CHAPTER 1

Overview

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

Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

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.

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

- 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
  - 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, switch stack, and switch cluster management from anywhere in your intranet.
  - 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 the RPS, the switch must be running the LAN Base image.

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

- Cisco FlexStack technology on Catalyst 2960-S switches running the LAN base image for
  - Connecting up to four switches through their FlexStack ports to operate as a single switch in the network.
  - Creating a bidirectional 20-Gb/s switching fabric across the switch stack, with all stack members having full access to the system bandwidth.
  - Using a single IP address and configuration file to manage the entire switch stack.
  - Automatic Cisco IOS version-check of new stack members with the option to automatically load images from the stack master or from a TFTP server.
  - Adding, removing, and replacing switches in the stack without disrupting the operation of the stack.
  - Provisioning a new member for a switch stack with the offline configuration feature. You can configure in advance the interface configuration for a specific stack member number and for a specific switch type of a new switch that is not part of the stack. The switch stack retains this information across stack reloads whether or not the provisioned switch is part of the stack.
  - Displaying stack-ring activity statistics (the number of frames sent by each stack member to the ring).
- 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.
- Stack troubleshooting enhancements
- Auto Smartports
  - Cisco-default and user-defined macros for dynamic port configuration based on the device type detected on the port.
  - Enhancements to add support for global macros, last-resort macros, event trigger control, access points, EtherChannels, auto-QoS with Cisco Medianet, and IP phones.
  - Enhancements to add support for macro persistency, LLDP-based triggers, MAC address and OUI-based triggers, remote macros as well as for automatic configuration based on these two new device types: Cisco Digital Media Player (Cisco DMP) and Cisco IP Video Surveillance Camera (Cisco IPVSC).
  - Auto Smartports enhancement to enable auto-QoS on a CDP-capable Cisco digital media player.

  For information, see the *Auto Smartports Configuration Guide*.
- Smart Install to allow a single point of management (director) in a network. You can use Smart Install to provide zero touch image and configuration upgrade of newly deployed switches and image and configuration downloads for any client switches. For more information, see the *Cisco Smart Install Configuration Guide.*

  - Smart Install enhancements supporting client backup files, zero-touch replacement for clients with the same product-ID, automatic generation of the image list file, configurable file repository, hostname changes, transparent connection of the director to client, and USB storage for image and seed configuration.
  - Smart Install enhancements in Cisco IOS Release 12.2(58)SE including the ability to manually change a client switch health state from denied to allowed or hold for on-demand upgrades, to remove selected clients from the director database, to allow simultaneous on-demand upgrade of multiple clients, and to provide more information about client devices, including device status, health status, and upgrade status.
- Call Home to provide e-mail-based and web-based notification of critical system events. Users with a service contract directly with Cisco Systems can register Call Home devices for the Cisco Smart Call Home service that generates automatic service requests with the Cisco TAC.

Performance Features

- Cisco EnergyWise manages the energy usage of endpoints connected to domain members. For more information, see the Cisco EnergyWise documentation on Cisco.com.
- EnergyWise Phase 2.5 enhancements that add support for a query to analyze and display domain information and for Wake on LAN (WoL) to remotely power on a WoL-capable PC.
- 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.
- SFP+ support for 10Gigabit speeds (Catalyst 2960-S only)
- 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).
- Up to 20 Gb/s of forwarding rates in a Catalyst 2960-S switch stack.
- 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 across the switches in the stack.
- 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.
- 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.

- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.
- Support for QoS marking of CPU-generated traffic and queue CPU-generated traffic on the egress network ports.
- Memory consistency check routines to detect and correct invalid ternary content addressable memory (TCAM) table entries.

Management Options

- 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 by connecting your management station directly to the switch console port, by connecting your PC directly to the Ethernet management port, or by using Telnet from a remote management station or PC. You can manage the switch stack by connecting to the console port or Ethernet management port of any stack member. For more information about the CLI, see Chapter 1, "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 1, "Configuring SNMP."
- Cisco IOS Configuration Engine (previously known to as the Cisco IOS CNS agent)-—Configuration service automates 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 1, "Configuring Cisco IOS Configuration Engine."

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

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

- Support for CDP and LLDP enhancements for exchanging location information with video end points for dynamic location-based content distribution from servers
- Network Time Protocol (NTP) version 4 for NTP time synchronization for both IPv4 and IPv6
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch uses
- 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
- Support for SSH for IPv6.
- Support for IPv6 Host on the LAN Base and LAN Lite image (Catalyst 2960 and 2960-S).
- 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
- Out-of-band management access through the Ethernet management port to a PC (Catalyst 2960-only)
- 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) for both IPv4 and IPv6
- 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.
- Wired location service sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE)

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

- CPU utilization threshold trap monitors CPU utilization

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

- LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode

Note Supported on all images in Cisco IOS Release 12.2(55)SE.

- Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol
- DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field
- Increased support for LLPD-MED by allowing the switch to grant power to the power device (PD), based on the power policy TLV request
- USB mini-Type B console port in addition to the standard RJ-45 console port. Console input is active on only one port at a time. (Catalyst 2960-S only)
- USB Type A port for external Cisco USB flash memory devices (thumb drives or USB keys). You can use standard Cisco CLI commands to read, write, erase, copy, or boot from the flash memory. (Catalyst 2960-S only)

Availability and Redundancy Features

- Automatic stack master re-election for replacing stack masters that become unavailable (failover support)

  The newly elected stack master begins accepting Layer 2 traffic in less than 1 second and Layer 3 traffic between 3 to 5 seconds. If traffic loss exceeds this time period, use the **stack-mac persistent timer** global configuration command to enable the persistent MAC address feature. When this feature is enabled, if the stack master changes, the stack MAC address does not change for a configured time value (1 to 60 minutes) or for an indefinite time period.
- Cross-stack EtherChannel for providing redundant links across the switch stack
- 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 on switches 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, cross-stack UplinkFast, and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks and cross-stack Gigabit uplinks
  - 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

- 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 on switches 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.

- Support for 802.1x authentication with restricted VLANs (also known as *authentication failed VLANs*)
- Support for VTP version 3 that includes support for configuring extended range VLANs (VLANs 1006 to 4094) in any VTP mode, enhanced authentication (hidden or secret passwords), propagation of other databases in addition to VTP, VTP primary and secondary servers, and the option to turn VTP on or off by port

Security Features

- 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
- Protocol storm protection to control the rate of incoming protocol traffic to a switch by dropping packets that exceed a specified ingress rate.
- 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
- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings
- Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN
- 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 802.1x-authenticated users to a specified VLAN
  - Support for VLAN assignment on a port configured for multi-auth mode. The RADIUS server assigns a VLAN to the first host to authenticate on the port, and subsequent hosts use the same VLAN. Voice VLAN assignment is supported for one IP phone.

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

  - Port security for controlling access to 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-802.1x-compliant users
  - Restricted VLAN to provide limited services to users who are 802.1x compliant, but do not have the credentials to authenticate via the standard 802.1x processes

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

  - 802.1x accounting to track network usage

- 802.1x with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame
- 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch

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

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

Note To use voice aware 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 2 802.1x validation of the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access.

  For information about configuring NAC Layer 2 802.1x validation, see the "Configuring NAC Layer 2 802.1x Validation" section on page 1-58.

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

- Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.
- IEEE 802.1x with open access to allow a host to access the network before being authenticated.
- IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch.
- Support for dynamic creation or attachment of an auth-default ACL on a port that has no configured static ACLs.

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

- Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host.
- Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port.

- TACACS+, a proprietary feature for managing network security through a TACACS server for both IPv4 and IPv6
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services for both IPv4 and IPv6
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.

- 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
- Support for IP source guard on static hosts.
- RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Secure ACS to reinitialize authentication, and apply to the new policies.
- IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
- Support for critical VLAN with multiple-host authentication so that when a port is configured for multi-auth, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources.
- Customizable web authentication enhancement to allow the creation of user-defined *login*, *success*, *failure* and *expire* web pages for local web authentication.
- Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.
- VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.
- MAC move to allow hosts (including the hosts connected behind an IP phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port in the same way as a completely new MAC address.
- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.

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

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

- 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
  - 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.

Note Ingress queueing is not supported on Catalyst 2960-S switches.

- 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.

- Auto-QoS enhancements that add automatic configuration classification of traffic flow from video devices, such as the Cisco Telepresence System and Cisco Surveillance Camera.

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

Layer 3 Features

- When you configure the **lanbase-routing** SDM template, the switch supports static routing and router ACLs on SVIs (supported only on switches running the LAN base 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

- 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 IEEE 802.3at, (PoE+) that increases the available power that can be drawn by powered devices from 15.4 W per port to 30 W per port (Catalyst 2960-S only)
- 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

- Switch LEDs that provide port- and switch-level status
- Switch LEDs that provide port-, switch-, and stack-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
- Generic online diagnostics to test hardware functionality of the supervisor engine, modules, and switch while the switch is connected to a live network (Catalyst 2960-S only).
- On-board failure logging (OBFL) to collect information about the switch and the power supplies connected to it (Catalyst 2960-S only)
- 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.

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- and stack-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 1, "Assigning the Switch IP Address and Default Gateway," and Chapter 1, "Configuring DHCP and IP Source Guard Features."
- Default domain name is not configured. For more information, see Chapter 1, "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 1, "Assigning the Switch IP Address and Default Gateway," and Chapter 1, "Configuring DHCP and IP Source Guard Features."
- Switch cluster is disabled. For more information about switch clusters, see Chapter 1, "Clustering Switches," and the *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- No passwords are defined. For more information, see Chapter 1, "Administering the Switch."
- System name and prompt is *Switch.* For more information, see Chapter 1, "Administering the Switch."
- NTP is enabled. For more information, see Chapter 1, "Administering the Switch."
- DNS is enabled. For more information, see Chapter 1, "Administering the Switch."
- TACACS+ is disabled. For more information, see Chapter 1, "Configuring Switch-Based Authentication."
- RADIUS is disabled. For more information, see Chapter 1, "Configuring Switch-Based Authentication."
- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see Chapter 1, "Configuring Switch-Based Authentication."
- IEEE 802.1x is disabled. For more information, see Chapter 1, "Configuring IEEE 802.1x Port-Based Authentication."
- Port parameters
  - Interface speed and duplex mode is autonegotiate. For more information, see
  - Auto-MDIX is enabled. For more information, see
  - Flow control is off. For more information, see
  - PoE is autonegotiate. For more information, see
- VLANs
  - Default VLAN is VLAN 1. For more information, see Chapter 1, "Configuring VLANs."
  - VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 1, "Configuring VLANs."
  - Trunk encapsulation is negotiate. For more information, see Chapter 1, "Configuring VLANs."
  - VTP mode is server. For more information, see Chapter 1, "Configuring VTP."
  - VTP version is Version 1. For more information, see Chapter 1, "Configuring VTP."
  - Voice VLAN is disabled. For more information, see Chapter 1, "Configuring Voice VLAN."
- STP, PVST+ is enabled on VLAN 1. For more information, see Chapter 1, "Configuring STP."
- MSTP is disabled. For more information, see Chapter 1, "Configuring MSTP."

- Optional spanning-tree features are disabled. For more information, see Chapter 1, "Configuring Optional Spanning-Tree Features."
- Flex Links are not configured. For more information, see Chapter 1, "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 1, "Configuring DHCP and IP Source Guard Features."
- IP source guard is disabled. For more information, see Chapter 1, "Configuring DHCP and IP Source Guard Features."
- DHCP server port-based address allocation is disabled. For more information, see Chapter 1, "Configuring DHCP and IP Source Guard Features."
- Dynamic ARP inspection is disabled on all VLANs. For more information, see Chapter 1, "Configuring Dynamic ARP Inspection."
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see Chapter 1, "Configuring IGMP Snooping and MVR."
- IGMP throttling setting is deny. For more information, see Chapter 1, "Configuring IGMP Snooping and MVR."
- The IGMP snooping querier feature is disabled. For more information, see Chapter 1, "Configuring IGMP Snooping and MVR."
- MVR is disabled. For more information, see Chapter 1, "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 1, "Configuring Port-Based Traffic Control."
  - No protected ports are defined. For more information, see Chapter 1, "Configuring Port-Based Traffic Control."
  - Unicast and multicast traffic flooding is not blocked. For more information, see Chapter 1, "Configuring Port-Based Traffic Control."
  - No secure ports are configured. For more information, see Chapter 1, "Configuring Port-Based Traffic Control."
- CDP is enabled. For more information, see Chapter 1, "Configuring CDP."
- UDLD is disabled. For more information, see Chapter 1, "Configuring UDLD."
- SPAN and RSPAN are disabled. For more information, see Chapter 1, "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 1, "Configuring RMON."

- Syslog messages are enabled and appear on the console. For more information, see Chapter 1, "Configuring System Message Logging."
- SNMP is enabled (Version 1). For more information, see Chapter 1, "Configuring SNMP."
- No ACLs are configured. For more information, see Chapter 1, "Configuring Network Security with ACLs."
- QoS is disabled. For more information, see Chapter 1, "Configuring QoS."
- No EtherChannels are configured. For more information, see Chapter 1, "Configuring EtherChannels and Link-State Tracking."

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

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 switch stacks, where all stack members are eligible stack masters in case of stack-master failure. All stack members have synchronized copies of the saved and running configuration files of the switch stack. **Note** Stacking is supported only on Catalyst 2960-S switches running the LAN base image. • Use cross-stack EtherChannels for providing redundant links across the switch stack. • Use VLAN trunks, cross-stack UplinkFast, 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.
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.

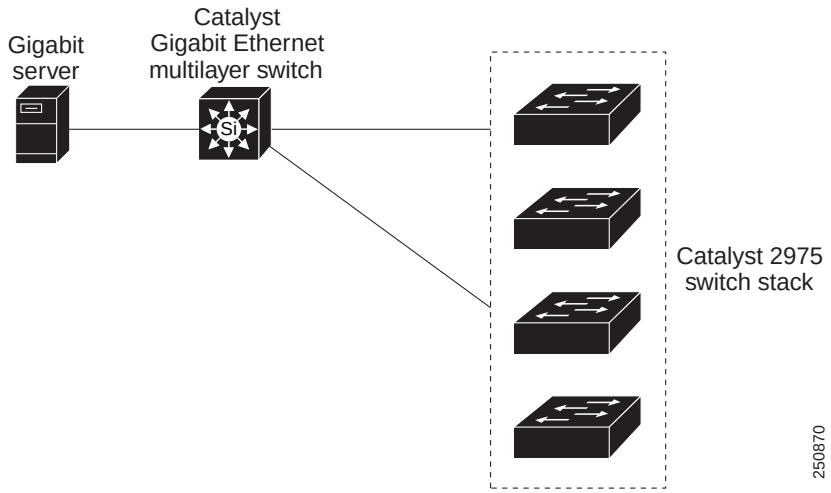
You can use the switches and switch stacks to create the following:

- Catalyst 2960-S switches. To preserve switch connectivity if one switch in the stack fails, connect the switches as recommended in the hardware installation guide, and enable either cross-stack Etherchannel or cross-stack UplinkFast.

  You can have redundant uplink connections, using SFP modules in the switch stack to a Gigabit backbone switch, such as a Catalyst 4500 or Catalyst 3750-12S Gigabit switch. You can also create backup paths by using Fast Ethernet, Gigabit, or EtherChannel links. If one of the redundant connections fails, the other can serve as a backup path. If the Gigabit switch is cluster-capable, you can configure it and the switch stack as a switch cluster to manage them through a single IP address. The Gigabit switch can be connected to a Gigabit server through a 1000BASE-T connection.

Note Stacking is supported only on Catalyst 2960-S switches running the LAN base image.

Figure 1-1 Cost-Effective Wiring Closet



- 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.

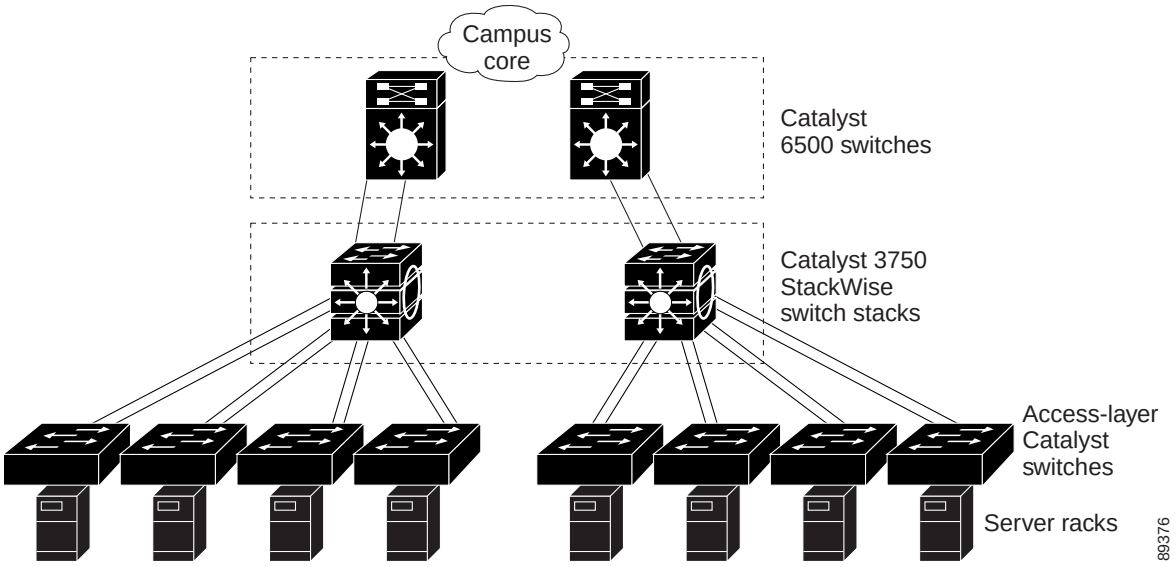
  QoS and policing on the switches provide preferential treatment for certain data streams. They segment traffic streams into different paths for processing. Security features on the switch ensure rapid handling of packets.

  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.

  The various lengths of stack cable available, ranging from 0.5 meter to 3 meters provide extended connections to the switch stacks across multiple server racks, for multiple stack aggregation.

Figure 1-2 Server Aggregation



Small to Medium-Sized Network Using Catalyst 2960 and 2960-S Switches

Figure 1-3 shows a configuration for a network of up to 500 employees. This network uses 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.

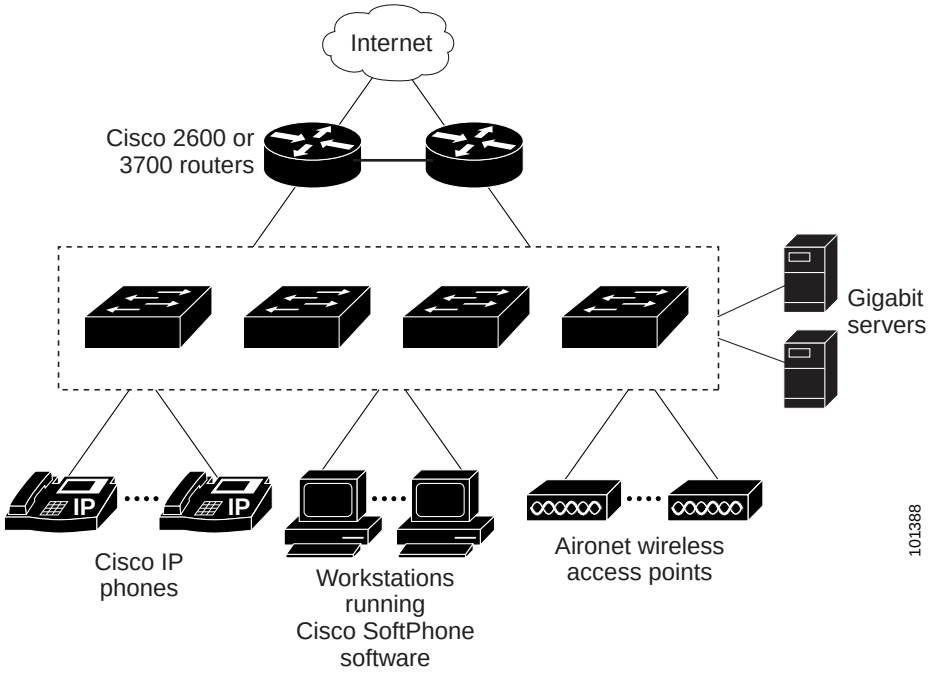
When an end station in one VLAN needs to communicate with an end station in another VLAN, a router or Layer 3 switch routes the traffic to the destination VLAN. In this network, the routers are providing inter-VLAN routing. VLAN access control lists (VLAN maps) on the switch provide intra-VLAN security 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 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 or 2960-S 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 1, “Using the Command-Line Interface”
- Chapter 1, “Assigning the Switch IP Address and Default Gateway”

To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.