C H A P T E R 1

Overview

This chapter provides these topics about the Catalyst 2960 switch software:

-
-
-
-

In this document, IP refers to IP Version 4 (IPv4) unless there is a specific reference to IP Version 6 (IPv6).

Features

Some features described in this chapter are available only on the cryptographic (supports encryption) version of the software. You must obtain authorization to use this feature and to download the cryptographic version of the software from Cisco.com. For more information, see the release notes for this release.

The switch has these features:

-
-
-
- (includes a feature requiring the cryptographic version of the software)
-
-
- (includes a feature requiring the cryptographic version of the software)
-
-

Ease-of-Deployment and Ease-of-Use Features

The switch ships with these features to make the deployment and the use easier:

- Express Setup for quickly configuring a switch for the first time with basic IP information, contact information, switch and Telnet passwords, and Simple Network Management Protocol (SNMP) information through a browser-based program. For more information about Express Setup, see the getting started guide.

- User-defined and Cisco-default Smartports macros for creating custom switch configurations for simplified deployment across the network.

- An embedded device manager GUI for configuring and monitoring a single switch through a web browser. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the switch online help.

- Cisco Network Assistant (hereafter referred to as *Network Assistant*) for

> **Note**   The Network Assistant must be downloaded from cisco.com/go/cna.

- Managing communities, which are device groups like clusters, except that they can contain routers and access points and can be made more secure.

- Simplifying and minimizing switch and switch cluster management from anywhere in your intranet.

- Accomplishing multiple configuration tasks from a single graphical interface without needing to remember command-line interface (CLI) commands to accomplish specific tasks.

- Interactive guide mode that guides you in configuring complex features such as VLANs, ACLs, and quality of service (QoS).

> **Note**   If the switch is running the LAN Lite image, you can configure ACLs, but you cannot attach them to interfaces or VLANs.

- Configuration wizards that prompt you to provide only the minimum required information to configure complex features such as QoS priorities for traffic, priority levels for data applications, and security.

- Downloading an image to a switch.

- Applying actions to multiple ports and multiple switches at the same time, such as VLAN and QoS settings, inventory and statistic reports, link- and switch-level monitoring and troubleshooting, and multiple switch software upgrades.

- Viewing a topology of interconnected devices to identify existing switch clusters and eligible switches that can join a cluster and to identify link information between switches.

- Monitoring real-time status of a switch or multiple switches from the LEDs on the front-panel images. The system, redundant power system (RPS), and port LED colors on the images are similar to those used on the physical LEDs.

> **Note**   To use RPS, the switch must be running the LAN Base image.

- Switch clustering technology for

  - Unified configuration, monitoring, authentication, and software upgrade of multiple, cluster-capable switches, regardless of their geographic proximity and interconnection media, including Ethernet, Fast Ethernet, Fast EtherChannel, small form-factor pluggable (SFP) modules, Gigabit Ethernet, and Gigabit EtherChannel connections. For a list of cluster-capable switches, see the release notes.

  - Automatic discovery of candidate switches and creation of clusters of up to 16 switches that can be managed through a single IP address.

  - Extended discovery of cluster candidates that are not directly connected to the command switch.

Performance Features

The switch ships with these performance features:

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports for optimizing bandwidth

- Automatic-medium-dependent interface crossover (auto-MDIX) capability on 10/100 and 10/100/1000 Mb/s interfaces and on 10/100/1000 BASE-TX SFP module interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately

- Support for up to 9000 bytes for frames that are bridged in hardware, and up to 2000 bytes for frames that are bridged by software

- IEEE 802.3x flow control on all ports (the switch does not send pause frames)

- EtherChannel for enhanced fault tolerance and for providing up to 8 Gb/s (Gigabit EtherChannel) or 800 Mb/s (Fast EtherChannel) full-duplex bandwidth among switches, routers, and servers

- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links

- Forwarding of Layer 2 packets at Gigabit line rate

- Per-port storm control for preventing broadcast, multicast, and unicast storms

- Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic

- Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3 for efficiently forwarding multimedia and multicast traffic

- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)

- IGMP snooping querier support to configure switch to generate periodic IGMP general query messages

- IPv6 host support for basic IPv6 management

- Multicast Listener Discovery (MLD) snooping to enable efficient distribution of IP version 6 (IPv6) multicast data to clients and routers in a switched network

Note   To use IPv6 features, the switch must be running the LAN Base image.

- Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons

Note To use MVR, the switch must be running the LAN Base image.

- IGMP filtering for controlling the set of multicast groups to which hosts on a switch port can belong
- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP leave timer for configuring the leave latency for the network
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features
- Support for Cisco IOS IP Service Level Agreements (SLAs) responder that allows the system to anticipate and respond to Cisco IOS IP SLAs request packets for monitoring network performance. See the release notes for responder configuration
- Configurable small-frame arrival threshold to prevent storm control when small frames (64 bytes or less) arrive on an interface at a specified rate (the threshold)
- Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure

Note To use Flex Link Multicast Fast Convergence, the switch must be running the LAN Base image.

Management Options

These are the options for configuring and managing the switch:

- An embedded device manager—The device manager is a GUI that is integrated in the software image. You use it to configure and to monitor a single switch. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the switch online help.
- Network Assistant—Network Assistant is a network management application that can be downloaded from Cisco.com. You use it to manage a single switch, a cluster of switches, or a community of devices. For more information about Network Assistant, see *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- CLI—The Cisco IOS software supports desktop- and multilayer-switching features. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station. For more information about the CLI, see Chapter 2, "Using the Command-Line Interface."
- SNMP—SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The switch supports a comprehensive set of MIB extensions and four remote monitoring (RMON) groups. For more information about using SNMP, see Chapter 28, "Configuring SNMP."

- CNS—Cisco Networking Services is network management software that acts as a configuration service for automating the deployment and management of network devices and services. You can automate initial configurations and configuration updates by generating switch-specific configuration changes, sending them to the switch, executing the configuration change, and logging the results.

  For more information about CNS, see Chapter 4, "Configuring Cisco IOS CNS Agents."

Manageability Features

These are the manageability features:

- CNS embedded agents for automating switch management, configuration storage, and delivery

- DHCP for automating configuration of switch information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)

- DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients

- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts

- DHCP-based autoconfiguration and image update to download a specified configuration a new image to a large number of switches

- DHCP server port-based address allocation for the preassignment of an IP address to a switch port

- Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding hostname and to a TFTP server for administering software upgrades from a TFTP server

- Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding MAC address

- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses

- Configurable MAC address scaling that allows disabling MAC address learning on a VLAN to limit the size of the MAC address table

- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network

- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones

> **Note** To use LLDP-MED, the switch must be running the LAN Base image.

- LLDP media extensions (LLDP-MED) location TLV that provides location information from the switch to the endpoint device

- Network Time Protocol (NTP) for providing a consistent time stamp to all switches from an external source

- Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch uses

- Support for the SSM PIM protocol to optimize multicast applications, such as video

- Source Specific Multicast (SSM) mapping for multicast applications provides a mapping of source to group, allowing listeners to connect to multicast sources dynamically and reduces dependencies on the application

- Support for Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 to utilize IPv6 transport, communicate with IPv6 peers, and advertise IPv6 routes

- Support for these IP services, making them VRF aware so that they can operate on multiple routing instances: HSRP, GLBP, uRPF, ARP, SNMP, IP SLA, TFTP, FTP, syslog, traceroute, and ping

- Configuration logging to log and to view changes to the switch configuration

- Unique device identifier to provide product identification information through a **show inventory** user EXEC command display

- In-band management access through the device manager over a Netscape Navigator or Microsoft Internet Explorer browser session

- In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network

- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic version of the software)

- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests

- Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem

- Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying switch configuration or switch image files (requires the cryptographic version of the software)

- Configuration replacement and rollback to replace the running configuration on a switch with any saved Cisco IOS configuration file

- The HTTP client in Cisco IOS supports can send requests to both IPv4 and IPv6 HTTP server, and the HTTP server in Cisco IOS can service HTTP requests from both IPv4 and IPv6 HTTP clients

- Simple Network and Management Protocol (SNMP) can be configured over IPv6 transport so that an IPv6 host can send SNMP queries and receive SNMP notifications from a device running IPv6

- IPv6 stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses

- Disabling MAC address learning on a VLAN

- DHCP server port-based address allocation for the preassignment of an IP address to a switch port.

Availability and Redundancy Features

These are the availability and redundancy features:

- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults

- IEEE 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:

    - Up to 128 spanning-tree instances supported

    Note   Up to 64 spanning-tree instances are supported when the switch is running the LAN Lite image.

    - Per-VLAN spanning-tree plus (PVST+) for load balancing across VLANs

    - Rapid PVST+ for load balancing across VLANs and providing rapid convergence of spanning-tree instances

    - UplinkFast and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks

- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately changing root and designated ports to the forwarding state

- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:

    - Port Fast for eliminating the forwarding delay by enabling a port to immediately change from the blocking state to the forwarding state

    - BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)

    - BPDU filtering for preventing a Port Fast-enabled port from sending or receiving BPDUs

    - Root guard for preventing switches outside the network core from becoming the spanning-tree root

    - Loop guard for preventing alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link

- Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy

    Note   To use Flex Links, the switch must be running the LAN Base image.

- Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers, and to allow the failover of the server traffic to an operational link on another Cisco Ethernet switch.

    Note   To use Link-state Tracking, the switch must be running the LAN Base image.

VLAN Features

These are the VLAN features:

- Support for up to 255 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth

Note   Up to 64 VLANs are supported when the switch is running the LAN Lite image.

- Support for VLAN IDs in the 1 to 4094 range as allowed by the IEEE 802.1Q standard
- VLAN Query Protocol (VQP) for dynamic VLAN membership
- IEEE 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
- Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (IEEE 802.1Q) to be used
- VLAN Trunking Protocol (VTP) and VTP pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic
- Voice VLAN for creating subnets for voice traffic from Cisco IP Phones
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The switch CPU continues to send and receive control protocol frames.
- VLAN Flex Link Load Balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.

Note   To use VLAN Flex Link Load Balancing, the switch must be running the LAN Base image.

Security Features

The switch ships with these security features:

- IP Service Level Agreements (IP SLAs) responder support that allows the switch to be a target device for IP SLAs active traffic monitoring

Note   To use IP SLAs, the switch must be running the LAN Base image.

- Web authentication to allow a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser

Note   To use Web Authentication, the switch must be running the LAN Base image.

- Local web authentication banner so that a custom banner or an image file can be displayed at a web authentication login screen

- IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute

    Note   To use this feature, the switch must be running the LAN Base image.

- Password-protected access (read-only and read-write access) to management interfaces (device manager, Network Assistant, and the CLI) for protection against unauthorized configuration changes

- Multilevel security for a choice of security level, notification, and resulting actions

- Static MAC addressing for ensuring security

- Protected port option for restricting the forwarding of traffic to designated ports on the same switch

- Port security option for limiting and identifying MAC addresses of the stations allowed to access the port

- VLAN aware port security option to shut down the VLAN on the port when a violation occurs, instead of shutting down the entire port.

- Port security aging to set the aging time for secure addresses on a port

- BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs

- Standard and extended IP access control lists (ACLs) for defining inbound security policies on Layer 2 interfaces (port ACLs)

- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces

- Source and destination MAC-based ACLs for filtering non-IP traffic

- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers

- IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:

    – Multidomain authentication (MDA) to allow both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), to independently authenticate on the same IEEE 802.1x-enabled switch port

    Note   To use MDA, the switch must be running the LAN Base image.

    – Dynamic voice virtual LAN (VLAN) for MDA to allow a dynamic voice VLAN on an MDA-enabled port

    – VLAN assignment for restricting IEEE 802.1x-authenticated users to a specified VLAN

    – Port security for controlling access to IEEE 802.1x ports

    – Voice VLAN to permit a Cisco IP Phone to access the voice VLAN regardless of the authorized or unauthorized state of the port

    – IP phone detection enhancement to detect and recognize a Cisco IP phone.

– Guest VLAN to provide limited services to non-IEEE 802.1x-compliant users

– Restricted VLAN to provide limited services to users who are IEEE 802.1x compliant, but do not have the credentials to authenticate via the standard IEEE 802.1x processes

Note To use authentication with restricted VLANs, the switch must be running the LAN Base image.

– IEEE 802.1x accounting to track network usage

– IEEE 802.1x with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame

Note To use authentication with wake-on-LAN, the switch must be running the LAN Base image.

- IEEE 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch

Note To use IEEE 802.1x readiness check, the switch must be running the LAN Base image.

- Voice aware IEEE 802.1x security to apply traffic violation actions only on the VLAN on which a security violation occurs.

Note To use voice aware IEEE 802.1x authentication, the switch must be running the LAN Base image.

- MAC authentication bypass to authorize clients based on the client MAC address.

Note To use MAC authentication bypass, the switch must be running the LAN Base image.

- Network Admission Control (NAC) Layer 2 IEEE 802.1x validation of the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access.

  For information about configuring NAC Layer 2 IEEE 802.1x validation, see the "Configuring NAC Layer 2 IEEE 802.1x Validation" section on page 9-48.

Note To use NAC, the switch must be running the LAN Base image.

- TACACS+, a proprietary feature for managing network security through a TACACS server

- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services

- Secure Socket Layer (SSL) Version 3.0 support for the HTTP 1.1 server authentication, encryption, and message integrity and HTTP client authentication to allow secure HTTP communications (requires the cryptographic version of the software)

- IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute

QoS and CoS Features

These are the QoS and CoS features:

- Automatic QoS (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues

  Note   To use auto-QoS, the switch must be running the LAN Base image.

- Classification

  - IP type-of-service/Differentiated Services Code Point (IP ToS/DSCP) and IEEE 802.1p CoS marking priorities on a per-port basis for protecting the performance of mission-critical applications

    Note   To use DSCP, the switch must be running the LAN Base image.

  - IP ToS/DSCP and IEEE 802.1p CoS marking based on flow-based packet classification (classification based on information in the MAC, IP, and TCP/UDP headers) for high-performance quality of service at the network edge, allowing for differentiated service levels for different types of network traffic and for prioritizing mission-critical traffic in the network

    Note   To use flow-based packet classification, the switch must be running the LAN Base image.

  - Trusted port states (CoS, DSCP, and IP precedence) within a QoS domain and with a port bordering another QoS domain

  - Trusted boundary for detecting the presence of a Cisco IP Phone, trusting the CoS value received, and ensuring port security

- Policing

  Note   To use policy maps, the switch must be running the LAN Base image

  - Traffic-policing policies on the switch port for managing how much of the port bandwidth should be allocated to a specific traffic flow

  - In Cisco IOS Release 12.2(25)SED and later, if you configure multiple class maps for a hierarchical policy map, each class map can be associated with its own port-level (second-level) policy map. Each second-level policy map can have a different policer.

  - Aggregate policing for policing traffic flows in aggregate to restrict specific applications or traffic flows to metered, predefined rates

- Out-of-Profile

  - Out-of-profile markdown for packets that exceed bandwidth utilization limits

- Ingress queueing and scheduling
  - Two configurable ingress queues for user traffic (one queue can be the priority queue)
  - Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications

  Note   To use WTD, the switch must be running the LAN Base image.

  - Shaped round robin (SRR) as the scheduling service for specifying the rate at which packets are sent to the internal ring (sharing is the only supported mode on ingress queues)

  Note   To use ingress queueing, the switch must be running the LAN Base image.

- Egress queues and scheduling
  - Four egress queues per port
  - WTD as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
  - SRR as the scheduling service for specifying the rate at which packets are dequeued to the egress interface (shaping or sharing is supported on egress queues). Shaped egress queues are guaranteed but limited to using a share of port bandwidth. Shared egress queues are also guaranteed a configured share of bandwidth, but can use more than the guarantee if other queues become empty and do not use their share of the bandwidth.

  Note   To use egress queueing, the switch must be running the LAN Base image.

  - HSRP for IPv6 (requires the advanced IP services image)
- DHCP for IPv6 relay, client, server address assignment and prefix delegation (requires the advanced IP services image)
- IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router (requires the LAN Base image)

Power over Ethernet Features

These are the Power over Ethernet (PoE) features:

- Ability to provide power to connected Cisco pre-standard and IEEE 802.3af-compliant powered devices from Power over Ethernet (PoE)-capable ports if the switch detects that there is no power on the circuit.
- Support for CDP with power consumption. The powered device notifies the switch of the amount of power it is consuming.
- Support for Cisco intelligent power management. The powered device and the switch negotiate through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-power Cisco powered device to operate at its highest power mode.

- Automatic detection and power budgeting; the switch maintains a power budget, monitors and tracks requests for power, and grants power only when it is available.

- Ability to monitor the real-time power consumption. On a per-PoE port basis, the switch senses the total power consumption, polices the power usage, and reports the power usage.

Monitoring Features

These are the monitoring features:

- Switch LEDs that provide port- and switch-level status

- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the switch has learned or removed

- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN

- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations

- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis

- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events

- Layer 2 traceroute to identify the physical path that a packet takes from a source device to a destination device

- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on 10/100 and 10/100/1000 copper Ethernet ports

- SFP module diagnostic management interface to monitor physical or operational status of an SFP module

Default Settings After Initial Switch Configuration

The switch is designed for plug-and-play operation, requiring only that you assign basic IP information to the switch and connect it to the other devices in your network. If you have specific network needs, you can change the interface-specific and system-wide settings.

> **Note**   For information about assigning an IP address by using the browser-based Express Setup program, see the getting started guide. For information about assigning an IP address by using the CLI-based setup program, see the hardware installation guide.

If you do not configure the switch at all, the switch operates with these default settings:

- Default switch IP address, subnet mask, and default gateway is 0.0.0.0. For more information, see Chapter 3, "Assigning the Switch IP Address and Default Gateway," and Chapter 19, "Configuring DHCP Features."

- Default domain name is not configured. For more information, see Chapter 3, "Assigning the Switch IP Address and Default Gateway."

- DHCP client is enabled, the DHCP server is enabled (only if the device acting as a DHCP server is configured and is enabled), and the DHCP relay agent is enabled (only if the device is acting as a DHCP relay agent is configured and is enabled). For more information, see Chapter 3, "Assigning the Switch IP Address and Default Gateway," and Chapter 19, "Configuring DHCP Features."

- Switch cluster is disabled. For more information about switch clusters, see Chapter 5, "Clustering Switches," and the *Getting Started with Cisco Network Assistant*, available on Cisco.com.

- No passwords are defined. For more information, see Chapter 6, "Administering the Switch."

- System name and prompt is *Switch.* For more information, see Chapter 6, "Administering the Switch."

- NTP is enabled. For more information, see Chapter 6, "Administering the Switch."

- DNS is enabled. For more information, see Chapter 6, "Administering the Switch."

- TACACS+ is disabled. For more information, see Chapter 8, "Configuring Switch-Based Authentication."

- RADIUS is disabled. For more information, see Chapter 8, "Configuring Switch-Based Authentication."

- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see Chapter 8, "Configuring Switch-Based Authentication."

- IEEE 802.1x is disabled. For more information, see Chapter 9, "Configuring IEEE 802.1x Port-Based Authentication."

- Port parameters

    - Interface speed and duplex mode is autonegotiate. For more information, see Chapter 10, "Configuring Interface Characteristics."

    - Auto-MDIX is enabled. For more information, see Chapter 10, "Configuring Interface Characteristics."

    - Flow control is off. For more information, see Chapter 10, "Configuring Interface Characteristics."

    - PoE is autonegotiate. For more information, see Chapter 10, "Configuring Interface Characteristics."

- VLANs

    - Default VLAN is VLAN 1. For more information, see Chapter 12, "Configuring VLANs."

    - VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 12, "Configuring VLANs."

    - Trunk encapsulation is negotiate. For more information, see Chapter 12, "Configuring VLANs."

    - VTP mode is server. For more information, see Chapter 13, "Configuring VTP."

    - VTP version is Version 1. For more information, see Chapter 13, "Configuring VTP."

    - Voice VLAN is disabled. For more information, see Chapter 14, "Configuring Voice VLAN."

- STP, PVST+ is enabled on VLAN 1. For more information, see Chapter 15, "Configuring STP."

- MSTP is disabled. For more information, see Chapter 16, "Configuring MSTP."

- Optional spanning-tree features are disabled. For more information, see Chapter 17, "Configuring Optional Spanning-Tree Features."

- Flex Links are not configured. For more information, see Chapter 18, "Configuring Flex Links and the MAC Address-Table Move Update Feature."

> **Note**   To use Flex Links, the switch must be running the LAN Base image.

- DHCP snooping is disabled. The DHCP snooping information option is enabled. For more information, see Chapter 19, "Configuring DHCP Features."
- DHCP server port-based address allocation is disabled. For more information, see Chapter 19, "Configuring DHCP Features."
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see Chapter 20, "Configuring IGMP Snooping and MVR."
- IGMP throttling setting is deny. For more information, see Chapter 20, "Configuring IGMP Snooping and MVR."
- The IGMP snooping querier feature is disabled. For more information, see Chapter 20, "Configuring IGMP Snooping and MVR."
- MVR is disabled. For more information, see Chapter 20, "Configuring IGMP Snooping and MVR."

> **Note**   To use MVR, the switch must be running the LAN Base image.

- Port-based traffic
    - Broadcast, multicast, and unicast storm control is disabled. For more information, see Chapter 21, "Configuring Port-Based Traffic Control."
    - No protected ports are defined. For more information, see Chapter 21, "Configuring Port-Based Traffic Control."
    - Unicast and multicast traffic flooding is not blocked. For more information, see Chapter 21, "Configuring Port-Based Traffic Control."
    - No secure ports are configured. For more information, see Chapter 21, "Configuring Port-Based Traffic Control."
- CDP is enabled. For more information, see Chapter 22, "Configuring CDP."
- UDLD is disabled. For more information, see Chapter 24, "Configuring UDLD."
- SPAN and RSPAN are disabled. For more information, see Chapter 25, "Configuring SPAN and RSPAN."

> **Note**   To use RSPAN, the switch must be running the LAN Base image.

- RMON is disabled. For more information, see Chapter 26, "Configuring RMON."
- Syslog messages are enabled and appear on the console. For more information, see Chapter 27, "Configuring System Message Logging."
- SNMP is enabled (Version 1). For more information, see Chapter 28, "Configuring SNMP."
- No ACLs are configured. For more information, see Chapter 29, "Configuring Network Security with ACLs."
- QoS is disabled. For more information, see Chapter 31, "Configuring QoS."

- No EtherChannels are configured. For more information, see Chapter 34, "Configuring EtherChannels and Link-State Tracking."

- IPv6 unicast routing is disabled. For more information, see Chapter 32, "Configuring IPv6 Host Functions."

Network Configuration Examples

This section provides network configuration concepts and includes examples of using the switch to create dedicated network segments and interconnecting the segments through Fast Ethernet and Gigabit Ethernet connections.

- "Design Concepts for Using the Switch" section on page 1-16
- "Small to Medium-Sized Network Using Catalyst 2960 Switches" section on page 1-19
- "Long-Distance, High-Bandwidth Transport Configuration" section on page 1-20

Design Concepts for Using the Switch

As your network users compete for network bandwidth, it takes longer to send and receive data. When you configure your network, consider the bandwidth required by your network users and the relative priority of the network applications that they use.

Table 1-1 describes what can cause network performance to degrade and how you can configure your network to increase the bandwidth available to your network users.

Table 1-1   *Increasing Network Performance*

Network Demands	Suggested Design Methods
Too many users on a single network segment and a growing number of users accessing the Internet	• Create smaller network segments so that fewer users share the bandwidth, and use VLANs and IP subnets to place the network resources in the same logical network as the users who access those resources most. • Use full-duplex operation between the switch and its connected workstations.
• Increased power of new PCs, workstations, and servers • High bandwidth demand from networked applications (such as e-mail with large attached files) and from bandwidth-intensive applications (such as multimedia)	• Connect global resources—such as servers and routers to which the network users require equal access—directly to the high-speed switch ports so that they have their own high-speed segment. • Use the EtherChannel feature between the switch and its connected servers and routers.

Bandwidth alone is not the only consideration when designing your network. As your network traffic profiles evolve, consider providing network services that can support applications for voice and data integration, multimedia integration, application prioritization, and security. Table 1-2 describes some network demands and how you can meet them.

Table 1-2 *Providing Network Services*

| Network Demands	Suggested Design Methods
Efficient bandwidth usage for multimedia applications and guaranteed bandwidth for critical applications	• Use IGMP snooping to efficiently forward multimedia and multicast traffic. • Use other QoS mechanisms such as packet classification, marking, scheduling, and congestion avoidance to classify traffic with the appropriate priority level, thereby providing maximum flexibility and support for mission-critical, unicast, and multicast and multimedia applications. • Use MVR to continuously send multicast streams in a multicast VLAN but to isolate the streams from subscriber VLANs for bandwidth and security reasons.
High demand on network redundancy and availability to provide *always on* mission-critical applications	• Use VLAN trunks and BackboneFast for traffic-load balancing on the uplink ports so that the uplink port with a lower relative port cost is selected to carry the VLAN traffic.
An evolving demand for IP telephony	• Use QoS to prioritize applications such as IP telephony during congestion and to help control both delay and jitter within the network. • Use switches that support at least two queues per port to prioritize voice and data traffic as either high- or low-priority, based on IEEE 802.1p/Q. The switch supports at least four queues per port. • Use voice VLAN IDs (VVIDs) to provide separate VLANs for voice traffic.
A growing demand for using existing infrastructure to transport data and voice from a home or office to the Internet or an intranet at higher speeds	Use the Catalyst Long-Reach Ethernet (LRE) switches to provide up to 15 Mb of IP connectivity over existing infrastructure, such as existing telephone lines. Note To use LRE, the switch must be running the LAN Base image. Note LRE is the technology used in the Catalyst 2900 LRE XL and Catalyst 2950 LRE switches. See the documentation sets specific to these switches for LRE information.

You can use the switches to create the following:

• Cost-effective Gigabit-to-the-desktop for high-performance workgroups (Figure 1-1)—For high-speed access to network resources, you can use the Cisco Catalyst 2960 switches in the access layer to provide Gigabit Ethernet to the desktop. To prevent congestion, use QoS DSCP marking priorities on these switches. For high-speed IP forwarding at the distribution layer, connect the switches in the access layer to a Gigabit multilayer switch with routing capability, such as a Catalyst 3750 switch, or to a router.

The first illustration is of an isolated high-performance workgroup, where the Catalyst 2960 switches are connected to Catalyst 3750 switches in the distribution layer. The second illustration is of a high-performance workgroup in a branch office, where the Catalyst 2960 switches are connected to a router in the distribution layer.

Each switch in this configuration provides users with a dedicated 1-Gb/s connection to network resources. Using SFP modules also provides flexibility in media and distance options through fiber-optic connections.

Figure 1-1   *High-Performance Workgroup (Gigabit-to-the-Desktop)*
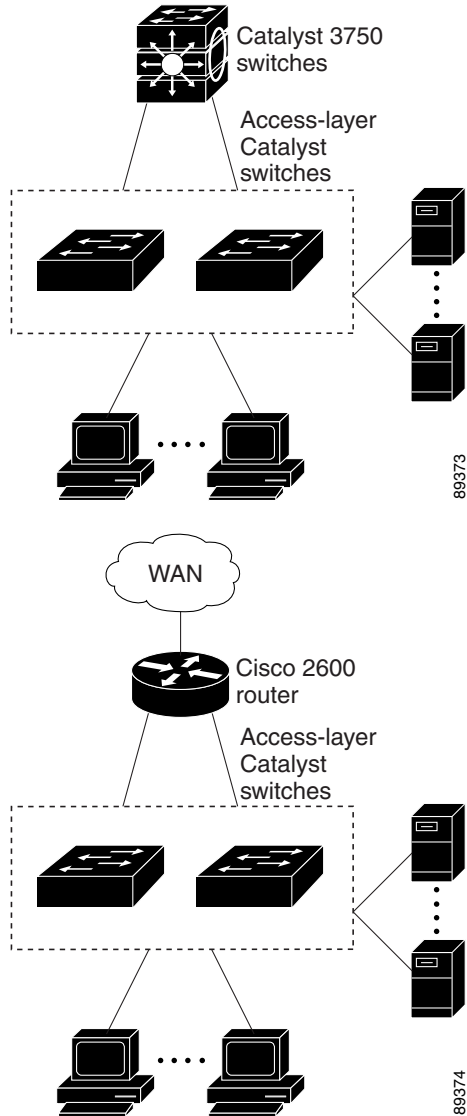
- Server aggregation (Figure 1-2)—You can use the switches to interconnect groups of servers, centralizing physical security and administration of your network. For high-speed IP forwarding at the distribution layer, connect the switches in the access layer to multilayer switches with routing capability. The Gigabit interconnections minimize latency in the data flow.

  QoS and policing on the switches provide preferential treatment for certain data streams. They segment traffic streams into different paths for processing. Security features on the switch ensure rapid handling of packets.

  Fault tolerance from the server racks to the core is achieved through dual homing of servers connected to switches, which have redundant Gigabit EtherChannels.

  Using dual SFP module uplinks from the switches provides redundant uplinks to the network core. Using SFP modules provides flexibility in media and distance options through fiber-optic connections.

Figure 1-2   Server Aggregation

Small to Medium-Sized Network Using Catalyst 2960 Switches

Figure 1-3 shows a configuration for a network of up to 500 employees. This network uses Catalyst 2960 switches with high-speed connections to two routers. This ensures connectivity to the Internet, WAN, and mission-critical network resources in case one of the routers fails. The switches are using EtherChannel for load sharing.

The switches are connected to workstations and local servers. The server farm includes a call-processing server running Cisco CallManager software. Cisco CallManager controls call processing, routing, and Cisco IP Phone features and configuration. The switches are interconnected through Gigabit interfaces.

This network uses VLANs to logically segment the network into well-defined broadcast groups and for security management. Data and multimedia traffic are configured on the same VLAN. Voice traffic from the Cisco IP Phones are configured on separate VVIDs. If data, multimedia, and voice traffic are assigned to the same VLAN, only one VLAN can be configured per wiring closet.

When an end station in one VLAN needs to communicate with an end station in another VLAN, a router routes the traffic to the destination VLAN. In this network, the routers are providing inter-VLAN routing. VLAN access control lists (VLAN maps) on the switch provide intra-VLAN security and prevent unauthorized users from accessing critical areas of the network.

In addition to inter-VLAN routing, the routers provide QoS mechanisms such as DSCP priorities to prioritize the different types of network traffic and to deliver high-priority traffic. If congestion occurs, QoS drops low-priority traffic to allow delivery of high-priority traffic.

Cisco CallManager controls call processing, routing, and Cisco IP Phone features and configuration. Users with workstations running Cisco SoftPhone software can place, receive, and control calls from their PCs. Using Cisco IP Phones, Cisco CallManager software, and Cisco SoftPhone software integrates telephony and IP networks, and the IP network supports both voice and data.

The routers also provide firewall services, Network Address Translation (NAT) services, voice-over-IP (VoIP) gateway services, and WAN and Internet access.

Figure 1-3   *Catalyst 2960 Switchesin a Collapsed Backbone Configuration*
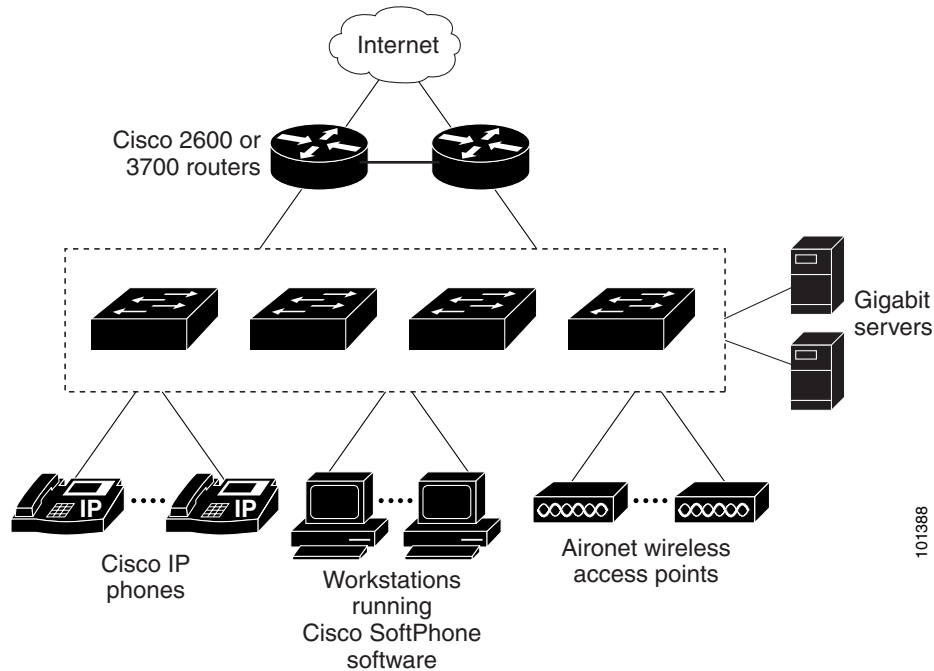
# Long-Distance, High-Bandwidth Transport Configuration

Note   To use CWDM SFPs, the switch must be running the LAN Base image.

Figure 1-4 shows a configuration for sending 8 Gigabits of data over a single fiber-optic cable. The Catalyst 2960 switches have coarse wavelength-division multiplexing (CWDM) fiber-optic SFP modules installed. Depending on the CWDM SFP module, data is sent at wavelengths from 1470 to 1610 nm. The higher the wavelength, the farther the transmission can travel. A common wavelength used for long-distance transmissions is 1550 nm.

The CWDM SFP modules connect to CWDM optical add/drop multiplexer (OADM) modules over distances of up to 393,701 feet (74.5 miles or 120 km). The CWDM OADM modules combine (or *multiplex*) the different CWDM wavelengths, allowing them to travel simultaneously on the same fiber-optic cable. The CWDM OADM modules on the receiving end separate (or *demultiplex*) the different wavelengths.

For more information about the CWDM SFP modules and CWDM OADM modules, see the *Cisco CWDM GBIC and CWDM SFP Installation Note*.

Figure 1-4   Long-Distance, High-Bandwidth Transport Configuration
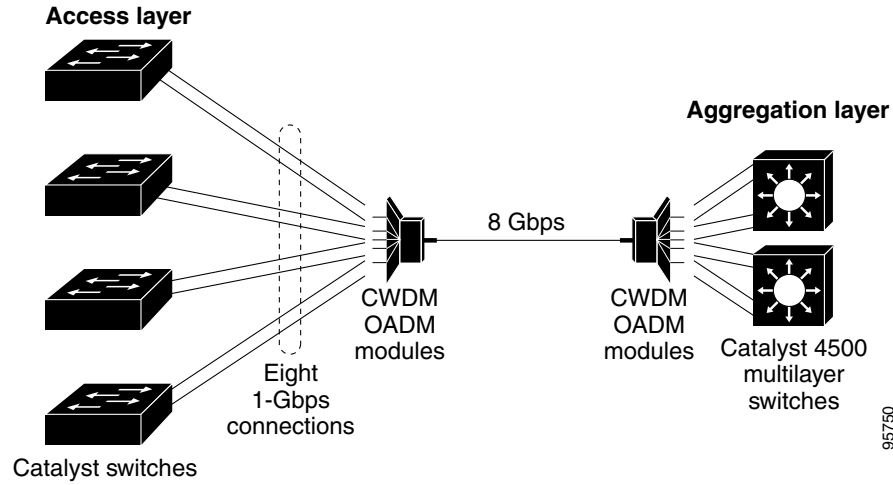
Where to Go Next

Before configuring the switch, review these sections for startup information:

- Chapter 2, "Using the Command-Line Interface"
- Chapter 3, "Assigning the Switch IP Address and Default Gateway"