. You must save the changes to the switch's flash memory and reboot the switch for the new IP settings to take effect.

NOTE

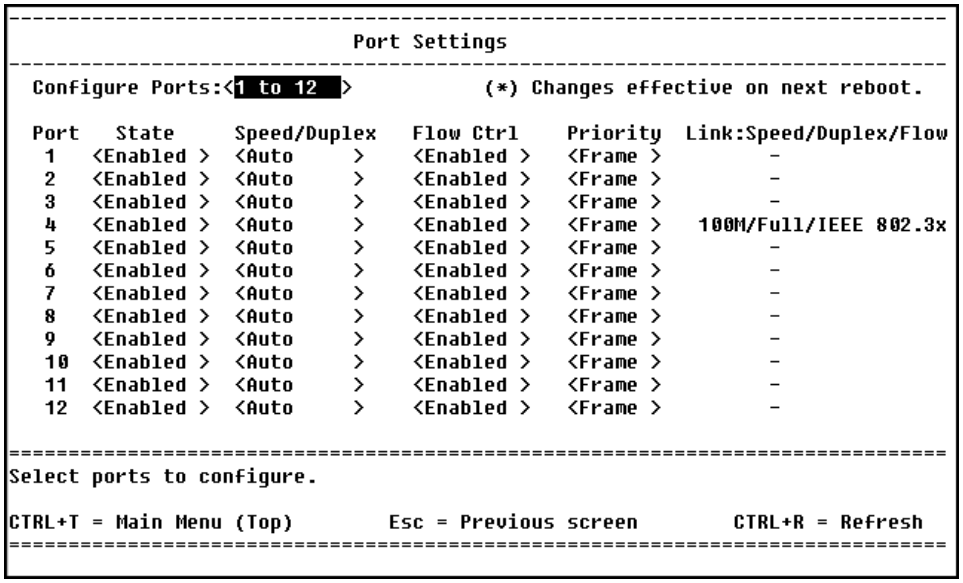
The default IP address for the switch is 192.0.2.1

Default VLAN for SNMP agent:

Port-based:DEFAULT_VLAN

802.1Q-based: VID=1

Port Configuration



Description

LOCATION

Main Menu

Configure Device

Port Settings

Configure ports: Press the Spacebar to select a range of ports to configure.

State: Press the Spacebar to toggle the field and disable or enable ports.

Speed/Duplex: Press the Spacebar to toggle the field options and change the speed and duplex of the port. You can set the port to auto-negotiate speed, or to 10 Mbps or 100 Mbps at half-duplex or full-duplex.

Flow Ctrl (Control): Press the Spacebar to enable or disable flow control.

Priority: Press the Spacebar to change the settings. The <Frame> setting reads the packet's 802.1p priority tag and handles it accordingly. The <Low> and <High > settings force the packet into one of two priority queues. Forcing a packet into a queue does not retag the packet.

Link: Indicates the port's current link status:

--: Indicates there is no device link or the port is disabled.

10M/100M: Indicates the port's speed, either 10 Mbps or 100 Mbps.

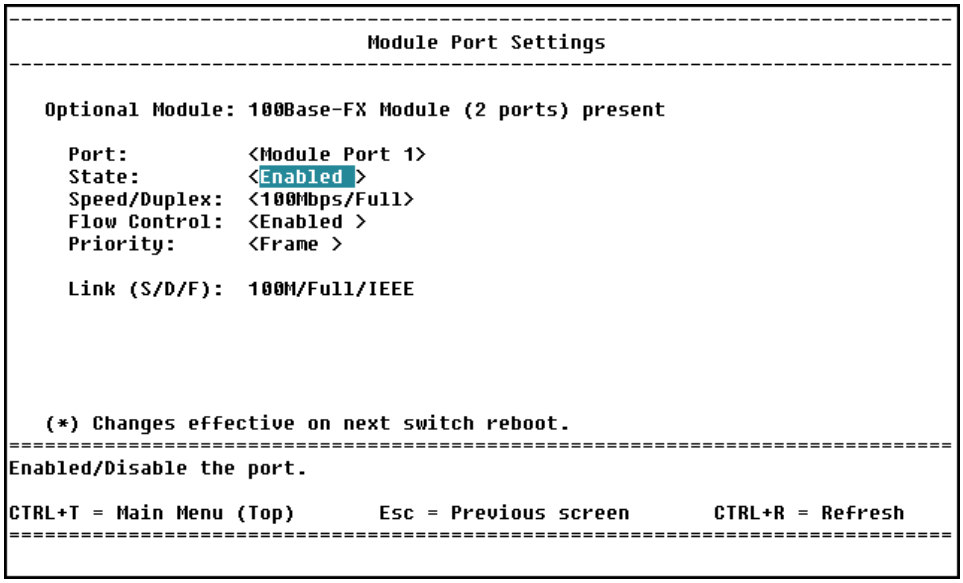
Full/Half: Indicates a device is connected at full-duplex or half-duplex.

IEEE/BackP: Indicates the type of flow control, either IEEE PAUSE frames or backpressure.

Partitioned: Indicates port was disabled due to a partition error.

Source mirror/Target mirror: Indicates the port being mirrored and where the data is being sent.

Module Port Settings



LOCATION

Main Menu

Configure Device

Module Port Settings

Description

Ports: Press the Spacebar to select a port on the module (FX Module only).

State: Press the Spacebar to toggle the field and disable or enable ports.

Speed/Duplex: Press the Spacebar to toggle the field options and change the speed and duplex of the port. You can set the port to auto-negotiate speed or set it to 100 Mbps at half-duplex or full-duplex (FX Module only).

Flow Ctrl (Control): Press the Spacebar to enable or disable flow control.

Priority: Press the Spacebar to change the settings. The <Frame> setting reads the packet's 802.1 priority tag and handles it accordingly. The <Low> and <High > settings force the packet into one of two priority queues. Forcing a packet into a queue does not retag the packet.

Link: Indicates the port's current link status:

--: Indicates there is no device link or that the port is disabled.

10M/100M: Indicates the port's speed, either 10 Mbps or 100 Mbps.

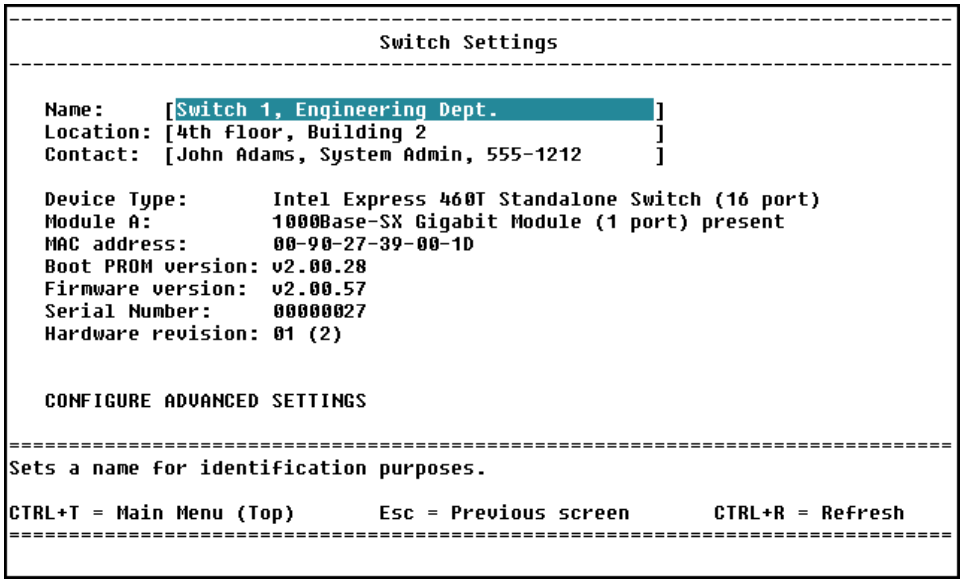
Full/Half: Indicates a device is connected at full-duplex or half-duplex.

IEEE/BackP: Indicates the type of flow control, either IEEE PAUSE frames or backpressure.

Partitioned: Indicates port was disabled due to a partition error.

Source mirror/Target mirror: Indicates the port being mirrored and where the data is being sent.

Switch Settings



Description

LOCATION

Main Menu

Configure Device

Switch Settings

Name: Assigns a name to the switch, up to 40 characters long.

Location: Assigns a location to the switch, up to 40 characters long.

Contact: Assigns a contact person or phone number to the switch, up to 40 characters long.

Device Type: Displays the manufacturer-assigned type of switch.

Module A: Displays any module and its type installed in the switch.

MAC address: The unique hardware address assigned by Intel.

NOTE

It's a good idea to write down both the firmware version and Boot PROM version, in case you need to contact Intel Customer Support.

Boot PROM version: Displays the version of the switch's boot code.

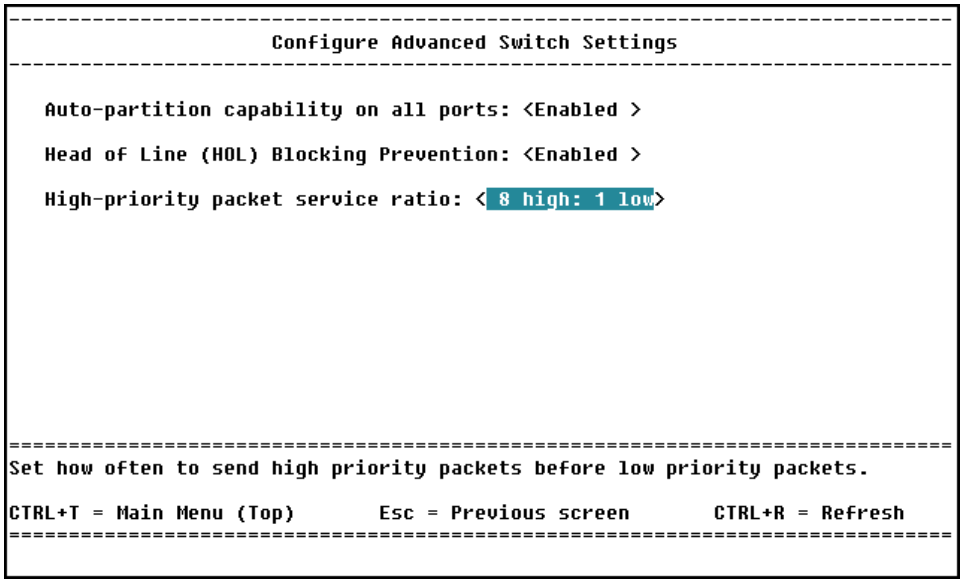
Firmware version: The version of the firmware installed on the switch. You can update this software on the Update Firmware and Configuration Files screen.

Serial Number: Displays the hardware serial number for the switch.

Hardware revision: Displays the version of the switch's printed circuit board.

CONFIGURE ADVANCED SETTINGS: Sets advanced switch settings like port auto-partition and Head of Line blocking.

Configure Advanced Switch Settings



LOCATION

Main Menu
- Configure Device
  - Switch Settings
    - Advanced Switch Settings

Description

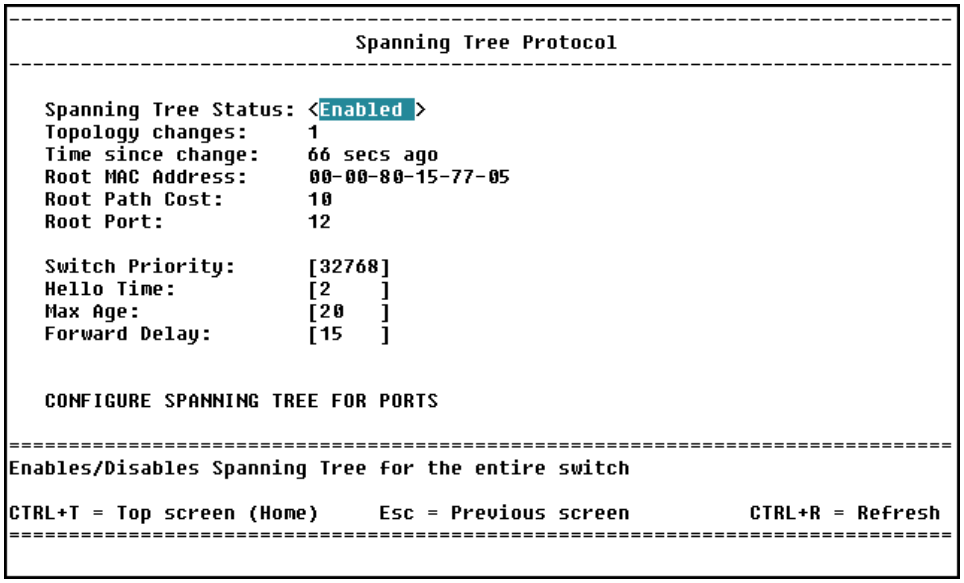
Auto-partition capability on all ports: If this option is enabled, the switch partitions the port when more than 61 consecutive collisions occur while receiving data. The first time the switch receives a good packet it unpartitions the port. If a port is partitioned the switch can transmit data over this port, but cannot receive data.

Head of Line (HOL) Blocking Prevention: If this option is enabled it prevents the forwarding of data to a port that is blocked. Normally, when the switch sends traffic to a port it goes to the port's transmit queue and is sent out. If the port's transmit queue is already busy trying to send out data, the switch places the waiting traffic in the buffer memory until the port is ready to send it out.

However, if the port's transmit queue remains full, the switch fills up more of the buffer with traffic waiting to be sent on that port. HOL blocking assumes that it is better to drop the traffic waiting in the buffer than to continue using more memory and impacting performance across all the ports.

High-priority packet service ratio: Determines how many high-priority packets the switch sends before sending a low-priority packet. For example, a ratio of 8 high:1 low means that the switch sends out eight high-priority packets before sending out one low-priority packet.

Configure Spanning Tree Protocol



LOCATION

Main Menu

Configure Device

Spanning Tree Protocol

Description

The IEEE 802.1D Spanning Tree Protocol specification is prevents loops in a network by allowing only one active path between any two network devices at a time.

Spanning Tree status: Use the Spacebar to enable or disable support for the Spanning Tree Protocol, where the entire switch is a bridge for which you can set spanning tree parameters. (**Note**: If you are running 802.1Q VLANs, spanning tree must be enabled and is turned on automatically by the switch.)

Topology changes: The number of times the spanning tree has changed its configuration.

Time since last change: The elapsed time (since the last switch reboot) since the spanning tree last changed its topology (the paths used to get through the network).

Root MAC address, Root path cost, Root port: Information used by the root bridge in the same spanning tree as the switch.

Switch Priority: Type a number from 0 to 65535 (default is 32768). The device with the lowest number becomes the root device (starting point for the spanning tree).

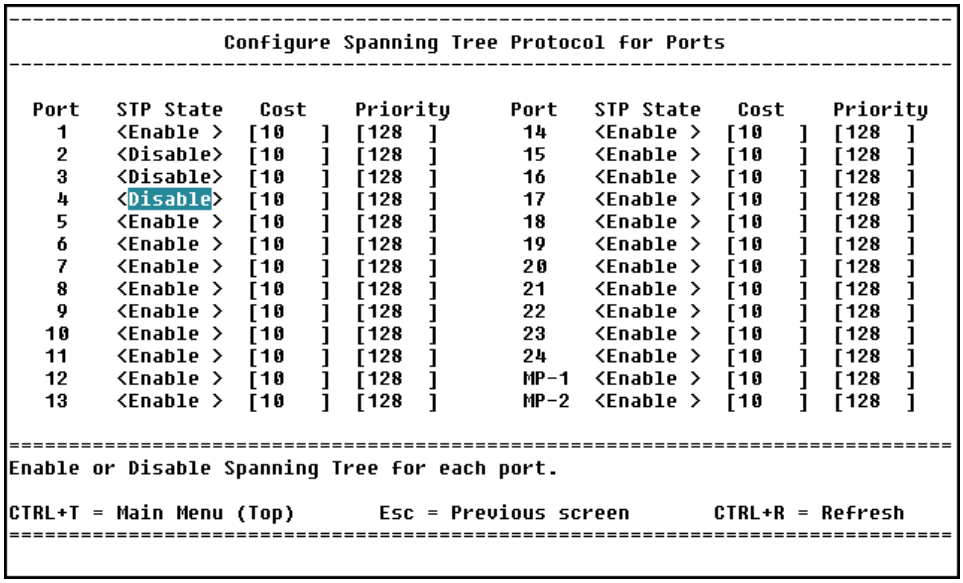
Hello Time: Type a number from 1 to 10 seconds (default is 2 seconds). This is the time between transmissions of configuration BPDUs (Bridge Protocol Data Units) when the switch is, or is attempting to become, the root in the spanning tree.

Max Age: Type a number from 6 to 40 seconds (default is 20 seconds). This is the maximum time that information from a configuration BPDU is used by the switch before it is discarded.

Forward Delay: Type a number from 4 to 30 seconds (default is 15 seconds). This is the amount of time between port states when the spanning tree is changing its status from blocking to forwarding.

CONFIGURE SPANNING TREE FOR PORTS: Takes you to the screen where you can set spanning tree values for individual ports.

Configure Spanning Tree for Ports



Description

LOCATION

Main Menu

Configure Device

Spanning Tree Protocol

Configure STP for ports

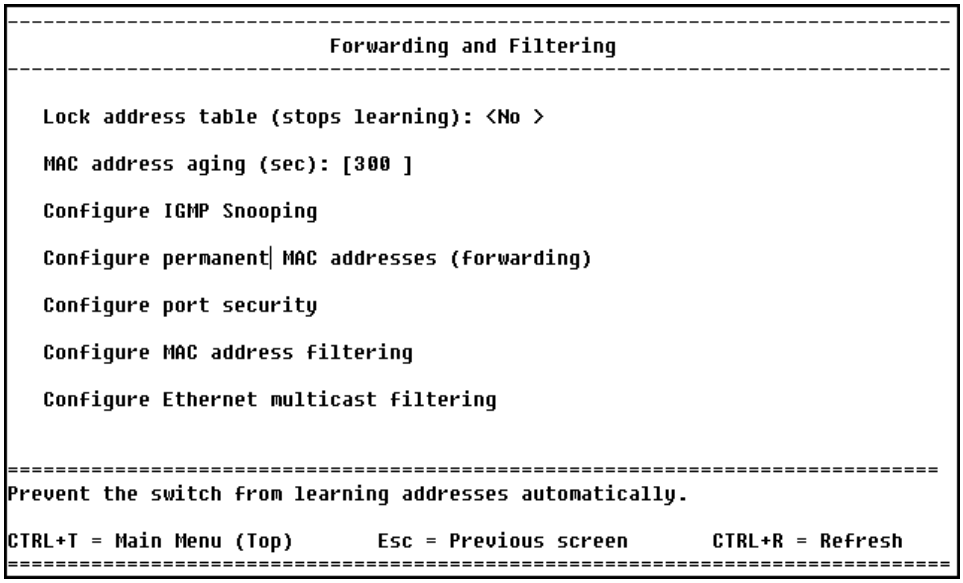
Port: Select the port you want to configure for spanning tree.

STP State: Use the Spacebar to enable or disable each port to be active in the spanning tree.

Cost: Type in a number from 1 to 65535 (default is 10). This value is used by the Spanning Tree Protocol to determine alternate routes in the network. The higher the cost of a port, the lower the chance it will be used to forward traffic. When possible, assign a port a low cost if it is connected to a fast network segment.

Priority: Type in a number from 0 to 255 (default is 128) to set the port's priority in the spanning tree. The higher the value, the lower the chance oit will be used as the root port. If two ports on the switch have the same priority value, the spanning tree uses the port with the lowest number. For example, the spanning tree would choose port 1 over port 4 if they both had the same priority setting.

Forwarding and Filtering



LOCATION

Main Menu

Configure Device

Forwarding and Filtering

Description

Lock address table: Use the Spacebar to toggle field values. <Yes> prevents the switch from learning new MAC addresses. Any existing addresses the switch has learned remain in the address table.

MAC address aging: Sets the time interval at which the switch scans its MAC address table to determine the age of entries.

Configure IGMP snooping: Sets Internet Group Management Protocols (IGMP) options for multimedia applications, such as desktop video conferencing, that use IP multicast addresses.

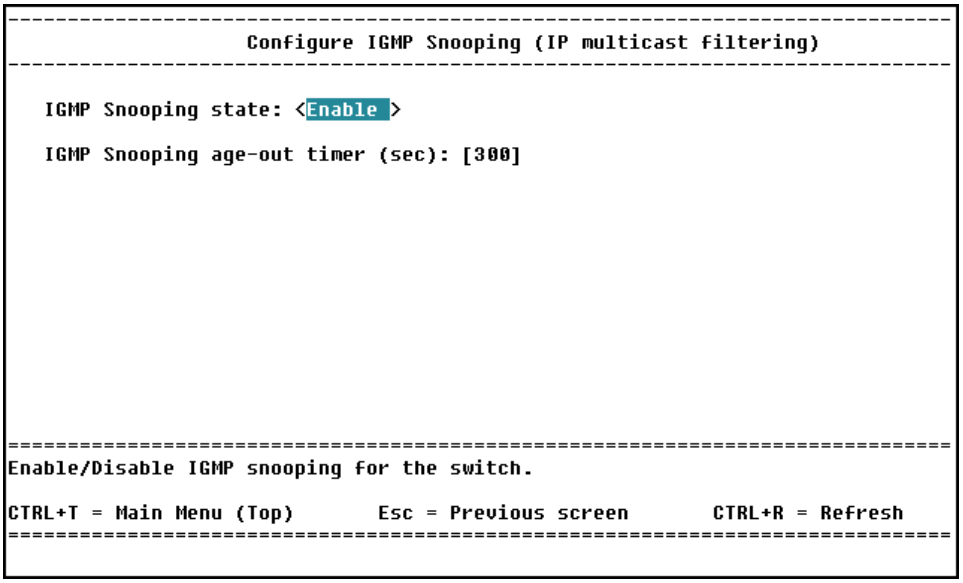
Configure static MAC addresses: Allows permanent mapping between a network device and a port.

Configure port security: Configures the switch to only allow the transmission of authorized traffic over a particular port.

Configure MAC address filtering: Allows the switch to drop traffic from a specific source.

Configure Ethernet multicast filtering: Blocks or forwards traffic over each port for Ethernet (MAC-based) multicast groups.

Configure IGMP Snooping



LOCATION

Main Menu
Configure Device
Forwarding and Filtering
IGMP Snooping

NOTE

If tag-based (IEEE 802.1Q) or port-based VLANs are currently running, you must enable IGMP snooping for each VLAN. The switch supports up to 12 VLAN IGMP snooping sessions.

Description

IGMP Snooping (Internet Group Management Protocol) allows the switch to forward multicast traffic intelligently. The switch “snoops” the IGMP query and report messages and forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

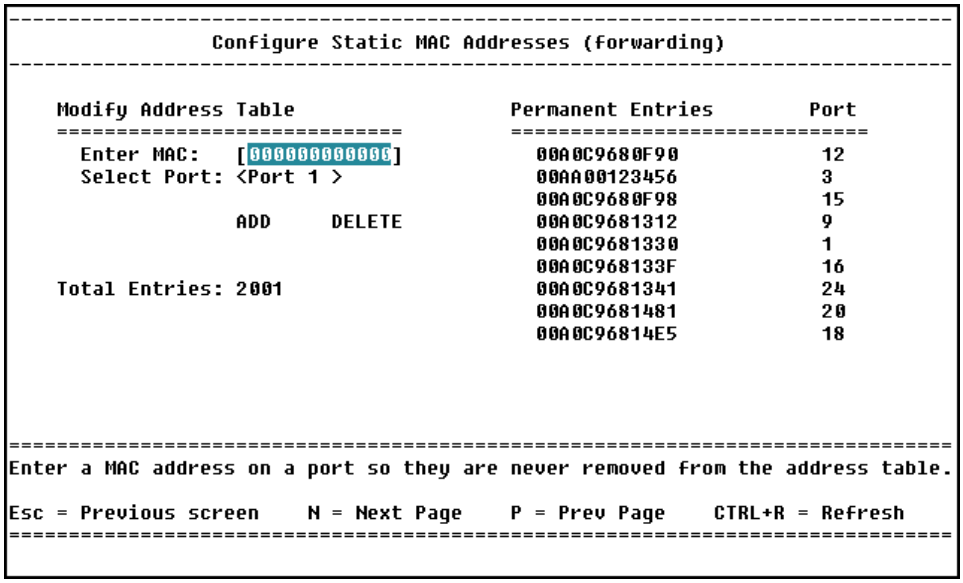
IGMP requires a router that learns about the presence of multicast groups on its subnets and keeps track of group membership. Remember that multicasting is not connection oriented, so data is delivered to the requesting hosts on a best-effort level of service.

VLAN Name (port-based or tag-based VLANs only): The VLAN for which IGMP snooping is enabled. You can also enable IGMP snooping for a VLAN in the Configure VLAN screen.

IGMP Snooping state: Use the Spacebar to enable or disable IGMP Snooping.

IGMP Snooping age-out timer: Specify the acceptable time (in seconds) between IGMP queries, starting when the switch last received an IGMP query from the multicast server. The default time is 300 seconds. A query allows the server to determine which network hosts are (or want to be) part of the IP multicast group, and are configured and ready to receive traffic for the given application.

Configure Static MAC Addresses



Description

LOCATION

Main Menu

Configure Device

Forwarding and Filtering

Static MAC Addresses

Static MAC addresses remain in the switch's address table, whether or not the device is physically connected to the switch. After you define a static MAC address, it remains in the switch's address table until you remove it.

Enter MAC: Type the MAC address you want to add to the address table.

VLAN or VLAN ID: When VLANs are active on the switch you can define static MAC addresses for each VLAN. If port-based VLANs are active press the Spacebar to select a VLAN. If tag-based VLANs are active type the VLAN ID that the static MAC address will be assigned to.

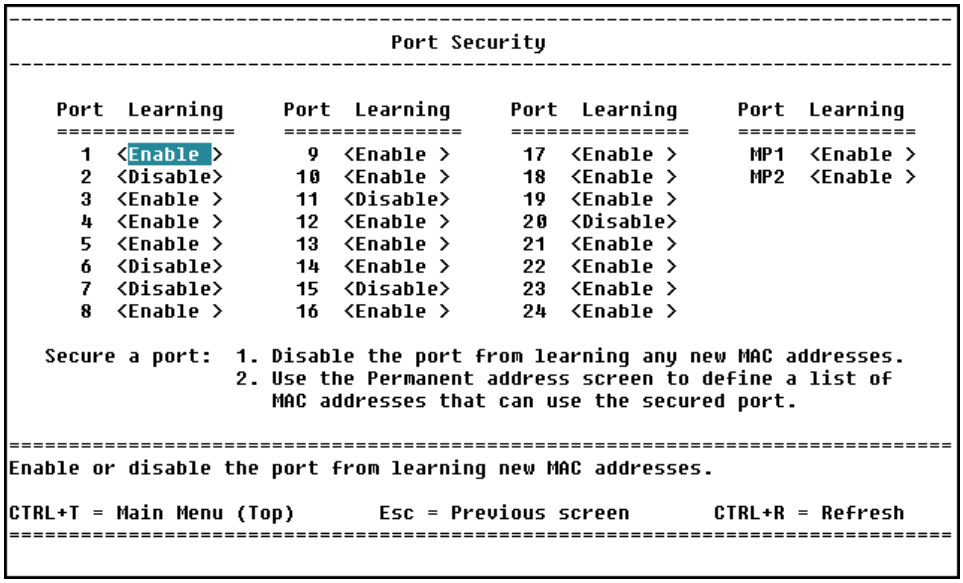
NOTE

If tag-based or port-based VLANs are currently running, you must assign each static MAC address to a specific VLAN.

Select Port: Use the Spacebar to select a port on the switch where the switch forwards traffic.

ADD/DELETE: Adds or removes a MAC address from the switch's table.

Configure Port Security



Description

Port security prevents unauthorized access of a port by “securing” a list of specific MAC addresses to a port. If the switch sees a MAC address that is not on the secured list, it discards the traffic. When port security is active, the switch forwards traffic from a single static address automatically learned by the switch, or from a list of static MAC addresses defined by the administrator.

LOCATION

Main Menu

Configure Device

Forwarding and Filtering

Configure Port Security

To set port security from Local Management

1 On the Configure Device screen, select Forwarding and Filtering.

2 Select Configure Port Security from this menu.

Then choose one of the following options.

Option 1 - Automatically use the first MAC address seen on the port: The switch remembers the first MAC address seen on the port and accepts traffic only from that MAC address. The secured port will not learn any new MAC addresses.

1 To set the switch to use the first MAC address seen on the port you are securing, in the MAC Learning column, press Spacebar until <Single> displays.

2 Click Submit.

NOTE

When you set port security to Disable, you must manually place static MAC addresses into the forwarding table. Only traffic from these static MAC addresses go through the port. Other traffic is dropped, and the port is still enabled.

When you set port security to Single, the first MAC address to hit that port is automatically placed into the forwarding table. Traffic from any other MAC address disabled the port.

Option 2 - Accept a list of user-defined static MAC addresses

1. In the MAC Learning column, press Spacebar until <Disabled> displays, to disable MAC learning for the ports you are securing.
2. Click Submit.

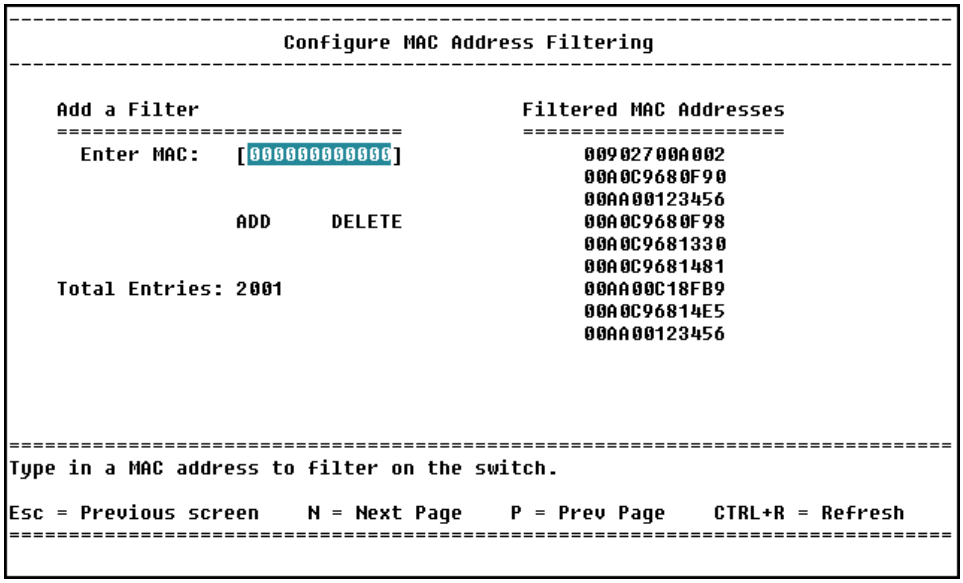
Then set static MAC addresses that can use the secured port.

1. Press Esc to move up a level and select the Configure Static MAC Addresses screen.
2. Click Add.
3. On the Add Static MAC Addresses screen, type a MAC address allowed to use the secured port.
4. In the Port Number box, select the port you are securing.
5. If port-based or tag-based (IEEE 802.1Q) VLANs are set up on the switch, the address will be used by a specific VLAN. Type the name or VID of the VLAN to use the MAC address.
6. Repeat steps 3-5 until you have added all MAC addresses allowed to use the secured port.
7. Click Submit.

To turn off port security

1. On the Configure Device screen, select Forwarding and Filtering.
2. Select Configure Port Security from this menu.
3. Select the port you want to disable security on. Press the Spacebar in the Learning field until <Enabled> appears, to disable security and allow the port to learn new MAC addresses.

Configure MAC Address Filtering



Description

MAC address filtering enables the switch to drop unwanted traffic. The switch drops traffic when it sees the specified MAC address in either the source address or destination address of the incoming packet. For example, if your network is congested because of high utilization from a specific MAC address, you can filter all traffic transmitted from that address and restore network flow while you troubleshoot the problem.

Enter MAC: Type in the MAC address you want to filter.

VLAN/VLAN ID: If VLANs are active on the switch you can set MAC address filtering for each VLAN. For port-based VLANs, press the Spacebar to select the name of VLAN. For tag-based VLANs, type the VLAN ID for the MAC address you want to filter.

ADD: Activates the filter and adds the MAC address to the list.

DELETE: Removes the filter for the specified MAC address.

LOCATION

Main Menu

Configure Device

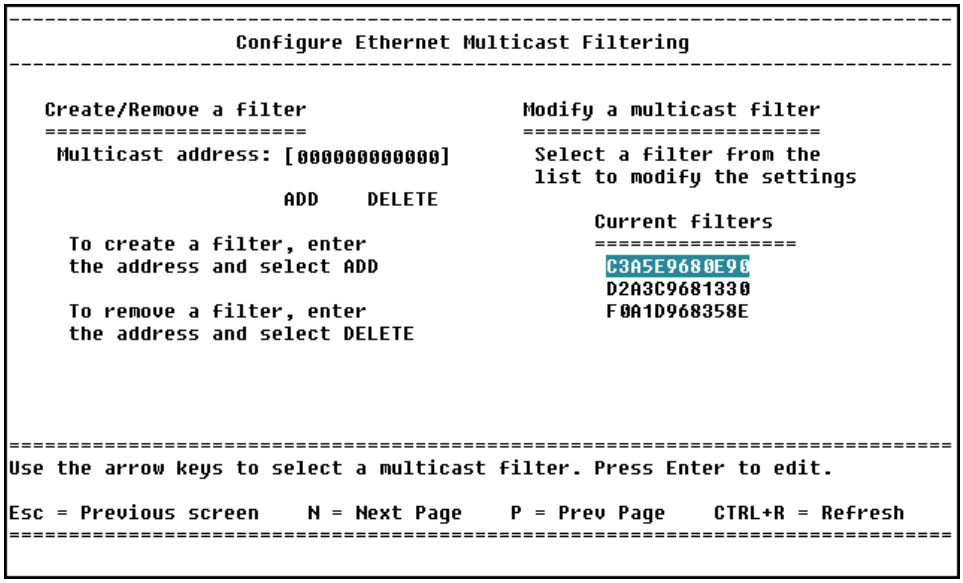
Forwarding and Filtering

MAC address Filtering

NOTE

If tag-based (IEEE 802.1Q) or port-based VLANs are currently running, you must assign each MAC address filter to a specific VLAN.

Configure Ethernet Multicast Filtering



Description

LOCATION

Main Menu
Configure Device
Forwarding and Filtering
Ethernet Multicast Filtering

Use Ethernet multicast filters to define which ports can receive multicast traffic from a specific multicast MAC address. This is similar to IGMP snooping, except you define everything manually.

VLAN/VLAN ID: If VLANs are active on the switch you can set Ethernet Multicast filtering for each VLAN. For port-based VLANs, press the Spacebar to select the name of VLAN. For tag-based VLANs, type the VLAN ID for the specified multicast address.

Multicast address: Type the MAC address you want to apply a filter to.

ADD: Activates the filter and adds the address to the list.

DELETE: Removes the filter for the specified address.

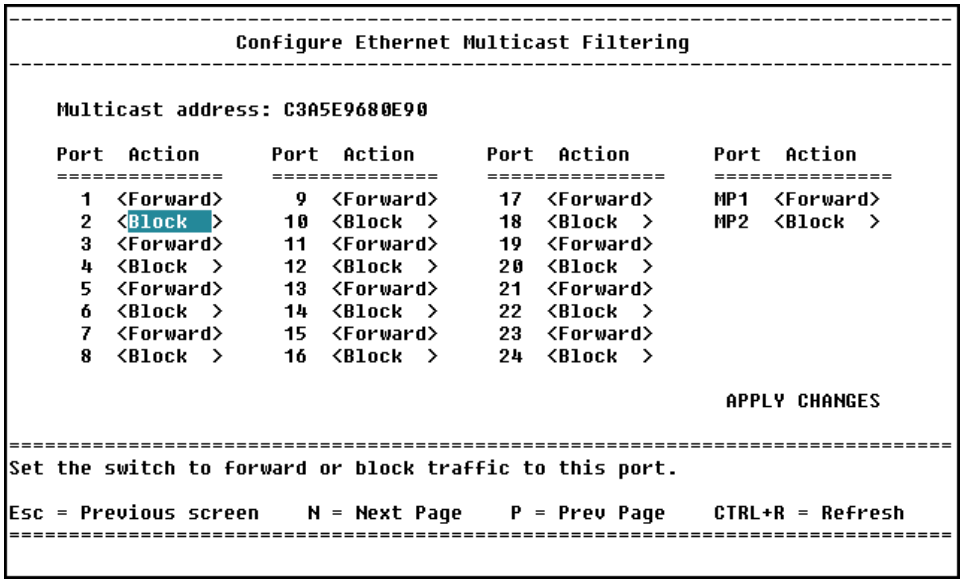
NOTE

If tag-based (IEEE 802.1Q) or port-based VLANs are currently running, you must assign each multicast filter to a specific VLAN.

To add or delete a multicast filter

1. In the Multicast address field, type a multicast address.
2. If the switch is running tag-based or port-based VLANs, select a VLAN to locate the filter.
3. Select ADD using the arrow keys and press Enter.
4. To remove a filter, type in the MAC address in the Multicast field, select DELETE, and press Enter.

Ethernet Multicast Filtering (Ports)



Description

LOCATION

Main Menu
- Configure Device
  - Forwarding and Filtering
    - Ethernet Multicast Filtering
      - Multicast Filters Per Port

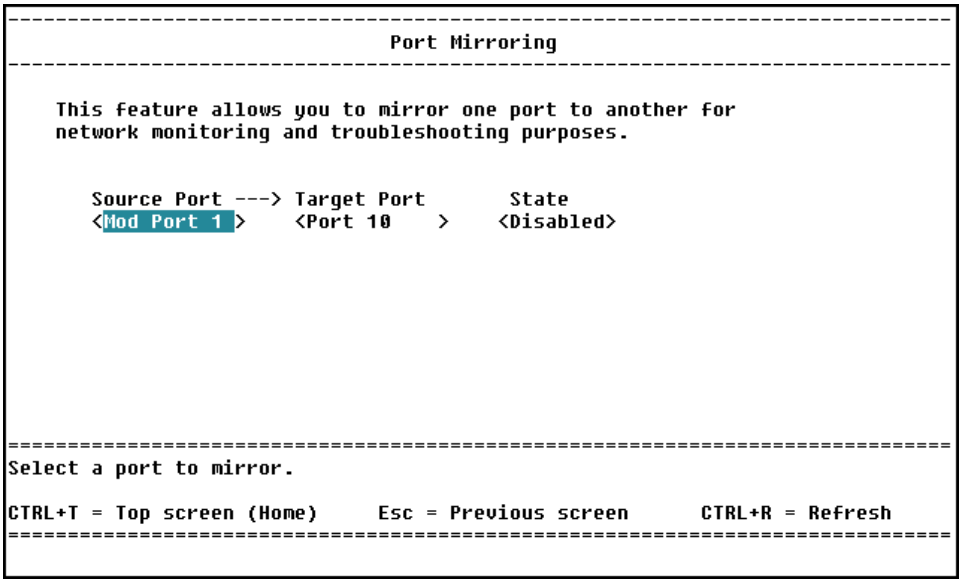
Action: Use the Spacebar to select whether to block or forward traffic to the selected port.

APPLY CHANGES: Applies the changes to the multicast filter after you have configured the ports.

To modify a multicast filter

1. On the right side of the Configure Ethernet Multicast Filter screen use the arrow keys to select an address from the list. Press Enter.
2. Decide which ports should receive the multicast traffic by using the Spacebar to set Forward or Block for each port.
3. Select APPLY CHANGES and press Enter. This activates the changes to the multicast filter and returns you to the previous screen.

Port Mirroring



Description

LOCATION

Main Menu

Configure Device

Port Mirroring

Port mirroring is a diagnostic tool you can use to send a copy of the good Ethernet frames transmitted or received on one port to another port. On the second port you can attach a protocol analyzer to capture and analyze the data without interfering with the client on the original port.

Source Port: Use the Spacebar to select the port whose traffic you want to mirror.

Target Port: Use the Spacebar to select a port to receive the mirrored traffic. It is a good idea to connect a protocol analyzer to this port.

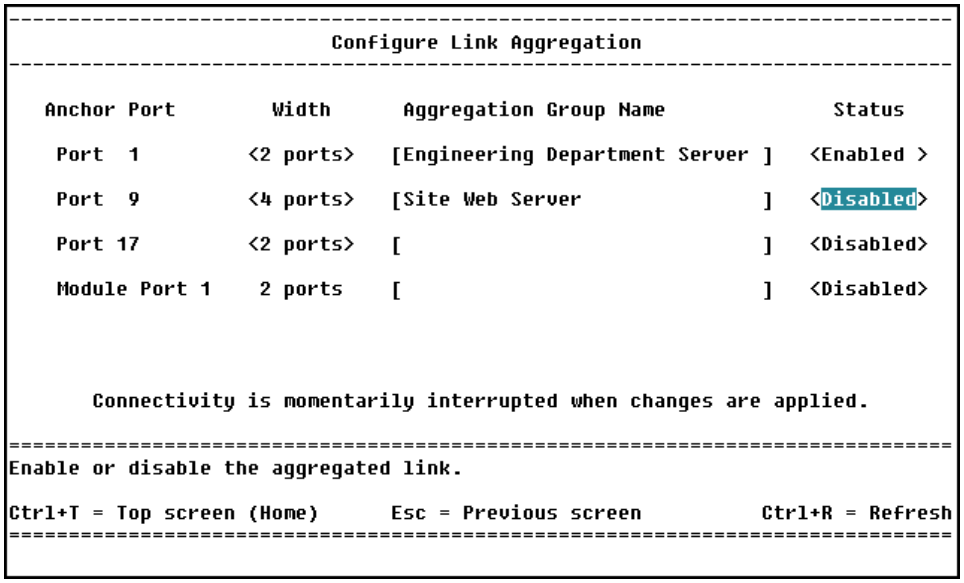
State: Use the Spacebar to enable or disable port mirror mirroring.

NOTE

Do not mirror traffic to a target port that is connected to network devices other than a protocol analyzer. Their behavior may be unpredictable.

If a port is part of an aggregated link, it cannot be configured as the target port for a port mirror. However, a port in an aggregated link can serve as the source port for a port mirror.

Link Aggregation



Description

LOCATION

Main Menu

Configure Device

Link Aggregation

Use link aggregation to combine ports on the switch to increase the available bandwidth and provide redundancy. All ports in the aggregated link take on the characteristics of the anchor port. For example, if you set the anchor port to 100 Mbps and full duplex, all the ports aggregated to that anchor port are 100 Mbps and full duplex.

Anchor Port: Shows the first port in the link aggregation.

Width: Use the Spacebar to set the total number of (consecutive) member ports in the aggregated link. The minimum number of ports for an aggregated link is two, and the maximum is eight, including the anchor port.

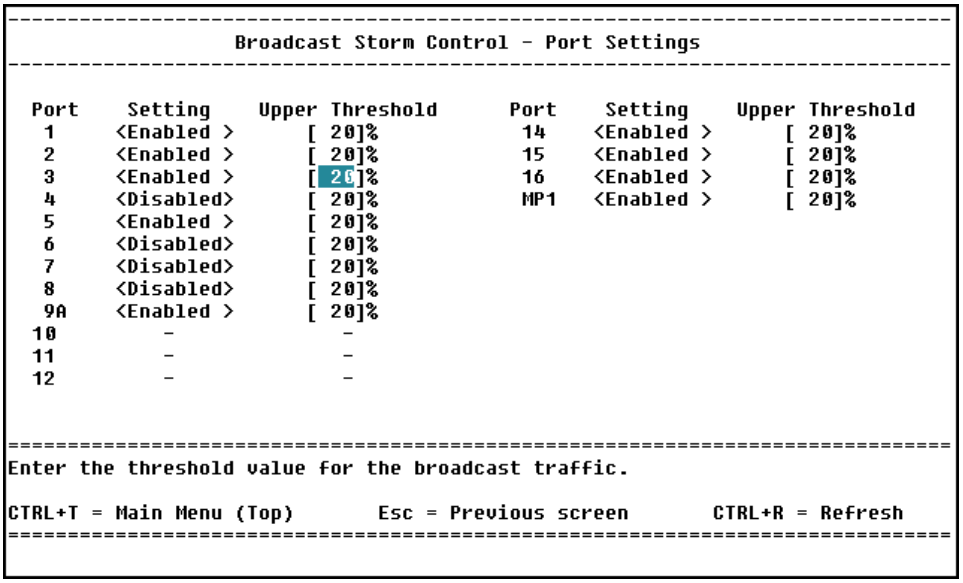
NOTE

All custom settings for a port (including VLAN membership) are lost when you add that port to a link aggregation.

Aggregation Group Name: Assigns a name to the aggregated links for management or identification purposes.

Status: Use the Spacebar to enable or disable the aggregated link.

Broadcast Storm Control



Description

LOCATION

Main Menu

Configure Device

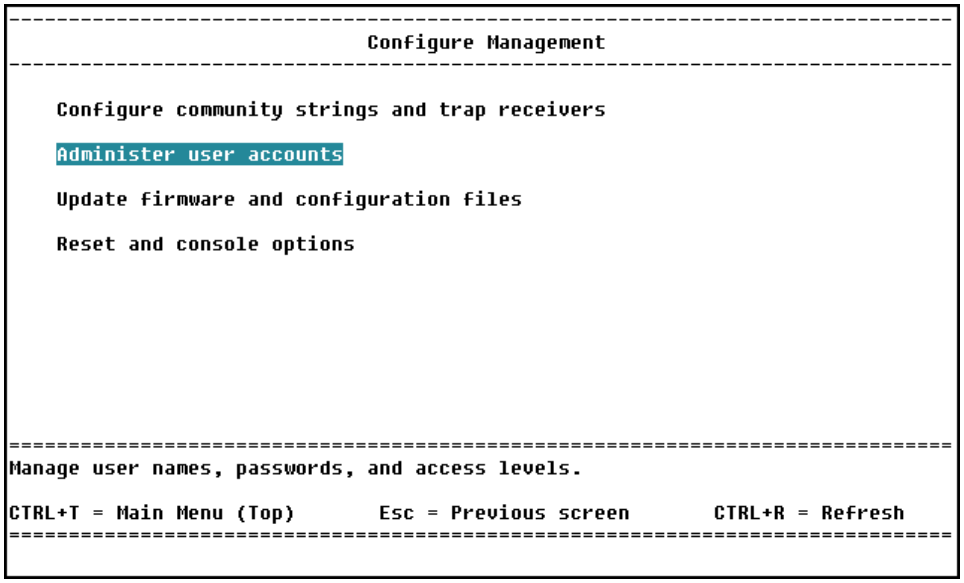
Broadcast Storm Control

Use this feature to filter out broadcasts from faulty devices and prevent them from degrading network performance.

Setting: Use the Spacebar to enable or disable broadcast storm control on this port.

Upper Threshold: Type a value from 1-20%. The default value is 20%. This control lets you set the threshold of broadcast traffic on a port (shown as a percentage of the port's total bandwidth) that will activate broadcast storm control. When the amount of broadcast traffic on the port exceeds the upper threshold, the port drops all broadcast traffic. When broadcast traffic falls below the threshold the switch automatically starts forwarding broadcast traffic again.

Configure Management Menu



LOCATION

Main Menu

Configure Management

Description

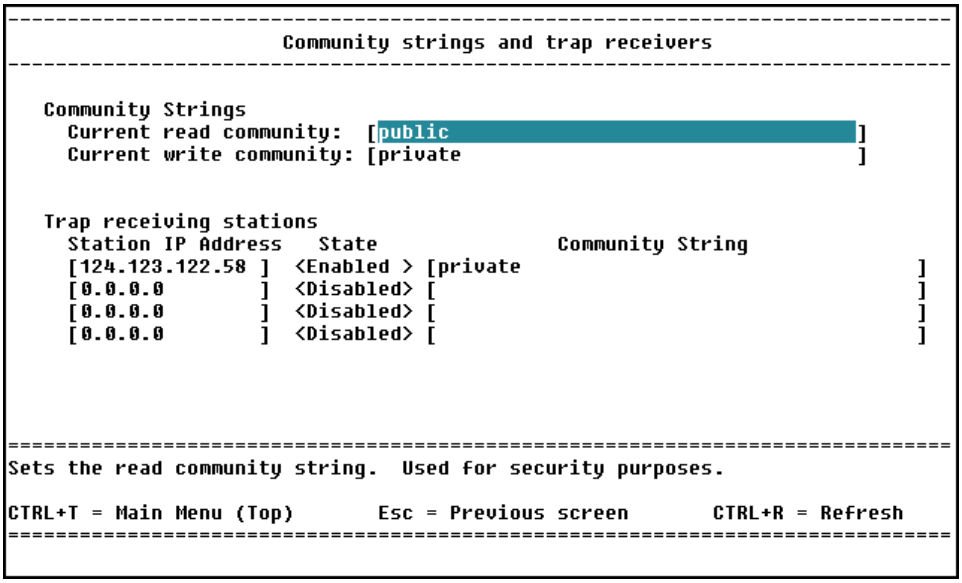
Configure community strings and trap receivers: Sets the switch's community strings and specify trap monitoring stations.

Administer user accounts: Configures user accounts. You can add or delete users, update passwords, and change a user's access rights.

Update firmware and configuration files: Configures the switch's internal software and specifies the location of configuration files.

Reset and console options: Reboot the switch or change the settings on the serial port. You can also set the switch back to its factory defaults.

Community Strings & Trap Receivers



Description

Use this screen to send alerts to PCs with SNMP management applications (such as OpenView*) installed.

Community Strings

Current read community: Sets a password for viewing (not changing) the switch configuration. The string you define here must match the read community string defined in an SNMP application. The default read community string is “public.”

Current write community: Sets a password for viewing and changing the switch configuration. The string you define here must match the write community string defined in an SNMP application. The default write community string is “private.”

Trap receiving stations: When an event occurs, the switch automatically alerts the SNMP management application by sending a trap to the SNMP management stations (for example, PCs) defined here.

Station IP address: The IP addresses of PCs with SNMP applications (such as Intel® Device View or LANDesk® Network Manager) installed.

State: Enables or disables sending of traps to the specified trap receiver.

Community string: Type a string for the trap that matches the community string defined in the SNMP management application. The default is “public.”

LOCATION

Main Menu

Configure Management

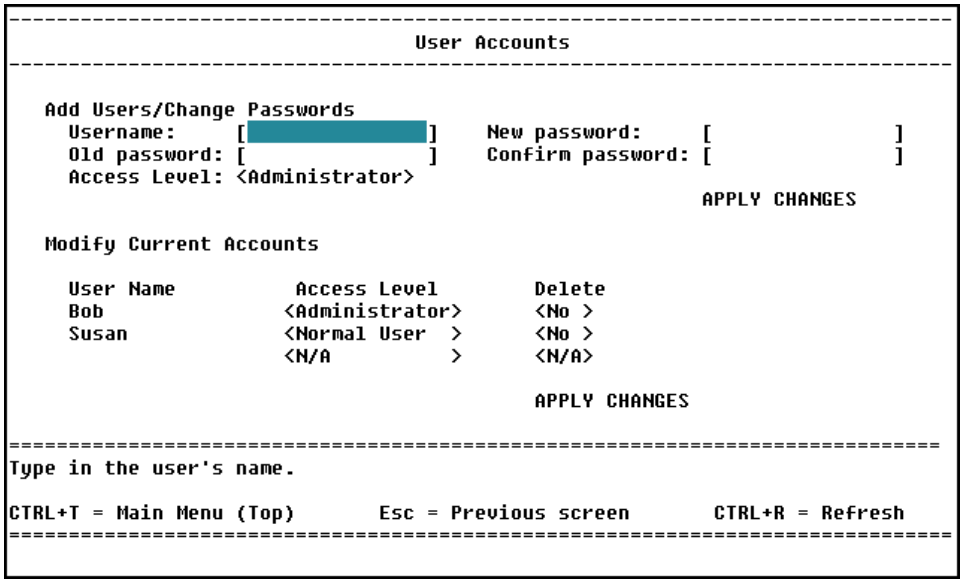
Community Strings and . . .

NOTE

These are the traps supported by the switch:

- Power to the switch was cycled or reset.
- Link, speed, or other status changes on a port.
- A port is partitioned.
- Authentication failure.
- A security violation occurs on the port.

User Accounts



Description

LOCATION

Main Menu

Configure Management

Administer User Accounts

Add Users/Change Passwords

Username: By default, no username is assigned. Usernames can consist of any character and can be up to fifteen characters long. You can define three usernames.

Old Password: Used when changing the password of a current user. If this is a new account, you can skip over to the **New Password** field. By default, no password is assigned.

New password: Sets a new password for accessing Local Management. The one you specify here is used the next time you reset the switch or log out and log in on Local Management. Passwords are case-sensitive and can be up to fifteen characters long.

Confirm new password: Verifies the entry in the **New password** field.

Access Level: Use the Spacebar to determine a user's access rights. Administrators can make any changes to Local Management. All other users (categorized under Normal user) can view information but cannot make changes. To change a user's access rights, see "Modify User Accounts."

APPLY CHANGES: Saves changes when adding users or changing passwords.

Modify User Accounts

Access Level: Use the Spacebar to change access rights for the user.

Delete: The default value is <No>. To delete an account, use the Spacebar to change the value to <Yes> .

APPLY CHANGES: Saves changes when modifying or deleting user accounts.

Managing User Accounts

As a system administrator, you can create up to three user accounts for managing the switch. You can also change the access rights for current users and delete user accounts. Make sure you always set up at least one Administrator account.

To create a user account

1. On the Main Menu, select Configure Management. Select Administer User Accounts and press Enter.
2. On the User Accounts screen, type the name of the new user in the Username field and press Enter.
3. Because this is a new user, press Tab to skip the Old password field and go to the New password field.
4. Type the password for the new user and press Enter. Passwords are case-sensitive and can be up to fifteen characters long.
5. To confirm the new password, retype it in the Confirm new password field. Press Enter.
6. Select the access rights for the new user by pressing the Spacebar.
7. To save the information, press Tab to select **SAVE CHANGE**S (below the Confirm new password field) and press Enter. The new account appears in the list under Modify User Accounts.

To change a password

1. On the Main Menu, select Configure Management and press Enter. Select Administer User Accounts and press Enter.
2. In the Username field, type the username of the account for which you want to change the password. Press Enter.
3. Type the current password in the Old password field and press Enter.
4. Type the new password in the New password field and press Enter.
5. To confirm the password, retype it in the Confirm new password field. Press Enter.
6. To save the new password, press Tab to select SAVE CHANGES (below the Confirm new password field) and press Enter.

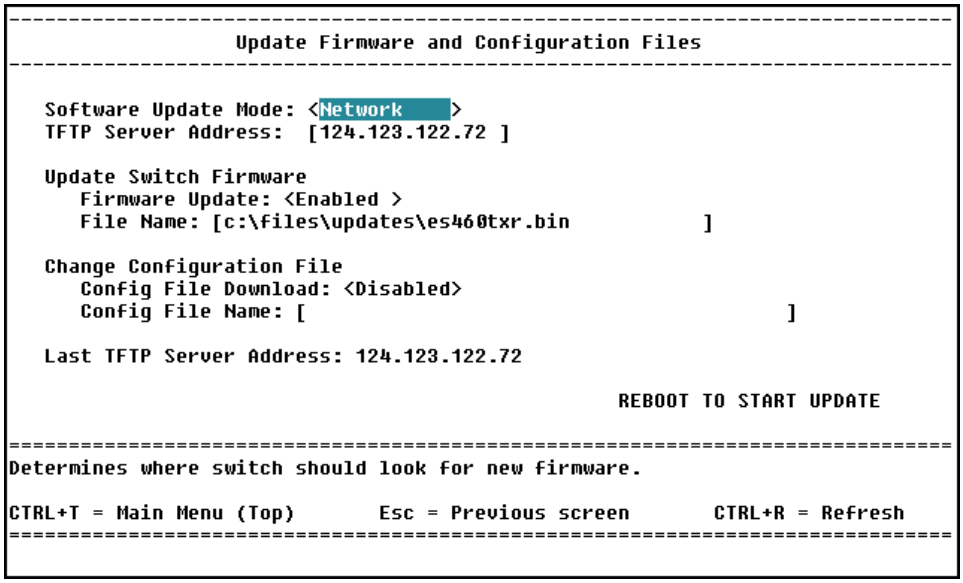
To modify a user's access level

1. On the Main Menu, select Configure Management, press Enter. Select Administer User Accounts and press Enter.
2. Under Access Level, press Tab to select the account to be modified .
3. Press the Spacebar to change the user's access rights. Users with Administrator access can make changes to the management configuration; users with Normal User access can view the configuration but cannot make changes.
4. To save changes, press Tab to select SAVE CHANGES at the bottom of the screen and press Enter.

To delete a user account

1. On the Main Menu, select Configure Management, press Enter. Select Administer User Accounts and press Enter.
2. Under Delete, select the account to be removed.
3. Press the Spacebar to toggle the field from <No> to <Yes>.
4. To remove the user account, press Tab to select SAVE CHANGES at the bottom of the screen and press Enter.

Update Firmware and Config Files



Description

LOCATION

Main Menu

Configure Management

Update Firmware and . . .

Software Update Mode: Use the Spacebar to select whether to update the switch's firmware over the network or through a SLIP connection.

TFTP Server Address: IP address of the server used as the TFTP server.

Update Switch Firmware:

Firmware Update: Use the Spacebar to enable or disable the firmware update. When enabled, the switch searches for the TFTP server specified at the top of the screen and attempts to update the firmware.

File Name: Path and filename of the firmware located on the server.

Change Configuration File:

Config File Download: Use the Spacebar to enable or disable the ability to download a configuration file. When this field is enabled, the switch searches the TFTP server specified at the top of the screen.

Config File Name: Path and filename of the configuration file located on the server.

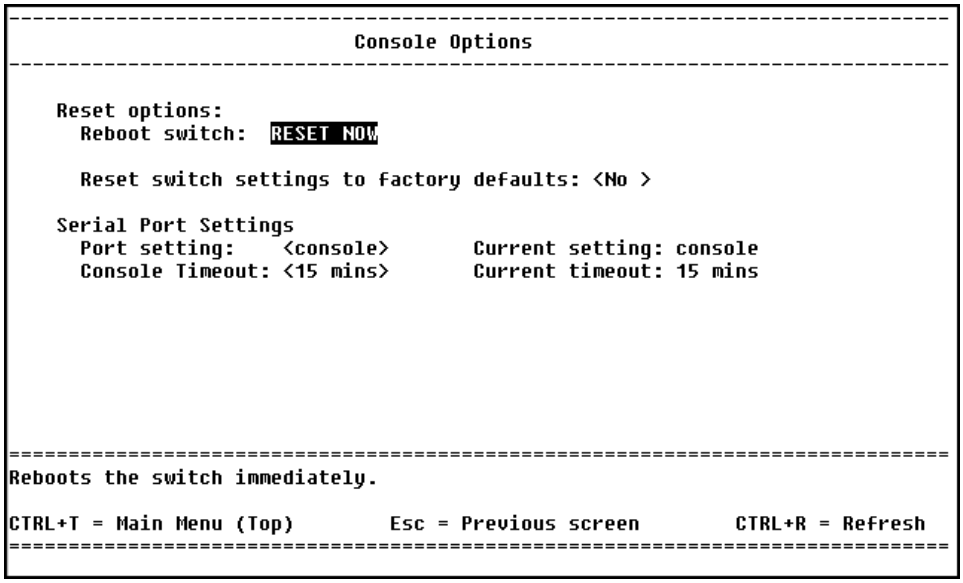
Last TFTP Server Address: Displays the IP address of the last TFTP server accessed by the switch.

REBOOT TO START UPDATE: Starts the update process. The switch reboots and downloads the specified file.

NOTE

Check the Intel Customer Support Web site for firmware updates to the Intel Express 460T Standalone Switch.

Reset and Console Options



LOCATION

Main Menu

Configure Management

Reset and Console Options

Description

Reset options

Reboot switch: Resets the switch. If you changed the IP configuration or login setting, the new settings take effect after you select this option.

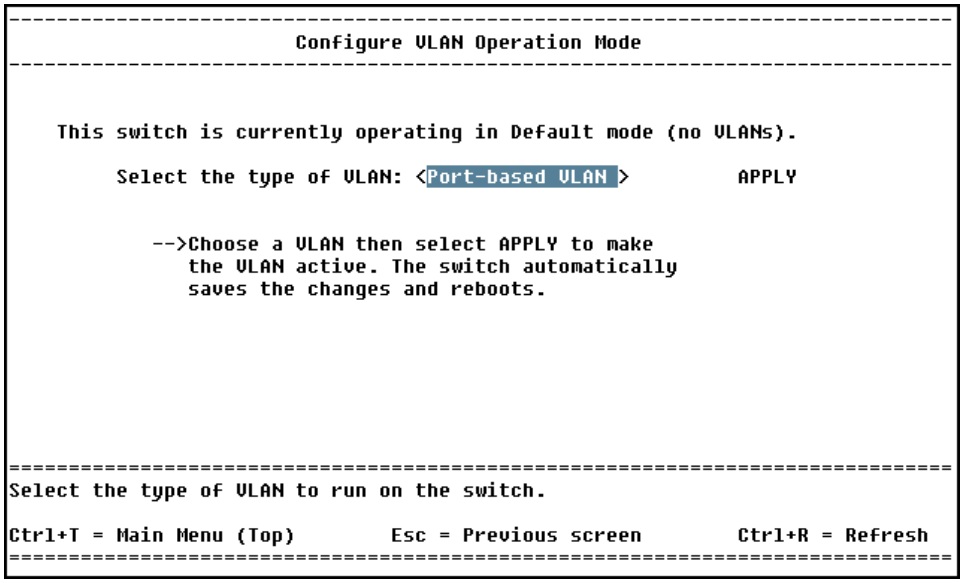
Reset switch settings to factory defaults: Clears any IP address or current changes and resets the switch back to its factory defaults. All counters are cleared and the switch starts sending BOOTP requests.

Serial Port Settings

Port Setting: Configures the switch's serial port for out-of-band (SLIP) management. Press the Spacebar to toggle the field from <Console> to <SLIP>. Settings take effect on the next reboot.

Console Timeout: Log a user out after a period of inactivity. Settings are from 0-90 minutes in 15-minute increments. A setting of <0 mins> means no timeout. The default is 60 minutes.

Configure VLAN Operation Mode



LOCATION

Main Menu

Configure VLAN
(if switch is in Default Mode)

Description

Use this screen to activate or change the type of VLAN operating on the switch. If there are no VLANs active on the switch, this is the first screen displayed when you select Configure VLAN from the Main Menu. By default, VLANs are not active on the 460T switch so they must be turned on before you can start configuring them.

The 460T switch supports operation of only one type of VLAN at a time. It supports multiple VLANs of the same type.

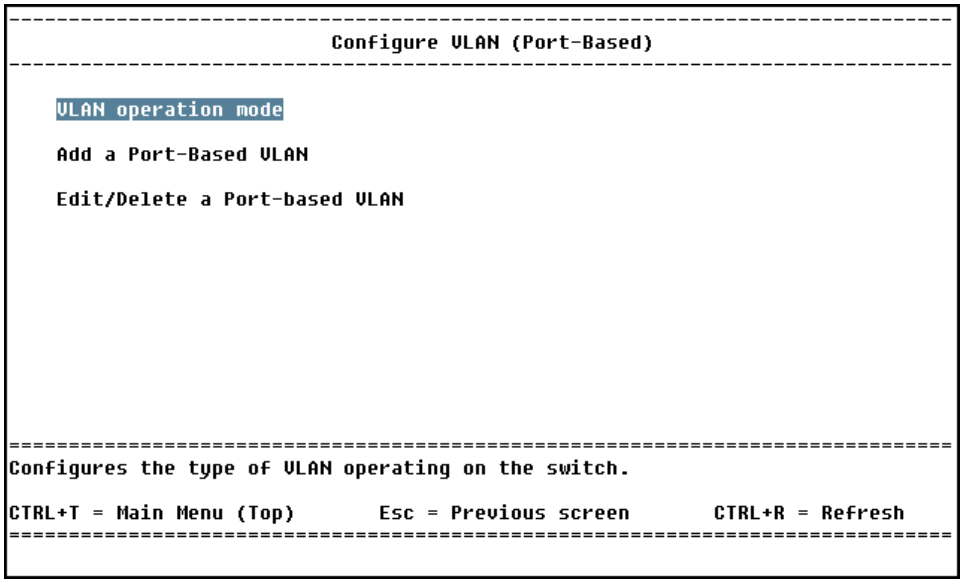
Select the type of VLAN: Press Spacebar to change the type of VLAN on the switch. The 460T Switch supports three types of VLANs: port-based, MAC-based, and IEEE 802.1Q (tag-based) VLANs.

APPLY: Activates the changes to the VLAN and reboots the switch. **Note:** To change between VLAN types, the switch must be rebooted.

To change VLAN modes

1. On the Main Menu, select Configure VLAN.
2. On the Configure VLAN menu, select VLAN Operation Mode.
3. Press Spacebar to change the type of VLAN on the switch. Press Enter.
4. Select the APPLY button and press Enter. This reboots the switch and changes the VLAN mode.

Port-based VLANs



Description

LOCATION

Main Menu

Configure VLAN

Port-based VLANs are the simplest type of VLAN. You can use a port-based VLAN to create multiple VLANs each with its own broadcast domain and member ports. For example, if port 5 is in VLAN_1 and port 10 is in VLAN_2 the two ports cannot communicate with each other even though they are part of the same switch. A port can be a member of only one port-based VLAN. Any port that is not a member of a user-defined VLAN is a member of the DEFAULT_VLAN.

NOTE

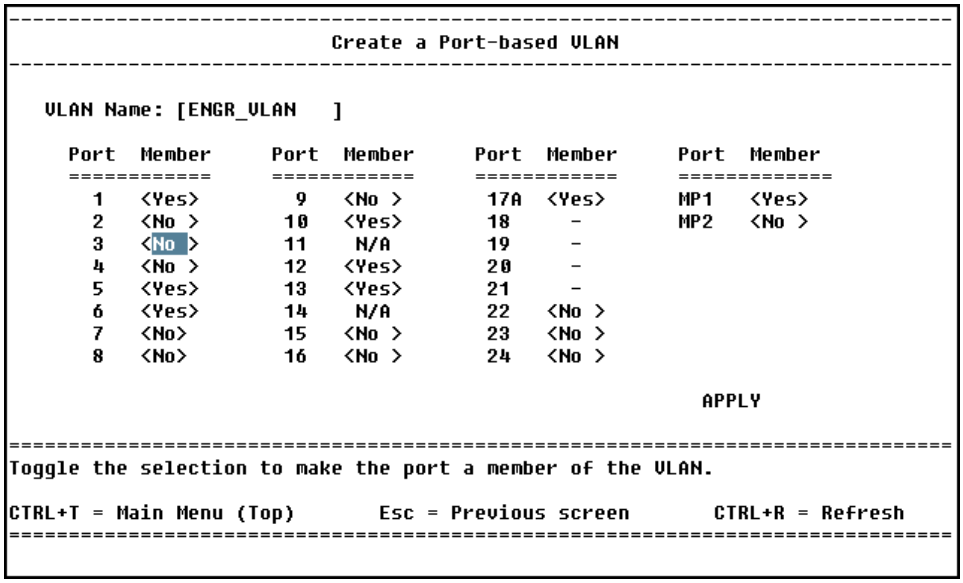
You can have up to 12 port-based VLANs on the switch.

VLAN Operation Mode: Changes the type of VLAN operating on the switch, or disables VLANs entirely.

Add a Port-Based VLAN: Creates a port-based VLAN and adds ports to the VLAN.

Edit/Delete a Port-Based VLAN: Selects a VLAN so you can change port membership in the VLAN, or removes a VLAN from the switch.

Add a Port-based VLAN



Description

LOCATION

Main Menu

Configure VLAN

Add a Port-based VLAN

VLAN Name: Assigns a name to the VLAN. Names can consist of any character (no spaces) and be up to 12 characters long. After a VLAN is created the name cannot be changed. If you want to change the name, you must delete the VLAN, create a new one, and assign the ports to the new VLAN.

Port: Selects the port you want to participate in the VLAN.

Member: Determines which ports will participate in the VLAN. Ports can be members of only one port-based VLAN. Press the Spacebar to toggle the field for the following options:

<Yes>	The port will be a member of the VLAN
<No >	The port will not be a member of the VLAN.
–	The port is part of an aggregated link.
N/A	The port is already participating in another VLAN. Ports can belong to only one VLAN.

APPLY: Creates the VLAN and activates the settings.

To create a port-based VLAN

1. On the main menu, select Configure VLAN. **Note**: Make sure the switch's current VLAN operation mode is set to port-based VLAN. If another type of VLAN is running, see "Configure VLAN Operation Mode" to change the VLAN operation mode.
2. Select Add a Port-based VLAN and press Enter.
3. Type a name for the new VLAN and press Enter.
4. Select ports to add to the VLAN by using the Spacebar to toggle the Member field to Yes.
5. Select the APPLY button and press Enter.

Edit/Delete a Port-based VLAN

LOCATION

Main Menu
- Configure VLAN
  - Edit/Delete a Port-based VLAN
    - Edit VLAN

```
------------------------------------------------------------------------------
                        Edit/Delete a Port-based VLAN
------------------------------------------------------------------------------

   Edit/Delete a VLAN              VLAN Name         Ports
  ====================            ========================
    Action: <Edit  >                DEFAULT_VLAN     10
                                    ENGR_VLAN         5
                                    MRKT_VLAN         7
   After choosing an                MFG_VLAN          2
   action, select a VLAN
   from the list at the
   right and press Enter.




==============================================================================
Choose to edit or delete a VLAN.

Esc = Previous screen    N = Next Page    P = Prev Page    CTRL+R = Refresh
==============================================================================
```

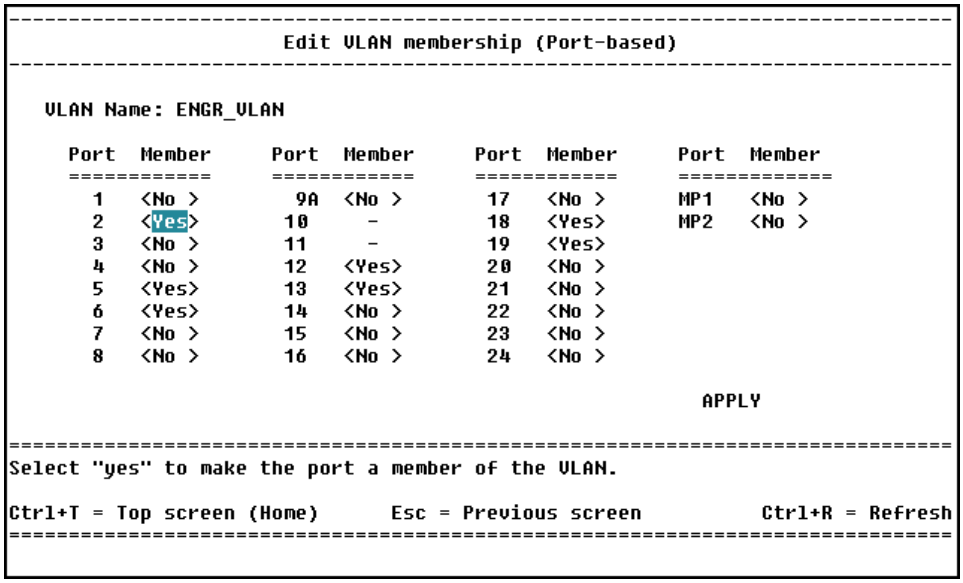
Description

Action: Specifies whether to delete a VLAN or to change its port membership. Press the Spacebar to toggle Edit or Delete and then use the Tab or → keys to select a VLAN and press Enter. The DEFAULT_VLAN cannot be deleted from the switch.

VLAN Name: The names of existing port-based VLANs.

Ports: Total number of member ports in the specified VLAN.

Change Port Membership in a VLAN



LOCATION

Main Menu

Configure VLAN

Edit/Delete a Port-based VLAN

Description

This screen is similar to the VLAN creation screen. You can change the membership status of ports within the VLAN but you cannot change the name of the VLAN.

VLAN Name: The name of the VLAN you are editing.

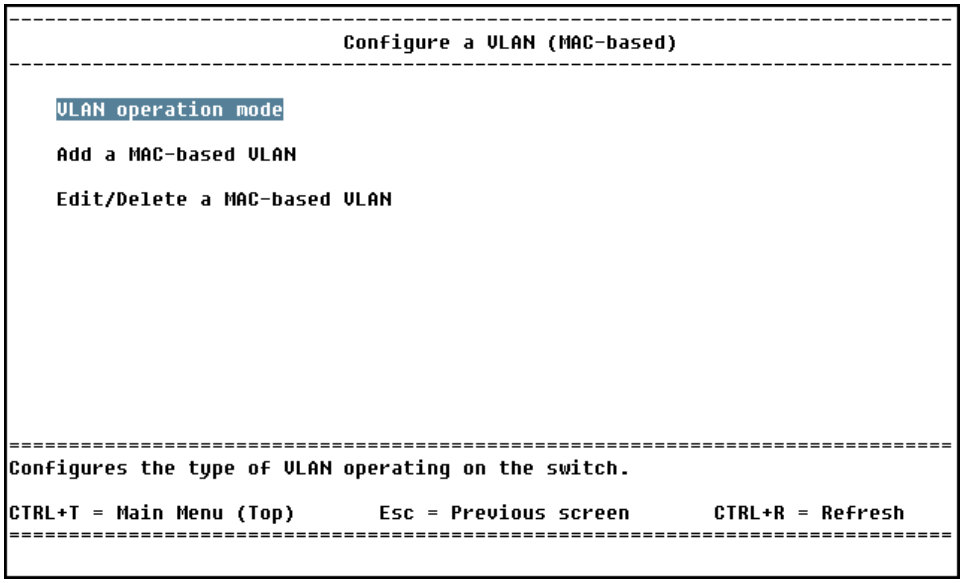
Port: Selects the port you want to participate in the VLAN.

Member: This option determines which ports will participate in the current VLAN. Ports can be members of only one VLAN. Press the Spacebar to toggle the field for the following options:

<Yes>	The port will be a member of the VLAN.
<No >	The port will not be a member of the VLAN.
–	The port is part of an aggregated link.
N/A	The port is already participating in another VLAN. Ports can belong to only one VLAN.

APPLY: Activates the settings.

MAC-Based VLANs



LOCATION

Main Menu

Configure VLAN

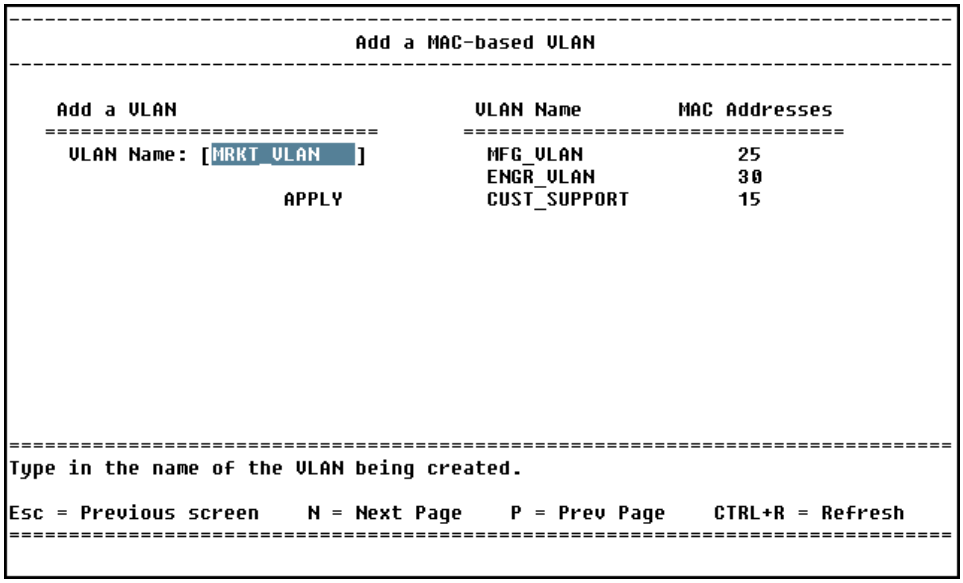
Description

VLAN Operation Mode: Changes the type of VLAN operating on the switch, or disables VLANs entirely.

Add a MAC-based VLAN: Creates a new MAC-based VLAN. You can create up to 12 MAC-based VLANs on the switch.

Edit/Delete a MAC-based VLAN: Adds member MAC addresses to a MAC-based VLAN, or deletes a VLAN entirely.

Add a MAC-Based VLAN



LOCATION

Main Menu

Configure VLAN

Add a MAC-based VLAN

Description

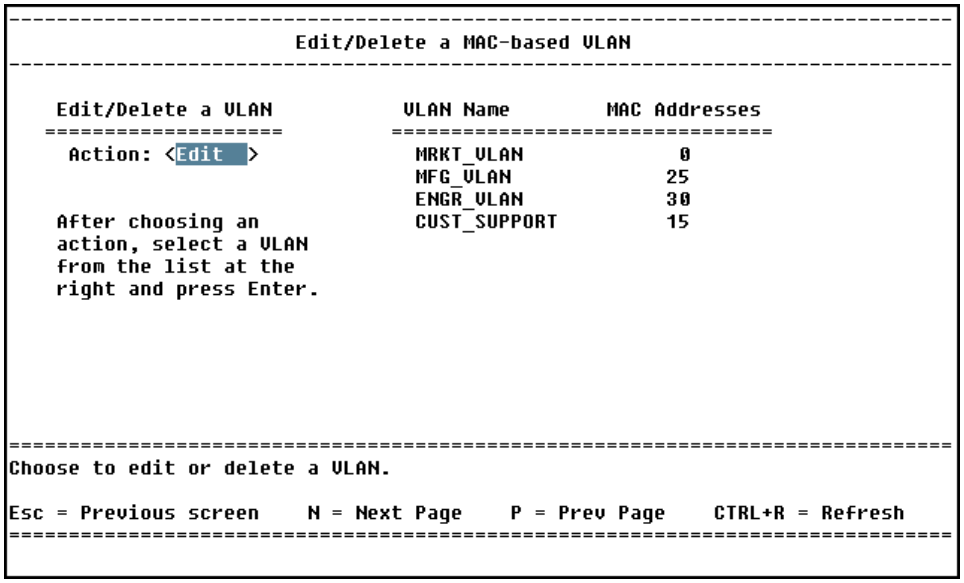
VLAN Name: Assigns a name to the VLAN. The name can consist of any character (no spaces) and be up to 12 characters long. After a VLAN is created the name cannot be changed. If you want to change the name you must delete the VLAN, create a new one, and assign the addresses to the new VLAN.

VLAN Name: The name of existing MAC-based VLANs.

MAC Addresses: Total number of MAC addresses that belong to the VLAN. The switch supports up to 256 address entries per VLAN.

APPLY: Creates the VLAN.

Edit/Delete a MAC-Based VLAN



LOCATION

Main Menu

Configure VLAN

Edit/Delete a MAC-based VLAN

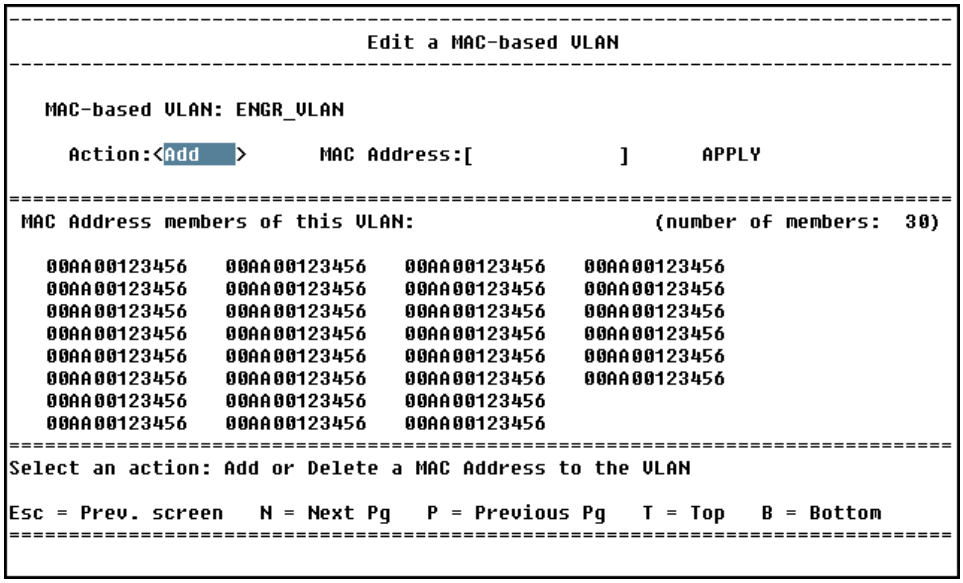
Description

Action: Specify whether to edit a VLAN's membership or delete the VLAN entirely. Use the Spacebar to toggle <Edit> to add/remove member MAC addresses or <Delete> to remove a VLAN from the switch.

VLAN Name: The names of MAC-based VLANs active on the switch.

MAC Addresses: Total number of MAC addresses in the specified VLAN.

Edit a MAC-based VLAN



LOCATION

Main Menu
- Configure VLAN
  - Edit/Delete a Mac-based VLAN
    - Edit a MAC-based VLAN

Description

Use this screen to add or remove member MAC addresses from a MAC-based VLAN.

Action: Use the Spacebar to toggle the field and specify whether to add a new MAC address to the VLAN or to remove an address that is currently in the VLAN.

MAC Address: Type the MAC address (without hyphens) of a device such as a PC or server to be a VLAN member.

APPLY: Makes changes to the VLAN's membership.

To create a MAC-Based VLAN

When creating a MAC-based VLAN, unlike port-based VLANs, you must first create the VLAN and then add members to the VLAN.

1. Select Configure VLAN.

   Note: Make sure the switch's current VLAN operation mode is set to MAC-based VLAN. If another type of VLAN is running, see "Configure VLAN Operation Mode" to change the VLAN operation mode.
2. Select Add a MAC-based VLAN and press Enter.
3. Type a name for the new VLAN and press Enter.
4. Select the APPLY button and press Enter. The new VLAN appears in the list on the left.

To add MAC addresses to a MAC-based VLAN

1. On the Configure VLAN menu select Edit/Delete a MAC-based VLAN and press Enter.
2. Set the Action toggle to Edit using the Spacebar and press Enter.
3. Select a VLAN from the list using the arrow keys and press Enter.
4. On the Edit MAC-based VLAN screen, set the Action toggle to Add using the Spacebar and press Enter.
5. Type the MAC address you want to add to the VLAN.
6. Select the APPLY button and press Enter. The new MAC address appears in the list below.

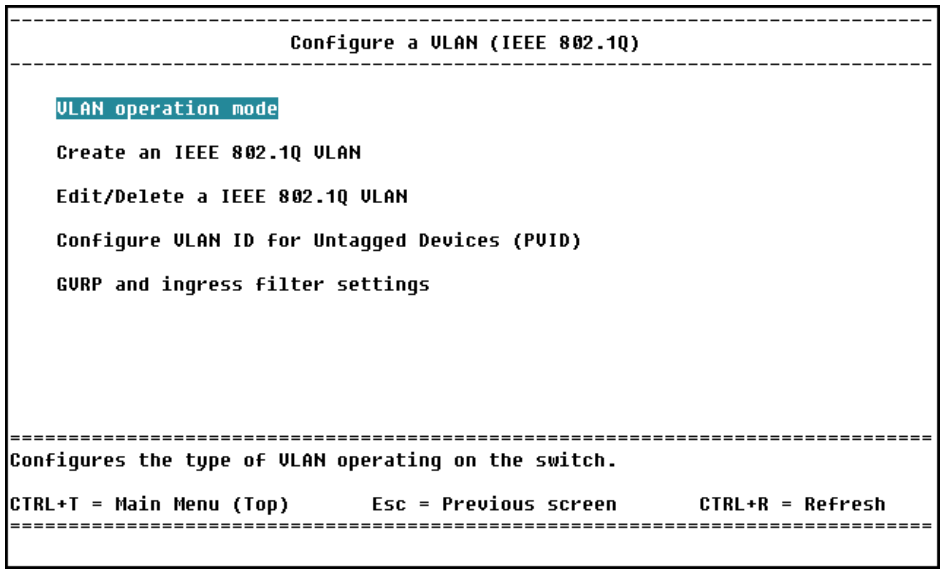
To remove a MAC-based VLAN

1. On the Configure VLAN menu select Edit/Delete a MAC-based VLAN and press Enter.
2. Set the Action toggle to Delete using the Spacebar and press Enter.
3. Select a VLAN from the list using the arrow keys and press Enter. The VLAN is removed from the list.

Security considerations

MAC-based VLANs, as designed on the 460T switch, are meant to limit broadcast and multicast traffic over the network. The switch relies on limiting broadcast traffic to constrain network visibility of network applications (such as TCP/IP) that rely on broadcasts (such as ARP) for station discovery. The 460T MAC-based VLANs are not intended to be a secure solution. For secure VLANs use either port-based or IEEE 802.1Q-based VLANs.

Configure 802.1Q VLANs



Description

LOCATION

Main Menu

Configure VLAN

VLAN operation mode: Change the type of VLAN operating on the switch, or disable VLANs entirely.

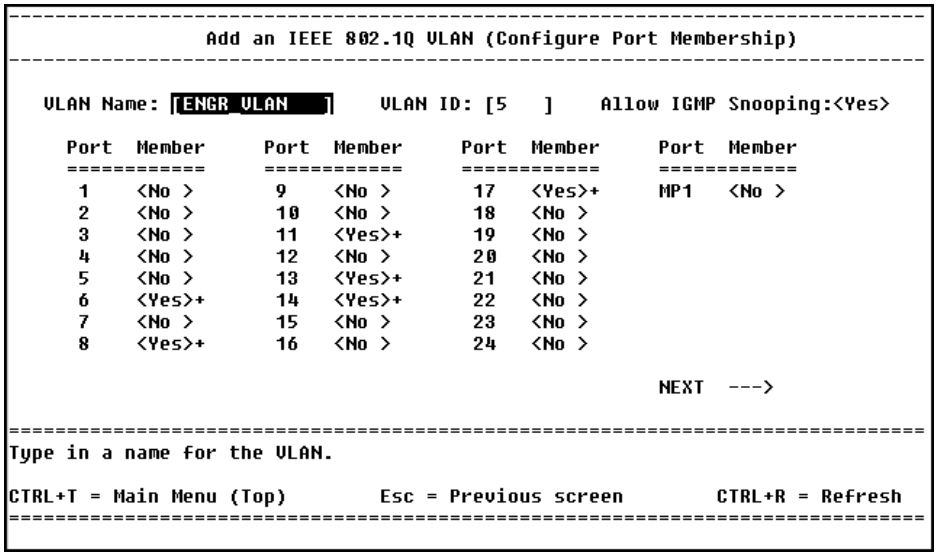
Create an IEEE 802.1Q VLAN: Create a new 802.1Q VLAN and add ports to the VLAN.

Edit/Delete an IEEE 802.1Q VLAN: Change port membership of an existing VLAN, or remove a VLAN from the switch.

Configure VLAN ID for untagged devices (PVID): Assign a VLAN to incoming packets without a VID.

GVRP and ingress filter settings: Set port-level options for dynamic VLAN creation and packet filtering by VLAN.

Add an IEEE 802.1Q VLAN (Configure Port Membership)



LOCATION

Main Menu

Configure VLAN

Create an 802.1Q VLAN

Description

VLAN Name: Assign a name to the VLAN. The name can consist of any character (no spaces) and be up to 12 characters long. Once a VLAN is created the name cannot be changed.

VLAN ID: Assign a unique ID number to the VLAN. This number is used to identify all packets belonging to that VLAN. Type a number from 2 to 4094. The DEFAULT_VLAN (created when you select a VLAN operation mode) is assigned a VID of 1.

Allow IGMP Snooping: Press the Spacebar to determine if the switch will perform IGMP snooping on this VLAN. Up to12 IGMP snooping sessions are allowed.

Member: Identifies which ports will participate in the VLAN. Press the Spacebar to toggle the field for the following options:

<Yes> The port is a member of the VLAN

<No > The port is not a member of the VLAN.

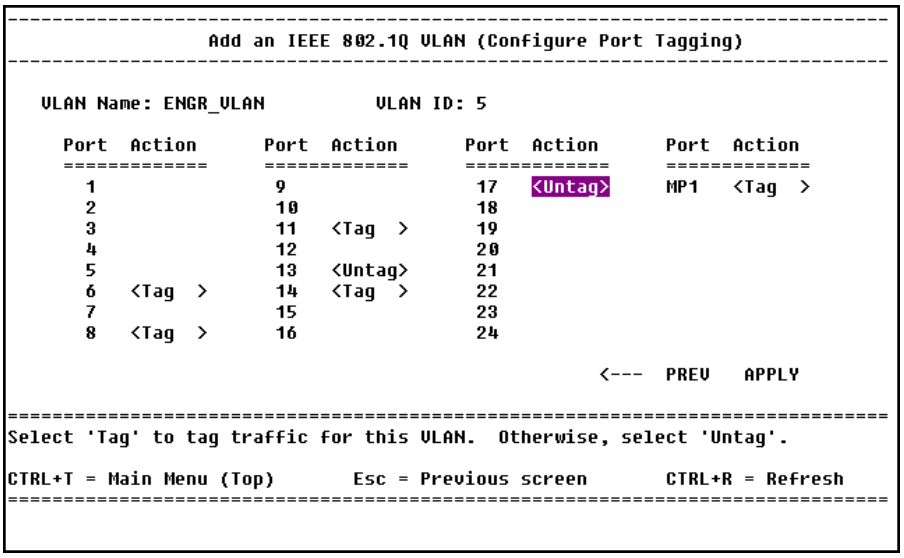
– The port is part of an aggregated link.

NEXT: Accesses the Add an 802.1Q VLAN (Configure Port Tagging) screen.

NOTE

A '+' next to the Member toggle indicates that port is a member of more than one VLAN.

Add an IEEE 802.1Q VLAN (Configure Port Tagging)



LOCATION

Main Menu
- Configure VLAN
  - Create an 802.1Q VLAN
    - Add an 802.1Q VLAN...

Description

VLAN Name: Displays the VLAN name assigned on the Add an IEEE 802.1Q VLAN (Configure Port Membership) screen.

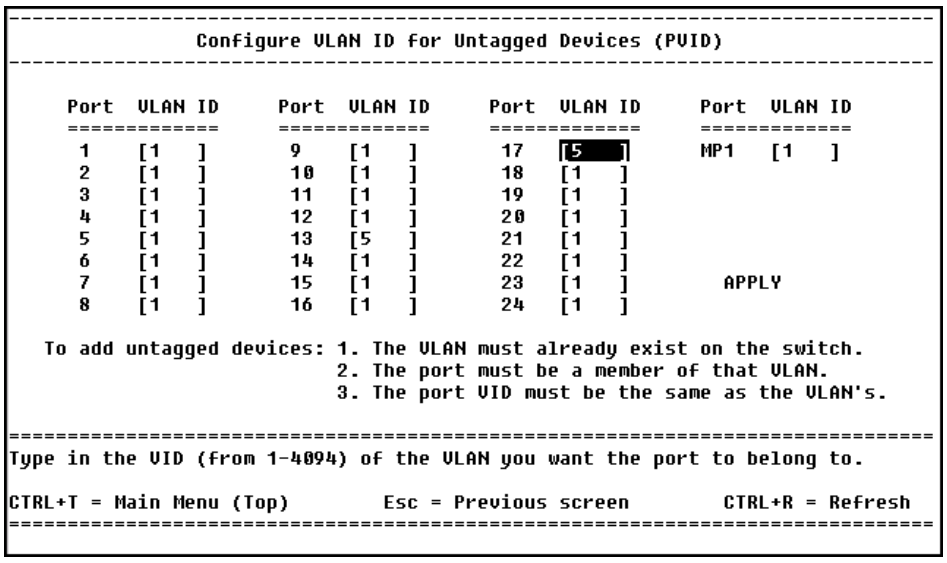
VLAN ID: Displays the VLAN ID assigned on the Add an IEEE 802.1Q VLAN screen.

Action: Indicates whether the device connected to this port supports tagging (press Spacebar).

PREV: Returns you to the Add an IEEE 802.1Q VLAN (Configure Port Membership) screen.

APPLY: Returns you to the Configure 802.1Q VLANs screen.

Configure PVID for Untagged/Priority Traffic



LOCATION

Main Menu

Configure VLAN

Configure PVID for...

Description

Use this screen to set up the switch to manage incoming packets that do not contain IEEE 802.1Q VLAN tags or priority-tagged traffic (packets with a VID of zero). This applies to ingress traffic; it does not apply to outbound traffic.

Untagged traffic is ordinarily assigned to VLAN 1 (the DEFAULT_VLAN), which includes all ports on the switch. However, if you want to send untagged traffic on a port other than the default VLAN, you can assign a different PVID.

For example, if you set a port's PVID to 5, all untagged traffic on the port is assigned to VID 5.

PVID: Sets the PVID for untagged devices. This is used for incoming traffic from an untagged device.

APPLY: Applies changes on this page.

Configuring 802.1Q VLANs

NOTE

You must determine which devices on your network support tag-based VLANs and which do not, before you start this procedure.

Setting up a 802.1Q VLAN is a two-step process: create a VLAN on the switch, assigning member ports to it, then set up tagging properly for your attached devices. For those devices that don't support tagging an extra configuration step is required.

Step 1: Create an 802.1Q VLAN and add ports

1. On the Main Menu, select Configure VLAN.

   Note: Make sure the switch's current VLAN operation mode is set to IEEE 802.1Q VLAN. For information about changing the VLAN operation mode, see "Configure VLAN Operation Mode".
2. Select Create an IEEE 802.1Q VLAN and press Enter.
3. Type a name for the new VLAN (no spaces) and press Enter.
4. Type a VLAN ID and press Enter. The ID number can be any number from 2 to 4094.
5. Determine if you want to allow IGMP Snooping on this VLAN. This is important because the switch can support more 802.1Q VLANs than the maximum of 12 IGMP Snooping sessions available.
6. Select ports to add to the VLAN. Use Spacebar to toggle the Member field to Yes.
7. Select the NEXT button and press Enter.

Step 2: Configure tagging for member ports

If the device on a particular port does not support tags, configure that port as untagged. Configuring a device as untagged ensures that the switch removes tags from packets before they leave the switch for the device. If you configure a port as untagged, proceed to step 3 (Configure VLAN for untagged devices) when you are finished with this step.

1. Press Spacebar to select Tag or Untag for each port that is a member of the VLAN.
2. Select the DONE button and press Enter.

If you configured any of the ports in the VLAN as Untagged, proceed to step 3 to configure ports for untagged devices and associate those ports with a PVID (port VLAN ID).

Step 3: Configure VLAN for untagged devices

Even if the device attached to the switch doesn't support 802.1Q tags it is still possible for the device to participate in the VLAN. When communicating with untagged devices the switch:

Determines how to forward untagged traffic. For untagged traffic, the switch assigns a default VID to the incoming traffic from the untagged device. Normally, all untagged traffic received on the switch is assigned a VLAN ID=1 or the DEFAULT_VLAN. You can change this PVID to the VID of the VLAN you want the port to use.

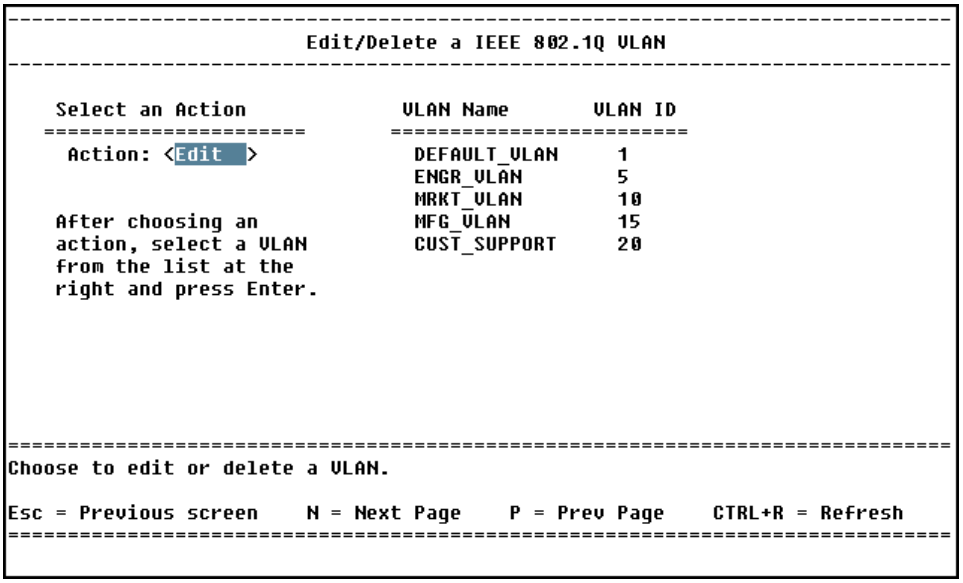
Strips 802.1Q tags before sending traffic to the untagged device. When the switch needs to send traffic from a port to an untagged device, it strips the 802.1Q tag. Otherwise the untagged device may not understand how to process the VID tag.

To add an untagged device to an 802.1Q VLAN

1. Ensure that the port is a member of the VLAN. Follow the procedure in step 1, "Create an 802.1Q VLAN and add ports," to add a port to an 802.1QVLAN.
2. On the Configure VLAN menu, select Configure VLAN ID for untagged and priority-tagged traffic and press Enter.
3. Select the port where the untagged device is connected. For example, port 7.
4. Type the VID of the VLAN you want the port to belong to and press Enter. This is the same ID number you entered in step 1.
5. Select APPLY and press Enter to activate the changes.

By specifying a VID you set the switch to assign a particular VID to any incoming traffic it receives on that port.

Edit/Delete 802.1Q VLANs



LOCATION

Main Menu

Configure VLAN

Edit/Delete an 802.1Q VLAN

Description

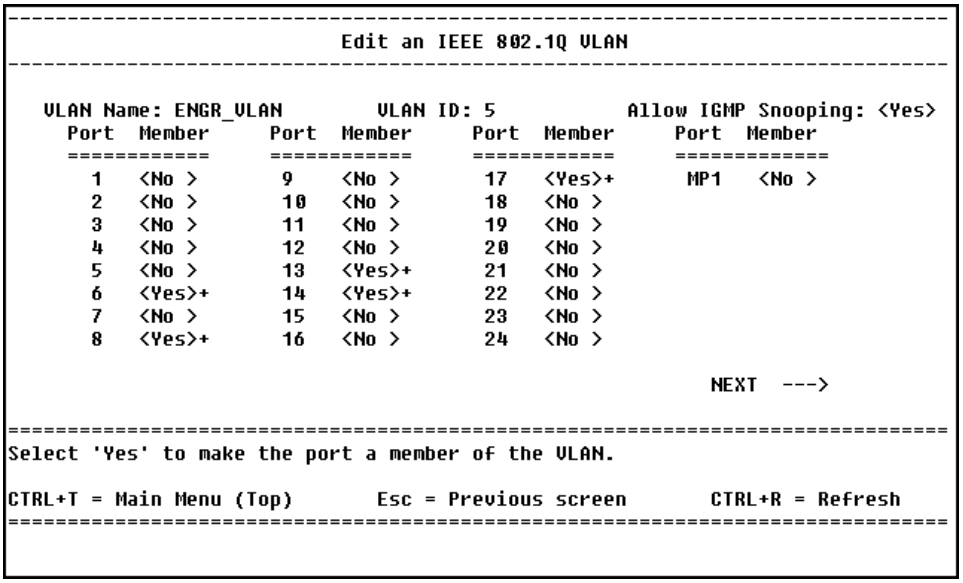
Use this screen to select a VLAN to edit the port membership in the VLAN or delete the VLAN from the switch.

Action: Press the Spacebar to toggle between <Edit> and <Delete>, then select a VLAN from the list and press Enter.

VLAN Name: The name of the VLAN you are configuring.

VLAN ID: Unique number assigned to identify an 802.1Q VLAN.

Edit an IEEE 802.1Q VLAN



LOCATION

Main Menu

Configure VLAN

Edit IEEE 802.1Q VLAN

Description

VLAN Name: Name of the VLAN you are editing or deleting.

VLAN ID: Assign a unique ID number to the VLAN. This number is used to identify all packets belonging to that VLAN. Type a number from 2 to 4094.

Allow IGMP Snooping: Press the Spacebar to determine if the switch will perform IGMP snooping on this VLAN. Up to 12 IGMP snooping sessions are allowed.

Member: Determines which ports are part of the VLAN being created. Press the Spacebar to toggle the field for the following options:

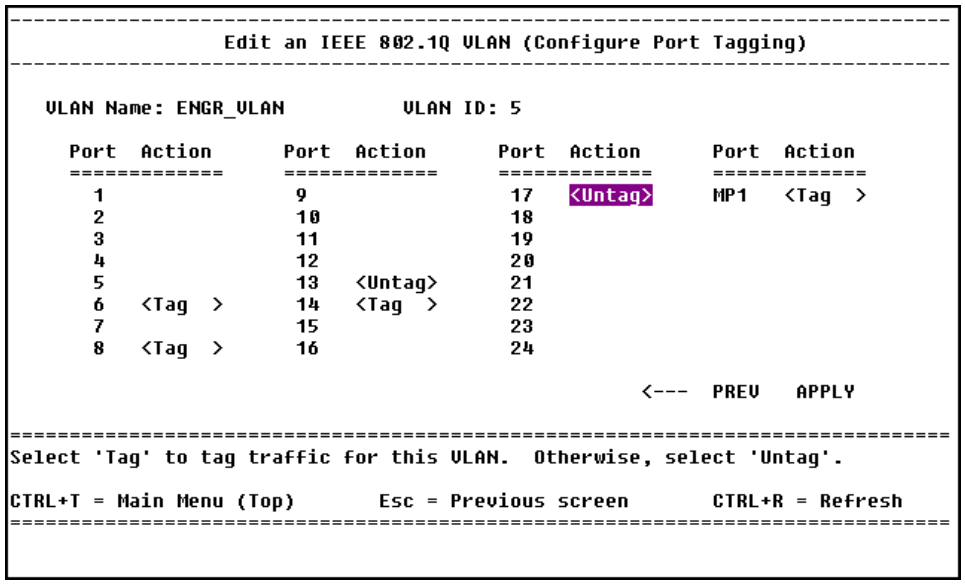
<Yes>	The port is a member of the VLAN.
<No >	The port is not a member of the VLAN.
–	The port is part of an aggregated link.

NEXT: Accesses the Edit an IEEE 802.1Q VLAN (Configure Port Tagging) screen.

NOTE

A '+' next to the Member toggle indicates that port is a member of more than one VLAN.

Edit an IEEE 802.1Q VLAN (Configure Port Tagging)



Description

Use this screen to set up the switch to manage outgoing packets that do not contain IEEE 802.1Q VLAN tags.

VLAN Name: Displays the name of the VLAN you are editing or deleting.

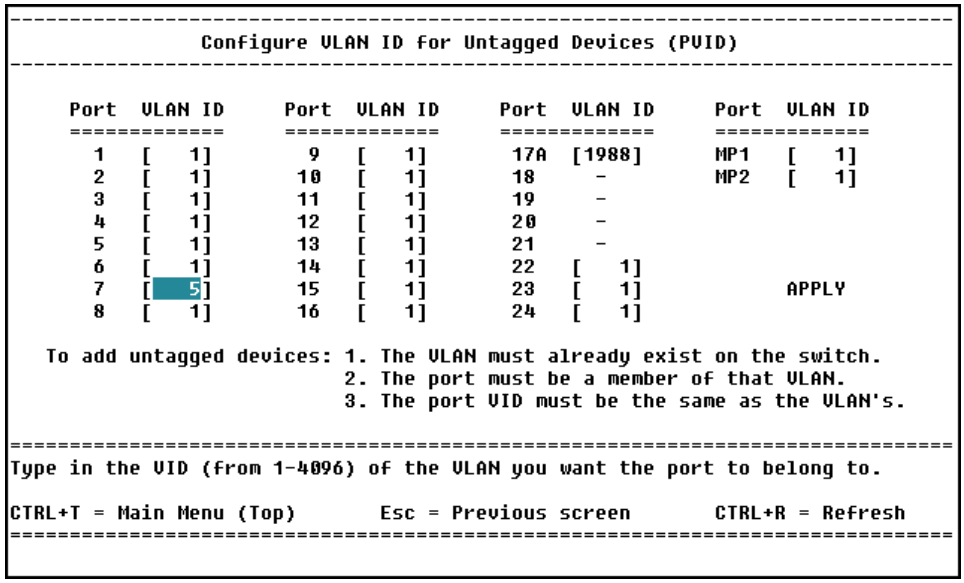
VLAN ID: Displays the ID number of the VLAN. This number identifies all packets belonging to that VLAN.

Action: Determines whether outgoing traffic from that port is untagged by the switch.

PREV: Returns you to the Edit an IEEE 802.1Q VLAN screen.

APPLY: Returns you to the Configure VLAN (IEEE 802.1Q) screen.

Configure VLAN ID for Untagged Traffic



Description

LOCATION

Main Menu

Configure VLAN

Configure Port VLAN ID...

Use this screen to set up the switch to manage incoming packets that do not contain IEEE 802.1Q VLAN tags or priority-tagged traffic (packets with a VID of zero). This applies to ingress traffic only; it does not apply to outbound traffic.

Untagged traffic is ordinarily assigned to VLAN 1 (the DEFAULT_VLAN), which includes all ports on the switch. However, if you don't want to send untagged traffic on a port to the default VLAN, you can assign a different PVID.

For example, if you set a port's PVID to 5, all untagged traffic on the port is assigned to VID 5—even if the port does not belong to that VLAN.

PVID: Type the VID of the existing 802.1Q VLAN where you want to send untagged traffic.

APPLY: Applies the changes on this page.

GVRP and Ingress Filter Settings

```
------------------------------------------------------------------------------
                        GVRP and Ingress Filter Settings
------------------------------------------------------------------------------
  Configure Ports: < 1 to 12 >

  Port     GVRP              Ingress Filtering
   1     <Disabled>             <Disabled>
   2     <Disabled>             <Disabled>
   3     <Disabled>             <Enabled >
   4     <Enabled >             <Enabled >
   5     <Disabled>             <Disabled>
   6     <Disabled>             <Disabled>
   7     <Disabled>             <Disabled>
   8     <Disabled>             <Disabled>
   9A    <Enabled >             <Enabled >
  10         -                      -
  11         -                      -
  12         -                      -

==============================================================================
Configure the switch to automatically discover 802.1Q VLANs on this port.

CTRL+T = Main Menu (Top)       Esc = Previous screen       CTRL+R = Refresh
==============================================================================
```

LOCATION

Main Menu

Configure VLAN

GVRP/Ingress Filter Settings

Description

Configure Ports: Use the Spacebar to toggle the range of ports that you can configure.

GVRP: Enables the switch to create VLANs dynamically. Use the Spacebar to toggle the action for each port.

<Enabled>: The switch monitors traffic on this port for GVRP requests from network nodes. If a GVRP-enabled device sends a request to this port, the switch creates a VLAN dynamically and adds the requesting device to the new VLAN. This is the default setting.

<Disabled>: The switch ignores GVRP requests in incoming packets on this port.

Ingress Filtering: Enables the switch to filter incoming packets based on VLAN membership. Use the Spacebar to toggle the action for each port.

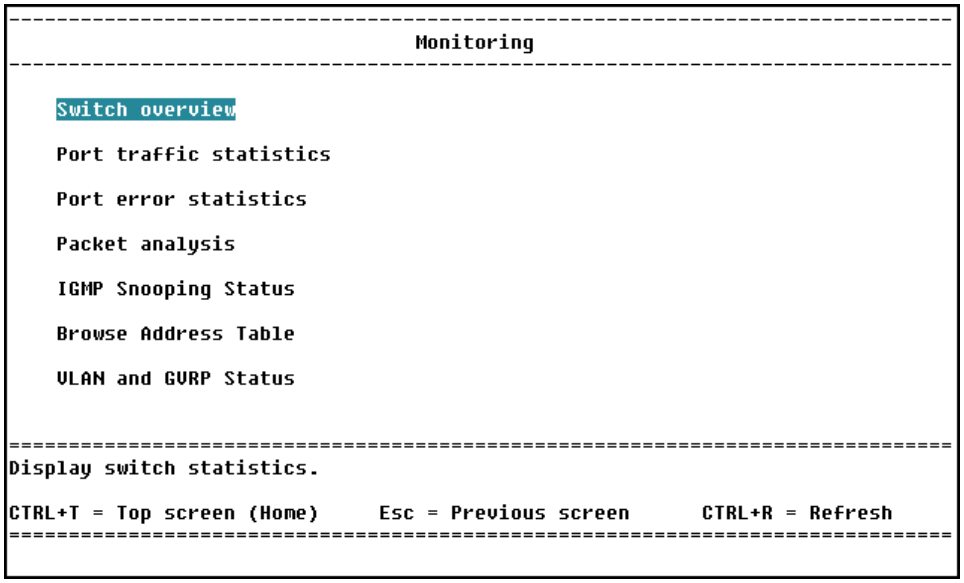
<Enabled>: Incoming packets belonging to a specific VLAN are forwarded only if the port belongs to that VLAN. This is the default setting.

<Disabled>: All packets coming into the port are forwarded, regardless of the port's VLAN membership.

NOTE

In order for GVRP to work, the port must be connected to a switch that supports GVRP.

Monitor (Network Statistics)



Description

LOCATION

Main Menu

Monitoring

Switch overview: Displays an overview of all ports on the switch.

Port traffic statistics: Displays port traffic statistics and utilization.

Port error statistics: Displays port error statistics.

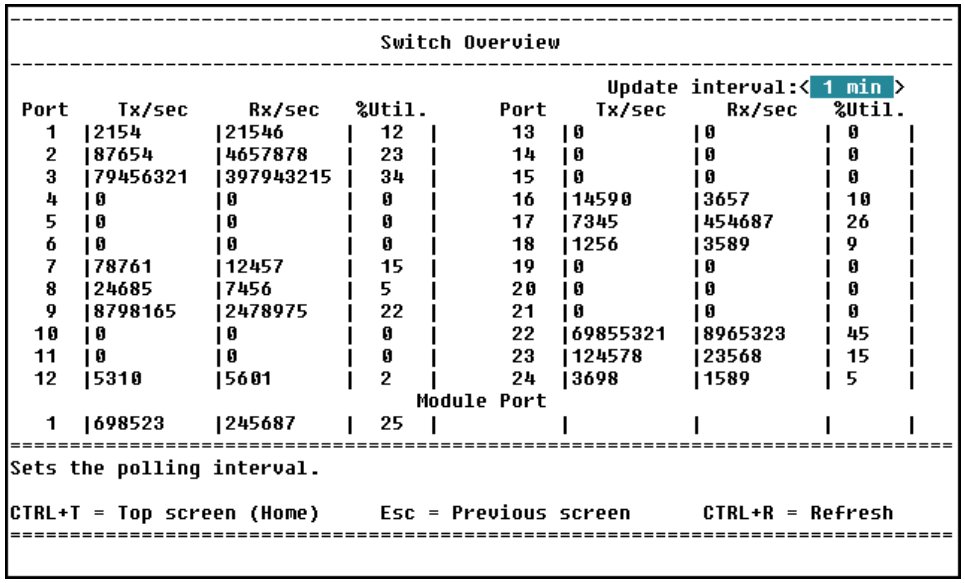
Packet analysis: Displays traffic per port by packet size and type.

IGMP Snooping Status: Displays active IP multicast groups detected by the switch.

Browse the address table: Displays the entries in the switch's address table by port or MAC address.

VLAN/GVRP Status: Displays status for static and dynamic tag-based (IEEE 802.1Q) VLANs. This option is available only when the switch is running 802.1Q VLANs.

Switch Overview



Description

LOCATION

Main Menu

Monitoring

Switch Overview

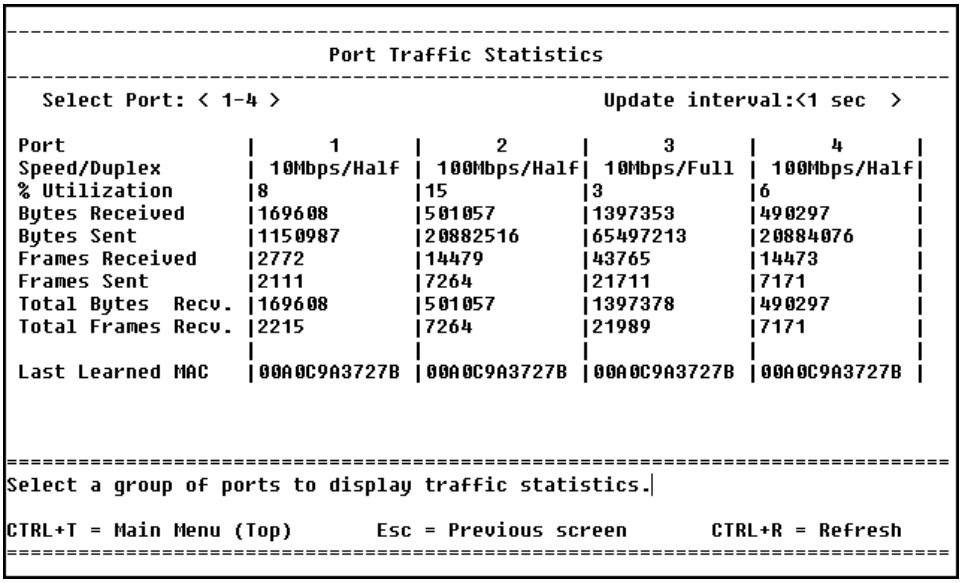
Use this screen to view activity on the switch. The screen displays the traffic sent and received for each port on the switch, including any optional modules, and the percent utilization for that port.

Update interval: Press the Spacebar to select the time period between updates. For example, an Update interval of 5 sec means Local Management collects and displays information from the switch every five seconds.

Tx/sec or Rx/sec: The current rate of error-free frames that were transmitted or received by the port.

% Utilization: The percentage of Ethernet bandwidth (10 Mbps,100 Mbps, or 1000 Mbps) used by the device attached to that port.

Port Traffic Statistics



Description

LOCATION

Main Menu

Monitoring

Port Traffic Statistics

Select Port: Selects the range of ports to view. Statistics are displayed four ports at a time. Press the Spacebar to toggle between port numbers and the optional module. The example shows ports 1-4 on a 24-port switch.

Update interval: Press the Spacebar to select the time period between updates. For example, an Update interval of 5 sec means Local Management collects and displays information from the switch every five seconds.

Speed/Duplex: The current connection status of the port.

% Utilization: The percentage of Ethernet bandwidth (10 Mbps,100 Mbps, or 1000 Mbps) used by the device attached to that port.

Bytes Received: The number of bytes (octets) contained in error-free frames. This includes octets in unicast, broadcast, or multicast frames and packets whose destination address is mapped to the receiving port. It also includes octets in packets dropped because of full buffers, spanning tree, disabled ports, no link, or empty distribution list.

Bytes Sent: The number of error-free bytes (octets) sent over this port.

Frames received: The number of error-free frames detected. Includes unicast, broadcast, or multicast frames and frames whose destination address is mapped to the receiving port. It also includes frames dropped because of full buffers, spanning tree, disabled ports, no link, or empty distribution list.

Frames sent: The number of error-free frames sent over this port.

Total Bytes Recv (Received): The number of bytes (octets) contained in all frames received by this port. This counter reflects all bytes received on the port. This includes bytes contained in frames that contain errors, dropped frames, frames whose destination address is mapped to the receiving port, and frames that were not forwarded through the switch.

Total Frames Recv (Received): The total number of frames received on the port. This includes frames that contain errors, dropped frames, frames whose destination address is mapped to the receiving port, and frames that were not forwarded through the switch.

Last Learned MAC: The MAC address of the last device added to the forwarding database table for this port.

Port Error Statistics

```
------------------------------------------------------------------------------
                          Port Error Statistics
------------------------------------------------------------------------------
  Select Port: <1-4>                          Update interval:< 1 min >

 Port              |     1       |      2       |     3       |     4       |
 Speed/Duplex      |   10M/Half  |   100M/Half  |   -         |   -         |
   CRC Error       |32           |0             |0            |0            |
   Oversize Frames |5            |12            |0            |0            |
   Fragments       |120          |8             |0            |0            |
   Jabber          |0            |0             |0            |0            |
   Late Collision  |0            |0             |0            |0            |
   MAC Rx Error    |0            |0             |0            |0            |
   Dropped Frames  |10           |3             |0            |0            |
   Undersize Frames|7            |2             |0            |0            |
 Total errors      |174          |25            |0            |0            |
                   |             |              |             |             |
 Collisions        |25           |120           |0            |0            |

==============================================================================
Select a group of ports to display statistics.

CTRL+T = Main Menu (Top)       Esc = Previous screen       CTRL+R = Refresh
==============================================================================
```

Description

Select Port: Select the range of ports to view. Statistics are displayed four ports at a time. Press the Spacebar to toggle between port numbers and the optional module. The example shows ports 1-4 on a 24-port switch.

Update interval: Press the Spacebar to select the time period between updates. For example, an Update interval of 5 sec means Local Management collects and displays information from the switch every five seconds.

Speed/Duplex: The current connection status of the port.

CRC Errors: The number of valid length frames (between 64 and 1536 bytes) that had a bad Frame Check Sequence (FCS).

Oversize Frames: Number of frames that exceed the maximum allowed frame size but are otherwise valid Ethernet frames (good CRC).

Fragment: The number of frames that are less than 64 bytes. This number includes frames without a start-of-frame delimiter. A fragmented frame also has an invalid CRC.

Jabber: Indicates that a device (such as a faulty NIC) on the network is sending improper electrical signals. Because Ethernet uses electrical signaling to determine whether it can transmit, a jabber condition can halt all traffic on a segment.

LOCATION

Main Menu

Monitoring

Port Error Statistics

Late Collision: The number of collisions detected after the allowable detection period. This usually occurs in networks where cables are longer than the IEEE specification.

MAC Rx Error: The number of received packets containing Rx Error events.

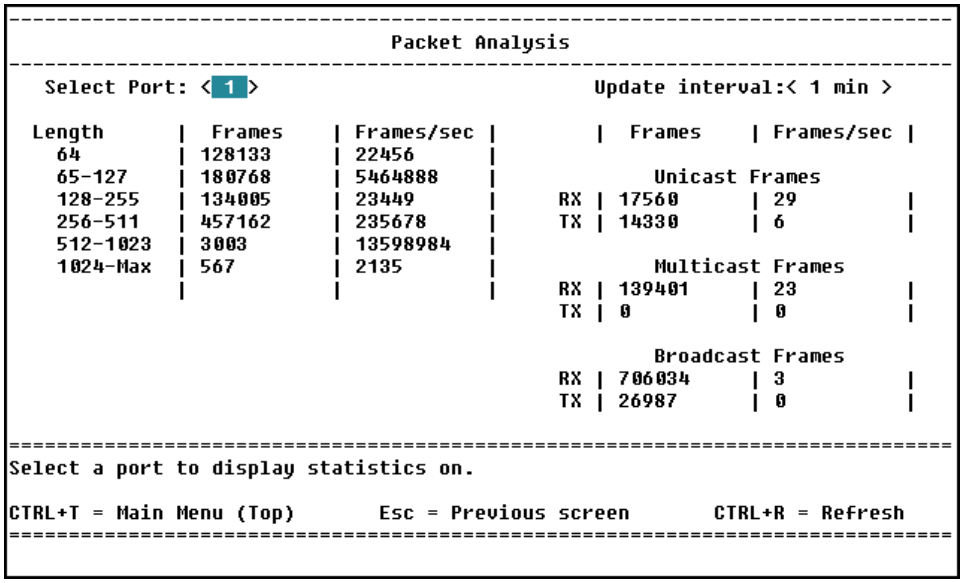
Dropped Frames: The number of frames dropped by this port since the last switch reboot.

Undersize Frames: The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersized frames usually indicate collision fragments, a normal network event.

Total errors: The total number of errors detected since the last switch reboot. Total errors include everything listed in this error table.

Collisions: A collision occurs when two devices try to transmit at the same time. This counter tracks the number of times packets have collided on this port. Collisions are normal in an Ethernet network and tend to increase as network utilization rises. Therefore, an increased collision rate without an increase in network utilization might indicate a problem.

Packet Analysis



LOCATION

Main Menu

Monitoring

Packet Analysis

Description

This screen displays a breakdown of the traffic received on a port by size and type of frame.

Select Port: Selects the port to view. Statistics are displayed one at a time. Press the Spacebar to toggle between the ports and the optional module.

Update interval: Press the Spacebar to select the time period between updates. For example, an update interval of 5 sec means the switch collects and displays information every five seconds.

Length: Indicates the number of frames received of different lengths. This also includes dropped frames and frames whose destination address is mapped to the receiving port. It does not include frames that contain errors.

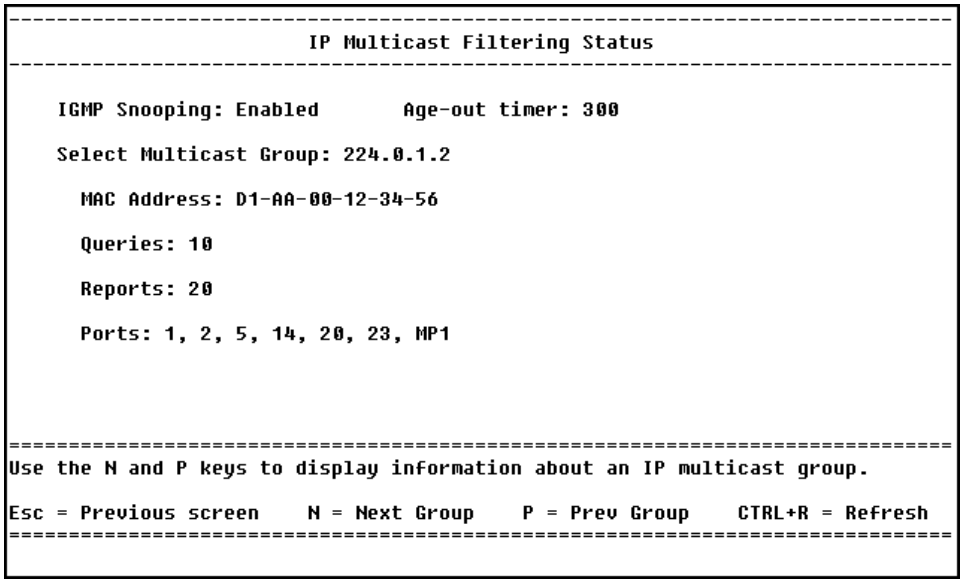
Frames

Unicast: The number of error-free unicast frames received and transmitted on this port. Unicast frames are sent from one network node to another network node.

Broadcast: The number of error-free broadcast frames received and transmitted on this port. Broadcast frames are sent from one network node to all nodes on a segment.

Multicast: Tthe number of error-free multicast frames received and transmitted on this port. Multicast frames are sent from one node to multiple nodes on the segment.

IGMP Snooping Status



LOCATION

Main Menu

Monitoring

IGMP Snooping Status

Description

Use this screen to view active multicast groups detected by the switch. The switch uses these groups for filtering purposes when you enable IGMP snooping.

VLAN: The name of the VLAN with IGMP snooping enabled. This field only appears when port-based or tag-based VLANs are active on the switch.

Age-out timer: The time the switch waits between IGMP queries.

Multicast group: The IP address of the multicast group.

MAC address: The MAC address of the multicast group.

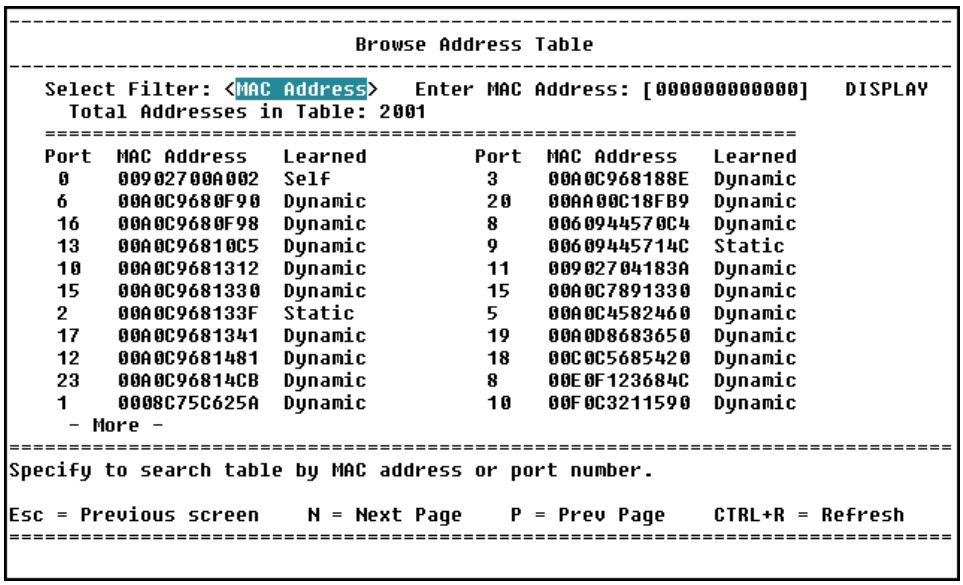
Queries: The number of IGMP requests sent from the IGMP multicast server or router to individual network hosts.

Reports: The number of notifications sent from each host to the server, signifying that the host is still (or wants to be) part of the multicast group.

Ports: The ports on the switch that have devices belonging to the selected multicast group.

Use the **N** (next group) and **P** (previous group) keys to display the status of different IP multicast groups on the switch.

Browse Address Table



Description

LOCATION

Main Menu

Monitoring

Browse Address Table

Use this screen to sort through the switch's MAC address table and view the addresses the switch has learned. The switch uses this table when making forwarding decisions to avoid broadcasting traffic over every port. You can search this table by MAC address or by port.

VLAN (port-based)/**VLAN ID** (tag-based): When the switch is running port-based or tag-based VLANs, the address table associates MAC addresses with specific VLANs. Use the Spacebar to select a VLAN.

Select Filter: Use the Spacebar to select how to view the address table. You can sort by <MAC address> or by <Port>.

Enter MAC Address: Use this field to search for a specific MAC address in the switch's table.

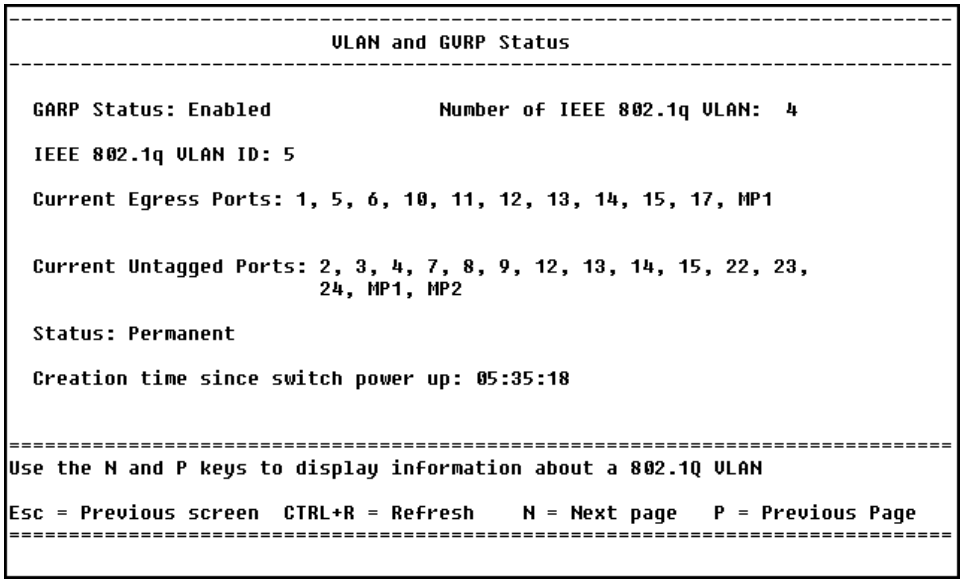
Port Number: Use the Spacebar to select a port and display the MAC addresses seen on the specified port. This search is useful for monitoring which ports a device is using, or which devices are using one port.

DISPLAY: After you enter a MAC address, or choose a port, select this button and press Enter to display the results.

Total Addresses in Table: The total number of addresses learned by the switch. This number includes addresses that have been entered manually using the Static MAC Addresses screen.

Learned: Displays how the switch learned the particular MAC address. Dynamic means the switch learned the address by sending out a query. Static means the address was entered using the Static MAC Addresses screen.

VLAN and GVRP Status



LOCATION

Main Menu

Monitoring

VLAN/GVRP Status

Description

This screen is available only if the switch is running tag-based (IEEE 802.1Q) VLANs. The screen shows information about one VLAN at a time. Press N or P to view status information for other tag-based VLANs on the switch.

GARP Status: Shows whether the VLAN can process GVRP requests.

Number of IEEE 802.1Q VLANs: Total number of tag-based VLANs (both static and dynamically created) currently configured on the switch.

IEEE 802.1Q VLAN ID: VLAN ID of the selected tag-based VLAN.

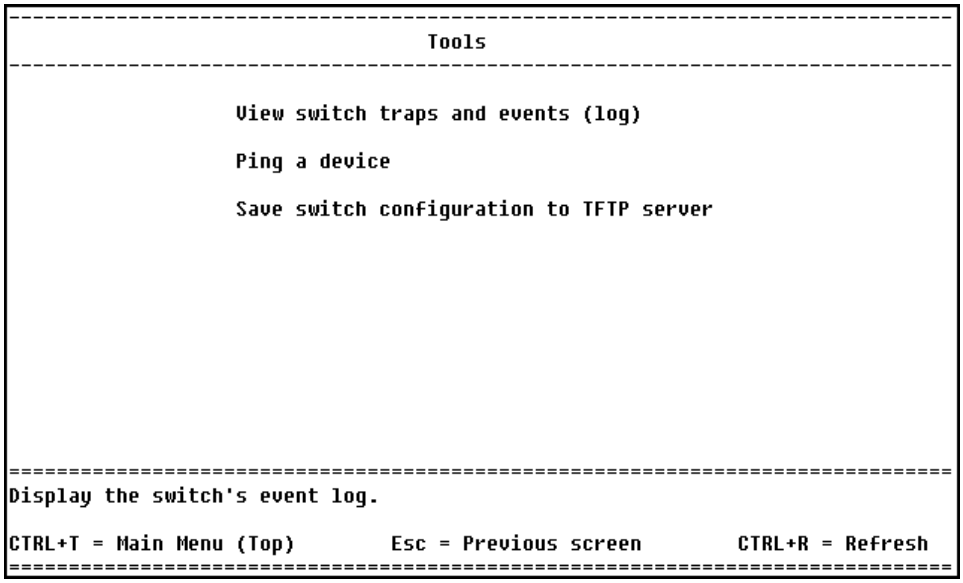
Current Egress Ports: All ports that belong to the specified tag-based VLAN.

Current Untagged Ports: All ports that are configured to strip 802.1Q VLAN information from packets leaving the switch.

Status: Whether the VLAN is permanent or dynamic. A permanent (static) tag-based VLAN is created and configured by the switch administrator. A dynamic VLAN is created by the switch in response to GVRP requests from GVRP-enabled network nodes.

Creation time since switch power up: Amount of time the VLAN has been active since the last time the switch was rebooted.

Tools



Description

LOCATION

Main Menu

Tools

View switch traps and events (log): View events contained in the switch's internal log.

Ping a device: Ping another device on the network to test connectivity.

Save switch configuration to a TFTP server: Back up the switch's current settings to a TFTP server.

Switch Event Log

```
--------------------------------------------------------------------------------
                              Switch Event Log
--------------------------------------------------------------------------------
 Seq.#     Time      Description
================================================================================
 067     010d22h31m   STP status: Topology change.
 066     009d12h18m   STP status: This switch became the new root of tree.
 065     009d08h52m   Port 15 Link Up
 064     008d01h35m   Port 16 is experiencing a broadcast storm!
 063     007d00h13m   Port 12 is auto-partitioned.
 062     007d04h12m   Operator logged out.
 061     007d10h09m   Successful login through telnet.
 060     007d15h00m   Gigabit-SX module's port 1 uplink has lost link.
 059     006d21h00m   Port 5 has lost link.
 058     006d06h00m   Port 1 has changed speed to 100Mbps.
 057     005d09h00m   Switch and Firmware OS is fully operational.
 056     005d02h00m   Power up.  Express 460T Firmware OS loaded.

  - MORE - (12 of 154)
================================================================================
Use the N, P, B, and E keys to view the log.

N = Next Page   P = Prev Page   B = Log Begin   E = Log End   C = Clear Log
================================================================================
```

Description

LOCATION

Main Menu

Tools

View Switch Traps and Events

Use this screen to view and navigate the switch's log. The log is similar to a trap and event receiver but it only captures traps/events generated by the switch itself. For example, the log includes events such as when a port is disabled, when an unauthorized user attempts to access a management interface, and when the switch reboots.

The log entries are listed chronologically from the last time the switch was rebooted. Use the following keys to navigate the log:

N = next page

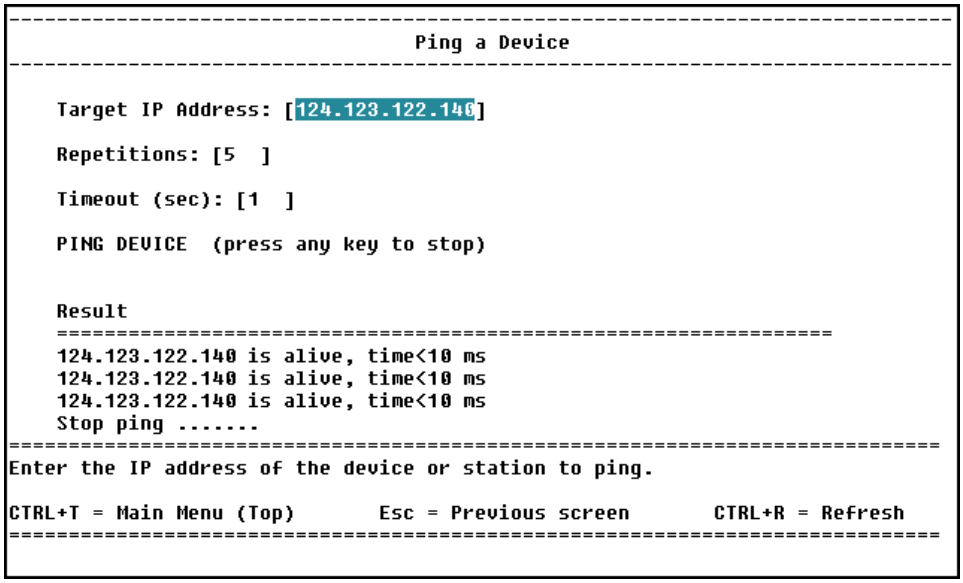
P = previous page

B = Go to the beginning of the log

E = Go to the end of the log

C = Clear the log

Ping a Device



LOCATION

Main Menu
Tools
Ping a Device

Description

Target IP address: Type the IP address of the device you want the switch to ping.

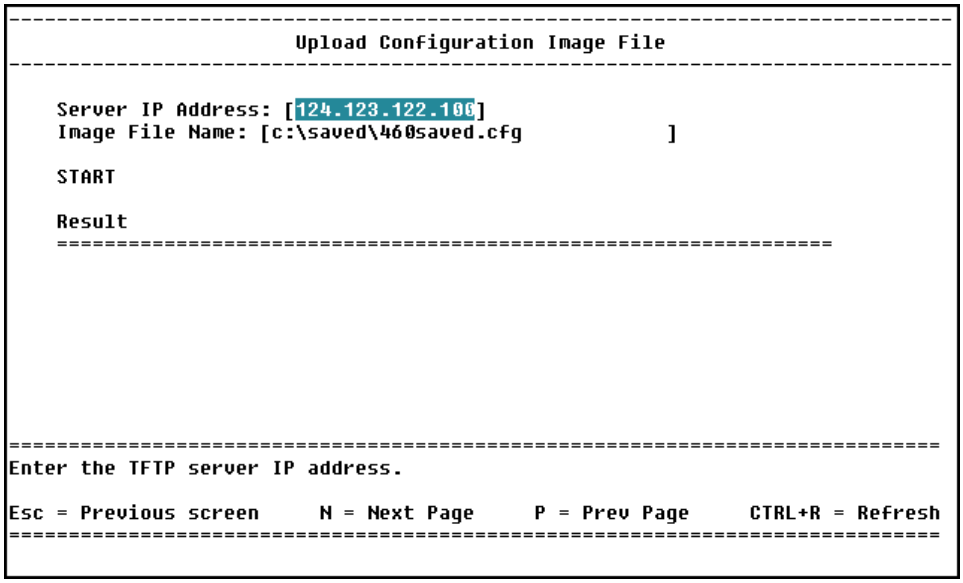
Repetitions: Type the number of times (1–255) you want the switch to ping the specified device.

Timeout: Type the number of seconds (0–999) the switch waits before retrying a ping if it doesn't receive a response from the first ping.

PING DEVICE: Starts pinging a device. To stop a ping, press any key on the keyboard.

Result: The target device's response to the ping.

Upload Configuration Image File



Description

Use this screen to save an image of the switch's configuration to a file and upload it to a TFTP server.

Server IP Address: Type the IP address of your TFTP server.

Image File Name: Type a file name and location to save the image file on the server.

START: Backs up the switch settings.

LOCATION

Main Menu

Tools

Upload Configuration File

NOTE

This feature creates an image of the switch configuration and saves it in binary format. This is not the same as a .CFG file, which is saved in ASCII text. See Appendix A for information about configuration files.

Appendix A: Technical Info

What is a configuration file?

A configuration file is an ASCII text file that contains initialization information and configuration settings for the switch specified by the network administrator. The switch's configuration file (.CFG) can be up to 10 KB in size and is stored on a central server where it is downloaded into the hub using TFTP.

You can use a text editor like Microsoft Windows* Notepad to make changes to the configuration file. The switch interprets file lines beginning with the pound (#) sign as comments. It interprets all other lines as commands. When the switch initializes, it uses this file to configure parameters like port speed, port security, and SNMP trap receivers.

Use of a standard configuration file can make managing multiple switches much simpler. Instead of requiring a network administrator to make changes to each manually, the switch uses the file to configure itself.

Sample Configuration File

The following is an example of a configuration file.

```
###### Intel Express 460T Standalone Switch Configuration File ##############
#
# Lines beginning with a "#" character are comment lines.

###### IP Address Configuration ##########################################
#
#   Ip_addr= <ipaddress>              IP address used by the switch
#   Subnet_mask= <ipaddress>          Specify default gateway
#   Default_gateway= <ipaddress>      Specify subnet mask
#
                Ip_addr= 124.123.122.121
                Subnet_mask= 255.255.255.0
                Default_gateway= 124.123.122.254

###### Console and Configuration File Information ########################
#
#  Specify the code type of the image file
#
#  Code_type=PROM         Image type is PROM code
#  Code_type=RUNTIME      Image type is runtime firmware
#  Code_type=CONFIG       Image type is saved configuration file

                Code_type=PROM
#
#    Image_file= <path>     Path and filename of runtime image or PROM image files

                Image_file="e:\update\E460PROM.tfp"

###### Port Level Configuration ##########################################
#
#   Static_fdb_list={(MAC address, port #)}                    MAC address and port# of static entries
#   Port_nway_enabled_list={port#, port#, . . }                Ports set to auto-negotiate
#   Port_flow_ctrl_enabled_list= {port#, port#, . .}           Ports that have flow control enabled
#   Port_backpressure_enabled_list= {port#, port#, .}          Ports that have back pressure set
#   Port_priority_list= { H (high), L (low), . .}              Sets 802.1p priority queues
#   Port_stp_enabled_list= {port#, port #, . .}                Ports that are enabled
#   Port_disabled_list= {port#, port#, . .}                    Ports that are disabled

                Static_fdb_list={ (0080c8001121, 1) (0080c8001122, 2) (0080c8001123, 3) }
                Port_nway_enabled_list={3,5,7}
                Port_flow_ctrl_enabled_list = {3,4,5,7}
                Port_backpressure_enabled_list = {16, 15, 14 }
                Port_priority_list = { H,L,A,L,H,A,A,L,H }
                Port_stp_enabled_list = {8,9,10,11, 20, 21, 23 }
                Port_disabled_list = { 20,21,22,23,24,25 }
###### Link Aggregation ##################################################
#
```

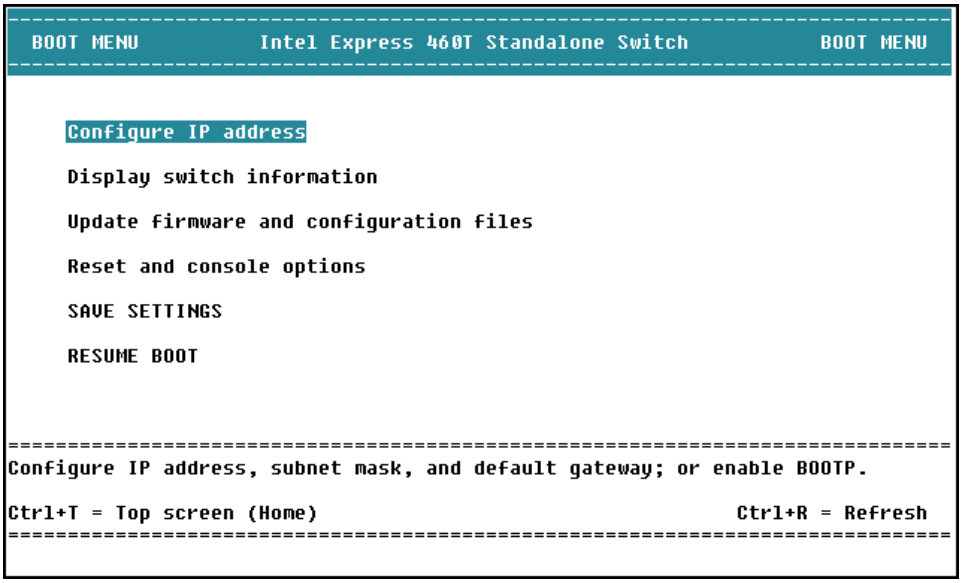
```
# linkaggr_list={(index “name”, width of the aggregated group, “state”
#               index=from 1 to 4 (4=max number of aggregated groups possible)
#               name=name of the aggregated group
#               width=total port width of aggregated group
#               state=”enable” or “disable” (default=disable)
#
               linkaggr_list={(1 “Engineering Server”, 2 “disable”) (2 “Marketing Server”, 3, “enable”)
               (3 “3rd Floor Switch”, 2, “enable)}

 ###### Configure PVID for Untagged Ports ##########################################
#
# pvid_list={(port#, PVIDvalue) (port#, PVIDvalue) ...}
#               port#=port attached to device that does not support tags
#               PVIDvalue=VID of port to which you want untagged traffic routed
#
               pvid_list={(2, 100) (3, 100) (6, 15)}

###### Create 802.1Q VLAN on the Switch (Static Entries) ##################################
#
# 802_1q_static_list={(VID, “VLANstring”, M/N U/T,...) (VID, “VLANstring”, M/N U/T,...)}
#               M=member port (on ingress)
#               N=non member port (on ingress)
#               U=untagged device (on egress)
#               T=tagged device (on egress)
#               Either M or N can be specified for each port; not both
#               Either U or T can be specified for each port; not both
#
               802_1q_static_list={(2, “VLAN2”, MT, MU, MT, NT, MT, NU, NT, NU) (10, “VLAN10”, MT, MU,
               NT, NT, MT, MU, NT, MU)}

###### GVRP (Dynamic VLAN Registration) ##################################
#
# gvrp_enabled={port#, port#,  ...}
# gvrp_disabled={port#, port#, ...}
#               gvrp_enabled=VLAN dynamically registered with the switch
#               gvrp_disabled=VLAN not dynamically registered with the switch
#
               gvrp_enabled={1, 3, 5, 7}
               gvrp_disabled={2, 4, 6, 8}
```

BOOT Menu



Description

Under normal circumstances you don't need to use the BOOT Menu. The BOOT Menu is only available by connecting to the switch's serial port. It is used when the firmware fails to load.

To access the BOOT Menu, press Ctrl + C while the switch is starting up. The menu above displays. Most of the options available from the BOOT Menu are simplified versions of the normal runtime firmware; navigation is the same.

Configure IP address: Configures the switch's IP address.

Display switch information: Configures identification and displays hardware information about the switch.

Update firmware and configuration files: Configures the switch's internal software. Also used to specify the location of configuration files.

Reset and Console Options: Use to reset the switch to factory defaults to configure the port mode for the switch's serial port. Also sets the console timeout.

SAVE SETTINGS: Saves the changes to the switch's flash memory.

RESUME BOOT: Resumes the switch's boot process and loading of the firmware.

List of Factory Defaults

- Software upgrade mode: Network
- TFTP Server Address: 0.0.0.0
- Load configuration file: Disabled
- Console baud rate: 9600
- Console port data bits : 8
- Console port stop bit: 1
- IGMP Snooping: Disabled
- System port partition state: Enabled
- Lock Address Table: Disabled
- MAC Address Aging (sec): 300
- System HOL-blocking state: Enabled
- System console timeout : 15 minute
- System IGMP timeout: 300 sec
- System IP address: 192.0.2.1
- System Subnet mask: 255.255.255.0
- System Default gateway: 0.0.0.0
- System BootP request: Enabled
- Port Nway state: Enabled (Auto-Negotiate)
- Port flow control state: Auto-Negotiate IEEE 802.3x
- Port back pressure state: Auto-Negotiate
- Port priority state: Use Frame Tag
- Port HOL state: Enabled
- Ping IP address: 0.0.0.0
- Ping repeat time: 1 time
- Ping time out: 5 sec
- Port Mirroring state: Disabled
- Port Mirroring source port: 1
- Port Mirroring destination port: 2
- System Spanning Tree state: Disabled-IEEE 802.1d
- System Bridge Max age: 20 sec
- System Bridge Hello time: 2 sec
- System Bridge Forward delay: 15 sec
- System Bridge Priority: 32768
- System aging time: 300 sec
- Per Port spanning tree path cost: 10
- Per Port spanning tree priority: 128
- Per Port state: Enabled
- Per Port spanning tree state: Enabled
- Read community string: public
- Write community string: private
- Console user account: No username
- Console user password: No password

Optional module default settings

- FX Module Port Speed: 100 Mbps
- FX Module Port Duplex: Full duplex
- FX Module Flow Control: IEEE 802.3x
- FX Module Priority: Use Frame Tag
- SX\LX Module Port Speed: 1000 Mbps
- SX\LX Module Port Duplex: Full-duplex
- SX Module Flow Control: IEEE 802.3x
- SX Module Priority: Use Frame Tag

Troubleshooting/FAQs

I booted the switch, and the status LED stays orange. Is something wrong?

By default, the switch is in BootP mode, and the LED stays orange while the switch waits for an IP address from the BootP server. In order to proceed with the boot, either bypass the BootP phase (refer to the Quick Start guide for instructions), or manually assign an IP address.

If the switch doesn't receive an IP address from the BootP server within ten minutes, it will continue the boot process as normal.

How can I set the speed or duplex on individual ports?

Normally the switch handles all connections automatically but if you need to force speed or duplex, (for example, to accommodate older devices that don't support autonegotiation) use the Local Management or Web Device View.

When I set the 460T to autonegotiate with flow control enabled and try to connect to another device, there is no link. Why?

Check the settings of the other device and disable flow control on the switch. If you want to use flow control on the port, force the speed, duplex, and flow control settings so that they match.

I've connected the cable but the left LED (link) is off. Why?

- Remove the cable and plug it in again. Wait up to six seconds for a link.
- Make sure you're using the correct type of cable (straight-through–MDI or crossover–MDI-X) for the device you want to connect to. If you're using the wrong cable, the link LED will not turn on.
- Make sure the device you've connected to a port is a 10Base-T or 100Base-TX device. The 460T switches don't support 100Base-T4 devices running at 100 Mbps. However, they do support T4 devices running at 10 Mbps.
- Check the speed and duplex settings on the PC's network adapter.
- The cable may be defective.

The port's left LED (link) is on but I'm not seeing any activity when I try to ping a device on that port. Why?

- The port might be disabled through management. Go into the Local Management or Web Device view to enable the port and try pinging the device again.
- The port might be partitioned (auto-disabled). This condition is usually caused by a malfunctioning network adapter or an overloaded network segment. The switch waits until it stops receiving collisions then clears the port automatically.

After I connect to Local Management I see a blank screen. Why?

- Make sure you are using a null modem cable (included).
- Check the settings in your terminal program. They should be set to 9600 baud, 8 data bits, No parity, 1 stop bit, and No flow control.
- Try pressing Ctrl + R to force the screen to refresh.

I keep getting an intermittent loss of link. (or data is not being transmitted) Why?

- You may be using the wrong grade of cable. The wrong cable can cause erratic performance and you may eventually lose the connection between the port and the attached device.
- Check the duplex setting for the device connected to the port. You may have to use the Local Management or Web Device Manager to force the port to half or full duplex.
- A cable segment somewhere in your collision domain may be too long. Make sure none of your UTP cabling is longer than 100 meters.
- Check the Ethernet cable pairs. The TX pairs (pins 1 and 2) and the RX pairs (pins 3 and 6) should be twisted pairs. See diagram in page 10.

I created a tag-based VLAN, and I have tag-capable LAN adapters in my PCs, but I can still communicate with devices outside the VLAN. Why?

Check to make sure that you have assigned a VID to the PC. If you don't assign a VID to the NIC in the PC it will behave as an untagged device. The default VID for untagged devices=1 so all untagged PCs will be a member of the DEFAULT_VLAN.

Locating MIB files

If you use a MIB browser, you can configure or view statistics for the switch. You can find these switch MIB files at the Intel Customer Support Web site at *http://support.intel.com/support/express/switches*.

- intel.mib
- int_gen.mib
- int_s460.mib
- int_pbrd.mib
- int_qprd.mib

When compiling the MIBs into an SNMP-compliant management application, compile the intel.mib first then compile the int_gen.mib, int_s460.mib, int_pbrd.mib, and int_qprb.mib files.

Regulatory Information

FCC Part 15 Compliance Statement

This product 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 product 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning this equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Change the direction of the radio or TV antenna.
- To the extent possible, relocate the radio, TV, or other receiver away from the product.
- Plug the product into a different electrical outlet so that the product and the receiver are on different branch circuits.

If these suggestions don't help, consult your dealer or an experienced radio/TV repair technician for more suggestions.

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

CAUTION If you make any modification to the equipment not expressly approved by Intel, you could void your authority to operate the equipment.

Canada Compliance Statement (Industry Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le Ministre Canadien des Communications.

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled: "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

Manufacturer Declaration

This certifies that the Intel® Express 460T Standalone Switch complies with the EU Directive 89/336/EEC, using the EMC standards EN55022 (Class A) and EN55024. This product also meets or exceeds EN 60950 (safety) requirements. These products have been tested and verified to meet CISPR 22 Class A requirements.

Australia Statement

Taiwan Class A EMI Statement

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

VCCI Statement

Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Warnings

WARNING

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

Internal access to Intel® Express 460T Standalone Switch is intended only for qualified service personnel. Do not remove any covers.

WARNING

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean and free of airborne particles (other than normal room dust).
- Well ventilated and away from sources of heat including direct sunlight.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.
- Provided with a properly grounded wall outlet.

Do not attempt to modify or use the supplied AC power cord if it is not the exact type required.

Ensure that the system is disconnected from its power source and from all telecommunications links, networks, or modems lines whenever the chassis cover is to be removed. Do not operate the system with the cover removed.

AVERTISSEMENT

Le système a été conçu pour fonctionner dans un cadre de travail normal. L'emplacement choisi doit être:

- Propre et dépourvu de poussière en suspension (sauf la poussière normale).
- Bien aéré et loin des sources de chaleur, y compris du soleil direct.
- A l'abri des chocs et des sources de vibrations.
- Isolé de forts champs magnétiques géenérés par des appareils électriques.
- Dans les régions sujettes aux orages magnétiques il est recomandé de brancher votre système à un supresseur de surtension, et de débrancher toutes les lignes de télécommunications de votre modem durant un orage.
- Muni d'une prise murale correctement mise à la terre.

Ne pas utiliser ni modifier le câble d'alimentation C. A. fourni, s'il ne correspond pas exactement au type requis.

Assurez vous que le système soit débranché de son alimentation ainsi que de toutes les liaisons de télécomunication, des réseaux, et des lignes de modem avant d'enlever le capot. Ne pas utiliser le système quand le capot est enlevé.

AVVERTENZA

Il sistema è progettato per funzionare in un ambiente di lavoro tipico. Scegliere una postazione che sia:

- Pulita e libera da particelle in sospensione (a parte la normale polvere presente nell'ambiente).
- Ben ventilata e lontana da fonti di calore, compresa la luce solare diretta.
- Al riparo da urti e lontana da fonti divibrazione.
- Isolata dai forti campi magnetici prodotti da dispositivi elettrici.
- In aree soggette a temporali, è consigliabile collegare il sistema ad un limitatore di corrente. In caso di temporali, scollegare le linee di comunicazione dal modem.
- Dotata di una presa a muro correttamente installata.

Non modificare o utilizzare il cavo di alimentazione in c. a. fornito dal produttore, se non corrisponde esattamente al tipo richiesto.

Prima di rimuovere il coperchio del telaio, assicurarsi che il sistema sia scollegato dall'alimentazione, da tutti i collegamenti di comunicazione, reti o linee di modem. Non avviare il sistema senza aver prima messo a posto il coperchio.

WARNUNG

Das System wurde für den Betrieb in einer normalen Büroumgebung entwickelt. Der entwickelt. Der Standort sollte:

- sauber und staubfrei sein (Hausstaub ausgenommen);
- gut gelüftet und keinen Heizquellen ausgesetzt sein (einschließlich direkter Sonneneinstrahlung);
- keinen Erschütterungen ausgesetzt sein;
- keine starken, von elektrischen Geräten erzeugten elektromagnetischen Felder aufweisen;
- in Regionen, in denen elektrische Stürme auftreten, mit einem Überspannungsschutzgerät verbunden sein; während eines elektrischen Sturms sollte keine Verbindung der Telekommunikationsleitungen mit dem Modem bestehen;
- mit einer geerdeten Wechselstromsteckdose ausgerüstet sein.

Versuchen Sie nicht, das mitgelieferte Netzkabel zu ändern oder zu verwenden, wenn es sich nicht um genau den erforderlichen Typ handelt.

Das System darf weder an eine Stromquelle angeschlossen sein noch eine Verbindung mit einer Telekommunikationseinrichtung, einem Netzwerk oder einer Modem-Leitung haben, wenn die Gehäuseabdeckung entfernt wird. Nehmen Sie das System nicht ohne die Abdeckung in Betrieb.

ADVERTENCIAS

El sistema está diseñado para funcionar en un entorno de trabajo normal. Escoja un lugar:

- Limpio y libre de partículas en suspensión (salvo el polvo normal)
- Bien ventilado y alejado de fuentes de calor, incluida la luz solar directa.
- Alejado de fuentes de vibración.
- Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos.
- En regiones con frecuentes tormentas eléctricas, se recomienda conectar su sistema a un eliminador de sobrevoltage y desconectar el módem de las líneas de telecomunicación durante las tormentas.
- Previsto de una toma de tierra correctamente instalada.

No intente modificar ni usar el cable de alimentación de corriente alterna, si no se corresponde exactamente con el tipo requerido.

Asegúrese de que cada vez que se quite la cubierta del chasis, el sistema haya sido desconectado de la red de alimentación y de todos lo enlaces de telecomunicaciones, de red y de líneas de módem. No ponga en funcionamiento el sistema mientras la cubierta esté quitada

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einerqualifizierten Servicestelle zu überprüfen:
    a— Netzkabel oder Netzstecker sint beschädigt.
    b— Flüssigkeit ist in das Gerät eingedrungen.
    c— Das Gerät war Feuchtigkeit ausgesetzt.
    d— Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e— Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f— Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanscluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

Limited Hardware Warranty

Intel warrants to the original owner that the hardware product delivered in this package will be free from defects in material and workmanship for three (3) years following the latter of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within thirty (30) days from purchase. This warranty does not cover the product if it is damaged in the process of being installed. Intel recommends that you have the company from whom you purchased this product install the product.

INTEL RESERVES THE RIGHT TO FILL YOUR ORDER WITH A PRODUCT CONTAINING NEW OR REMANUFACTURED COMPONENTS. THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF NONINFRINGEMENT OF INTELLECTUAL PROPERTY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION, SAMPLE OR OTHERWISE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number either to the company from whom you purchased it or to Intel (North America only). If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either new or remanufactured product or parts, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original three (3) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

Returning a Defective Product (RMA)
Before returning any product, contact an Intel Customer Support Group and obtain an RMA number by calling:

North America only: (916) 377-7000
Other locations: Return the product to the place of purchase.

If the Customer Support Group verifies that the product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the product. Intel cannot accept any product without an RMA number on the package.

LIMITATION OF LIABILITY AND REMEDIES

INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, INFRINGEMENT OF INTELLECTUAL PROPERTY, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.

Critical Control Applications: Intel specifically disclaims liability for use of the hardware product in critical control applications (including, for example only, safety or health care control systems, nuclear energy control systems, or air or ground traffic control systems) by Licensee or Sublicensees, and such use is entirely at the user's risk. Licensee agrees to defend, indemnify, and hold Intel harmless from and against any and all claims arising out of use of the hardware product in such applications by Licensee or Sublicensees.

Software: Software provided with the hardware product is not covered under the hardware warranty described above. See the applicable software license agreement which shipped with the hardware product for details on any software warranty.

Limited Hardware Warranty (Europe only)

Intel warrants to the original owner that the hardware product delivered in this package will be free from defects in material and workmanship for three (3) years following the latter of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within thirty (30) days from purchase. This warranty does not cover the product if it is damaged in the process of being installed. Intel recommends that you have the company from whom you purchased this product install the product.

INTEL RESERVES THE RIGHT TO FILL YOUR ORDER WITH A PRODUCT CONTAINING NEW OR REMANUFACTURED COMPONENTS. THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF NONINFRINGEMENT OF INTELLECTUAL PROPERTY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION, SAMPLE OR OTHERWISE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number either to (a) the company from whom you purchased it or (b) to Intel, North America only (if purchased in Europe you must deliver the product to "(a)". If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either new or remanufactured product or parts, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original three (3) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

Returning a Defective Product (RMA)
Before returning any product, contact an Intel Customer Support Group and obtain an RMA number by calling the non-toll free numbers below:

Country	Number	Language
France	+33 (0) 1 41 91 85 29	French
Germany	+49 (0) 69 9509 6099	German
Italy	+39 (0) 2 696 33276	Italian
UK	+44 (0) 870 607 2439	English

If the Customer Support Group verifies that the product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the product. Intel cannot accept any product without an RMA number on the package.

LIMITATION OF LIABILITY AND REMEDIES

INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, INFRINGEMENT OF INTELLECTUAL PROPERTY, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Critical Control Applications: Intel specifically disclaims liability for use of the hardware product in critical control applications (including, for example only, safety or health care control systems, nuclear energy control systems, or air or ground traffic control systems) by Licensee or Sublicensees, and such use is entirely at the user's risk. Licensee agrees to defend, indemnify, and hold Intel harmless from and against any and all claims arising out of use of the hardware product in such applications by Licensee or Sublicensees.

Software: Software provided with the hardware product is not covered under the hardware warranty described above. See the applicable software license agreement which shipped with the hardware product for details on any software warranty.

This limited hardware warranty shall be governed by and construed in accordance with the laws of England and Wales. The courts of England shall have exclusive jurisdiction regarding any claim brought under this warranty.

Limitation de garantie du matériel (Europe)

Intel garantit au propriétaire original que le produit matériel livré dans le présent coffret est exempt de défaut matériel ou de fabrication pour une période de trois (3) ans à compter de la plus récente des dates suivantes : (i) la date d'achat uniquement si vous vous êtes inscrit en renvoyant la carte d'inscription de la façon indiquée, avec une preuve d'achat ; (ii) la date de fabrication ou (iii) la date d'inscription électronique à condition qu'elle ait lieu dans les 30 jours suivant l'achat. La présente garantie sera nulle si le produit matériel est endommagé lors de son installation. Intel recommande de faire installer le produit matériel par la société auprès de laquelle il a été acheté.

INTEL SE RESERVE LE DROIT DE VOUS LIVRER UN PRODUIT CONTENANT DES COMPOSANTS NOUVEAUX OU REPARES. CETTE GARANTIE REMPLACE TOUTES LES AUTRES GARANTIES, EXPRESSES, TACITES OU LEGALES, Y COMPRIS, MAIS SANS QUE CETTE ENUMERATION SOIT LIMITATIVE, LES GARANTIES CONCERNANT LE NON RESPECT DE LA PROPRIETE INTELLECTUELLE, LA QUALITE SATISFAISANTE, L'ADEQUATION POUR UN USAGE PARTICULIER, OU TOUTE AUTRE GARANTIE ISSUE DE TOUT AUTRE PROPOSITION, SPECIFICATION, ECHANTILLON OU AUTRE.

La présente garantie ne couvre pas le remplacement de produits matériels endommagés par abus, accident, mauvaise utilisation, négligence, altération, réparation, catastrophe, installation ou tests incorrects. Si le produit matériel s'avère défectueux pour une autre raison, Intel décidera de le remplacer ou de le réparer gratuitement, à l'exception des cas énumérés ci-après, à condition que le produit soit renvoyé avec un numéro d'autorisation de retour du matériel (ARM) à (a) la société auprès de laquelle il a été acheté ou (b) à Intel, en Amérique du Nord seulement (si l'achat a eu lieu en Europe vous devez le renvoyer à "(a)". Si vous expediéz le produit matériel, vous devez assumer le risque de dégâts ou de perte pendant le transport. Vous devez utiliser le coffret original (ou l'équivalent) et payer les frais de transport. Intel peut réparer le produit matériel ou le remplacer par un produit neuf ou remis à neuf, le produit renvoyé devenant la propriété d'Intel. Intel garantit que le produit matériel réparé ou de remplacement est exempt de défaut matériel ou de fabrication pendant la plus longue des périodes suivantes: (i) quatre-vingt-dix (90) jours à compter de la date de retour; ou (ii) la période encore couverte par la garantie originale de trois (3) ans.

La présente garantie vous accorde des droits juridiques spécifiques et vous pouvez également disposer d'autres droits variant d'un Etat à l'autre. Tous les composants ou pièces du produit matériel sont couverts par la garantie limitée d'Intel relative à ce dernier ; il peut contenir des pièces recyclées, entièrement testées et garanties comme neuves. Pour plus d'informations sur la garantie, appelez l'un des numéros énumérés ci-après.

Retour d'un produit défectueux (ARM)
Avant de retourner un produit matériel, contactez le service d'assistance à la clientèle Intel pour obtenir un numéro ARM.

Pays	Numéro	Langue
France	+33 (0) 1 41 91 85 29	Français
Allemagne	+49 (0) 69 9509 6099	Allemand
Italie	+39 (0) 2 696 33276	Italien
R.U.	+44 (0) 870 607 2439	Anglais

Si le service d'assistance confirme que le produit est défectueux, il demandera au Département d'autorisation de retour de matériel de vous attribuer un numéro ARM à indiquer sur l'emballage externe. Intel ne peut accepter aucun produit sans numéro ARM.

LIMITATION DE RESPONSABILITE ET DE RECOURS

INTEL DECLINE TOUTE RESPONSABILITE RELATIVE A DES DOMMAGES INDIRECTS OU SPECULATIFS (Y COMPRIS, SANS LIMITATION DES ELEMENTS CI-DESSUS, LES DOMMAGES CONSECUTIFS, ACCIDENTELS ET SPECIAUX) DECOULANT DE L'UTILISATION OU DE L'INCAPACITE D'UTILISER CE PRODUIT, DUS A UN CONTRAT, UNE NEGLIGENCE, UN TORT OU COUVERTS PAR TOUTE GARANTIE, MEME SI LA POSSIBILITE D'UN TEL DOMMAGE A DEJA ETE PORTEE A LA CONNAISSANCE D'INTEL, Y COMPRIS, MAIS SANS QUE CETTE ENUMERATION SOIT LIMITATIVE, UNE PRIVATION DE JOUISSANCE, UN NON RESPECT DE LA PROPRIETE INTELLECTUELLE, UNE INTERRUPTION DES ACTIVITES ET UN MANQUE A GAGNER . NONOBSTANT LA DECLARATION QUI PRECEDE, LA RESPONSABILITE GLOBALE DE INTEL CONCERNANT TOUS LES LITIGES RELATIFS AU PRESENT ACCORD NE SERA PAS SUPERIEURE AU PRIX PAYE POUR LE PRODUIT. CES LIMITATIONS DE RESPONSABILITE POTENTIELLE ONT CONSTITUE UN FACTEUR DETERMINANT LORS DE LA FIXATION DU PRIX DU PRODUIT. INTEL N'ASSUME AUCUNE AUTRE RESPONSABILITE ET N'AUTORISE QUICONQUE A LE FAIRE EN SON NOM.

Applications de contrôle critique: Intel décline toute responsabilité en cas d'utilisation du produit matériel dans le cadre d'applications de contrôle critique (y compris et pour ne citer que des exemples, les systèmes de contrôle de sécurité ou de services médicaux, les systèmes de contrôle d'énergie nucléaire, ou de trafic terrestre ou aérien) par le licencié ou le sous-licencié, l'utilisateur encourt entièrement les risques d'une telle utilisation. Le titulaire de la licence accepte de défendre, d'indemniser et de garantir Intel de toute réclamation survenant par suite de l'utilisation du produit matériel dans de telles applications par le licencié ou le sous-licencié.

Logiciel: Le logiciel fourni avec le produit matériel n'est pas couvert par la garantie du matériel décrite ci-dessus. Consultez l'accord de licence du logiciel qui accompagne le produit matériel pour obtenir des détails sur la garantie du logiciel.

La garantie limitée du matériel est régie et interprétée par les lois en vigueur en Angleterre et au Pays de Galles. Les tribunaux anglais jouissent d'une juridiction exclusive en matière de litige concernant cette garantie.

Garanzia limitata sull'hardware (valida solo in Europa)

Intel garantisce al proprietario originale che il prodotto hardware incluso in questo pacchetto è privo di difetti in materiale e in lavorazione per un periodo di tre (3) anni a partire dall'ultima data tra: (i) la data di acquisto, solo nel caso in cui l'utente effettua la registrazione tramite la scheda di registrazione, come indicato, accompagnata dalla prova di acquisto; oppure (ii) la data di fabbricazione; oppure (iii) la data di registrazione, se effettuata per via elettronica, a condizione che tale registrazione avvenga entro trenta (30) giorni dall'acquisto. Questa garanzia non copre il prodotto nel caso questo fosse danneggiato durante l'installazione. Intel raccomanda di fare installare il prodotto dall'azienda da cui il prodotto è stato acquistato.

INTEL SI RISERVA IL DIRITTO DI ONORARE L'ORDINAZIONE CON UN PRODOTTO CONTENENTE PARTI NUOVE O RIFABBRICATO. LA GARANZIA QUI SOPRA SOSTITUISCE QUALSIASI ALTRA GARANZIA, SIA QUELLA ESPLICITA, IMPLICITA O STATUTORIA, INCLUSO, MA NON LIMITATO A, QUALSIASI GARANZIA DI NON VIOLAZIONE DI PROPRIETÀ INTELLETTUALE, QUALITÀ SODDISFACENTE, IDONEITÀ A QUALSIASI SCOPO PARTICOLARE O QUALSIASI GARANZIA DERIVANTE DA PROPOSTA, SPECIFICAZIONI, CAMPIONI O ALTRO.

Questa garanzia non include la sostituzione di prodotti danneggiati a causa di abuso, incidente, uso inappropriato, negligenza, alterazione, riparazione, disastro, installazione o controllo inadeguati. Se il prodotto viene considerato difettoso per altri motivi, Intel, a sua discrezione, sostituirà o riparerà il prodotto, a proprie spese, eccetto nei casi qui sotto menzionati, a condizione che il prodotto venga consegnato congiuntamente al numero di autorizzazione per la restituzione del materiale (RMA, Return Material Authorization) (a) all'azienda da cui si è acquistato il prodotto, oppure (b) a Intel, solo quando in Nord America (se il prodotto è stato acquistato in Europa, sarà necessario consegnare il prodotto seguendo le modalità indicate in "(a)"). Se il prodotto viene inviato, il mittente si assume la responsabilità in caso di danni o di perdita durante il tragitto. È necessario utilizzare l'imballaggio originale del prodotto (o un suo equivalente) e pagare le spese di spedizione. Intel sostituirà o riparerà il prodotto (o la parte) con uno nuovo o uno rifabbricato, e il prodotto restituito diventerà proprietà di Intel. Intel garantisce che il prodotto riparato o sostituito sarà privo di difetti in materiale e in lavorazione per un periodo comunque non superiore: (i) a novanta (90) giorni dalla data di spedizione all'utente; oppure (ii) al periodo rimanente nella garanzia originale di tre (3) anni.

Questa garanzia dà all'utente diritti legali specifici; potrebbero esistere altri diritti, variabili da stato a stato. Tutte le parti e i componenti contenuti in questo prodotto sono coperti dalla garanzia limitata di Intel relativa a questo prodotto; il prodotto potrebbe contenere parti riciclate, completamente collaudate e garantite come nuove. Per maggiori informazioni sulla garanzia, chiamare uno dei numeri indicati qui sotto.

Restituzione di prodotti difettosi (RMA)
Prima di restituire un prodotto, contattare l'assistenza tecnica di Intel e richiedere un numero RMA; i numeri verdi sono qui sotto elencati:

Paese	Numero	Lingua
Francia	+33 (0) 1 41 91 85 29	Francese
Germania	+49 (0) 69 9509 6099	Tedesco
Italia	+39 (0) 2 696 33276	Italiano
Regno Unito	+44 (0) 870 607 2439	Inglese

Se il gruppo di supporto alla clientela determina che il prodotto è difettoso, richiederà l'emissione di un numero di autorizzazione per la restituzione del materiale (RMA) da porre all'esterno dell'imballaggio del prodotto. Intel non accetterà prodotti sprovvisti di tale numero visibile sull'imballaggio.

LIMITAZIONI DI RESPONSABILITÀ E RIMEDI

INTEL NON POTRÀ ESSERE CONSIDERATA RESPONSABILE DI ALCUN DANNO, DIRETTO O SPECULATIVO (INCLUSI, SENZA LIMITAZIONI COME INDICATO IN PRECEDENZA, I DANNI CONSEQUENZIALI, INCIDENTALI E SPECIALI) DERIVANTI DALL'USO O DALLA IMPOSSIBILITÀ DI UTILIZZARE QUESTO PRODOTTO, PER MOTIVI NON CONTEMPLATI NEL CONTRATTO, O DOVUTI A NEGLIGENZA, TORTO O SOTTO QUALSIASI GARANZIA, INDIPENDENTEMENTE DAL FATTO CHE INTEL SIA A CONOSCENZA O MENO DELLA POSSIBILITÀ DI TALI DANNI, INCLUSI, MA NON LIMITATI ALLA PERDITA D'USO, VIOLAZIONE DI PROPRIETÀ INTELLETTUALE, INTERRUZIONI D'AFFARI E PERDITA DI PROFITTI, NONOSTANTE QUANTO DETTO IN PRECEDENZA, LA RESPONSABILITÀ TOTALE DI INTEL NEI CONFRONTI DEI RECLAMI, SECONDO QUESTO ACCORDO, NON ECCEDERÀ IL PREZZO PAGATO PER IL PRODOTTO. QUESTE LIMITAZIONI SULLE RESPONSABILITÀ POTENZIALI SONO STATE FATTORE DECISIVO NELLA DETERMINAZIONE DEL PREZZO DEL PRODOTTO. INTEL NON ASSUME, NÉ AUTORIZZA ALCUNO AD ASSUMERE PER SÉ, NESSUN'ALTRA RESPONSABILITÀ.

Applicazioni di controllo di situazioni critiche: Intel disconosce specificatamente la responsabilità nel caso di uso dell'hardware in applicazioni di controllo di situazioni critiche (inclusi, al solo scopo di esempio, sistemi di controllo della sicurezza o della salute, dell'energia nucleare, o sistemi di controllo aereo o terrestre) da parte dei licenziatari o dei sottolicenziatari, e tale uso fa parte completamente del rischio intrapreso dall'utente. Il licenziatario è d'accordo nel difendere, indennizzare e liberare Intel da ogni reclamo risultante dall'uso del prodotto hardware in tale applicazioni da parte del licenziatario o del sottolicenziatario.

Software: il software accluso al prodotto hardware non è coperto dalla garanzia dell'hardware sopra descritta. Per maggiori dettagli sulla garanzia del software, vedere l'accordo di licenza relativo al software, inviato assieme al prodotto hardware.

Questa garanzia limitata dell'hardware è governata da, ed è conforme a, le leggi di Inghilterra e Galles. Il tribunale di Inghilterra avrà la completa giurisdizione su qualsiasi reclamo presentato sotto questa garanzia.

Beschränkte Hardwaregarantie (Nur für Europa)

Intel garantiert dem ursprünglichen Eigentümer, daß die in diesem Paket enthaltene Hardware keine Material- oder Herstellungsfehler aufweist. Diese Garantie gilt für drei (3) Jahre (a) nach dem Kaufdatum, wenn die ausgefüllte Registrierungskarte entsprechend den darauf enthaltenen Angaben zusammen mit einem Kaufnachweis eingesendet wurde; oder (b) nach dem Herstellungsdatum; oder (c) nach dem Registrierungsdatum, wenn die Registrierung innerhalb von 30 Tagen auf elektronischem Weg durchgeführt wird. Diese Garantie entfällt, wenn die Hardware bei der Installation beschädigt wird. Intel empfiehlt, die Installation durch den Verkäufer der Hardware durchführen zu lassen.

INTEL BEHÄLT SICH DAS RECHT VOR, IHREN AUFTRAG MIT EINEM PRODUKT ZU ERFÜLLEN, DAS NEUE ODER ERNEUERTE KOMPONENTEN ENTHÄLT. OBIGE GARANTIE GILT ANSTELLE ALLER ANDEREN AUSDRÜCKLICHEN, STILLSCHWEIGENDEN ODER GESETZLICH FESTGELEGTEN GARANTIEN. AUSGESCHLOSSEN SIND DAMIT AUCH UNTER ANDEREM ALLE GARANTIEN FÜR DIE VERKEHRSFÄHIGKEIT, DIE VERLETZUNG DER RECHTE VON DRITTEN, DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER GARANTIEN, DIE IM ZUSAMMENHANG MIT EINEM ANGEBOT, EINER SPEZIFIKATION ODER EINEM MUSTER GEGEBEN WURDEN.

Diese Garantie schließt den Hardware-Ersatz bei Beschädigung aufgrund von Mutwilligkeit, Unfall, falscher Verwendung, Fahrlässigkeit, Umänderung, Reparatur, Katastrophen, falscher Installation oder unvorschriftsmäßigem Testen aus. Wenn das Hardwareprodukt aus anderen Gründen beschädigt ist, liegt die Entscheidung bei Intel, ob die Hardware mit Ausnahme der im folgenden beschriebenen Einschränkungen kostenlos ersetzt oder repariert wird. Hierzu müssen Sie das Produkt zusammen mit einer Rückgabenummer (RMA-Nummer, siehe unten) entweder (a) an den Verkäufer des Produkts oder (b) an Intel zurücksenden (bei Kauf in Europa muß das Produkt an "(a)" geliefert werden). Das Risiko des Verlusts oder der Beschädigung während des Transports liegt bei Ihnen als Käufer. Sie müssen zum Versenden die Originalverpackung (oder einen gleichwertigen Ersatz) verwenden und die Versandkosten übernehmen. Intel ersetzt die Hardware entweder durch ein neues oder ein neuwertiges Produkt. Das zurückgegebene Hardwareprodukt wird Eigentum von Intel. Intel garantiert, daß das reparierte oder ersetzte Hardwareprodukt für einen Zeitraum von: (i) neunzig (90) Tagen ab Rückgabedatum oder (ii) für die verbleibende Zeit der ursprünglichen Garantie von drei (3) Jahren frei von Material- und Herstellungsfehlern ist. Dabei gilt jeweils der längere Zeitraum.

Mit dieser Garantie erhalten Sie bestimmte Rechte, die je nach Staat durch weitere Rechte ergänzt werden können. Alle Teile oder Komponenten dieses Hardwareprodukts werden durch die beschränkte Hardwaregarantie von Intel abgedeckt. Das Hardwareprodukt kann vollständig getestete, wiederverwendete Teile enthalten, die derselben Garantie wie neue Produkte unterliegen. Informationen zur Garantie erhalten Sie unter einer der Intel Kundendienstnummern, die am Ende dieses Handbuchs zu finden sind.

Rückgabe eines beschädigten Produkts (RMA)

Bevor Sie ein Hardwareprodukt zurücksenden, sollten Sie sich vom Intel Kundendienst eine sogenannte RMA-Nummer zuweisen lassen, indem Sie eine der folgenden gebührenpflichtigen Telefonnummern anrufen:

Land	Telefon	Sprache
Frankreich	+33 (0) 1 41 91 85 29	Französisch
Deutschland	+49 (0) 69 9509 6099	Deutsch
Italien	+39 (0) 2 696 33276	Italienisch
GB	+44 (0) 870 607 2439	Englisch

Nachdem die Beschädigung vom Kundendienst bestätigt worden ist, wird von der zuständigen Abteilung eine Rückgabenummer (RMA-Nummer) ausgegeben, die auf der äußeren Verpackung der Hardware angebracht werden muß. Intel akzeptiert kein Produkt ohne RMA-Nummer auf der Verpackung.

Haftungsbeschränkung und Rechtsmittel

INTEL HAFTET NICHT FÜR INDIREKTE ODER SPEKULATIVE SCHÄDEN (EINSCHLIESSLICH ALLER FOLGESCHÄDEN SOWIE ALLER ZUFÄLLIGEN UND BESONDEREN SCHÄDEN), DIE DURCH DIE VERWENDUNG ODER NICHTVERWENDBARKEIT DIESES PRODUKTS ENTSTEHEN, SEI DIES IM ZUSAMMENHANG MIT EINER VERTRAGLICHEN VERPFLICHTUNG, AUFGRUND VON FAHRLÄSSIGKEIT, DURCH UNERLAUBTE HANDLUNGEN ODER IM RAHMEN EINER GARANTIE. DIES GILT AUCH FÜR FÄLLE, IN DENEN INTEL ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN, DIE SICH UNTER ANDEREM DURCH NUTZUNGSAUSFÄLLE, BETRIEBSUNTERBRECHUNGEN UND GEWINNVERLUSTE ERGEBEN KÖNNEN, IN KENNTNIS GESETZT WURDE.

UNGEACHTET DER GEWÄHRTEN GARANTIE ÜBERSTEIGT DIE HAFTUNG VON INTEL IM RAHMEN DIESER VEREINBARUNG IN KEINEM FALL DEN KAUFPREIS DES HARDWAREPRODUKTS. DIESE HAFTUNGSBESCHRÄNKUNG IST EIN WESENTLICHER FAKTOR BEI DER FESTLEGUNG DES PREISES FÜR DAS HARDWAREPRODUKT. INTEL ÜBERNIMMT KEINE WEITERE HAFTUNG UND ERTEILT DRITTEN KEINERLEI BEFUGNIS, FÜR INTEL EINE WEITERE HAFTUNG ZU ÜBERNEHMEN.

Steuer- und Überwachungsanwendung von hoher Wichtigkeit: Intel schließt insbesondere die Haftung bei der Verwendung des Hardwareprodukts mit Steueranwendungen von hoher Wichtigkeit (z.B. Sicherheits- und Krankenversicherungssysteme, Steuersysteme für Nuklearanlagen sowie Verkehrsüberwachungssysteme für Boden- und Luftverkehr) durch den Lizenznehmer oder Unterlizenznehmer ab, und eine derartige Verwendung liegt ausschließlich in der Verantwortung des Benutzers. Der Lizenznehmer erklärt sich bereit, Intel zu verteidigen und schadlos zu halten bezüglich aller Klagen, die aus der Verwendung eines Hardwareprodukts für solche Zwecke vom Lizenznehmer oder Unterlizenznehmern erhoben werden.

Software: Die mit diesem Hardwareprodukt gelieferte Software wird von der oben beschriebenen Hardwaregarantie nicht abgedeckt. Bitte lesen Sie die entsprechende Softwarelizenzvereinbarung, die mit dem Hardwareprodukt geliefert wurde, um genaue Informationen zur Softwaregarantie zu erhalten.

Diese eingeschränkte Hardwaregarantie unterliegt den Gesetzen von England und Wales. Die englischen Gerichte sind Gerichtsstand für alle Klagen, die im Rahmen der Garantie erhoben werden.

Garantía limitada de hardware (sólo para Europa)

Intel garantiza al propietario original que el producto de hardware entregado en este paquete no tendrá defectos de materiales ni fabricación durante tres (3) años contados a partir de la fecha que resulte más reciente de entre las opciones siguientes: (i) la fecha de compra, sólo si devuelve la tarjeta de registro con prueba de compra de la forma indicada al respecto para registrarse; o bien (ii) la fecha de fabricación; o (iii) la fecha de registro, si éste se ha producido por medios electrónicos y dentro de los treinta (30) días siguientes a la compra. Esta garantía no cubre los daños sufridos por el producto durante el proceso de instalación. Intel recomienda que sea la empresa a la que adquirió el producto la que se encargue de su instalación.

INTEL SE RESERVA EL DERECHO DE CUMPLIMENTAR EL PEDIDO CON UN PRODUCTO QUE CONTENGA COMPONENTES NUEVOS O REFRABRICADOS. LA GARANTÍA ANTERIOR PREVALECE SOBRE CUALQUIER OTRA GARANTÍA, YA SEA EXPLÍCITA, IMPLÍCITA O REGLAMENTARIA, INCLUIDAS, SIN LIMITACIÓN, CUALESQUIERA GARANTÍAS DE NO INFRINGIMIENTO DE LA PROPIEDAD INTELECTUAL, CALIDAD SATISFACTORIA, ADECUACIÓN PARA UNA FINALIDAD DETERMINADA O CUALQUIER GARANTÍA SURGIDA DE CUALQUIER PROPUESTA, ESPECIFICACIÓN, MUESTRA O DE OTRA CLASE.

Esta garantía no cubre la sustitución de productos dañados por abuso, accidente, mal uso, negligencia, alteración, reparación, desastre, instalación incorrecta o pruebas incorrectas. Si el producto tuviera cualquier otro defecto, Intel se reserva la opción de reemplazar o reparar el producto sin cargo alguno, excepto los descritos a continuación, siempre que el producto se entregue con un número de autorización de devolución de material (RMA), a (a) la empresa a la que se adquirió o (b) a Intel, sólo en América del Norte (si lo adquirió en Europa, debe entregar el producto a "(a)". Si envía el producto, debe asumir el riesgo de daños o pérdida en el transporte. Debe utilizar el embalaje original (o equivalente) y costear los gastos de envío. Intel puede reemplazar o reparar el producto con piezas o productos nuevos o refabricados, y el producto devuelto pasa a ser propiedad de Intel. Intel garantiza que el producto reparado o reemplazado no tendrá defectos materiales ni de fabricación durante el periodo que resulte mayor de los siguientes: (i) noventa (90) días desde la fecha de envío; o (ii) el periodo de tiempo restante de la garantía original de tres (3) años.

Esta garantía le otorga derechos legales concretos y puede tener otros derechos que varían según la jurisdicción. Todas las piezas o componentes que contiene este producto están cubiertos por la garantía limitada de Intel sobre este producto; el producto puede contener piezas recicladas, completamente comprobadas, garantizadas como si de piezas nuevas se tratase. Si desea obtener más información sobre la garantía, puede llamar a uno de los números indicados a continuación.

Devolución de productos defectuosos (RMA)

Antes de devolver cualquier producto, póngase en contacto con el grupo de Asistencia al cliente de Intel y obtenga un número RMA en uno de los siguientes números no gratuitos:

País	Número	Idioma
Francia	+33 (0) 1 41 91 85 29	Francés
Alemania	+49 (0) 69 9509 6099	Alemán
Italia	+39 (0) 2 696 33276	Italiano
Reino Unido	+44 (0) 870 607 2439	Inglés

Si el grupo de Asistencia al cliente comprueba que el producto es defectuoso, se podrá en contacto con el Departamento de autorización de devolución de material para que éste le envíe un número RMA que debe colocar en el envoltorio externo del producto. Intel no puede aceptar productos sin el número RMA en el paquete.

LIMITACIÓN DE RESPONSABILIDAD Y REPARACIONES

INTEL NO SERÁ RESPONSABLE DE NINGÚN DAÑO INDIRECTO O ESPECULATIVO (INCLUIDOS, SIN LIMITAR A LOS ANTERIORES, LOS DAÑOS INDIRECTOS, INCIDENTALES Y ESPECIALES) PRODUCIDO POR EL USO O POR LA IMPOSIBILIDAD DEL USO DE ESTE PRODUCTO, YA PROVENGA DE CONTRATO, NEGLIGENCIA, AGRAVIO O BAJO CUALQUIER GARANTÍA, SIN IMPORTAR QUE INTEL HAYA RECIBIDO PREVIO AVISO DE LA POSIBILIDAD DE DICHOS DAÑOS, INCLUIDOS, AUNQUE NO LIMITADOS A, PÉRDIDAS DE USO, INFRINGIMIENTO DE LA PROPIEDAD INTELECTUAL, SUSPENSIÓN DEL EJERCICIO COMERCIAL Y PÉRDIDA DE BENEFICIOS, A PESAR DE LO ANTERIOR, TODA LA RESPONSABILIDAD DE INTEL SOBRE LAS RECLAMACIONES REALIZADAS BAJO ESTE ACUERDO NO EXCEDERÁ EL PRECIO PAGADO POR EL PRODUCTO. ESTAS LIMITACIONES SOBRE LAS RESPONSABILIDADES POTENCIALES HAN CONSTITUIDO UN ELEMENTO ESENCIAL A LA HORA DE DETERMINAR EL PRECIO DEL PRODUCTO. INTEL NO ASUME NI AUTORIZA QUE NINGUNA PERSONA ASUMA EN SU LUGAR NINGUNA OTRA RESPONSABILIDAD.

Aplicaciones de control crítico: Intel deniega específicamente la responsabilidad por el uso del producto de hardware en aplicaciones de control crítico (incluidos, sólo a modo de ejemplo, los sistemas de seguridad o atención sanitaria, sistemas de control de energía nuclear o sistemas de control de tráfico aéreo o rodado) por Receptores o Subreceptores de la Licencia, y dicho uso queda enteramente a riesgo del usuario. El Receptor de la Licencia acuerda defender, indemnizar y mantener la inocencia de Intel por y contra toda reclamación surgida del uso del producto de hardware en tales aplicaciones por parte del Receptor o Subreceptor de la Licencia.

Software: El software proporcionado con el producto de hardware no está cubierto por la garantía de hardware descrita anteriormente. Si desea obtener información detallada sobre las garantías de software, consulte el acuerdo de licencia correspondiente al software incluido con el producto de hardware.

Esta garantía limitada de hardware se regirá e interpretará de acuerdo con las leyes de Inglaterra y Gales. Los tribunales de Inglaterra tendrán la exclusiva jurisdicción sobre todas las reclamaciones presentadas bajo esta garantía.

Index

Symbols

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Intel Customer Support

You can purchase a range of support services including hardware, software, phone and on-site installation services. Services are designed and packaged for ease of ordering and provide reliable, flexible support for your networking equipment. For details about Intel® support services, go to www.intel.com/network/services.

Worldwide Access to Technical Support

Intel has technical support centers worldwide. Technicians who speak the local languages staff many of the centers. Visit our Web site at support.intel.com or contact your local dealer/distributor.

United States and Canada only

For support, call **(800) 838-7136** or **(916) 377-7000**.

Japan only

For support, call **0120-868686**.

Other areas (Access number + 800-838-7136)

For support in other countries, use the following table to dial the toll-free support number. Using the table, locate the country from which you are calling, dial the access number, wait for the dial tone, and then dial 800-838-7136.

Country	Access Number
Australia	1-800-881-011
Austria [1 4]	022-903-011
Belgium [1]	0-800-100-10
China [3]	10811
Denmark	8001-0010
Finland [1]	9800-100-10
France (Includes Andorra)	19-0011
Germany	0130-0010
Hong Kong	800-1111
India [5]	000-117

Indonesia [2]	001-801-10
Italy (Includes Vatican City) [1]	172-1011
Korea [1]	0-911
Malaysia [4]	800-0011
Netherlands [1]	06-022-9111
New Zealand	000-911
Norway	800-190-11
Pakistan	0080001001
Philippines	105-11
Poland [1 3]	0-0-800-111-1111
Portugal [3]	05017-1-288
RSA (South Africa)	0-800-99-0123
Russia [1 2 3]	755-5042
Singapore	800-0111-111
Spain	900-99-00-11
Sri Lanka	430-430
Sweden	020-795-611
Switzerland [1]	0-800-550011
Taiwan [1]	0080-10288-0
Thailand [5]	0019-991-1111
United Kingdom (BT) [3]	0800-89-0011
United Kingdom (Mercury) [3]	0500-89-0011
Vietnam	12010288

Notes:

1 Public phones require coin deposit

2 Use phones allowing international access

3 May not be available from every phone

4 Public phones require local phone payment through the call duration

5 Not available from public phones