User Guide for the Catalyst Express 500 Switches

Cisco IOS Release Number 12.2(25)FY
September 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8122-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

User Guide for the Catalyst Express 500 Switches

CONTENTS

CHAPTER 2

CHAPTER 3

APPENDIX A

APPENDIX B

INDEX

Welcome

Welcome to the user guide for the Catalyst Express 500 switches.

This guide provides information for those who will install or manage the switch. Although extensive networking knowledge is not necessary, we recommend familiarity with the fundamentals. For this information, see Cisco Networking Basics at:

http://www.cisco.com/en/US/netsol/ns339/ns392/networking_solutions_networking_basics_home.html

Note This guide focuses on the concepts and tasks that are available from the switch hardware and the device manager GUI that is embedded in the switch software.

Enhanced Catalyst Express 500 features and procedures are only available from the Cisco Network Assistant network management application. This application can be downloaded from Cisco.com. Refer to the Network Assistant documentation about these enhanced switch features.

How to Use This Guide

This guide covers the topics to help you learn about the switch and how to effectively use it. This guide is organized in this way:

Chapters	Purpose
Introduction	This chapter describes the software and hardware features and benefits so that you can decide how to use the switch to meet your network objectives. It includes a description of the device manager user interface, the switch hardware and software requirements, and the supported related products.
Setup and Installation	This chapter provides the recommendations, the guidelines, and the procedures so that you can set up the switch for the first time and install it. It also includes procedures on how to display the device manager interface through a secured mode. Use this chapter with the procedures in the *Getting Started Guide for the Catalyst Express 500 Switches*.
Customization	This chapter describes the switch software features that you can tailor according to your network needs. Use this chapter with the procedures in the device manager online help.
Monitoring	This chapter describes the tools that you can use to monitor the status and the performance of the switch. Use this chapter with the procedures in the device manager online help.
Troubleshooting	This chapter describes the diagnostic tests and report and other troubleshooting features to help you resolve switch and network problems. Use this chapter with the procedures in the device manager online help.
Reference	This chapter has the switch technical specifications, cabling guidelines, and connector specifications.
Cisco Support Resources	This chapter describes the Cisco resources where you can learn more about networking and the switch, can obtain Cisco documentation, and can access Cisco Small and Medium-Sized Businesses (SMB) technical support.

Switch Documentation Set

These documents provide complete information about the switch and are available from this Cisco.com site:

http://www.cisco.com/univercd/cc/td/doc/product/lan/catex500/index.htm

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 3.

- *Release Notes for the Catalyst Express 500 Switches* (not orderable but available on Cisco.com).

  The release notes focus on important notes and issues that should be read before using the switch.

- *Getting Started Guide for the Catalyst Express 500 Switches* (order number DOC-7817084=).

  This guide focuses on the initial setup and installation of the switch.

- *User Guide for the Catalyst Express 500 Switches* (not orderable but available on Cisco.com).

  This guide describes the hardware and software features of the switch. It also provides the concepts that you need to know to optimize your use of the switch. Use this guide with the device manager online help.

- Device manager online help (available on the switch).

  The online help provides short descriptions of the software features and complete procedures on how to use the GUI to customize, monitor, and troubleshoot the switch.

- *Regulatory Compliance and Safety Information for the Catalyst Express 500 Switches* (order number DOC-7817085=).

  This document includes the regulatory statements and warnings, including translations.

Note Related product documentation is listed in the "Related Documentation" section on page xiv. Additional information about Cisco documentation and technical support resources are described in Chapter , "Cisco Support Resources."

Related Documentation

These documents provide information about the products supported on the switch:

- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide* (order number DOC-7815201=)

Introduction

Read this chapter to familiarize yourself with the features, benefits, and capabilities of the Catalyst Express 500 switches.

Note This chapter and the rest of this guide focus on the concepts and tasks that are available from the switch hardware and the device manager GUI that is embedded in the switch software.

Enhanced Catalyst Express 500 features and procedures are only available from the Cisco Network Assistant network management application. This application can be downloaded from Cisco.com. Refer to the Network Assistant documentation about these enhanced switch features.

Chapter Topics

Overview

The Catalyst Express switches (Table 1-1) provide networking for businesses with up to 250 employees. These switches provide network services to support data, voice, and mobile network demands. The services ensure transmission quality and reliability for data and voice traffic. They also provide security to protect against network attacks.

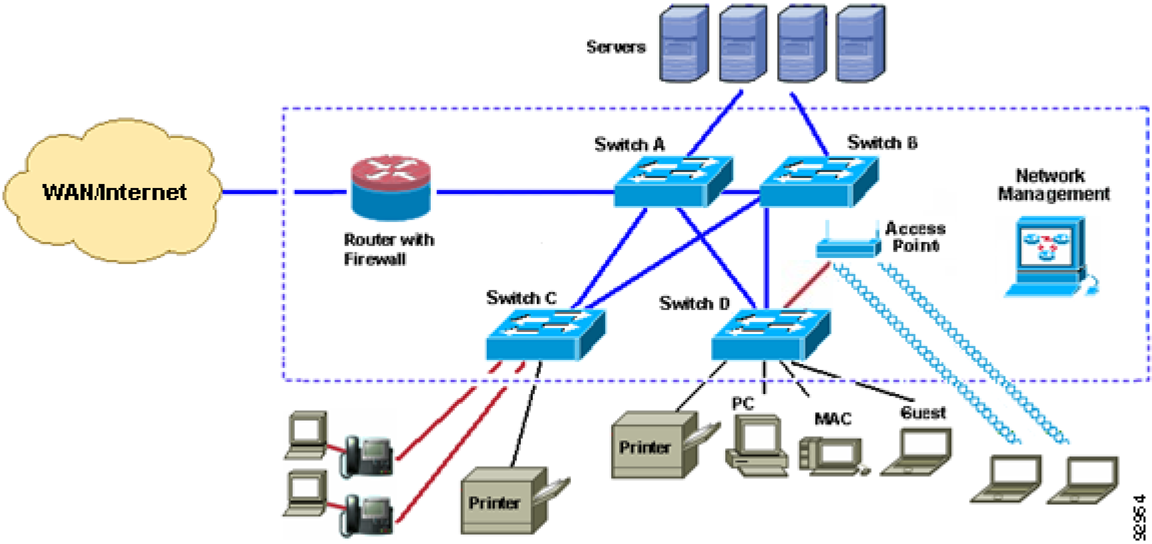
You can simply install the switch and allow it to operate without any further management intervention. You can also take advantage of the embedded software features—tools to quickly and easily set up, customize, monitor, and troubleshoot the switch—to optimize your use of the switch.

Table 1-1 Catalyst Express 500 Switch Models

Catalyst Express 500-24TT This switch is designed for providing standard connections to network users. It has: • 24 10/100 (*Fast Ethernet*) ports for desktop connectivity • 2 10/100/1000BASE-T (*Gigabit Ethernet*) ports for uplink or server connectivity
Catalyst Express 500-24LC This switch is designed for connecting wireless access points to your network. It has: • 20 10/100 ports for desktop connectivity • 4 10/100 Power-over-Ethernet (PoE) ports for desktop, wireless access point, IP telephony, or closed-circuit TV camera connectivity • 2 10/100/1000BASE-T or small form-factor pluggable (SFP) module ports for uplink or server connectivity
Catalyst Express 500-24PC This switch is designed for providing PoE connections to IP phones. It has: • 24 10/100 PoE ports for desktop, wireless, IP telephony, or closed-circuit TV camera connectivity • 2 10/100/1000BASE-T or SFP module ports for uplink or server connectivity
Catalyst Express 500G-12TC This switch is designed for high-speed connections to servers and switches. It has: • 8 10/100/1000BASE-T ports for high-speed, desktop connectivity • 4 10/100/1000BASE-T or SFP module ports for server aggregation or server connectivity

Figure 1-1 is an example network using Catalyst Express switches. Devices outside the dotted line are network users and network resources, such as servers and printers. Devices within the dotted line are switches, routers, and access points that enable communication between network users and provide access to network resources.

Figure 1-1 Catalyst Express Network Example



Any of the Catalyst Express switch models can be Switches A, B, C, and D in this network. To take full advantage of the different switch models, use the model that is designed for the type of connections that you require.

For example, use the Catalyst Express 500G-12TC for Switches A and B. This model has the most Gigabit Ethernet ports, and it is best suited to providing 1000-Mbps connections between switches and to servers.

Use either the Catalyst Express 500-24TT or the Catalyst Express 500G-12TC for Switches C and D. These switches are designed to provide high-speed (up to 100 Mbps and 1000 Mbps, respectively) connections to network users.

If you need to connect PoE devices to your network, use the Catalyst Express 500-24LC and the Catalyst Express 500-24PC. These switches can provide power to up to 4 or up to 24 PoE devices, respectively.

PoE connections from the switch provide both power and network access to PoE-capable devices, such as IP phones and access points. PoE devices can receive up to 15.4 W of power from their connections to the switch. PoE also helps reduce cabling costs. You can place PoE devices where power outlets are not available or are not convenient.

Multiple connections between the switches ensure that users maintain network access if any of the switches becomes overused or unavailable.

A network administrator can manage the network onsite or remotely through the device manager GUI (embedded in the Catalyst Express switches), through Cisco Network Assistant, or through a Simple Network Management Protocol (SNMP)-based network management application. For more information about managing the switches, see the "Device Manager GUI" section on page 1-8 and the "Switch Management Options" section on page 1-11.

For more information about how to optimize the connections in a Catalyst Express network, see the "Optimize Ports through Smartports Port Roles" section on page 3-2.

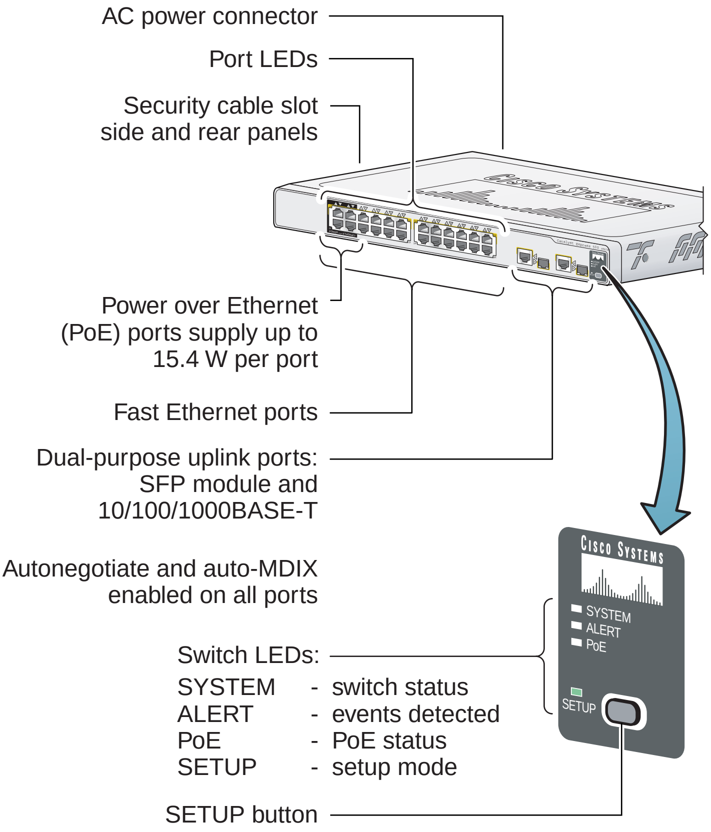
Features and Benefits

- Hardware Features, page 1-5
- Software Features, page 1-7
- Device Manager GUI, page 1-8

Hardware Features

Figure 1-2 and the list that follows describe the switch hardware features and the benefits that they provide. All switches can be installed on a table top, in a rack, or mounted on a wall. For hardware installation information, see the "Install the Switch" section on page 2-5.

Figure 1-2 Catalyst Express 500 Hardware Overview


AC power connector
Port LEDs
Security cable slot side and rear panels
Power over Ethernet (PoE) ports supply up to 15.4 W per port
Fast Ethernet ports
Dual-purpose uplink ports: SFP module and 10/100/1000BASE-T
Autonegotiate and auto-MDIX enabled on all ports
Switch LEDs:
SYSTEM - switch status
ALERT - events detected
PoE - PoE status
SETUP - setup mode
SETUP button
Cisco Systems
SYSTEM
ALERT
PoE
SETUP

10/100-Mbps Fast Ethernet Ports
10/100/1000-Mbps Gigabit Ethernet Ports

- Autosensing (autonegotiation) of port speed and autonegotiating of duplex mode optimizes port bandwidth.
- Automatic-medium-dependent interface crossover (auto-MDIX) capability automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.

PoE-Capable Ports (Available only on the Catalyst Express 500-24LC and Catalyst Express 500-24PC switches.)

- Up to 15.4 W of power provided to connected Cisco prestandard and IEEE 802.3af-compliant powered devices if the switch detects that there is no power on the circuit.

SFP Module Slots

- Fiber-optic SFP modules provide cable media and distance options for switch connectivity. A list of supported Cisco SFP modules is in the "Supported Hardware" section on page 1-13.

LEDs

- System LEDs show switch status, problem detection, PoE usage, and setup status.
- Port LEDs show port status. From the device manager GUI, port LEDs also show duplex mode, speed, and PoE status.
- RPS LED shows status of an installed Cisco redundant power supply (RPS). (Available only on the Catalyst Express 500-24PC model.)

Setup Button

- Button starts the Express Setup program.

Cisco Redundant Power Supply (RPS)

- Cisco redundant power supply (RPS) enhances power reliability. A list of supported RPS models is in the "Supported Hardware" section on page 1-13. (Available only on the Catalyst Express 500-24PC model.)

Security Slots

- Slots to attach a security cable to the switch.

Software Features

These are the switch software features and the benefits that they provide. You can configure these features through the device manager GUI (see the "Device Manager GUI" section on page 1-8). For details on these features, see the chapters on Customization, Monitoring, and Troubleshooting.

Note For enhanced switch features that are available only through Network Assistant and not through the device manager GUI, see the "Cisco Network Assistant" section on page 1-12.

Express Setup

- Initial setup only requires IP information for first-time switch configuration.
- Quick IP information updates if you relocate the switch to a different network.
- Date and time settings automatically synchronized between the switch and the network management station.
- Dynamic Host Configuration Protocol (DHCP) automatically assigns the switch an IP address, a default gateway, and a subnet mask from a DHCP server.

Troubleshooting

- General switch diagnostic test detects problems on the switch. Link diagnostic test detects cable-related issues on a specified port.
- General switch and link diagnostic reports describe problems detected on the switch and its ports and list recommended actions to resolve each problem.

Monitoring

- Alert LED notifies that one or more problems were detected on the switch.
- Alert Log lists all problems detected on the switch, including a timestamp of the most recent detection of each problem.
- Graphical front panel display, LEDs, gauges, graphs, and animated indicators show switch and port status, utilization, and error percentages, and temperature and fan status.
- Port status and statistics tables display port operating status and the statistics for data being received and sent on each port.

Customization

- Smartports port roles optimize switch ports according to their attached devices. Security and quality of service (QoS) benefits are built into the port roles.
- Secure Socket Layer (SSL) protocol authenticates and encrypts communications to the switch device manager GUI. (Requires the cryptographic version of the switch software available from the software download page on Cisco.com.)
- Username-and-password pair configuration for controlling switch access.
- VLANs for grouping network users according to functions, teams, or applications, and regardless of the physical location of the network users. The switch supports up to 32 VLANs.

  VLAN support includes these features:

  – Spanning Tree Protocol (STP) prevents network loops from developing and provides a redundant path if the active path becomes unavailable.

  – Internet Group Management Protocol (IGMP) snooping reduces duplicate and excess traffic on the network.
- EtherChannels for bundling multiple Fast Ethernet or Gigabit Ethernet ports into a single logical link to create a higher bandwidth link between the switch and another switch.
- Simple Network Management Protocol (SNMP) versions 1, 2C, and 3 to allow a remote network management station to access, monitor, and control the switch.

Device Manager GUI

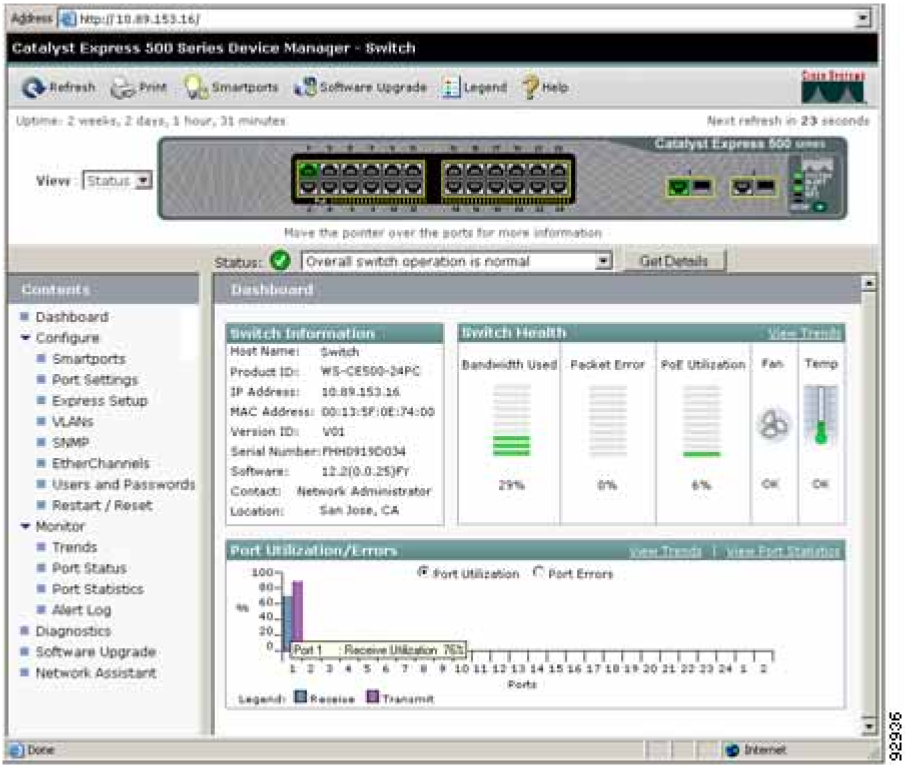
The device manager is a graphical device management tool for configuring, monitoring, and troubleshooting the switch (Figure 1-3).

It simplifies configuration tasks with features such as Express Setup and Smartports for quickly setting up the switch and its ports. It uses graphical, color-coded displays such as the switch front panel view, graphs, and animated indicators to simplify monitoring tasks. It provides alert and diagnostic tools to help you identify and solve networking problems.

Additional details about the device manager and procedures on using the device manager windows are available from the device manager online help (Figure 1-4).

You can display the device manager from anywhere in your network through a web browser such as Microsoft Internet Explorer or Netscape Navigator. For information on how to display the device manager, see the “Display the Device Manager” section on page 2-13.

Figure 1-3 Device Manager Interface



Address http://10.89.153.16/

Catalyst Express 500 Series Device Manager - Switch

Uptime: 2 weeks, 2 days, 1 hour, 31 minutes

Next refresh in 23 seconds

View : Status

Move the pointer over the ports for more information

Status: Overall switch operation is normal

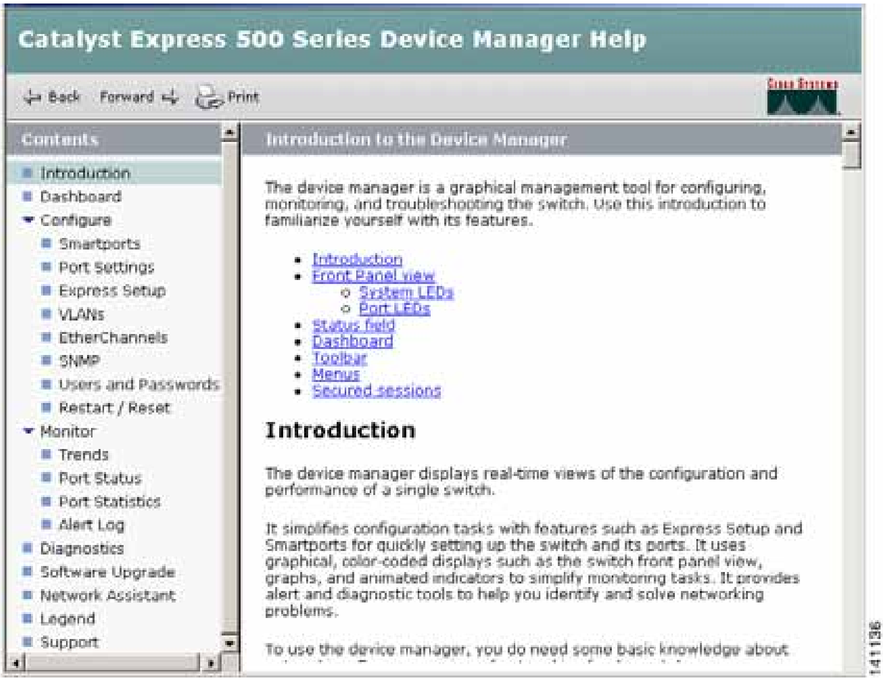
Switch Information

Host Name: Switch
Product ID: WS-CE500-24PC
IP Address: 10.89.153.16
MAC Address: 00:13:5F:0E:74:00
Version ID: V01
Serial Number: FHH0919D034
Software: 12.2(0.0.25)FY
Contact: Network Administrator
Location: San Jose, CA

Bandwidth Used	Packet Error	PoE Utilization	Fan	Temp
29%	0%	6%	OK	OK

Port 1 : Receive Utilization 76%

Figure 1-4 Device Manager Online Help



Introduction to the Device Manager

The device manager is a graphical management tool for configuring, monitoring, and troubleshooting the switch. Use this introduction to familiarize yourself with its features.

- Introduction
- Front Panel view
  - System LEDs
  - Port LEDs
- Status field
- Dashboard
- Toolbar
- Menus
- Secured sessions

Introduction

The device manager displays real-time views of the configuration and performance of a single switch.

It simplifies configuration tasks with features such as Express Setup and Smartports for quickly setting up the switch and its ports. It uses graphical, color-coded displays such as the switch front panel view, graphs, and animated indicators to simplify monitoring tasks. It provides alert and diagnostic tools to help you identify and solve networking problems.

To use the device manager, you do need some basic knowledge about

System Requirements

- Hardware Requirements, page 1-11
- Software Requirements, page 1-11

Hardware Requirements

Table 1-2 lists the minimum hardware requirements for running the device manager.

Table 1-2 Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II[1]	64 MB[2]	256	1024 x 768	Small

[1] We recommend Intel Pentium 4.

[2] We recommend 256-MB DRAM.

Software Requirements

Table 1-3 lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.

You should disable any pop-up blockers or proxy settings in your browser software and any wireless clients running on your PC.

Table 1-3 Supported Operating Systems and Browsers

Operating System	Microsoft Internet Explorer[1]	Netscape Navigator
Windows 2000	5.5 or 6.0	7.1
Windows XP	5.5 or 6.0	7.1

[1] Service Pack 1 or higher is required for Internet Explorer 5.5.

Switch Management Options

In addition to the device manager GUI, you can also use these tools to manage the switch:

- Cisco Network Assistant, page 1-12
- Simple Network Management Protocol, page 1-13

Cisco Network Assistant

The switches support the Cisco Network Assistant network management application. Network Assistant offers an enhanced set of features for configuring and monitoring one or more devices, including switches, device clusters, device stacks, routers, and access points.

Catalyst Express 500 features that are available on Network Assistant but not available from the device manager include:

- Levels (Low, Medium, or High) of network security and switch access for devices attached to the switch
- Smartports Diagnostics port role to optimize the connection between a switch port and a network troubleshooting device
- Device inventory to retrieve information such as the IP address, the MAC address, and the port role information of devices connected to the switch

Some general Network Assistant features include:

- Centralized, common services—such as software upgrades, configuration management, inventory reports, network events, alerts, and password synchronization—for Cisco switches, routers, and access points in the network
- Centralized network monitoring using two different views of all connected devices in the network: a physical view (front panel images) and a logical view (network topology image of different network devices, including IP phones)
- Drag-and-drop software upgrade for multiple switches, including backup-and-restore through a switch configuration file
- Security configuration for all the Cisco access points in the network
- Interactive tools (such as wizards) to simplify configuration of complex features

For more information, see the Cisco Network Assistant Introduction at this URL:

http://www.cisco.com/go/networkassistant

Simple Network Management Protocol

You can use Simple Network Management Protocol (SNMP) management applications to manage the switch. You also can manage it from an SNMP-compatible workstation.

Supported Hardware

The switches support the PWR675-AC-RPS RPS. (Available only on the Catalyst Express 500-24PC model.)

The switches support these Cisco SFP modules:

- 100BASE-BX
- 100BASE-FX
- 100BASE-LX
- 1000BASE-LX
- 1000BASE-SX

When You Are Done

If you have not already installed the switch and configured its basic settings, see Chapter 2, “Setup and Installation.”

If you already installed and configured the switch with its basic settings, see Chapter 3, “Customization,” to learn about features that can optimize the switch performance.

Setup and Installation

Read this chapter to learn more about the switch setup and installation. This chapter also includes instructions on how to display the device manager in standard and in secure modes.

Before You Begin

Make sure that you have met the software and hardware requirements, as described in the "System Requirements" section on page 1-10. Descriptions of the hardware features and benefits are in the "Hardware Features" section on page 1-5.

Follow the setup and installation procedure described in the *Getting Started Guide for the Catalyst Express 500 Switches*.

Chapter Topics

Set Up the Switch for the First Time

Prerequisite

To set up the switch for the first time, follow the procedure described in the *Getting Started Guide for the Catalyst Express 500 Switches*.

These are the configuration settings that you can set during initial setup:

- Network Settings, page 2-2
- Optional Settings, page 2-5

Network Settings

The network settings enable the switch to operate with its standard default settings and to be managed through the device manager. You must apply these settings to access and to take advantage of the monitoring, troubleshooting, and configuration features on the switch. Otherwise, the switch cannot be managed, and switch monitoring is limited to only its physical LEDs.

Management Interface (VLAN ID)	The ID of the management VLAN through which the switch will be managed. The management VLAN ID can be from 1 to 1001. The default ID is 1. The default name for the management VLAN is *default*. **Note** Make sure that the switch and your network management station are in the same VLAN. Otherwise, you cannot manage the switch from your management station. If they are in different VLANs, a router or Layer 3 switch is needed to communicate between VLANs. The management VLAN is the broadcast domain where management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that should only be limited to a specific group of users (such as the administrators of your network). It also ensures secure, administrative access to all devices in the network at all times. For more information about management VLANs and about VLANs in general, see the "VLAN Types" section on page 3-14.

IP Assignment Mode	The IP assignment mode determines if the switch IP information will be manually assigned (static) or be automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you select **Static** and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the device manager. If you select **DHCP**, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. As long as the switch is not restarted, the switch continues to use this information, and you can use the same IP address to access the device manager. **Note** If you manually assign the switch IP address and your network uses a DHCP server, make sure that the IP address that you give to the switch is not within the range of addresses that the DHCP server will automatically assign to other devices. This prevents IP address conflicts between the switch and another device.
IP Address	The IP address is a unique identifier for the switch in a network. The format is four numbers separated by periods. Each number can be from 0 to 255. This field is enabled only if the IP assignment mode is Static. **Note** Make sure that the IP address that you assign to the switch is not being used by another device in your network. The IP address and the default gateway cannot be the same. The IP addresses in the 10.0.0.0 network cannot be configured on the switch.
Subnet Mask List	The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets segment the devices in a network into smaller groups. The default is 255.255.255.0. This setting is enabled only if the IP assignment mode is Static.

Default Gateway	The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The IP address should be part of the same subnet as the switch IP address. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This setting is enabled only if the IP assignment mode is Static. **Note** You must specify a default gateway if your network management station and the switch are in different networks or subnetworks. Otherwise, the switch and your network management station will not be able to communicate with each other. The IP address and the default gateway cannot be the same.
Username	The name of a user who is authorized to access the device manager. The name can have up to 64 alphanumeric characters and is not case sensitive. The name cannot contain a ?, a space, or a tab. You must enter a username if you enter a password. We recommend that you provide a username-and-password pair to the switch to secure access to the device manager. After initial setup, you can add, delete, or modify username-and-password pairs from the Users and Passwords window on the device manager. To display this window, choose **Configure > Users and Passwords** from the device manager menu. For more information, see the "Control Access to the Switch" section on page 3-11.
Password	The password for the switch can have up to 25 alphanumeric characters, can start with a number, is case sensitive, and allows embedded spaces. The password cannot contain a ? or a tab and does not allow spaces at the beginning or end. We recommend that you provide a username-and-password pair to the switch to secure access to the device manager. After initial setup, you can add, delete, or modify username-and-password pairs from the Users and Passwords window on the device manager. To display this window, choose **Configure > Users and Passwords** from the device manager menu. For more information, see the "Control Access to the Switch" section on page 3-11.

Optional Settings

The optional settings identify and synchronize the switch so that it can be managed properly. The switch clock is automatically synchronized with the system clock on your network management station. You can manually set the system clock settings if the switch should have different time settings.

Host Name	A name for the switch. The name can have up to 31 alphanumeric characters. The name cannot contain a ?, a space, or a tab. The default is Switch. We recommend entering either the name, location, or IP address of the switch to help identify the switch during monitoring or troubleshooting.
System Date	The date that the switch automatically reads from the network management station. You can also manually set the date.
System Time	The time that the switch automatically reads from the network management station. You can also manually set the time.
Time Zone	The time zone that the switch automatically reads from the network management station. You can also manually set the time zone.
Daylight Saving Time	The check box is automatically enabled only when the selected time zone is in U.S., Europe, or Australia.

Install the Switch

This section includes these topics:

- Warnings, page 2-6
- Installation Guidelines, page 2-9
- Rack-Mounting, page 2-10
- Desktop-Mounting, page 2-11
- Wall-Mounting, page 2-12

Warnings

These warnings are translated into several languages in the *Regulatory Compliance and Safety Information for the Catalyst Express 500 Switches* document that shipped with the switch. Review these warnings before you power or install the switch.

Warning **To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.** Statement 17B

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.** Statement 43

Warning **Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.** Statement 48

Warning **Attach only the Cisco RPS (model PWR675-AC-RPS-N1=) to the RPS receptacle.** Statement 100C

Warning **Ethernet cables must be shielded when used in a central office environment.** Statement 171

Warning **If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.** Statement 265

Warning **To comply with safety regulations, mount switches on a wall with the front panel facing up.** Statement 266

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

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

This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Warning **Class 1 laser product.** Statement 1008

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.** Statement 1019

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Warning **For connections outside the building where the equipment is installed, the following ports must be connected through an approved network termination unit with integral circuit protection: 10/100/1000 Ethernet.** Statement 1044

Warning **Voltages that present a shock hazard may exist on Power over Ethernet (PoE) circuits if interconnections are made using uninsulated exposed metal contacts, conductors, or terminals. Avoid using such interconnection methods, unless the exposed metal parts are located within a restricted access location and users and service people who are authorized within the restricted access location are made aware of the hazard. A restricted access area can be accessed only through the use of a special tool, lock and key or other means of security.** Statement 1072

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

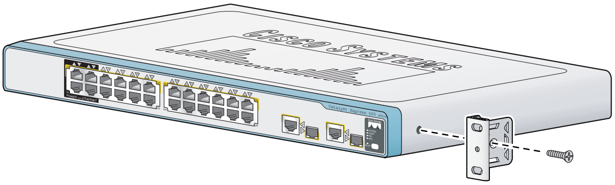
Installation Guidelines

When deciding where to place the switch, be sure to observe these requirements:

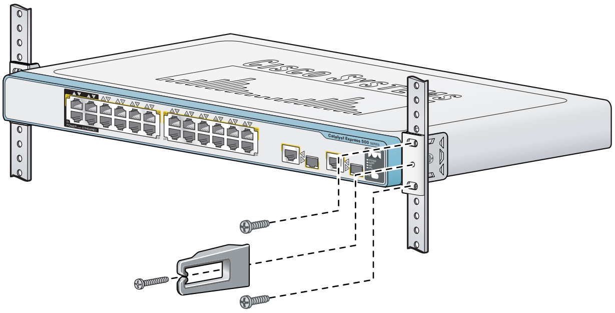
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.
- Clearance to front and rear panels is such that
  - Airflow around the switch and through the vents is unrestricted.
  - Front-panel LEDs can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - AC power cord can reach from the AC power outlet to the connector on the switch rear panel.
- Temperature does not exceed 113°F (45°C), humidity does not exceed 85 percent, and altitude at the installation site is not greater than 10,000 feet (3049 m).

  If the switch is installed in a closed or multirack assembly, the temperature around it might be greater than normal room temperature.
- For copper Ethernet ports, cable lengths from the switch to connected devices can be up to 328 feet (100 meters).
- For SFP module cable lengths, see Table A-2 and the documentation that shipped with the module.

Rack-Mounting

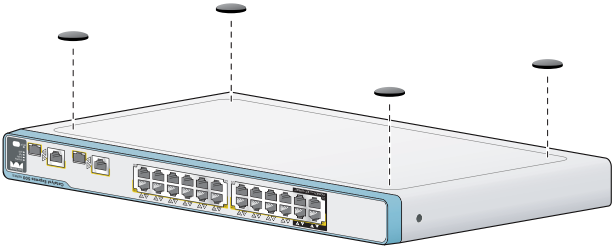


Position the mounting bracket and screw on the side of the switch. Tighten the screw with a screwdriver. Repeat on the opposite side.



Insert the switch into the 19-inch rack, and align the bracket in the rack. Use either the 10-32 pan-head screws or the 12-24 pan-slotted screws to secure the switch in the rack. Use the supplied black Phillips machine screw to attach the cable guide to either bracket.

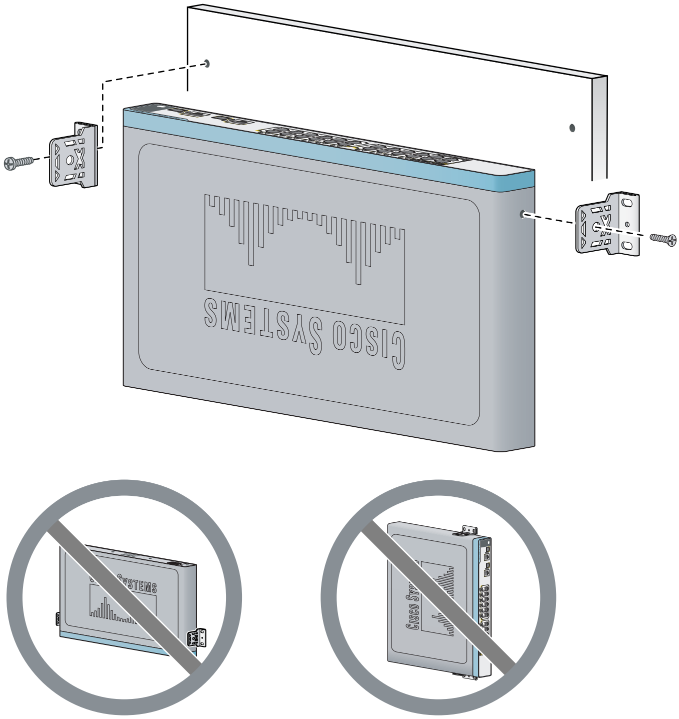
Desktop-Mounting



Place the switch upside-down on a flat surface. Attach the four rubber pads to the recessed areas on the bottom of the switch. Place the switch on a desktop near an AC power source.

If you are stacking switches, make sure that the mounting feet of the upper switch align with the recesses of the lower switch. Do not stack more than four units high.

Wall-Mounting



Position the mounting bracket and screw on the side of the switch, rotated 90-degrees from the view shown in the rack-mounting illustration. Tighten the screw with a screwdriver. Repeat on the opposite side.

Mount the switch on the wall with the front panel facing up. For the best support of the switch and cables, make sure that the switch is attached securely to wall studs or to a firmly attached plywood mounting backboard. Screws for wall-mounting are not provided.

Display the Device Manager

Prerequisite

Make sure that you meet the requirements described in the "System Requirements" section on page 1-10.

You can display the device manager (Figure 1-3) from anywhere in your network through a web browser such as Microsoft Internet Explorer or Netscape Navigator.

Follow these steps to display the device manager:

1. Open a web browser session on your PC or workstation.
2. Enter the switch IP address in the web browser, and press **Enter**. The device manager page appears.
3. Use the device manager to perform basic switch configuration and monitoring. See the device manager online help for information.

   For more advanced configuration, download and run the Cisco Network Assistant (see the "Cisco Network Assistant" section on page 1-12) application.

We recommend running the cryptographic software image on the switch and using the option to run a secured session with the switch. See the "Secured Sessions with the Switch" section on page 2-13 for information on how to ensure that your device manager session is protected from unauthorized access.

Secured Sessions with the Switch

The switch uses the Secure Sockets Layer (SSL) protocol to secure the HTTP communications between the switch and your network management station. When you attempt to display the device manager, this protocol:

- Authenticates the web-based connection between the switch and your network management station
- Encrypts and decrypts the information exchanged between the switch and your network management station to protect the information from unauthorized access over the Internet

SSL is enabled by default on the switch. It is available only on the cryptographic version of the switch software image.

More information about secured sessions is available from the device manager online help.

When You Are Done

Use the features that are described in Chapter 3, "Customization" and Chapter 4, "Monitoring" to configure and to monitor the switch in your network.

Customization

Read this chapter to understand the concepts and tasks necessary to customize the switch features to better suit your network needs. The tasks in this chapter are independent, unless otherwise noted, and are listed in no particular order.

Before You Begin

Before you can customize the switch settings, the switch must first have an IP address. If it does not have one, make sure that you have followed the steps to set up the switch in the *Getting Started Guide for the Catalyst Express 500 Switches*.

Chapter Topics

Optimize Ports through Smartports Port Roles

These are the concepts and procedures for using Smartports port roles:

What Are Smartports Port Roles

Tip Use Smartports port roles immediately after switch initial setup. The switch ports are then correctly configured before they are connected to devices.

The Smartports port roles are Cisco-recommended configurations for the switch ports. These configurations (referred to as port roles) optimize the switch connections and ensure security and transmission quality and reliability to traffic from the switch ports. They also prevent many problems caused by port misconfigurations.

The port roles (Table 3-1) are based on the type of devices to be connected to the switch ports. For example, the Desktop port role is specifically for switch ports that will be connected to desktop and laptop PCs.

Figure 3-1 shows different types of devices connected to the Catalyst Express switches. Through Smartports port roles, each connection from the switches is optimized for its attached device.

Figure 3-2 is an example of the Smartports window on the device manager. It shows port roles applied to the ports. Only port 22 does not have a port role applied to it.

Table 3-1 Smartports Port Roles

Port Role	Description
Desktop	Apply this role to ports that will be connected to desktop devices, such as desktop PCs, workstations, notebook PCs, and other client-based hosts. **Note** Do not apply this role to ports that will be connected to switches, routers, or access points.
IP Phone+Desktop	Apply this role to ports that will be connected to IP phones. A desktop device, such as a PC, can be connected to the IP phone. Both the IP phone and connected PC would have access to the network and the Internet through the switch port. This role prioritizes voice traffic over data traffic to ensure clear voice reception on the IP phones.
Switch	Apply this role to ports that will be connected to other switches.
Router	Apply this role to ports that will be connected to WAN devices that connect to the Internet, such as routers and Layer 3 switches with routing service capabilities, firewalls, or virtual private network concentrators.
Access Point	Apply this role to ports that will be connected to non-PoE and PoE-capable wireless access points. The access point can provide network access to up to 30 mobile (wireless) users.
Server	Apply this role to ports that will be connected to servers that provide network services, such as exchange servers, collaborative servers, terminal servers, file servers, Dynamic Host Configuration Protocol (DHCP) servers, IP PBX server, and so on. This role is for Gigabit or non-Gigabit ports, depending on the server type to be connected. This role prioritizes server traffic as trusted, critical, business, or standard, depending on the function of the server.
Printer	Apply this role to ports that will be connected to a printer, such as a network printer. This role prevents printer traffic from affecting voice and critical data traffic.

Table 3-1 Smartports Port Roles (continued)

Port Role	Description
Guest	Apply this role to ports that will be connected to desktop devices and to access points to provide guest wireless access. This role provides guests and visitors temporary access to the Internet but prevents them from accessing your internal network.
Other	Apply this role to ports if you do not want to apply a specialized Smartports role on the port. This role can be used on connections to guest or visitor devices, printers, desktops, servers, and IP phones. **Note** Do not apply this role to ports that will be connected to sniffer or intrusion detection system devices.

Figure 3-1 Smartports Port Roles in a Catalyst Express Network

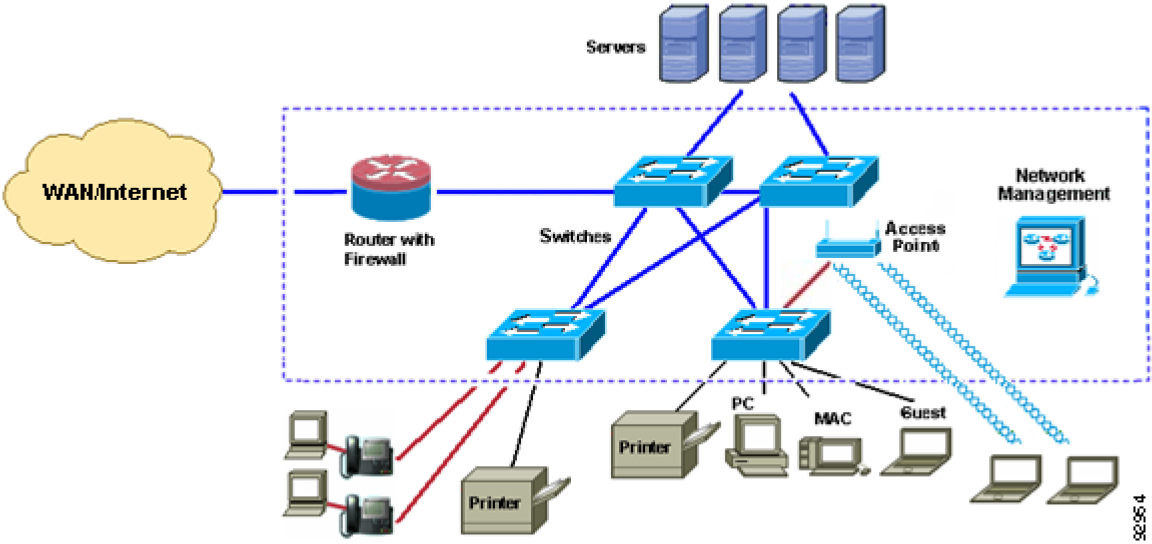
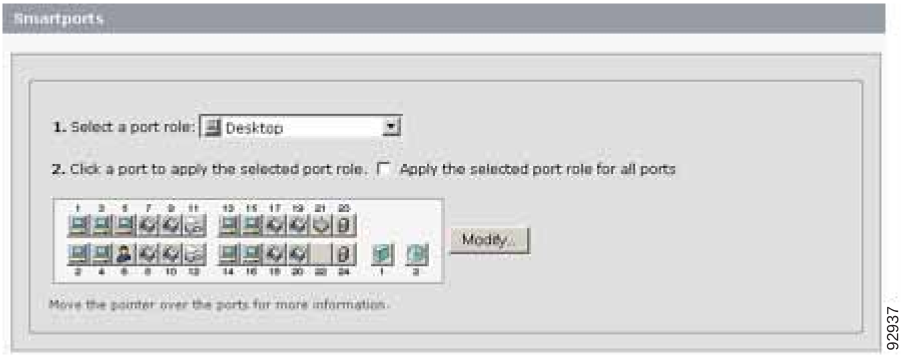


Figure 3-2 Smartports Window



Smartports

1. Select a port role: Desktop

2. Click a port to apply the selected port role. □ Apply the selected port role for all ports

Move the pointer over the ports for more information.

Recommended Smartports Assignments

The recommended port role assignments (Table 3-2) depend on the switch model and the port type. These assignments reflect the type of device connections intended for the switch model. If you decide to use most of the switch ports with their intended port roles, accept the recommended port roles, and change only the ports that need a different port role.

Immediately after initial setup, you can choose to have the recommended port roles applied to the ports. If you decline, the Other port role is applied to all ports.

Table 3-2 Recommended Smartports Assignments

Switch Model	Port Type and Number	Recommended Port Role
WS-CE500-24TT	Fast Ethernet ports 1 to 24	Desktop
	Gigabit Ethernet or SFP module ports 1 and 2	Switch
WS-CE500-24LC	Fast Ethernet ports 1 to 4	Access Point
	Fast Ethernet ports 5 to 24	Desktop
	Gigabit Ethernet or SFP module ports 1 and 2	Switch
WS-CE500-24PC	Fast Ethernet ports 1 to 24	IP Phone+Desktop
	Gigabit Ethernet or SFP module ports 1 and 2	Switch
WS-CE500G-12TC	Gigabit Ethernet ports 1 to 8	Server
	Gigabit Ethernet or SFP module ports 9 to 12	Switch

Avoid Smartports Mismatches

A Smartports mismatch is when an attached device does not match the Smartports role applied to the switch port. Mismatches can have adverse effects on devices and your network. For example, mismatches

- Affect the behavior of the attached device
- Lower network performance (reduce the level of QoS) on voice, wireless, switch, and router traffic
- Reduce restrictions on guest access to the network
- Reduce protection from denial of service (DoS) attacks on the network
- Disable or shut down the port

We recommend always checking which Smartports role is applied to a port *before* attaching a device to the port or reconnecting devices that have been moved.

Apply Roles to Ports

Prerequisite

Before using Smartports, decide which switch port will be connected to which device type.

Note

- We recommend that you do not change specific port settings after enabling a Smartports role on a port. Any port setting changes can alter the effectiveness of the Smartports role.
- Do not apply the Desktop port role on ports that are connected to routers or to other switches.

Use the Smartports window (Figure 3-2) to apply port roles to the switch ports. To display this window, choose **Configure** > **Smartports** from the device manager menu. You also can click **Smartports** from the device manager tool bar. See the device manager online help for additional guidelines and procedures.

Customize Port Role Attributes

These are the concepts and procedures for refining (customizing) port roles:

- Change VLAN Memberships, page 3-7
- Change the Server Priorities, page 3-8

Change VLAN Memberships

Prerequisite

Before changing VLAN memberships, you should understand what a VLAN is, its purpose, and how to create a VLAN. You should also understand the use of two special VLANs supported on the switch: Cisco-Guest and Cisco-Voice. For this information, see the "What Is a VLAN" section on page 3-12 and the "VLAN Types" section on page 3-14.

Each switch port is a member of a VLAN. Devices attached to switch ports that belong to the same VLAN share the same data broadcasts and system resources. Communication between VLANs requires a Layer 3 device (such as a router or a Layer 3 switch).

Depending on your network requirements, it might be sufficient to assign all ports to the default VLAN, which is named *default*. A small network might only need one VLAN.

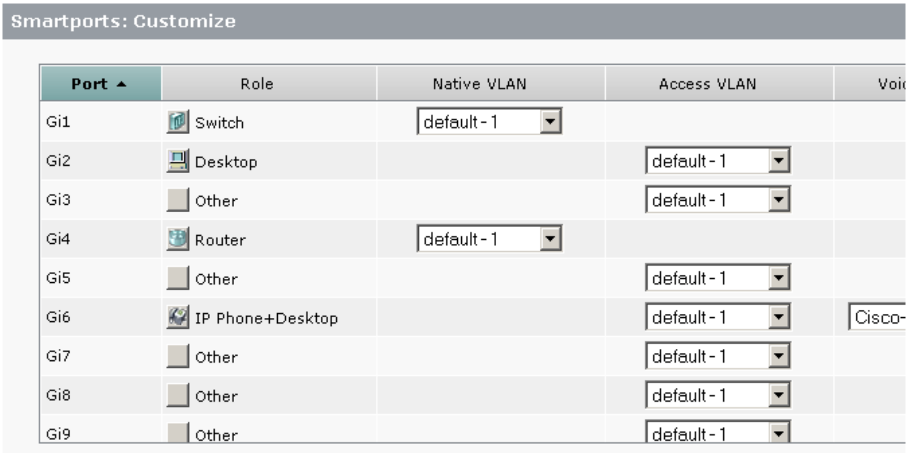
If the switch has only the default VLAN, ports applied with the Guest or IP Phone+Desktop port role can also belong to the default VLAN. However, if additional VLANs have been created:

- Ports applied with the Guest port role must belong to the Cisco-Guest VLAN.
- Ports applied with the IP Phone+Desktop port role must belong to the Cisco-Voice VLAN. These ports must be assigned to the Cisco-Voice VLAN for voice traffic. At the same time, these ports can also belong to an access VLAN for regular data traffic.

For more information about these special VLANs, see the "Cisco-Guest and Cisco-Voice VLANs" section on page 3-16. For information about creating VLANs, see the "Create, Modify, and Delete VLANs" section on page 3-16.

Use the Smartports Customize window (Figure 3-3) to assign ports to VLANs. To display this window, choose **Configure > Smartports** from the device manager menu, and then click the **Customize** button on the Smartports window. See the device manager online help for additional guidelines and procedures.

Figure 3-3 Smartports Customize Window



Smartports: Customize

Port ▲	Role	Native VLAN	Access VLAN	Voi
Gi1	Switch	default - 1		
Gi2	Desktop		default - 1	
Gi3	Other		default - 1	
Gi4	Router	default - 1		
Gi5	Other		default - 1	
Gi6	IP Phone+Desktop		default - 1	Cisco-
Gi7	Other		default - 1	
Gi8	Other		default - 1	
Gi9	Other		default - 1	

Change the Server Priorities

For ports applied with the Server port role, you can classify the priority of servers based on the server traffic. Use the Smartports Customize window (Figure 3-3) to change server priorities.

These are server priorities, from least to highest priority:

Standard	This server type is treated with the lowest priority compared to other server types. An example of a standard server is a web server or print server.
Business	This server type receives higher priority than a standard server but less priority than a critical or trusted server. An example of a business server is a server where business records are kept. This is the default server type.

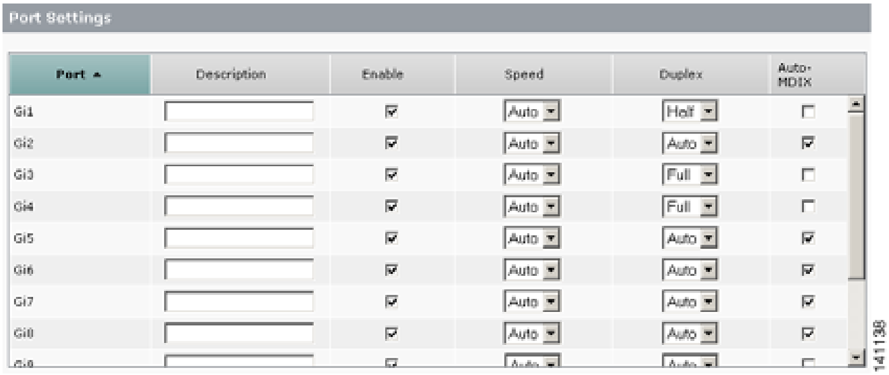
Critical	This server type typically provides the organization with more critical traffic than a business server and therefore has higher priority than business-type servers. An example of a critical server is a server for business transactions.
Trusted	This server type is for use with a voice-over-IP server. All traffic from this server type receives voice-quality priority as well as the same priority given to critical-type servers. An example of a trusted server is Cisco CallManager.

Update Basic Port Settings

The basic port settings determine how data is received and sent between the switch and the attached device. You can change these settings to fit your network needs and to troubleshoot network problems. The settings on a switch port should be compatible with the port settings of the connected device.

Use the Port Settings window (Figure 3-4) to change basic port settings. To display this window, choose **Configure > Port Settings** from the device manager menu. See the device manager online help for additional guidelines and procedures.

Figure 3-4 Port Settings Window



Port Settings

Port ▲	Description	Enable	Speed	Duplex	Auto-MDIX
Gi1		☑	Auto	Half	☐
Gi2		☑	Auto	Auto	☑
Gi3		☑	Auto	Full	☐
Gi4		☑	Auto	Full	☐
Gi5		☑	Auto	Auto	☑
Gi6		☑	Auto	Auto	☑
Gi7		☑	Auto	Auto	☑
Gi8		☑	Auto	Auto	☑

These are the basic settings for the switch ports:

Description	The description of the switch port. The limit is 18 characters. We recommend providing a port description to help identify the port during monitoring and troubleshooting. The description can be the location of the connected device or the name of the person using the connected device.
Enable	The state of the switch port. The default is Enable. Disable the port to administratively (manually) shut it down.
Speed	The operating speed of the switch port. Choose the speed or choose Auto (autonegotiation) if the connected device can negotiate the link speed with the switch port. The default is Auto. We recommend using the default so that the speed setting on the switch port automatically matches the setting on the connected device. Change the switch port speed if the connected device requires a specific speed.
Duplex	The duplex mode of the switch port. Choose the duplex mode: • Auto (autonegotiation) if the connected device can negotiate with the switch • Full (full duplex) if both devices can send data at the same time • Half (half duplex) if one or both devices cannot send data at the same time The default is Auto. **Note** On Gigabit Ethernet ports only, you cannot set the port to half duplex if the port speed is set to Auto. We recommend using the default so that the duplex setting on the switch port automatically matches the setting on the connected device. Change the duplex mode on the switch port if the connected device requires a specific mode.
Auto-MDIX	Whether the automatic medium-dependent interface crossover (auto-MDIX) feature will automatically detect the required cable connection type (straight-through or crossover) and configure the connection appropriately. The default is Enable. This setting is not available on the SFP module ports. **Note** To reenable auto-MDIX, first set the duplex mode and speed to Auto.

PoE	Whether PoE will be supplied to a connected device. Choose either: • Auto (automatically) to automatically provide power when an IEEE 802.af-compliant or Cisco pre-standard device is connected. • Never from the drop-down list. The default is Auto. **Note** This setting is available only on PoE ports.

Control Access to the Switch

Username-and-password pairs prevent unauthorized access by those who could guess the password. We recommend that the switch has at least one username-and-password pair to secure access to the device manager.

During initial setup, you can enter one username-and-password pair. You must enter both a username and password.

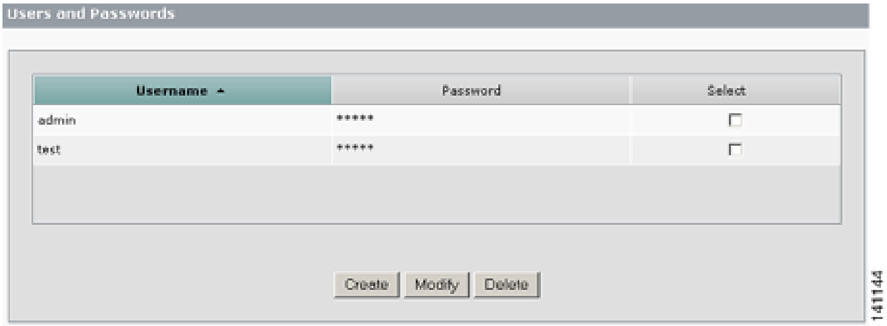
After initial setup, you can add, modify, and delete username-and-password pairs from the Users and Passwords window (Figure 3-5).

Many users can have the same password. However, a username can only have one password.

You can modify passwords but not usernames. If you no longer want a specific username, you must first delete it, and then add the new username. Deleting a password also deletes the username.

To display the Users and Passwords window, choose **Configure** > **Users and Passwords** from the device manager menu. See the device manager online help for additional guidelines and procedures.

Figure 3-5 Users and Passwords Window



Users and Passwords

Username ▲	Password	Select
admin	*****	☐
test	*****	☐

Isolate Traffic and Users through VLANs

These are the concepts and procedures for configuring VLANs:

- What Is a VLAN, page 3-12
- VLAN Types, page 3-14
- Cisco-Guest and Cisco-Voice VLANs, page 3-16
- Create, Modify, and Delete VLANs, page 3-16
- Advanced VLAN Configuration, page 3-17

What Is a VLAN

A virtual local area network (VLAN) is a logical segment of network users and resources grouped by function, team, or application. This segmentation is without regard to the physical location of the users and resources. For example, VLANs can be based on the departments in your company or by sets of users who communicate mostly with each other.

Using VLANs, you can isolate different types of traffic (such as voice and data) to preserve the quality of the transmission and to minimize excess traffic among the logical segments. You can also use VLANs to isolate different types of users. For example, you can restrict specific data broadcasts to specific logical workgroups for security purposes, such as keeping information about employee salaries only to devices in a VLAN created for payroll-related communications.

An added benefit to using VLANs is that it reduces the amount of administrative effort required to constantly examine requests to network resources.

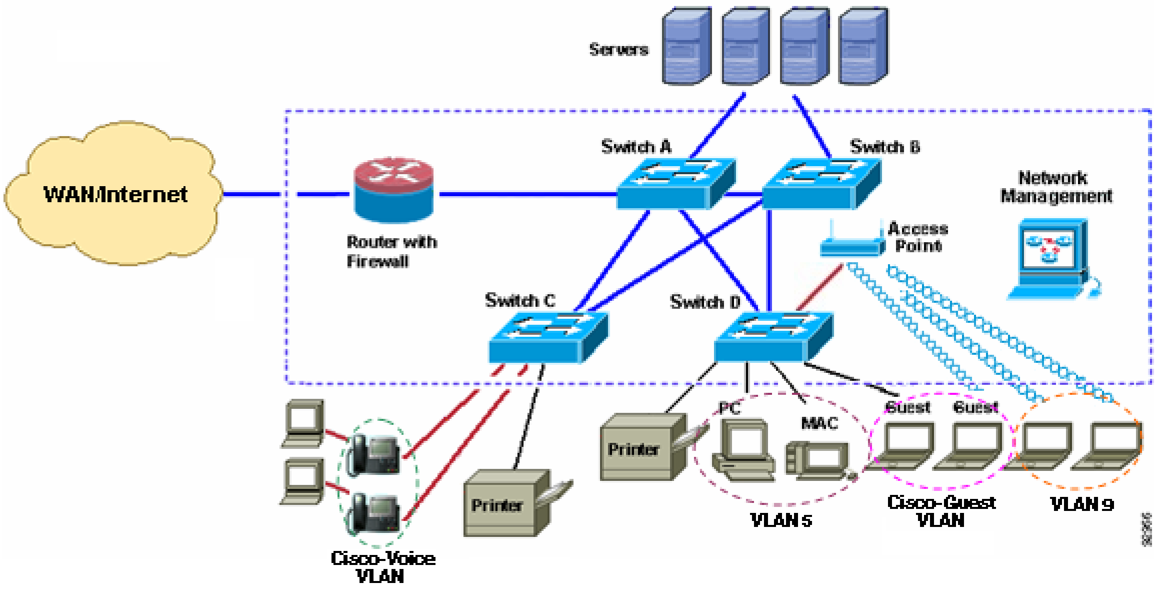
Note that a key concept about VLANs is that they isolate parts of your network. Therefore, devices that are attached to the switch ports in the same VLAN (network users in the same VLAN) can communicate only with each other and can share the same data.

Devices attached to switch ports in different VLANs cannot communicate with each other through the switch. Inter-VLAN communication requires a router or Layer 3 switch. The router or Layer 3 switch must be configured to allow routing across VLANs (inter-VLAN routing), and additional security policies must be set.

If your network is also using a DHCP server, ensure that the server is accessible to devices in *all* VLANs.

Figure 3-6 is an example network using VLANs based on different network traffic and network users. Organizing a network around these factors helps define the size and membership of the VLANs in the network.

Figure 3-6 VLANs in a Catalyst Express Network



Using VLANs to Isolate Different Traffic Types

Isolating data traffic from delay-sensitive traffic, such as voice traffic, ensures the quality of the voice transmission. In Figure 3-6, switch ports connected to the IP phones belong to the Cisco-Voice VLAN, a special VLAN supported on the switches. This VLAN automatically provides Voice over IP (VoIP) services on these connections, meaning priority is given to voice traffic over regular IP data traffic. Voice traffic from the phone and IP phone service requests to an IP PBX server have priority over traffic from the desktop devices attached to the IP phones.

To further isolate data traffic from voice traffic, data traffic from the attached desktop devices can be assigned to a separate VLAN.

Using VLANs to Group Users

The network in Figure 3-6 provides access to three types of network users: wired employees, wireless (or mobile) employees, and wired and wireless company visitors. Each user type requires different access levels to the company network.

VLANs and security policies on a router or Layer 3 switch can enforce privileges and restrictions to different user types. In Figure 3-6:

- VLAN 5 offers employee-level access to the company resources. This kind of network access requires a direct connection to the specific switch ports.
- Cisco-Guest VLAN offers Internet-only access to company visitors. Visitors with wired or wireless connections to switch ports are assigned to this VLAN, which automatically restricts guest access to only the Internet.
- VLAN 9, which has one or more switch ports connected to the access point, enforces security policies to identify the wireless user (for example, as employee or a guest) and to determine what the user can do on the network (for example, access only the Internet or access other network resources).

VLAN Types

The switch ships with a default VLAN to which each switch port initially belongs. The switch supports a maximum of 32 VLANs, including the default VLAN.

Every VLAN is identified by its name and ID number. The default VLAN is named *default*. During initial setup, you can assign the default VLAN ID. The ID can be from 1 to 1001 where 1 is the default ID. After initial setup, you cannot change the name or ID of the default VLAN.

You can assign switch ports to either the default VLAN or to VLANs that you have created. Using only the default VLAN might be sufficient based on the size and requirements of your network. We recommend that you first determine your VLAN needs before creating VLANs.

The default VLAN is, by default, the *management VLAN*. After initial setup, you can designate any VLAN on the switch as the management VLAN. The purpose of the management VLAN is to ensure unlimited administrative access to all users, devices, and traffic on the network. Because all network traffic flows through the switch, you should assign one of the switch ports to the management VLAN.

Depending on the type of device that is connected to the switch port:

- A switch port applied with one of these port roles—Desktop, IP Phone+Desktop, Printer, Server, Guest, and Other—can belong only to an *access* VLAN. The access VLAN provides the attached device with the specific access designed for that VLAN (for example, access only to personnel records).
- A switch port applied with one of these port roles—Switch, Router, and Access Point—can send and receive traffic for all VLANs configured on the switch, one of which can be identified as a *native* vlan. On this port, any traffic that is received or sent without the VLAN explicitly identified is assumed to belong to the native VLAN.

  Both the switch port and the attached device port must be in the same native VLAN.

A complete discussion about using VLANs is provided in *Cisco LAN Switching Fundamentals* published by Cisco Press.

Cisco-Guest and Cisco-Voice VLANs

It is important to note that you can assign all ports, regardless of their Smartports role, to the default VLAN (*default*). If your network requires segregating either or both voice and guest traffic and if you create additional VLANs, you must also create these VLANs:

- Cisco-Guest—The VLAN to which all ports that are applied with the Guest port role must be assigned. This VLAN ensures that all guest and visitor traffic is segregated from the rest of your network traffic and resources.
- Cisco-Voice—The VLAN to which all ports that are applied with the IP Phone+Desktop port role must be assigned. This VLAN ensures that all voice traffic has better quality of service and is not mixed with data traffic.

Note The VLAN names, Cisco-Guest and Cisco-Voice, are case sensitive.

Only ports with the Guest port role can be assigned to the Cisco-Guest VLAN. Only ports with the IP Phone+Desktop port role can be assigned to the Cisco-Voice VLAN.

Create, Modify, and Delete VLANs

Prerequisites

Using only the default VLAN might be sufficient based on the size and requirements of your network. We recommend that you first determine your VLAN needs before creating VLANs. If you decide to create additional VLANs, you must also create VLANs specifically for guest and voice traffic. The names for these VLANs, Cisco-Guest and Cisco-Voice, are case sensitive. For more information, see the "Cisco-Guest and Cisco-Voice VLANs" section on page 3-16.

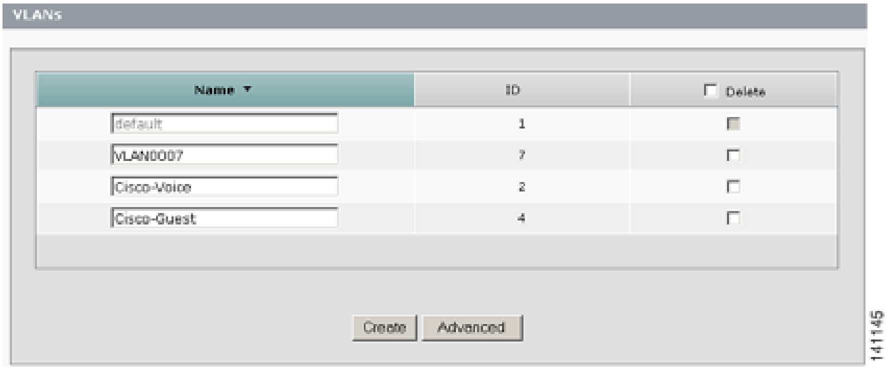
To create a VLAN, you must give the VLAN a name and a unique ID number. You can create up to 32 VLANs.

You can modify the name of a VLAN but not its number. You cannot modify or delete the default VLAN.

After creating VLANs, you can then assign the appropriate ports to those VLANs. Before assigning ports to VLANs, make sure that each port is applied with the appropriate port role. For more information, see the "Optimize Ports through Smartports Port Roles" section on page 3-2 and the "Change VLAN Memberships" section on page 3-7.

Use the VLANs window (Figure 3-7) to create, modify, and delete VLANs. To display this window, choose **Configure > VLANs** from the device manager menu. See the device manager online help for additional guidelines and procedures.

Figure 3-7 VLANs Window



VLANs

Name ▼	ID	□ Delete
default	1	□
VLAN0007	7	□
Cisco-Voice	2	□
Cisco-Guest	4	□

Advanced VLAN Configuration

The advanced VLAN options are the Spanning Tree Protocol (STP) and Internet Group Management Protocol (IGMP) snooping features on the switch ports. These options are enabled by default.

We recommend that you leave these options enabled for the benefits that they provide:

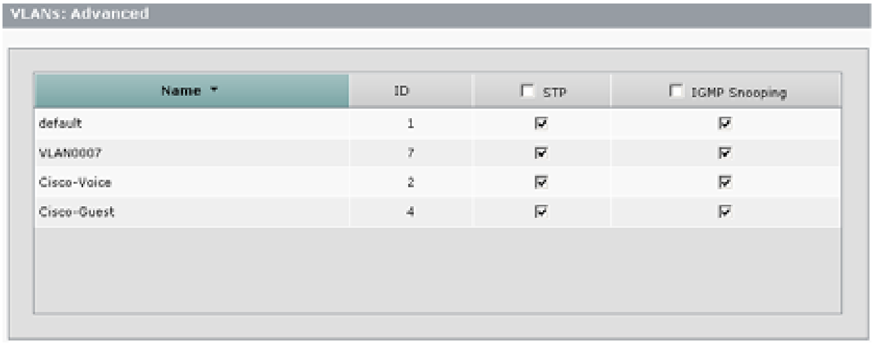
- STP prevents network loops by enabling only one active path for traffic to use. STP also provides a redundant path if the active path becomes unavailable.

- IGMP snooping reduces duplicate and excess traffic on the network by forwarding IP multicast traffic to specific switch ports rather than by flooding all ports. With IGMP snooping, only ports that are members of specific IP multicast groups receive multicast messages. The result is a more efficient use of bandwidth.

Note Disabling STP can affect connectivity to the network. Disabling IGMP snooping can adversely affect the network performance.

Use the VLANs Advanced window (Figure 3-8) to change the STP and IGMP snooping settings. To display this window, choose **Configure > VLANs** from the device manager menu, and then click the **Advanced** button on the VLANs window. See the device manager online help for additional guidelines and procedures.

Figure 3-8 VLANs Advanced Window



VLANs: Advanced

Name ▾	ID	□ STP	□ IGMP Snooping
default	1	☑	☑
VLAN0007	7	☑	☑
Cisco-Voice	2	☑	☑
Cisco-Guest	4	☑	☑

Increase Connection Bandwidth through EtherChannels

These are the concepts and procedures for configuring EtherChannels:

- What Is an EtherChannel, page 3-19
- Create, Modify, and Delete an EtherChannel, page 3-20

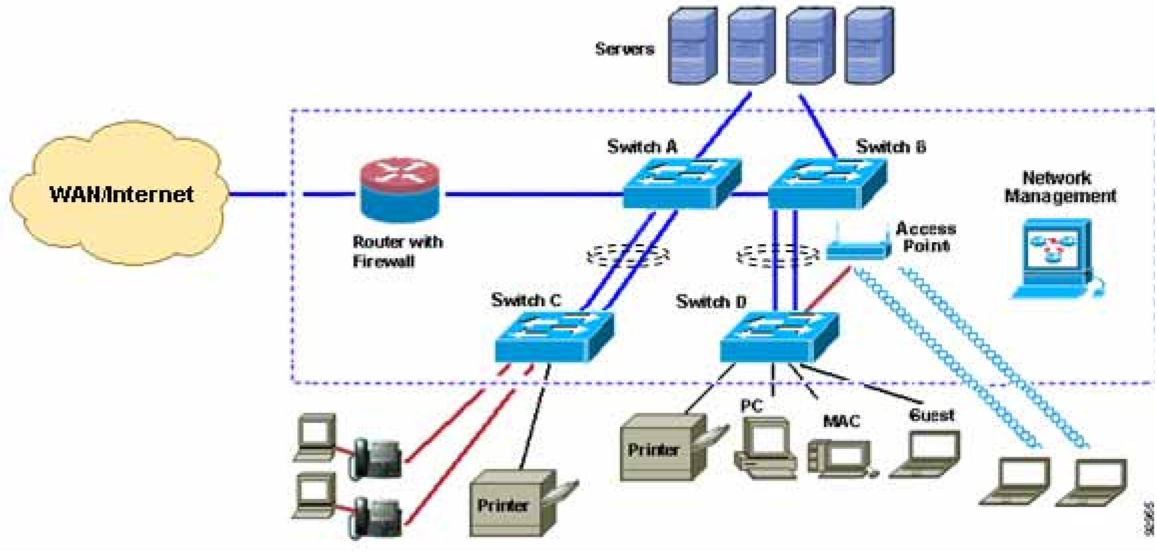
What Is an EtherChannel

An EtherChannel (or port group) is a group of two or more Fast Ethernet or Gigabit Ethernet switch ports bundled into a single logical link, creating a higher bandwidth link between two switches. The switch supports up to six EtherChannels.

Figure 3-9 shows two EtherChannels. Two full-duplex 10/100/1000-Mbps ports on Switches A and C create an EtherChannel with a bandwidth of up to 4 Gbps between both switches. Similarly, two full-duplex 10/100 ports on Switches B and D create an EtherChannel with a bandwidth of up to 400 Mbps between both switches.

If one of the ports in the EtherChannel becomes unavailable, traffic is carried over to the remaining ports within the EtherChannel. Note how redundancy is accomplished without EtherChannels in Figure 1-1 and Figure 3-6.

Figure 3-9 EtherChannels between Catalyst Express Switches



Create, Modify, and Delete an EtherChannel

Prerequisite

All ports in an EtherChannel must have the same characteristics:

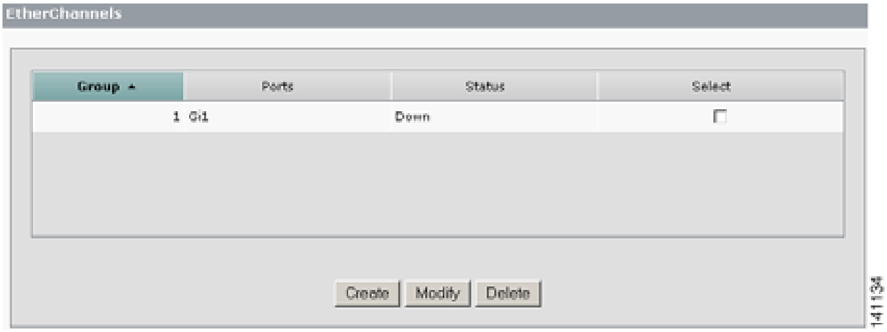
- All are either 10/100 ports or all 10/100/1000 ports. You cannot group a mix of 10/100 and 10/100/1000 ports in an EtherChannel.
- All have the same speed and duplex mode settings. A mismatch in speed or duplex disables the EtherChannel.
- All are enabled. A disabled port in an EtherChannel is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel.
- All are applied with the Smartports Switch port role and belong to the same VLAN. For information about port roles and VLAN memberships, see the "Optimize Ports through Smartports Port Roles" section on page 3-2 and the "Change VLAN Memberships" section on page 3-7.

You can create up to six EtherChannels, and you can configure each EtherChannel in either:

- IEEE 802.3ad (LACP) mode—This allows the switch to create one end of the EtherChannel if the other switch requests it.
- Static mode—This mode requires you to check that both ends of the EtherChannel have the same configuration and then to manually create the EtherChannel.

Use the EtherChannels window (Figure 3-10) to create, modify, and delete EtherChannels. To display this window, choose **Configure > EtherChannels** from the device manager menu. See the device manager online help for additional guidelines and procedures.

Figure 3-10 EtherChannels Window



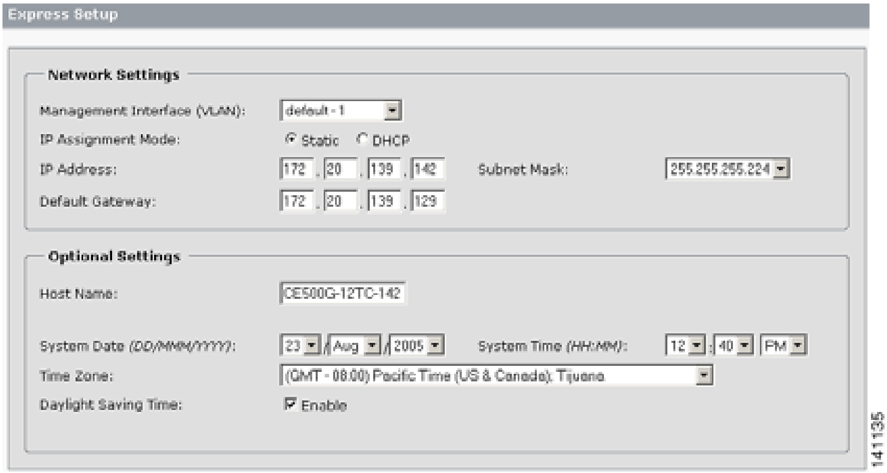
Group ▲	Ports	Status	Select
1	Gi1	Down	□

Update the Switch IP Information

The Express Setup network settings enable the switch to operate with its standard default settings and to be managed through the device manager. Existing settings were set during initial setup. You would need to change these settings if you want to move the switch to a different management VLAN or to a different network.

Use the Express Setup window (Figure 3-11) to update the switch IP information. To display this window, choose **Configure** > **Express Setup** from the device manager menu. See the device manager online help for additional guidelines and procedures.

Figure 3-11 Express Setup Window (after initial setup)



Express Setup

Network Settings

Management Interface (VLAN): default - 1

IP Assignment Mode: ● Static ○ DHCP

IP Address: 172 . 20 . 139 . 142

Subnet Mask: 255.255.255.224

Default Gateway: 172 . 20 . 139 . 129

Optional Settings

Host Name: CE500G-12TC-142

System Date *(DD/MMM/YYYY)*: 23 / Aug / 2005

System Time *(HH:MM)*: 12 : 40 PM

Time Zone: (GMT - 08:00) Pacific Time (US & Canada); Tijuana

Daylight Saving Time: ☑ Enable

These are the switch network settings:

Management Interface (VLAN ID)	The name and ID of the management VLAN through which the switch will be managed. Select an existing VLAN to be the management VLAN. The default name for the management VLAN is *default*. The management VLAN ID was set during initial set up. **Note** Make sure that the switch and your network management station are in the same VLAN. Otherwise, you cannot manage the switch from your management station. If they are in different VLANs, a router or Layer 3 switch is needed to communicate between VLANs. The management VLAN is the broadcast domain where management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that should be limited to a specific group of users (such as the administrators of your network). It also ensures secure, administrative access to all devices in the network at all times. For more information about management VLANs and about VLANs in general, see the "VLAN Types" section on page 3-14.

IP Assignment Mode	The IP assignment mode determines if the switch IP information will be manually assigned (static) or be automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you select **Static** and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the device manager. If you select **DHCP**, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. As long as the switch is not restarted, the switch continues to use the same information, and you can use the same IP address to access the device manager. **Note** If you manually assign the switch IP address and your network uses a DHCP server, make sure that the IP address that you give to the switch is not within the range of addresses that the DHCP server will automatically assign to other devices. This prevents IP address conflicts between the switch and another device.
IP Address	The IP address is a unique identifier for the switch in a network. The format is four numbers separated by periods. Each number can be from 0 to 255. This field is enabled only if the IP assignment mode is Static. **Note** Make sure that the IP address that you assign to the switch is not being used by another device in your network. The IP address and the default gateway cannot be the same. You cannot assign the switch with an IP address in the 10.0.0.0 network.
Subnet Mask List	The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is enabled only if the IP assignment mode is Static.

Default Gateway	The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The IP address should be part of the same subnet as the switch IP address. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This field is enabled only if the IP assignment mode is Static. **Note** You must specify a default gateway if your network management station and the switch are in different networks or subnetworks. Otherwise, the switch and your network management station cannot communicate with each other. The IP address and the default gateway cannot be the same.

Update Basic Administrative Settings

The Express Setup optional settings identify and synchronize the switch so that it can be managed properly. Existing settings might have been set during initial setup. Update these settings if you need to change the switch name or its system clock.

Use the Express Setup window (Figure 3-11) to update the switch administrative settings. To display this window, choose **Configure** > **Express Setup** from the device manager menu. See the device manager online help for additional guidelines and procedures.

These are the basic administrative settings:

.

Host Name	A name for the switch. The name can have up to 31 alphanumeric characters. The name cannot contain a ?, a space, or a tab. The default is Switch. We recommend entering either the name, location, or IP address of the switch to help identify the switch during monitoring or troubleshooting.
System Date	This is the date that the switch automatically read from the network management station or was manually set during initial setup.
System Time	This is the time that the switch automatically read from the network management station or was manually set during initial setup.

Time Zone	This is the time zone that the switch automatically read from the network management station or was manually set during initial setup.
Daylight Saving Time	The check box is automatically enabled only when the selected time zone is in U.S., Europe, or Australia. This check box is disabled for all of the other time zones.

Enable the Switch for Remote Management

Note This section is for advanced users with experience in managing networks.

These are the concepts and procedures for using SNMP:

- What Is SNMP, page 3-25
- Configuring SNMP, page 3-26
- Supported MIBs, page 3-28

What Is SNMP

The switch supports Simple Network Management Protocol (SNMP) versions 1, 2C, and 3. SNMP allows the switch to be remotely managed through other network management software.

SNMP is based on three concepts: SNMP managers (or management stations), SNMP agents (or network devices), and the Management Information Base (MIB). For the MIBs supported on the switch, see the "Supported MIBs" section on page 3-28.

The SNMP manager runs SNMP management software. Network devices to be managed, such as bridges, routers, servers, and workstations, are equipped with an agent software module. The agent provides access to a local MIB of objects that reflects the resources and activity of the device. The agent also responds to manager commands to retrieve values from the MIB and to set values in the MIB. The agent and MIB are on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

Both SNMPv1 and v2C use a community-based form of security. SNMP managers can access the agent MIB through passwords referred to as community strings. SNMPv1 and v2C are generally used for network monitoring without network control.

SNMPv3 provides network monitoring and control. It provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security model used by SNMPv3 is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used for an SNMP packet.

Note the following about SNMPv3 objects:

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy defines which SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications that its users can receive.
- A group also defines the security model and the security level for its users.
- An SNMP view is a list of MIBs that a group can access.
- Data can be securely collected from SNMP devices without fear of the data being tampered with or corrupted.
- Confidential information, for example, SNMP Set command packets that change a router configuration, can be encrypted to prevent the contents from being exposed on the network.

Configuring SNMP

Enable SNMP if you plan to have the switch managed through another network management application. By default, SNMP is disabled.

Other general SNMP settings include the name of the switch or the network administrator and the switch location. System name and system contact information appear in the Switch Information area on the Dashboard.

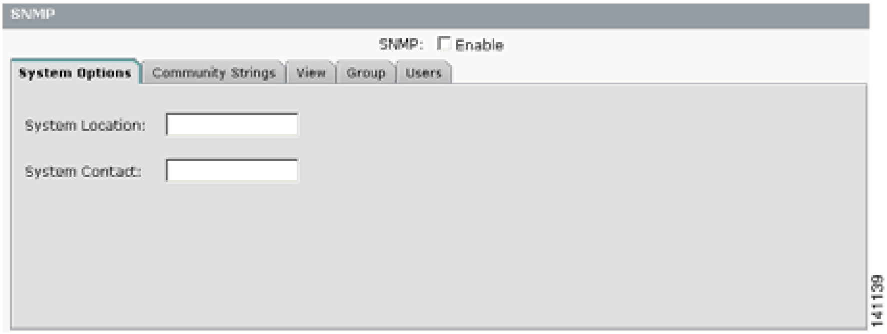
Community strings are forms of passwords to the switch Management Information Base (MIB). You can create community strings that allow a remote manager read-only or read-write access to the switch.

- The Read-Only community string operates as a password that enables the switch to validate Get (read-only) requests from a network management station. If you set the SNMP read community, users can access MIB objects, but cannot change them.
- The Read-Write community string operates as a password that enables the switch to validate Set (read-write) requests from a network management station. If you set the SNMP write community, users can access and change MIB objects.

Advanced SNMP settings include displaying the SNMP object identifiers (OIDs) of objects that can be accessed, displaying the attributes of the v1defaultGroup SNMP group, and changing the users of the v1defaultGroup SNMP group.

Use the SNMP window (Figure 3-12) to update change the SNMP settings. To display this window, choose **Configure** > **SNMP** from the device manager menu. See the device manager online help for additional guidelines and procedures.

Figure 3-12 SNMP Window



Supported MIBs

- BRIDGE-MIB
- CISCO-ENVMON-MIB
- CISCO-PRODUCTS-MIB
- CISCO-SYSLOG-MIB
- ENTITY-MIB
- RFC1213-MIB (MIB II)
- RFC1398-MIB (ETHERNET-MIB)
- RFC1573-MIB (IF-MIB)
- RMON-MIB (statistics, history, alarms, and events groups only)

When You Are Done

Monitor the performance of your network and the switch, as described in Chapter 4, “Monitoring.”

Monitoring

Read this chapter to understand the switch monitoring features that are used to evaluate the status and the performance of the switch. The tasks in this chapter are independent, unless otherwise noted, and are listed in no particular order.

Before You Begin:

The monitoring features described in this chapter are available if the switch has an IP address. Make sure that the switch has been set up as described in the *Getting Started Guide for the Catalyst Express 500 Switches*.

Chapter Topics:

Why Monitor the Switch

Any problem in your switch can affect a large proportion of your users. Implementing a preventive approach to switch monitoring helps you to detect problems early and to avoid potential problems.

With switch monitoring, you can gain visibility into the status and availability of switch ports. You can actively monitor switch ports and quickly notify users if a switch port or the switch fails.

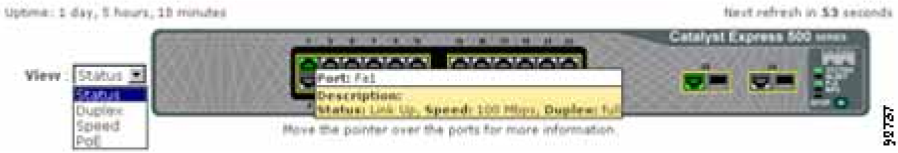
When you access the device manager Dashboard and monitoring windows, you can:

- Check the overall switch status and the switch vital signs.
- Verify connectivity for new users or devices.
- Check daily traffic patterns.
- Check for suspected problems by using the monitoring windows as a starting point for further troubleshooting.
- Check for specific ports that could be causing problems.
- Get an overview of switch bandwidth usage and port statistics.
- View a history of switch activity.

Check the Front Panel LEDs

You can get a quick view of the overall condition of the switch by checking the device manager Front Panel view (Figure 4-1).

Figure 4-1 Front Panel View



Uptime: 1 day, 5 hours, 18 minutes

Next refresh in 53 seconds

View : Status

Port: Fa1

Description:

Status: Link Up, Speed: 100 Mbps, Duplex: full

Move the pointer over the ports for more information.

The Front Panel view is a graphical display of the switch front panel. The system LEDs (Table 4-1) and port LEDs (Table 4-2) on the Front Panel view and on the physical switch match. You can use the device manager **View** list to change the type of information displayed by the port LEDs.

The Front Panel view shows all the switch components color-coded according to their status, and it is always visible during the device manager session. The colors help you to quickly see if a fault or an error condition exists. A Legend describes the meanings of the colors (see the "Legend of LED Colors" section on page 4-4).

Move the pointer over a port to display the port number, description, status, speed, duplex mode, and Power over Ethernet (PoE) status. The port speed and duplex mode for a port only appear in the pop-up window when a device is connected to the port. The PoE status is available only if the port is a PoE port.

The Uptime field shows how long the switch has been operating since it was last powered on or was restarted. Status is automatically refreshed every 60 seconds or when you click **Refresh** on the toolbar. The refresh counter shows the number of seconds left before the next refresh cycle starts.

System LEDs

For the meanings of the system LED colors, see Table 4-4.

Table 4-1 System LEDs

SYSTEM	The status of the switch (system).
ALERT	The presence of a switch problem. When the switch detects a problem on one or more ports, the Alert LED turns amber. Move the pointer over the Alert LED to display a description of the most recent problem detected, the port on which the problem exists, and the time that it was detected. The Alert LED stays amber until the Alert Log is cleared. The link to the Alert Log provides more details about the problem. For more information about the Alert Log, see the "Check the Alert Log" section on page 4-23.
PoE	The status of PoE being provided to the ports.
RPS	The status of the redundant power supply (RPS) if one is connected to the switch.
SETUP	The configuration mode in which the switch is operating. The **SETUP** button on the Front Panel view is not active.

Port LEDs

Choose an LED mode from the **View** list to change the type of information displayed through the port LEDs. Note that changing the modes of the LEDs is available only through the device manager.

For the meanings of the port LED colors, see Table 4-3.

Table 4-2 Port LEDs

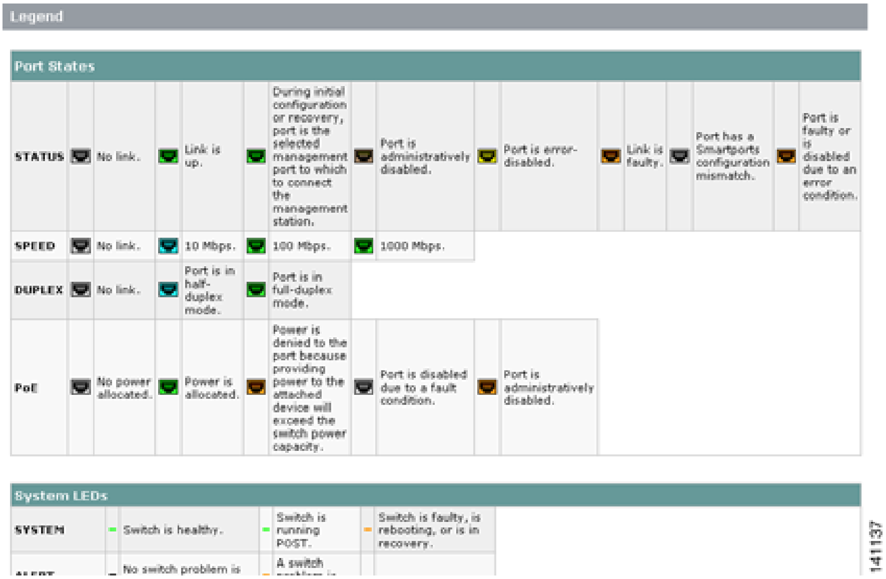
STATUS	The port status. This is the default mode.
DUPLEX	The port duplex mode (full duplex or half duplex). **Note** The 10/100/1000 ports operate only in full-duplex mode.
SPEED	The port operating speed (10, 100, or 1000 Mbps).
PoE	The power status on the PoE ports.

Legend of LED Colors

From the device manager, you can use the Legend (Figure 4-2, Table 4-3, and Table 4-4) to display a color-coded explanation of the icons and colors used on the device manager windows.

To display the Legend, click **Legend** from the device manager tool bar. You can also click **Legend** from the device manager online help menu.

Figure 4-2 LED Legend



Legend

Port States

STATUS	⬛ No link.	🟩 Link is up.	🟩 During initial configuration or recovery, port is the selected management port to which to connect the management station.	🟫 Port is administratively disabled.	🟨 Port is error-disabled.	🟧 Link is faulty.	⬛ Port has a Smartports configuration mismatch.	🟧 Port is faulty or is disabled due to an error condition.
SPEED	⬛ No link.	🟦 10 Mbps.	🟩 100 Mbps.	🟩 1000 Mbps.				
DUPLEX	⬛ No link.	🟦 Port is in half-duplex mode.	🟩 Port is in full-duplex mode.					
PoE	⬛ No power allocated.	🟩 Power is allocated.	🟧 Power is denied to the port because providing power to the attached device will exceed the switch power capacity.	⬛ Port is disabled due to a fault condition.	🟧 Port is administratively disabled.			

System LEDs

SYSTEM	🟩 Switch is healthy.	🟩 Switch is running POST.	🟧 Switch is faulty, is rebooting, or is in recovery.
ALERT	⬛ No switch problem is	🟧 A switch problem is	

Table 4-3 Port LED Colors in Legend

Port Mode	Color	Description
Status	Off (dark)	No link.
	Solid green	Link is up.
	Blinking green	During initial configuration or recovery, the port is the selected management port to which to connect the management station.
	Solid brown	Port is administratively disabled.
	Solid yellow	Port is error disabled.
	Blinking green and amber	Link is faulty.
	Blinking amber	Port has a Smartports configuration mismatch.
	Solid amber	Port is faulty or is disabled due to an error condition.

Table 4-3 Port LED Colors in Legend (continued)

Port Mode	Color	Description
Speed	Off (dark)	No link.
	Solid light blue	10 Mbps.
	Solid green	100 Mbps.
	Blinking green	1000 Mbps.
Duplex	Off (dark)	No link.
	Solid light blue	Port is in half-duplex mode.
	Solid green	Port is in full-duplex mode.
PoE	Off (dark)	No power is allocated.
	Solid green	Power is allocated.
	Blinking green and amber	Power is denied to the port because providing power to the attached device will exceed the switch power capacity.
	Blinking amber	Port is disabled due to a fault condition.

Table 4-4 System LED Colors in Legend

LED	Color	Description
SYSTEM	Solid green	Switch is healthy.
	Blinking green	Switch is running POST.
	Solid amber	Switch is faulty, is rebooting, or is in recovery.
ALERT	Off (dark)	No switch problem is detected.
	Solid amber	A switch problem is detected.
PoE	Off (dark)	PoE to the ports is off.
	Solid green	One or more ports is receiving PoE power.
	Blinking amber	One or more ports is not receiving PoE power because of a fault.

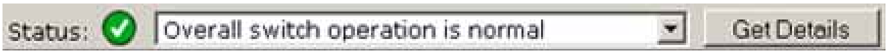
Table 4-4 System LED Colors in Legend (continued)

LED	Color	Description
RPS	Off (dark)	No redundant power supply (RPS) is connected.
	Solid green	RPS is available to provide back-up power.
	Blinking green	RPS is providing back-up power to another device.
	Blinking amber	RPS is providing power to the switch.
	Solid amber	RPS is in standby mode, or RPS is faulty.
SETUP	Off (dark)	Switch is configured as a managed switch, or switch is operating as an unmanaged switch.
	Solid green	Switch is in initial setup.
	Blinking green	Switch is in initial setup or in recovery, or initial setup is incomplete.
	Solid amber	Switch failed to start initial setup or recovery because there is no available switch port to which to connect the management station. Disconnect a device from a switch port, and then press the **SETUP** button.

Check the Status Field

The Status field (Figure 4-3) displays the severity and number of problems (hardware issues and misconfigurations) on the switch. If no problems exist, the field shows that the overall switch operation is normal. This field is always visible during the device manager session. It is below the Front Panel view.

Figure 4-3 Status Field



Status: ✓ Overall switch operation is normal

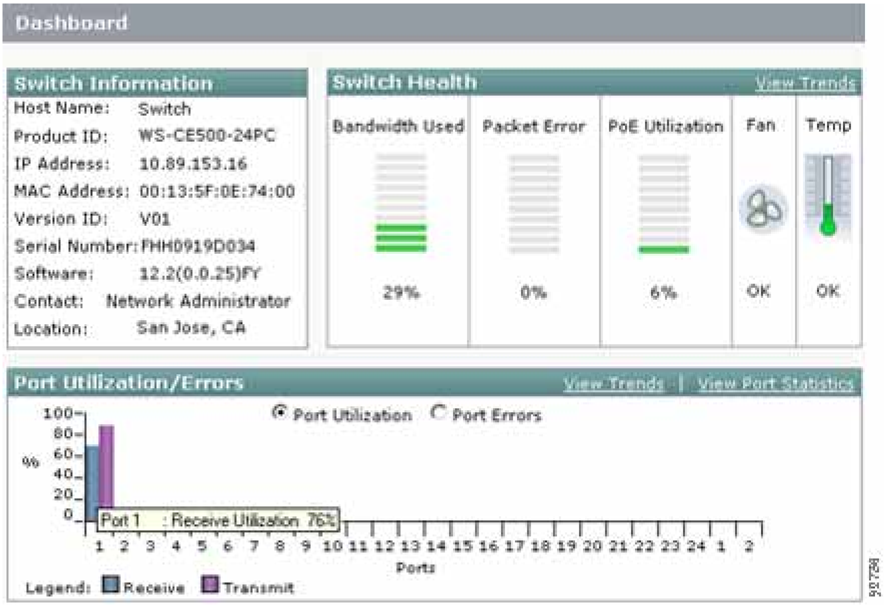
Choose a problem in the list, and then click **Get Details**. This displays a complete troubleshooting report, including the problem highlighted and recommended actions to resolve the problem. For information about diagnostics, see the “Run a Diagnostic Test” section on page 5-2.

View the Alert Log for the details of the problems and the most recent time at which the switch detected the problems. For information about the log, see the "Check the Alert Log" section on page 4-23.

Check the Dashboard

The Dashboard (Figure 4-4) is the main window for monitoring the switch status and performance. It is the default window and appears each time you display the device manager. To display the Dashboard, choose **Dashboard** from the device manager menu.

Figure 4-4 Switch Dashboard



Dashboard

Switch Information

Host Name: Switch
Product ID: WS-CE500-24PC
IP Address: 10.89.153.16
MAC Address: 00:13:5F:0E:74:00
Version ID: V01
Serial Number: FHH0919D034
Software: 12.2(0.0.25)FY
Contact: Network Administrator
Location: San Jose, CA

Switch Health

Bandwidth Used	Packet Error	PoE Utilization	Fan	Temp
29%	0%	6%	OK	OK

Port Utilization/Errors

● Port Utilization ○ Port Errors

Port 1 : Receive Utilization 76%

The Dashboard displays:

- "Switch Information" section on page 4-9
- "Bandwidth Used Gauge" section on page 4-10
- "Packet Error Gauge" section on page 4-11

- "PoE Gauge" section on page 4-12
- "Fan Status" section on page 4-12
- "Temperature Status" section on page 4-13
- "Port Utilization and Port Errors Graphs" section on page 4-13

Tip The gauges and graphs on the Dashboard correlate with the graphs on the Trends window. The Dashboard displays instantaneous status, while the Trends graphs displays historical status. Used together, you can gather the detailed conditions (vital signs) of the switch and its ports. For information about the Trends graphs, see the "Check the Trends Graphs" section on page 4-14.

Switch Information

The Switch Information area on the Dashboard displays this information about the switch:

Name	The name of this switch configured during initial setup or through Network Assistant. If no name was provided, this field displays the default name, *Switch*.
Product ID	The model of this switch. This information cannot be modified.
IP Address	The IP address of this switch configured during initial setup or through Network Assistant.
MAC Address	The MAC address of this switch. This information cannot be changed.
Version ID	The version ID of the switch. This information cannot be changed.
Serial Number	The serial number of this switch. This information cannot be changed.
Software	The Cisco IOS software version that this switch is running. This information is updated when you upgrade the switch software.
Contact	The name of the person who is the administrative contact for this switch. This information is entered on the SNMP window or through Network Assistant.
Location	The location of this switch. This information is configured from the SNMP window or through Network Assistant.

Bandwidth Used Gauge

The Bandwidth Used gauge shows the total percentage of the switch bandwidth being used. Each bar in the gauge represents 10 percent and does not show increments that are less than 10 percent. The gauge does not show total bandwidth under 5 percent.

Data is collected at each 60-second system refresh. For a graph that shows bandwidth utilization patterns over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days), see the "Bandwidth Utilization Graph" section on page 4-15.

The Bandwidth Used gauge changes as the switch experiences the network activity from devices sending data through the network. As network activity increases, so does contention between devices to send data through the network. As you monitor utilization on the switch, note whether the percentage of usage is what you expect during that given time of network activity. If utilization is high when you expect it to be low, perhaps a problem exists.

As you monitor the switch, note if the bandwidth utilization is consistently high. This can mean there is congestion in the network. If the switch reaches its maximum bandwidth (above 90 percent utilization) and its buffers become full, it begins to discard the data packets that it receives. Some packet loss in the network is not considered unusual, and the switch is configured to help recover lost packets (such as by signaling to other devices to resend data). However, excessive packet loss can create packet errors, which can degrade overall network performance.

To reduce congestion, consider segmenting the network into subnetworks that are connected by other switches or routers. Look for other causes, such as faulty devices or connections, that can also increase bandwidth utilization on the switch.

Packet Error Gauge

The Packet Error gauge shows the total packet error percentage for the switch. Each bar in the gauge represents 10 percent and does not show increments that are less than 10 percent. The gauge does not show total packet errors under 5 percent.

Data is collected at each 60-second system refresh. To see a graph that shows packet error percentages over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days), see the "Packet Error Graph" section on page 4-16.

The packet error percentage is calculated by comparing two values:

- The total number of packets that are sent and received
- The total number of packets with errors that are sent and received

If the packet-error percentage is high (that is, above 10 percent), the switch bandwidth utilization might also be too high (a sign that the network is congested). Other causes for packet errors are faulty cabling and port misconfigurations, such as a duplex mode mismatch. These problems can cause network users to experience intermittent connectivity or loss of connectivity to network resources (such as servers and printers) or to the Internet. Excessive collisions can cause transmission delays. For example, users might experience excessive delays in sending or receiving information through the network.

The Port Statistics window displays some of the types of packet errors (Table 4-5) collected by the switch. The type of packet error can help you to identify a more precise cause for some network problems. For more information about port statistics, see the "Check the Port Statistics" section on page 4-18.

These are some types of packet errors.

Table 4-5 Types of Packet Errors

Runt packets	Packets that are smaller than the allowed minimum size (less than 64 bytes).
Giant packets	Packets that are larger than the allowed maximum size (more than 1518 bytes).
Cyclic redundancy checksum (CRC) errors	Errors generated by the originating LAN station or far-end device do not match the checksum calculated from the data received. On a LAN, this usually means noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or of a station sending bad data.
Overrun packets	Packets that the receiving device was unable to receive.

Table 4-5 Types of Packet Errors (continued)

Frame packets	Packets received because of a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
Ignored packets	Packets that the interface ignores because the interface hardware is low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to increase.

PoE Gauge

The PoE Utilization gauge is only for switches with PoE ports.

The power gauge shows the total percentage of power that is allocated to connected devices that are receiving power from the switch. Move the pointer over the gauge to display the actual percentage of power (in watts) that is used and is remaining. Each bar in the gauge represents 10 percent and does not show increments that are less than 10 percent. The gauge does not show total PoE utilization under 5 percent.

Data is collected at each 60-second system refresh. For a graph that shows power utilization patterns over incremental instances in time (up to ten 60-second refresh cycles), see the "PoE Utilization Graph" section on page 4-16.

The switch automatically maintains a power budget, monitors and tracks requests for power, and grants power only when it is available. If the switch is powering attached PoE devices, you should expect to see activity on this gauge.

Fan Status

The animated fan shows whether the fan (or blower) on the switch is rotating and thus is functioning normally. If the fan is not rotating, check the physical switch. A malfunctioning fan can affect the internal temperature of the switch. Check the thermometer graphic to see if the switch has reached an unacceptably high temperature.

Temperature Status

Use the thermometer with the animated fan to monitor the switch internal temperature environment. The thermometer graphic displays:

OK	Green	Switch internal temperature is within the acceptable temperature range.
Faulty	Red	Switch internal temperature is above the upper temperature threshold.

For information about the switch temperature range and the operating environment guidelines, see the "Installation Guidelines" section on page 2-9 and the "Technical Specifications" section on page A-1.

Port Utilization and Port Errors Graphs

At a glance, you can see the following information on port performance:

- Port Utilization Graph—This graph displays the received utilization (blue) and sent utilization (purple) on each port. As you monitor utilization on the ports, note whether the percentage of usage is what you expect during that given time of network activity. If utilization is high when you expect it to be low, a problem might exist.

  Bandwidth allocation can also be based on whether the connection is operating in half-duplex or full-duplex mode.

- Port Errors Graph—This graph displays the total percentage of errors on each port.

  These are some of the reasons for errors received on and sent from the switch ports:

  - Bad cable connection
  - Defective ports
  - Software problems
  - Driver problems

Data is collected at each 60-second system refresh. For a graph that shows per-port patterns over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days), see the "Per-Port Utilization and Per-Port Errors Graphs" section on page 4-16. For details on the specific port errors detected on each port, see the "Check the Port Statistics" section on page 4-18.

Check the Trends Graphs

Use the Trends window (Figure 4-5) to display the historical trends graphs. Use these graphs to display the switch bandwidth, the port usage, and the percentage of packet errors detected by the switch. You can display the data in increments of seconds, minutes, hours, and days. The granularity of these graphs can help you to analyze traffic patterns and to identify problems with the switch and individual ports.

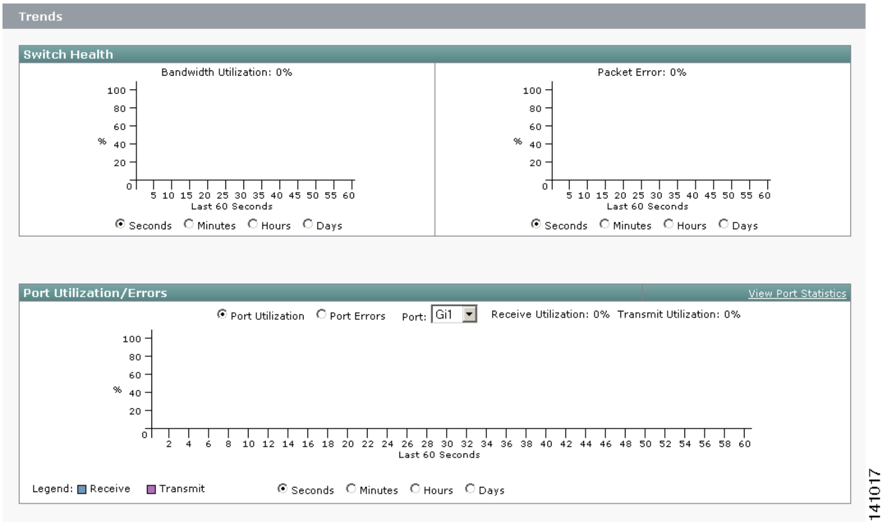
Tip If you are using the trends graphs to monitor the switch status over time, do not end your device manager session. Redisplaying the device manager clears the data from the PoE graph.

To display the Trends window, choose **Monitor** > **Trends**. You also can click the **View Trends** link from Dashboard.

The Trends window displays these graphs:

- Bandwidth Utilization Graph, page 4-15
- Bandwidth Utilization Graph, page 4-15
- Packet Error Graph, page 4-16
- PoE Utilization Graph, page 4-16
- Per-Port Utilization and Per-Port Errors Graphs, page 4-16

Figure 4-5 Trends Window



Trends

Switch Health

Bandwidth Utilization: 0%

● Seconds ○ Minutes ○ Hours ○ Days

Packet Error: 0%

● Seconds ○ Minutes ○ Hours ○ Days

Port Utilization/Errors

View Port Statistics

● Port Utilization ○ Port Errors Port: Gi1 Receive Utilization: 0% Transmit Utilization: 0%

Legend: ▨ Receive ▨ Transmit

● Seconds ○ Minutes ○ Hours ○ Days

Bandwidth Utilization Graph

The Bandwidth Utilization graph shows the same information as the Bandwidth Used gauge on the Dashboard, except that the graph can show bandwidth usage patterns over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). This graph also marks the highest peak reached. The default is 60 seconds.

If you see sharp increases in switch usage, use this graph to determine when unusual peaks in network usage occur. For more information about bandwidth usage, see the “Bandwidth Used Gauge” section on page 4-10.

Packet Error Graph

The Packet Error graph shows the same information as the Packet Error gauge on the Dashboard, except that the graph can show the percentage of packet errors collected over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). The default is 60 seconds.

Use this graph to audit the effects that connected devices have on the switch performance or the network. For example, if you suspect that a connected device is sending error packets, you can check if the data on the graph changes when you disconnect and reconnect the suspected device. For more information about packet errors, see the "Packet Error Gauge" section on page 4-11.

PoE Utilization Graph

The PoE Utilization graph is only available if the switch is a PoE switch. This graph shows the same information as the PoE Utilization gauge on the Dashboard. The percentage of power allocated is shown over ten 60-second system refresh cycles. For more information about power allocation, see the "PoE Gauge" section on page 4-12.

Per-Port Utilization and Per-Port Errors Graphs

The Port Utilization and Port Errors graphs on the Trends window show the same information as the Port Utilization and Port Errors graphs on the Dashboard, except that the graphs on the Trends window can show the usage patterns of a specific port over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). The default is 60 seconds.

To display the trends for a specific port, choose a port from the **Port** list.

Use these graphs to observe the performance of a specific port. For example, if a network user is having intermittent network connectivity, use the Port Utilization graph to observe the traffic patterns on the port to which the user's PC is connected, and use the Port Errors graph to see if the port is receiving or sending error packets.

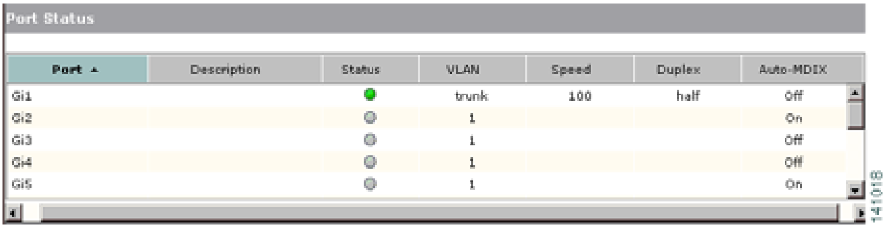
For more information about port usage and port errors, see the "Port Utilization and Port Errors Graphs" section on page 4-13.

Check the Port Status

If the switch has link issues, such as traffic not being received on a switch port, use the Port Status window (Figure 4-6) to check the basic port status, to make sure that the speed and duplex mode of the switch port and the connected device match, and to check that the port is in the correct VLAN.

If the switch has link issues, such as traffic is not being received on a switch port, use this window to verify that the port settings are correct. You can check switch ports before connecting devices to the port to confirm that the settings of both devices match.

Figure 4-6 Port Status Window



Port Status

Port ▲	Description	Status	VLAN	Speed	Duplex	Auto-MDIX
Gi1		●	trunk	100	half	Off
Gi2		○	1			On
Gi3		○	1			Off
Gi4		○	1			Off
Gi5		○	1			On

The Port Status window displays this information

Port	The number of the port, including the port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet) and the port number.
Description	The description of the port. This is configured from **Configure** > **Port Settings**.
Status	The state of the port. The state of a port can be up, down, or administratively (manually) enabled or disabled. For explanations of the colors used in this column, click **Legend** on the toolbar. You can administratively enable or disable the port from **Configure** > **Port Settings**.
VLAN	The VLAN ID to which the port belongs (also known as its VLAN membership). The default is 1. This is configured from **Configure** > **Smartports** > **Customize** or through Network Assistant. If the port belongs to more than one VLAN, *trunk* appears in this column. **Note** To assign the port to multiple VLANs, use Network Assistant.

Speed	The operating speed of the port. The speed can be 10, 100, or 1000 Mbps. This is configured from **Configure** > **Port Settings**.
Duplex	The duplex state of the port. The duplex mode can be full or half duplex. This is configured from **Configure** > **Port Settings**.
Auto-MDIX	The state of the automatic medium-dependent interface crossover (auto-MDIX) feature. The feature can be enabled or disabled. This is configured from **Configure** > **Port Settings**.
PoE	The PoE state of the port: • **Off**—A PoE device is not connected to the port. • **Admin Off**—The port is set to never provide power to a connected PoE device. • **Error-Disabled**—The port is disabled due to a misconfiguration or violation on the switch. • **On**—A PoE device is connected to the port, and this port can provide it with power. • **Power Deny**—The power budget is allocated to other ports, and this port cannot provide power to a connected PoE device. If the port is supplying power to a device, the state includes the number of watts that is allocated to the port. **Note** This status is available only on PoE ports.

Check the Port Statistics

Use the Port Statistics window to display the statistics for data sent from and received by the switch ports since the switch was last powered on, was restarted, or since the statistics were last cleared.

The types of port statistics collected and displayed are grouped under these tabs on the Port Statistics window:

- Overview Tab, page 4-19
- Transmit Detail Tab, page 4-20
- Receive Detail Tab, page 4-21

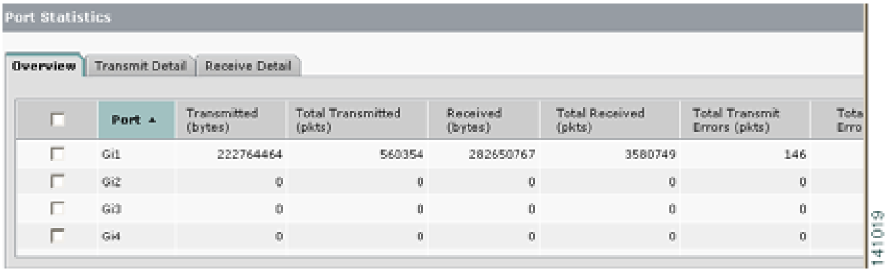
To display the Port Statistics window, choose **Monitor > Port Statistics** from the device manager menu. You also can click the **View Port Statistics** link from Dashboard.

To clear the data from the statistics tables, click **Clear Counters** from the window.

Note Clearing the statistics on one tab clears the statistics on the other tabs.

See the device manager online help for additional guidelines and procedures.

Figure 4-7 Port Statistics Window



□	Port ▲	Transmitted (bytes)	Total Transmitted (pkts)	Received (bytes)	Total Received (pkts)	Total Transmit Errors (pkts)	Tota Erro
□	Gi1	222764464	560354	282650767	3580749	146	
□	Gi2	0	0	0	0	0	
□	Gi3	0	0	0	0	0	
□	Gi4	0	0	0	0	0	

Overview Tab

The Overview tab displays:

- The total number of bytes sent and received on each port.
- The total number of packets sent and received on each port.
- The total number of error packets sent. This includes total collisions, late collisions, and excessive collisions.
- The total number of error packets received. This includes frame check sequence (FCS) and alignment errors. Equipment being powered on or off can cause FCS and alignment errors.

This tab displays the specific numbers of error packets received on and sent from the port, which is a granularity that is not available from the Dashboard and Trends graphs. The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity. For example, to troubleshoot problems regarding loss of connectivity, clear the statistics for the port in question, and see if the port continues to receive and send packets.

Table 4-6 Overview Tab Descriptions

Port	The number of the port, including the port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet) and the port number.
Transmitted bytes	The total number of bytes sent from each port.
Total transmitted packets	The total number of packets sent from each port. This includes unicast, multicast, and broadcast packets.
Received bytes	The total number of bytes received on each port.
Total received packets	The total number of packets received on each port. This includes well-formed unicast, multicast, and broadcast packets.
Total transmit error packets	The total number of error packets sent. This includes total runts, collisions, late collisions, and excessive collisions.
Total receive error packets	The total number of error packets received. This includes runts, and FCS and alignment errors.

Transmit Detail Tab

The Transmit Detail tab displays:

- Transmitted unicast, multicast, and broadcast packets on each port
- Detailed statistics of errors sent to each port

You can use the statistics on this tab to troubleshoot unusual changes in network traffic. If a port is sending an unusually high amount of traffic (such as multicast or broadcast packets), check the connected device to see if this traffic pattern is normal or could mean a problem.

Table 4-7 Transmit Detail Tab Descriptions

Port	The number of the port, including the port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet) and the port number.
Unicast packets	The total number of well-formed unicast packets sent by a port. It excludes packets sent with errors or with multicast or broadcast destination addresses.
Multicast packets	The total number of well-formed multicast packets sent by a port. It excludes packets sent with errors or with unicast or broadcast destination addresses.
Broadcast packets	The total number of well-formed broadcast packets sent by a port. It excludes packets sent with errors or with unicast or multicast destination addresses.
Total collision packets	The total number of packets sent without error after having 1 to 15 collisions. It includes packets of all destination address types and excludes packets discarded because of insufficient resources or late collisions.
Excessive collision packets	The total number of packets that were not sent after 16 collisions. It includes packets of all destination address types.
Late collision packets	The total number of packets discarded because of late collisions detected during transmission. It includes all sent packets that had a collision after the transmission of the packet sixty-fourth byte. The preamble and start frame delimiter (SFD) are not included in the frame byte count.

Receive Detail Tab

The Receive Detail tab displays:

- Received unicast, multicast, and broadcast packets on each port.
- Detailed statistics of receive errors on each port.

You can use the statistics on this tab to troubleshoot unusual changes in network traffic. If a port is receiving an unusually high amount of traffic (such as multicast or broadcast packets), check the connected device to see if this traffic pattern is normal for the connected device or could mean a problem.

Table 4-8 Receive Detail Tab Descriptions

Port	The number of the port, including the port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet) and the port number.
Unicast packets	The total number of well-formed unicast packets received by a port. It excludes packets received with errors, with multicast or broadcast destination addresses, or undersize packets, discarded packets, or those without a destination.
Multicast packets	The total number of well-formed multicast packets received by a port. It excludes packets received with errors, with unicast or broadcast destination addresses, with oversized or undersize packets, discarded packets, or those without a destination.
Broadcast packets	The total number of well-formed broadcast packets received by a port. It excludes packets received with errors, with unicast or multicast destination addresses, or with oversized or undersize packets, discarded packets, or those without a destination.
FCS error packets	The total number of packets received with FCS errors. It excludes undersized packets with FCS errors.
Alignment errors packets	The total number of packets received with alignment errors. It includes all the packets received with both an FCS error and a nonintegral number of bytes.
Oversize packets	The total number of received packets with more than 1518 bytes that had both good and bad FCS values.
Undersize packets	The total number of received packets that were smaller than 64 octets long and were otherwise well-formed.
Collision fragments	The total number of frames smaller than 64 bytes that have an integral number of bytes and bad FCS values.

Check the Alert Log

The Alert Log displays switch problems that happened since the log was last cleared. The problems are issues that should be or have already been solved.

To display the Alert Log, choose **Monitor > Alert Log** from the device manager menu. You can also click the **Alert Log** link in the popup when you move your pointer over the amber Alert LED.

Tip Use the Alert Log with the Alert LED on the Front Panel view. When the switch detects a problem, the Alert LED turns amber.

The Alert LED stays amber until the Alert Log is cleared. Click the **Clear Log** button to acknowledge that you have read the alerts and to turn off the amber Alert LED.

Note

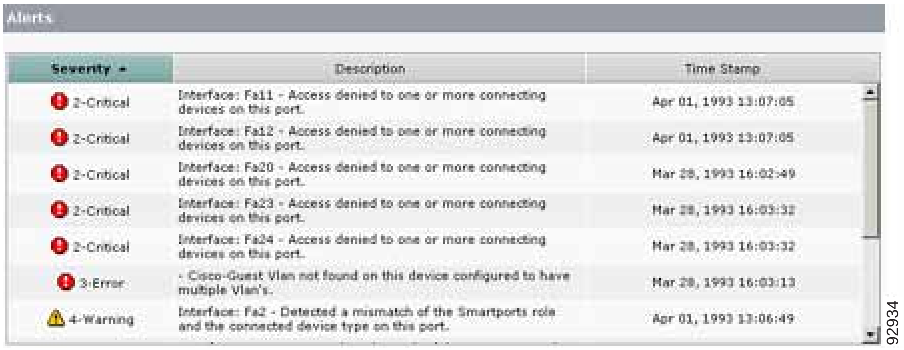
- The **Clear Log** button does not solve the problem. Use the Diagnostics window to generate a diagnostics report to solve problems detected by the switch.
- Solving the problems does not turn off the Alert LED. You must also click the **Clear Log** button.

See the device manager online help for the guidelines and procedures on how to use the Alert Log.

The Alert Log includes this information (see also Figure 4-8):

Severity Level	A single-digit code (0 to 5) that reflects the severity of the problem. The lower the number, the more serious the condition and the need to take action. ⊗ Emergency (0)—The switch is unusable. Alert (1)—The switch requires immediate action. ❗ Critical (2)—The switch has a critical condition. Error (3)—The switch has an error condition. ⚠ Warning (4)—The switch has a warning condition. ℹ Notifications (5)—The switch is operating normally but has a significant condition.
Description	The description of the problem, including the ports on which the problem was detected.
Time Stamp	The date and time of the refresh cycle during which the problem was last detected.

Figure 4-8 Sample Alert Log



Alerts

Severity ▾	Description	Time Stamp
❗ 2-Critical	Interface: Fa11 - Access denied to one or more connecting devices on this port.	Apr 01, 1993 13:07:05
❗ 2-Critical	Interface: Fa12 - Access denied to one or more connecting devices on this port.	Apr 01, 1993 13:07:05
❗ 2-Critical	Interface: Fa20 - Access denied to one or more connecting devices on this port.	Mar 28, 1993 16:02:49
❗ 2-Critical	Interface: Fa23 - Access denied to one or more connecting devices on this port.	Mar 28, 1993 16:03:32
❗ 2-Critical	Interface: Fa24 - Access denied to one or more connecting devices on this port.	Mar 28, 1993 16:03:32
❗ 3-Error	- Cisco-Guest Vlan not found on this device configured to have multiple Vlan's.	Mar 28, 1993 16:03:13
⚠ 4-Warning	Interface: Fa2 - Detected a mismatch of the Smartports role and the connected device type on this port.	Apr 01, 1993 13:06:49

When You Are Done

If needed, see Chapter 3, "Customization" to change or to verify feature settings, or see Chapter 5, "Troubleshooting" to identify and resolve problems.

Troubleshooting

Read this chapter to learn about the switch diagnostic tools and troubleshooting features designed to help you solve network-related problems. The tasks in this chapter are independent, unless otherwise noted, and are listed in no particular order.

Before You Begin

Familiarize yourself with the monitoring features (see Chapter 4, “Monitoring”) from which you can find out the specific problems on the switch and from which you can prevent problems by addressing problematic trends.

Chapter Topics

Run a Diagnostic Test

When the switch detects a problem, the Alert LED turns amber, and the Status field lists the detected problem. From the Diagnostics window (Figure 5-1), you can run switch and link diagnostic tests to solve the problems that the switch finds.

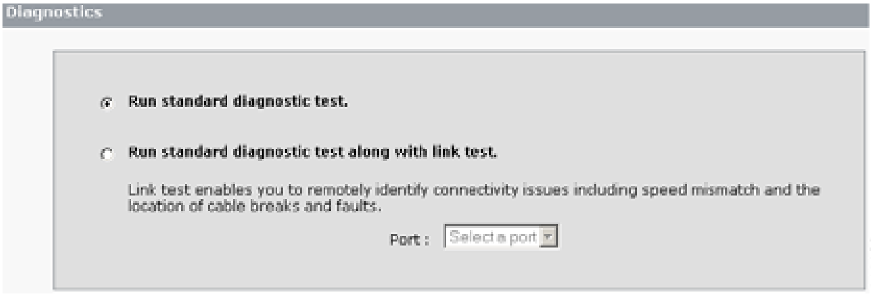
- The switch diagnostic test detects system and port problems on the switch. For example:
  - Power-on self-test (POST) error
  - Port-to-Smartports configuration mismatch
  - Duplex mode mismatch
- The link diagnostic test on a specific port detects speed mismatch and cable-related issues on the port or the circuit. For example:
  - Unconnected cable
  - Cable too short or too long
  - Faulty cable

Note The link test is run on a port that is not in a link-up state because it can interrupt traffic between the switch port and its connected device. Run the link test only on a port that has a suspected problem. Before running the link test, use the Front Panel view, the Port Status, and the Port Statistics windows to determine the details of the problem.

Tip Use the diagnostics report with the Alert Log. The log includes the last time at which the problems were detected by the switch. Solving the problems does not turn off the Alert LED. You must also click the **Clear Log** button in the Alert Log.

To display the Diagnostics window (Figure 5-1), choose **Diagnostics** from the device manager menu. You can also display the Diagnostics window by clicking the **Get Details** button in the Status field, which is displayed under the Front Panel view.

Figure 5-1 Diagnostics Window


Diagnostics

● Run standard diagnostic test.

○ Run standard diagnostic test along with link test.

Link test enables you to remotely identify connectivity issues including speed mismatch and the location of cable breaks and faults.

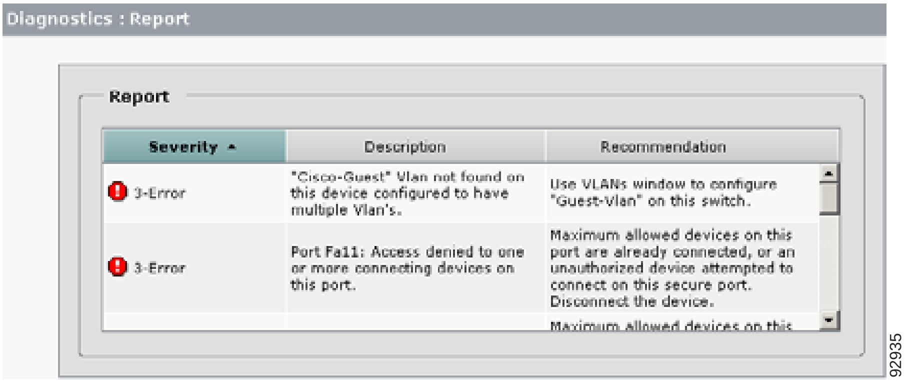
Port : Select a port

After running either or both tests, the window displays a report (Figure 5-2) of problems detected by the switch. The report also includes severity levels and recommended actions to help you solve the problems.

The diagnostics report includes this information:

Severity Level	A single-digit code (0 to 5) that reflects the severity of the problem. The lower the number, the more serious the condition and the need to take action. ⊗ Emergency (0)—The switch is unusable. Alert (1)—The switch requires immediate action. ❗ Critical (2)—The switch has a critical condition. Error (3)—The switch has an error condition. ⚠ Warning (4)—The switch has a warning condition. ℹ Notifications (5)—The switch is operating normally but has a significant condition.
Description	The description of the problem, including the ports on which the problem was detected.
Recommendation	The recommended actions to solve the problem.

Figure 5-2 Sample Diagnostics Report



Severity ▲	Description	Recommendation
❗ 3-Error	"Cisco-Guest" Vlan not found on this device configured to have multiple Vlan's.	Use VLANs window to configure "Guest-Vlan" on this switch.
❗ 3-Error	Port Fa11: Access denied to one or more connecting devices on this port.	Maximum allowed devices on this port are already connected, or an unauthorized device attempted to connect on this secure port. Disconnect the device.
		Maximum allowed devices on this

Restart or Reset the Switch

If you cannot solve a problem through the diagnostic report or by reconfiguring a feature, either restarting or resetting the switch might help to solve the problem or help you to eliminate probable causes. For example, if the problem exists after you reset the switch to its default settings, it is unlikely that the switch is causing the problem.

Use the Restart / Reset window to restart or reset the switch. To display this window, choose **Configure** > **Restart / Reset** from the device manager menu. See the device manager online help for additional guidelines and procedures.

From the Restart / Reset window, you can:

- Restart the switch without turning off power. The switch retains its saved configuration settings during the restart process. However, the device manager is unavailable during the process. When the process completes, the switch redisplays the device manager.

Note Restarting the switch interrupts connectivity of your devices to the network. You can reset the switch to its factory default settings and then restart the switch.

- Reset the switch to delete the current configuration settings, and then restart the switch.

Note Resetting the switch to its factory defaults deletes all customized switch settings, including the IP address. The same software image is retained. You will need to reconfigure the basic switch settings (as described in the *Getting Started Guide for the Catalyst Express 500 Switches*) and use the new IP address to display the device manager.

Resetting the switch interrupts connectivity of your devices to the network.

You can only reset the switch through the device manager.

Restore Switch Settings

You can restore your configuration settings by using Network Assistant to save the switch configuration file. After saving the configuration file, you must use the device manager Restart / Reset window to reset the switch. After resetting the switch, use the Express Setup window to assign a switch IP address and to assign the same host name that was used before the switch was reset. Then you can load the configuration file to the switch and restore the previous configuration settings. For information about saving configuration files, see the Network Assistant documentation.

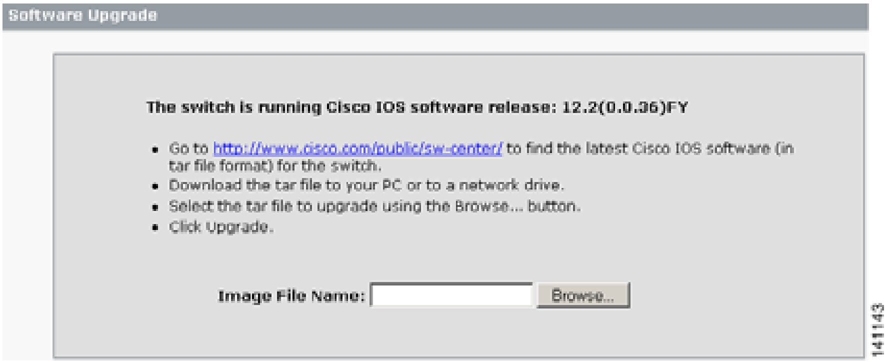
Upgrade the Switch Software

Prerequisite

You must have access to the Internet to download switch software from Cisco.com to your PC or network drive.

Use the Software Upgrade window (Figure 5-3) to update the switch with the latest software changes (such as software patches) and features. To display this window, choose **Software Upgrade** from the device manager menu.

Figure 5-3 Software Upgrade Window



Software Upgrade

The switch is running Cisco IOS software release: 12.2(0.0.36)FY

- Go to http://www.cisco.com/public/sw-center/ to find the latest Cisco IOS software (in tar file format) for the switch.
- Download the tar file to your PC or to a network drive.
- Select the tar file to upgrade using the Browse... button.
- Click Upgrade.

Image File Name:

Note Wait for the upgrade process to complete. Do not use or close the browser session with the device manager, and do not access the device manager from another browser session.

When the upgrade process completes, a success message appears, and the switch automatically restarts. It might take a few minutes for the switch to restart with the new software.

Check that the latest software version on the switch appears in the Software field in the Switch Information area of the Dashboard.

See the device manager online help for additional guidelines and procedures.

From the device manager, you can upgrade your switches one at a time. To upgrade multiple switches with the same configuration file, use Network Assistant.

Troubleshoot a Failed Software Upgrade

If the upgrade process does not complete or if the switch fails to restart after the upgrade process completes, follow these steps:

1. Make sure that you downloaded the correct tar file from Cisco.com.
2. If you downloaded the correct tar file, refresh your device manager browser session to make sure that there is connectivity between the switch and your PC or network drive.
3. Try to upgrade the switch again by following the procedures in the "Upgrade the Switch Software" section on page 5-5.

If the upgrade process fails again, follow these steps:

1. Select the **Reset the switch to factory defaults** option on the Restart / Reset window, and then click **Submit**.

   Resetting the switch to its factory defaults deletes all customized switch settings, including the IP address.
2. Reconfigure the switch settings, including assigning an IP address to the switch, as described in the *Getting Started Guide for the Catalyst Express 500 Switches*.
3. Use the new switch IP address to display the device manager.
4. Try to upgrade the switch again by following the procedures in the "Upgrade the Switch Software" section on page 5-5.

If the upgrade process still fails (for example, an `Upgrade Failed` message appears or the System LED does not turn solid green after a few seconds), follow the procedures in the "Recover the Switch Software" section on page 5-9.

Upgrade to a Noncryptographic Software Version

You can upgrade the switch from a cryptographic version of the switch software to a noncryptographic version. However, the device manager cannot automatically redisplay after the software upgrade completes if the switch was previously running the cryptographic version and if the device manager was accessed through a secured session. Close the existing browser session with the device manager. Then open a new browser session, and enter **http://** before the switch IP address.

Recover a Password

Prerequisites

- You must have physical access to the switch.
- Make sure that at least one switch port is enabled and is not connected to a device.

If you have lost or forgotten your username and password to the switch, follow these steps to delete all existing username-and-password pairs:

1. Make sure that the SYSTEM LED is solid green.
2. Press the **SETUP** button until the Setup LED blinks green and the LED of an available port blinks green.

   Note If the Setup LED is amber, there is no available switch port to which to connect your management station. Disconnect one of the switch ports, and then press the **Setup** button again until the Setup LED and the port LED blink green.

3. Connect your management station directly to the switch port with a blinking green port LED. The port LED turns solid green after the connection.
4. Press the **SETUP** button until the Setup LED blinks green, and then continue to press the **SETUP** button for approximately 5 seconds until the Setup LED turns solid green.

   All username-and-password pairs are deleted from the switch.

5. Open a web browser session, and display the device manager. The device manager appears without requiring a username and password from you.
6. Assign a username and password through the Usernames and Passwords window.

Recover the Switch Software

Prerequisites

- You must have physical access to the switch.
- Make sure that at least one switch port is enabled and is not connected to a device.

You might need to recover the switch software if the image is corrupted during an upgrade, if you installed the wrong image on the switch, or if you deleted the image. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity. A symptom of corrupted software is when the switch continuously tries to restart.

To display the Software Recovery window (Figure 5-4):

1. Power off and then power on the switch by disconnecting and then reconnecting the AC power cord to the connector on the switch rear panel.

   The System LED blinks green.

2. Immediately press the **Setup** button until all the system LEDs (System, Alert, Setup, and PoE) are solid amber.

3. Stop pressing the **Setup** button.

   The switch begins the power-on self-test (POST), a series of automatic tests that confirm proper operation. POST lasts approximately 1 minute. The System and Setup LEDs blink green during this process.

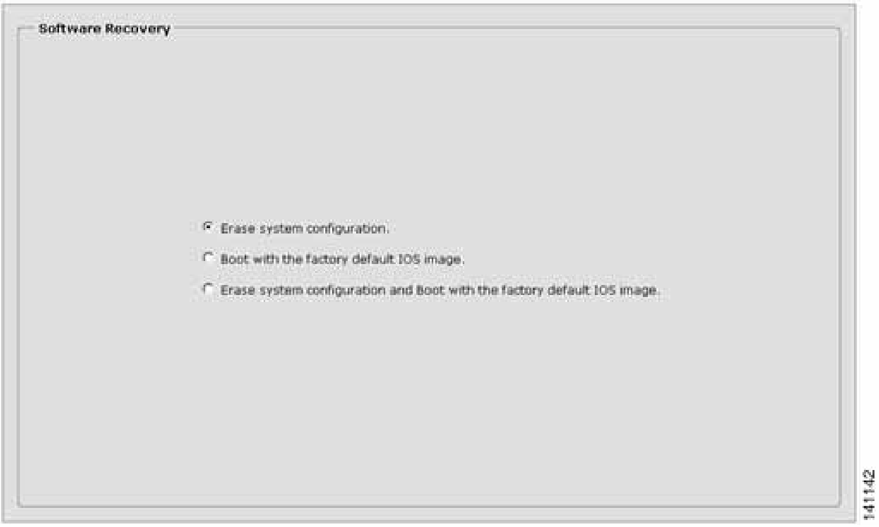
   When POST completes, the System LED turns solid amber, and the Setup LED blinks green. The LED of an available port blinks green; all other port LEDs remain off (dark).

   Note If the Setup LED is amber, it means that there is no available switch port to which to connect your management station. Disconnect one of the switch ports, and then press the **Setup** button again until the Setup LED and the port LED blink green.

4. Connect your management station directly to the switch port with a blinking green port LED. The port LED turns solid green after the connection.
5. Open a web browser session, and display the device manager. The device manager appears without requiring a username and password from you.

   The Software Recovery window appears (Figure 5-4).

Figure 5-4 Software Recovery Window



Software Recovery

● Erase system configuration.
○ Boot with the factory default IOS image.
○ Erase system configuration and Boot with the factory default IOS image.

From the Software Recovery window, you can choose:

Erase system configuration	Use this option to delete all the configuration settings on the switch, including the IP address, usernames, and passwords, but retain the software image. If you select this option, you must set up the switch again, as described in the *Getting Started Guide for the Catalyst Express 500 Switches*.

Boot with the factory default IOS image	Use this option to use the factory-default software image. Settings for features supported on the default software image are retained, including the IP address, usernames, and passwords. Use this option if a software upgrade fails. Display the device manager, and try to upgrade the switch software again.
Erase system configuration and boot with the factory default IOS image	Use this option to delete all of the configuration settings on the switch and to change to the factory-default software image. All files on the switch Flash image are deleted and the switch returns to using the factory default image. If you select this option, you must set up the switch again, as described in the *Getting Started Guide for the Catalyst Express 500 Switches*.

When You Are Done

Use the diagnostic tools and troubleshooting features to solve network problems as they come up.

For additional resources that can help you troubleshoot problems, see Chapter , "Cisco Support Resources."

Reference

Chapter Topics

- Technical Specifications, page A-1
- Cabling Guidelines, page A-3
- Connector Specifications, page A-6

Technical Specifications

This section lists the switch technical specifications in Table A-1.

Table A-1 Technical Specifications for the Catalyst Express 500 Switches

Specification	Description
AC input voltage	Catalyst Express 500-24TT: 100 to 240 VAC, 1.3–0.8 A (autoranging), 50 to 60 Hz Catalyst Express 500-24LC: 100 to 240 VAC, 2–1 A (autoranging), 50 to 60 Hz Catalyst Express 500-24PC: 100 to 240 VAC, 8–4 A (autoranging), 50 to 60 Hz Catalyst Express 500G-12TC: 100 to 240 VAC, 1.3–0.8 A (autoranging), 50 to 60 Hz
DC input voltages for RPS 675[1]	⎓ +12 V⎓ @14 A, –48 V @7.8 A

Table A-1 Technical Specifications for the Catalyst Express 500 Switches (continued)

Specification	Description
Power consumption	Catalyst Express 500-24TT: 30 W or 102 BTUs per hour Catalyst Express 500-24LC: 110 W or 375 BTUs per hour Catalyst Express 500-24PC: 460 W or 1570 BTUs per hour Catalyst Express 500G-12TC: 45 W or 154 BTUs per hour
Power dissipation	Catalyst Express 500-24TT: 30 W Catalyst Express 500-24LC: 45 W Catalyst Express 500-24PC: 90 W Catalyst Express 500G-12TC: 45 W
Power rating	Catalyst Express 500-24TT: 0.050 KVA Catalyst Express 500-24LC: 0.120 KVA Catalyst Express 500-24PC: 0.460 KVA Catalyst Express 500G-12TC: 0.075 KVA
Power over Ethernet	All 24 PoE ports on the Catalyst Express 500-24PC can supply up to 15.4 W (IEEE 802.3af standard maximum) of power over Category 5 cable, for a total of 370 W of inline power. All 4 PoE ports on Catalyst Express 500-24LC switches can supply up to 15.4 W of power over Category 5 cable, for a total of 62 W of inline power. Both the IEEE 802.3af PoE standard and Cisco prestandard inline power are supported.
Operating temperature	32 to 113°F (0 to 45°C)
Storage temperature	–13 to 158°F (–25 to 70°C)
Relative humidity	10 to 85% (noncondensing)
Operating altitude	Up to 10,000 ft (3049 m)
Storage altitude	Up to 15,000 ft (4573 m)
Weight	8 lb (3.7 kg) for Catalyst Express 500-24TT, 500-24LC, and 500G-12TC 12 lb (5.5 kg) for Catalyst Express 500-24PC

Table A-1 Technical Specifications for the Catalyst Express 500 Switches (continued)

Specification	Description
Dimensions (H x W x D)	1.73 x 17.5 x 9.9 in. (4.39 x 44.45 x 25.15 cm) for Catalyst Express 500-24TT, Catalyst Express 500-24LC, and Catalyst Express 500G-12TC 1.73 x 17.5 x 14.4 in. (4.39 x 44.45 x 36.58 cm) for Catalyst Express 500-24PC
Acoustic noise	ISO 7770, bystander position: Operating to an ambient temperature of 30°C Catalyst Express 500-24TT, 500-24LC, 500G-12TC: 40 dBa Catalyst Express 500-24PC: 48 dBa

[1] Only on Catalyst Express 500-24PC switch.

Cabling Guidelines

This section describes the cabling guidelines and port connections.

Ethernet Port Connections

For copper Ethernet ports, cable lengths from the switch to connected devices must be within 328 feet (100 meters).

Use either straight-through or crossover Category 5 cables with RJ-45 connectors to connect from the switch Ethernet ports to other devices.

Use Category 5 cables for 100BASE-TX and 1000BASE-T traffic. Use Category 3 or Category 4 cables for 10BASE-T traffic.

SFP Module Port Connections

For the SFP module port connections, Table A-2 lists the cable specifications. Each port must match the wave-length specifications on the other end of the cable, and for reliable communications, the cable must not exceed the stipulated cable length.

Table A-2 Fiber-Optic SFP Module Port Cabling Specifications

SFP Module	Wavelength (nanometers)	Fiber Type	Core Size (micron)	Model Bandwidth (MHz/km)	Cable Distance
100BASE-BX-D	1550 TX[1] 1310 RX[2]	SMF[3]	G.652[4]	—	32,810 feet (10 km)
100BASE-BX-U	1310 TX 1550 RX	SMF	G.652[2]	—	32,810 feet (10 km)
100BASE-FX	Min.:1270 Typical: 1300 Max.: 1380	MMF[5]	50/125 62.5/125	500	6,562 feet (2 km)
100BASE-LX	1310	SMF	9/125	—	32,810 feet (10 km)
1000BASE-LX	1300	MMF[6]	62.5	500	1804 feet (550 m)
			50	400	1804 feet (550 m)
			50	500	1804 feet (550 m)
		SMF	9/10[2]	—	32,810 feet (10 km)
1000BASE-SX	850	MMF	62.5	160	722 feet (220 m)
			62.5	200	902 feet (275 m)
			50	400	1640 feet (500 m)
			50	500	1804 feet (550 m)

[1] TX = send

[2] RX = receive

[3] SMF = single-mode fiber

[4] ITU-T G.652 SMF as specified by the IEEE 802.3z standard.

[5] MMF = multimode fiber

[6] A mode-conditioning patch cord is required. Using an ordinary patch cord with MMF, 1000BASE-LX SFP modules, and a short link distance can cause transceiver saturation, resulting in an elevated bit error rate (BER). When using the LX SFP module with 62.5-micron diameter MMF, you must also install a mode-conditioning patch cord between the SFP module and the MMF cable on both the sending and receiving ends of the link. The mode-conditioning patch cord is required for link distances greater than 984 feet (300 m).

For SMF connections, use one of the LCs listed in Table A-3 or Table A-4. For MMF connections, use one of the LCs listed in Table A-5. Use the Cisco part numbers to order the patchcords that you need, or order patchcords from your vendor.

Table A-3 LC-to-SC Single-Mode Fiber Patch Cables (SFP-to-GBIC Connections)

Type	Cisco Part Number
2-meter, LC-to-SC single-mode fiber patchcord	CAB-CP-LCSC-2M
8-inch, SC-to-LC single-mode fiber patchcord	CAB-CP-SCLC-8IN
10-foot, LC-to-SC single-mode fiber patchcord	CAB-SMF-SC-10
100-foot, LC-to-SC single-mode fiber patchcord	CAB-SMF-SC-100
25-foot, LC-to-SC single-mode fiber patchcord	CAB-SMF-SC-25
50-foot, LC-to-SC single-mode fiber patchcord	CAB-SMF-SC-50
75-foot, LC-to-SC single-mode fiber patchcord	CAB-SMF-SC-75

Table A-4 LC-to-LC Single-Mode Fiber Patch Cables (SFP-to-SFP Connections)

Type	Cisco Part Number
2-meter, LC-to-LC single-mode fiber patchcord	15454-LC-LC-2=
4-meter, LC-to-LC single-mode fiber patchcord	15216-LC-LC-5=
6-meter, LC-to-LC single-mode fiber patchcord	15216-LC-LC-10=
8-meter, LC-to-LC single-mode fiber patchcord	15216-LC-LC-20=

Table A-5 SX LC and SX LC-to-SC Multimode Fiber Patch Cables (SFP-to-SFP Connections)

Type	Cisco Part Number
10-meter, SX LC multimode fiber patchcord	CSS5-CABSX-LC=
10-meter, SX LC-to-SC multimode fiber patchcord	CSS5-CABSX-LCSC=

Connector Specifications

This section describes the connectors used with the Catalyst Express 500 switches.

10/100 and 10/100/1000 Ports

The Ethernet ports on the switches use standard RJ-45 connectors and Ethernet pinouts with internal crossovers (Figure A-1 and Figure A-2).

Figure A-1 10/100 Port Pinouts

Pin	Label
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

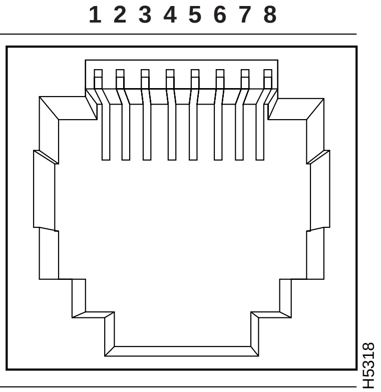
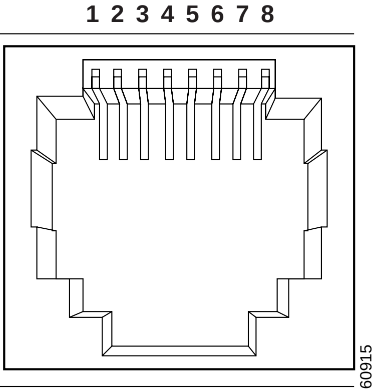


Figure A-2 10/100/1000 Port Pinouts

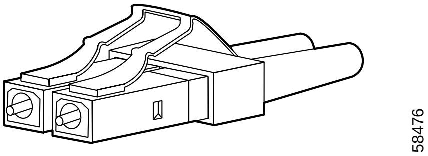
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



SFP Module Ports

The SFP module ports on switches use fiber-optic SFP modules with LC connectors (Figure A-3). See the "Supported Hardware" section on page 1-13 for a list of supported SFP modules.

Figure A-3 Fiber-Optic SFP Module LC Connector



Cisco Support Resources

Read this chapter for Cisco support resources if you need assistance or further information about the switch.

Before You Begin

Use the diagnostic tools (Chapter 4, "Monitoring") and troubleshooting features (Chapter 5, "Troubleshooting") to help you solve switch and network problems.

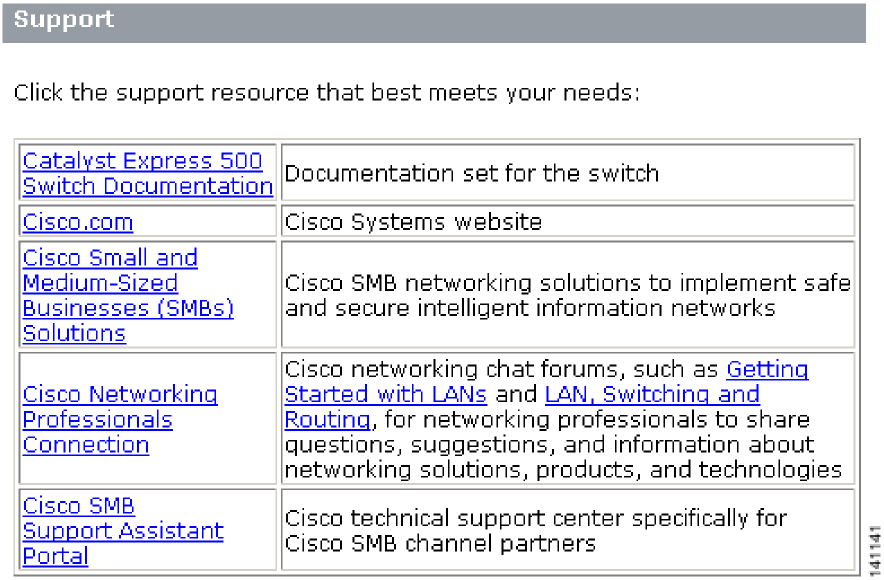
The other Catalyst Express 500 switch documents might also provide the information that you seek. See the "Switch Documentation Set" section on page xiii.

Chapter Topics

Support Links from the Device Manager Online Help

The device manager online help includes a Support window with links to Cisco support resources. To display this window, click **Help** from the device manager tool bar, and then click **Support** from the online help menu.

Figure B-1 Support Window



Support

Click the support resource that best meets your needs:

Catalyst Express 500 Switch Documentation	Documentation set for the switch
Cisco.com	Cisco Systems website
Cisco Small and Medium-Sized Businesses (SMBs) Solutions	Cisco SMB networking solutions to implement safe and secure intelligent information networks
Cisco Networking Professionals Connection	Cisco networking chat forums, such as Getting Started with LANs and LAN, Switching and Routing, for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies
Cisco SMB Support Assistant Portal	Cisco technical support center specifically for Cisco SMB channel partners

Cisco Small and Medium-Sized Businesses (SMBs) Solutions

Cisco SMB Class Solutions give your employees secure, reliable, and convenient access to the information they need, whether they are located in the main office, at a remote office, at home, or on the road.

You can access the Cisco SMB Class Solutions website at this URL:

http://www.cisco.com/en/US/netsol/ns339/networking_solutions_small_medium_sized_business_home.html

Cisco Networking Professionals Connection

Cisco Networking Professionals Connection is the gathering place for Networking Professionals to share questions, suggestions, and information about networking solutions, products, and technologies. These chat forums—**Getting Started with LANs** and **LAN, Switching and Routing**—discuss topics that can help you use the switch.

You can access the Cisco Networking Professionals Connection website at this URL:

http://forum.cisco.com/eforum/servlet/NetProf?page=main

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco SMB Support Assistant provides service and support for the Catalyst Express 500 switches and other Cisco networking products. Cisco SMB Support Assistant offers simple-to-use Portal and Client applications, 8 hours a day, 5 days a week TAC support, and Advanced Replacement Next Business Day. If you do not hold a valid Cisco service contract, please contact your reseller.

SMB Support Assistant Portal and Client

The Cisco SMB Support Assistant Portal and Client applications are management tools designed specifically for SMBs. This secure portfolio of tools helps you access information and inventory as well as providing device management and technical support tools for covered Cisco networking devices.

The Cisco SMB Support Assistant Portal (*Portal*) is the online tool, serving as the how-to arm and starting point for a particular task. It is specifically designed to offer self-help and support for products covered by Cisco SMB Support Assistant.

The Cisco SMB Support Assistant Client (*Client*) is the application stored locally on your computer hard drive and can be installed much like common Windows-based programs. It runs the tools for performing particular tasks and interacts with the Portal in launching the support functions.

The Portal and Client are available 24 hours a day, 365 days a year, at this URL:

http://tools.cisco.com/Support/SMBSA/Login.do

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

If you cannot successfully resolve an issue through the self-help tools, click the Open Service Request option in the Portal and fill out the online form. This will immediately submit the request to the Cisco SMB Technical Assistance Center (Cisco SMB TAC). Requests can be submitted at any time, 24 hours a day, 365 days a year. A Cisco SMB TAC engineer will then respond to the request within 1 business day during normal business hours.

If your issue is not resolved by using the recommended resources, your service request is assigned to a Cisco TAC engineer. To open a service request by telephone, use one of these numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking
- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

INDEX