CHAPTER 1

Overview

This chapter provides these topics about the Catalyst 3560 and 3660-C switch software:

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

Features

The switch ships with one of these software images installed:

- IP base image, which provides Layer 2+ features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), static routing, EIGRP stub routing, PIM stub routing, the Hot Standby Router Protocol (HSRP), and the Routing Information Protocol (RIP). Switches with the IP base image installed can be upgraded to IP services image.
- IP services image, which provides a richer set of enterprise-class intelligent services. It includes all IP base image features plus full Layer 3 routing (IP unicast routing, IP multicast routing, and fallback bridging). To distinguish it from the Layer 2+ static routing and RIP, the IP services image includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and the Open Shortest Path First (OSPF) Protocol.

  IP services image-only Layer 3 features are described in the "Layer 3 Features" section on page 1-14.

Note Unless otherwise noted, all features described in this chapter and in this guide are supported on both the IP base image and IP services image.

IPv6 Multicast Listener Discovery (MLD) snooping is supported in all Catalyst 3560 and 3750 images; for more information, see Chapter 44, "Configuring IPv6 MLD Snooping."

For full IPv6 support, the IP services image is required. For more information on IPv6 routing, see Chapter 42, "Configuring IPv6 Unicast Routing."

For information on IPv6 ACLs, see Chapter 43, "Configuring IPv6 ACLs."

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 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).
  - 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.

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

- 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.
- 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.
  - Improved device classification capabilities and accuracy, increased device visibility, and enhanced macro management. The device classifier is enabled by default, and can classify devices based on DHCP options.

  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.
- Support for up to 1546 bytes routed frames, 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 and Layer 3 packets at Gigabit line rate
- Multicast virtual routing and forwarding (VRF) Lite for configuring multiple private routing domains for network virtualization and virtual private multicast networks
- 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.
- Cisco Group Management Protocol (CGMP) server support and Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3:
  - (For CGMP devices) CGMP for limiting multicast traffic to specified end stations and reducing overall network traffic.
  - (For IGMP devices) IGMP snooping for 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.
- IGMP helper to allow the switch to forward a host request to join a multicast stream to a specific IP destination address.
- 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.
- 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.
- Web Cache Communication Protocol (WCCP) for redirecting traffic to local wide-area application engines, for enabling content requests to be fulfilled locally, and for localizing web-traffic patterns in the network (requires the IP services image).
  - Support for deny and permit ACL entries in WCCP redirect lists.
- 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.
- 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. 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 35, “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 4, “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
- 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
- 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, 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
- Support for SSH for IPv6.
- 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) 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)
- CPU utilization threshold trap monitors CPU utilization
- 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
- 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

Availability and Redundancy Features

- HSRP for command switch and Layer 3 router redundancy
- Virtual Router Redundancy Protocol (VRRP) which allows several routers on a multi-access link to use the same virtual IP address
- Enhanced object tracking, which separates the tracking mechanism from HSRP and creates a separate, standalone tracking process that can be used by processes other than HSRP
- 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
  - 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
- Equal-cost routing for link-level and switch-level redundancy
- Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy
- 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.
- RPS support through the Cisco Redundant Power System 2300, also referred to as the RPS 2300, for enhancing power reliability, configuring and managing the redundant power system. For more information about the RPS 2300, see the *Cisco Redundant Power System 2300 Hardware Installation Guide* that shipped with the device and that is also on Cisco.com.

VLAN Features

- Support for up to 1005 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
- 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
- Inter-Switch Link (ISL) and 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 or ISL) 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.
- Private VLANs to address VLAN scalability problems, to provide a more controlled IP address allocation, and to allow Layer 2 ports to be isolated from other ports on the switch
- Port security on a PVLAN host to limit the number of MAC addresses learned on a port, or define which MAC addresses may be learned on a port
- 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.
- 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

- Cisco IOS Release 15.0(2)SE1 on the Catalyst 3560, 3560-C405, and 3560-C405ex switches has been submitted for certification under FIPS 140-2 and Common Criteria compliance with the US Government, Security Requirements for Network Devices (pp_nd_v1.0), version 1.0, dated 10 December 2010.

  Note The images for the Cisco IOS Release 15.0(2)SE1 Catalyst 3560, 3560-C405, and 3560-C405ex switches are FIPS certified. For information about using FIPS certified images,the "Boot Loader Upgrade and Image Verification for the FIPS Mode of Operation" section on page 3-24 of the software configuration guide.

  FIPS 140-2 is a cryptographic-focused certification, required by many government and enterprise customers, which ensures the compliance of the encryption and decryption operations performed by the switch to the approved FIPS cryptographic strengths and management methods for safeguarding these operations. For more information, see:

  - The security policy document at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1657
  - The installation notes at: http://www.cisco.com/en/US/products/ps10745/prod_installation_guides_list.html

Common Criteria is an international standard (ISO/IEC 15408) for computer security certification. This standard is a set of requirements, tests, and evaluation methods that ensures that the Target of Evaluation complies with a specific Protection Profile or custom Security Target. For more information, see the security target document at: http://www.niap-ccevs.org/st/vid10488/

- Web authentication to allow a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser
- Local web authentication banner so that a custom banner or an image file can be displayed at a web authentication login screen
- MAC authentication bypass (MAB) aging timer to detect inactive hosts that have authenticated after they have authenticated by using MAB
- 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 security policies in both directions on routed interfaces (router ACLs) and VLANs and inbound on Layer 2 interfaces (port ACLs)
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces
- VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/UDP headers
- Source and destination MAC-based ACLs for filtering non-IP traffic
- IPv6 ACLs to be applied to interfaces to filter IPv6 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 802.1Q tunneling so that customers with users at remote sites across a service-provider network can keep VLANs segregated from other customers and Layer 2 protocol tunneling to ensure that the customer's network has complete STP, CDP, and VTP information about all users
- Layer 2 point-to-point tunneling to facilitate the automatic creation of EtherChannels
- Layer 2 protocol tunneling bypass feature to provide interoperability with third-party vendors

- 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
  - 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.
  - 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
  - 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
  - Voice aware 802.1x security to apply traffic violation actions only on the VLAN on which a security violation occurs.
  - MAC authentication bypass to authorize clients based on the client MAC address.
  - 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.
  - 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.
- Network Admission Control (NAC) features:
  - 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 10-59.

  - NAC Layer 2 IP validation of the posture of endpoint systems or clients before granting the devices network access.

    For information about configuring NAC Layer 2 IP validation, see the *Network Admission Control Software Configuration Guide*.

  - IEEE 802.1x inaccessible authentication bypass.

    For information about configuring this feature, see the "Configuring Inaccessible Authentication Bypass and Critical Voice VLAN" section on page 10-54.

  - Authentication, authorization, and accounting (AAA) down policy for a NAC Layer 2 IP validation of a host if the AAA server is not available when the posture validation occurs.

    For information about this feature, see the *Network Admission Control Software Configuration Guide*.

- 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 AAA services for both IPv4 and IPv6
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic versions of the software)
- 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)
- Voice aware IEEE 802.1x and MAC authentication bypass (MAB) security violation to shut down only the data VLAN on a port when a security violation occurs
- 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.
- Support for critical voice VLAN to so that when authentication is enabled and the access control server is not available, traffic from the host tagged with the voice VLAN is put into the configured voice VLAN for the port.
- 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.
- NEAT enhancement to control access to the supplicant port during authentication.
- 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.
- Support for the Security Group Tag (SCT) Exchange Protocol (SXP) component of Cisco TrustSec, a security architecture using authentication, encryption, and access control.
- SXP version 2, syslog messages and SNMP support for Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SxP).

  For more information about Cisco TrustSec, see the " SGT Exchange Protocol over TCP (SXP)" chapter in the *Cisco TrustSec Switch Configuration Guide* at this URL: http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/sxp_config.html
- Support for IEEE 802.1AE Media Access Control Security (MACsec) to provide MAC-layer encryption over wired networks using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) protocol provides the session keys and manages encryption keys (supported only on switches running the IP base or IP services feature set). (Catalyst 3560-C only)
- MACsec link layer switch-to-switch security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange. Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional). (Catalyst 3560-C only)

QoS and CoS Features

- Automatic QoS (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues
- Automatic quality of service (QoS) Voice over IP (VoIP) enhancement for port -based trust of DSCP and priority queuing for egress traffic
- 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
  - 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
  - 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
  - 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
  - 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)
- 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.
- Support for IPv6 QoS trust capability.
- Auto-QoS enhancements that add automatic configuration classification of traffic flow from video devices, such as the Cisco Telepresence System and Cisco Surveillance Camera.

Layer 3 Features

Note Some features noted in this section are available only on the IP services image.

- HSRP Version 1 (HSRPv1) and HSRP Version 2 (HSRPv2) for Layer 3 router redundancy
- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - RIP Versions 1 and 2
  - Full OSPF (requires the IP services feature set)

    Starting with Cisco IOS Release 12.2(55)SE, the IP base feature set supports OSPF for routed access to enable customers to extend Layer 3 routing capabilities to the access or wiring closet.
  - NSF IETF mode for OSPFv2—OSPFv2 graceful restart support for IPv4. (IP services feature set only)
  - NSF IETF mode for OSPFv3—OSPFv3 graceful restart support for IPv6. (IP services feature set only)
  - Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 to utilize IPv6 transport, communicate with IPv6 peers, and advertise IPv6 routes

  - HSRP for IPv6 (requires the IP services image)
  - Border Gateway Protocol (BGP) Version 4 (requires the IP services image)
- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
- Policy-based routing (PBR) for configuring defined policies for traffic flows
- Multiple VPN routing/forwarding (multi-VRF) instances in customer edge devices to allow service providers to support multiple virtual private networks (VPNs) and overlap IP addresses between VPNs (requires the IP services image)
- Fallback bridging for forwarding non-IP traffic between two or more VLANs (requires the IP services image)
- Static IP routing for manually building a routing table of network path information
- Equal-cost routing for load balancing and redundancy
- Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and router solicitation messages to discover the addresses of routers on directly attached subnets
- Protocol-Independent Multicast (PIM) for multicast routing within the network, allowing for devices in the network to receive the multicast feed requested and for switches not participating in the multicast to be pruned. Includes support for PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode (requires the IP services image)
- Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains (requires the IP services image)
- Distance Vector Multicast Routing Protocol (DVMRP) tunneling for interconnecting two multicast-enabled networks across nonmulticast networks (requires the IP services image)
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients
- DHCP for IPv6 relay, client, server address assignment and prefix delegation
- DHCPv6 bulk-lease query to support new bulk lease query type (as defined in RFC5460).
- The DHCPv6 relay source configuration feature to configure a source address for DHCPv6 relay agent.
- IPv6 unicast routing capability for forwarding IPv6 traffic through configured interfaces (requires the IP services image)
- IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router
- Nonstop forwarding (NSF) awareness to enable the Layer 3 switch to continue forwarding packets from an NSF-capable neighboring router when the primary route processor (RP) is failing and the backup RP is taking over, or when the primary RP is manually reloaded for a nondisruptive software upgrade (requires the IP services image)
- The ability to exclude a port in a VLAN from the SVI line-state up or down calculation
- Intermediate System-to-Intermediate System (IS-IS) routing supports dynamic routing protocols for Connectionless Network Service (CLNS) networks.
- Support for the Virtual Router Redundancy Protocol (VRRP) for IPv4, which dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing multiple routers on a multiaccess link to utilize the same virtual IP address.

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 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.

Universal Power over Ethernet Features

- Provides the ability to source up to 60 W of power over standard Ethernet cabling infrastructure.
- Sources up to 60 W of power (2X 30W) over both signal and spare pairs of the RJ-45 Ethernet cable based on IEEE802.3at standards.
- Automatically detects UPoE-compliant power devices and negotiates power up to 60 W by using Layer-2 power negotiation protocols, such as CDP or LLDP.
- Supports the third-party UPoE power device that complies with Cisco Catalyst 3000 switches.
- Sources up to 60 W of power by configuring the 4-pair forced mode interface even if the power device does not support the Layer-2 power negotiation protocol, such as CDP or LLDP.
- Supports 60 W of power per port, up to 30 ports, on a 48-port SKU or a total power budget of 1800 W with a combination of PoE, PoE+, and UPoE ports.

For more information on UPoE, see Universal Power Over Ethernet, page 14-12

Note Only Catalyst 3560-C switches supports Universal Power Over Ethernet.

Monitoring Features

- EOT and IP SLAs EOT static route support identify when a preconfigured static route or a DHCP route goes down
- Embedded event manager (EEM) for device and system management to monitor key system events and then act on them though a policy)
- Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and MAC-Address-Table.
- 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
- Smart logging to capture and export packet flows to a NetFlow collector. This release supports smart logging for DHCP snooping or dynamic ARP inspection violations, IP source guard denied traffic, and ACL
- VACL Logging to generate syslog messages for ACL denied IP packets.
- traffic permitted or denied on Layer 2 ports.
- 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 10/100/1000 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.
- Enhanced object tracking for HSRP.
- Digital optical monitoring (DOM) to check status of X2 small form-factor pluggable (SFP) modules
- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring
- IP SLAs EOT to use the output from IP SLAs tracking operations triggered by an action such as latency, jitter, or packet loss for a standby router failover takeover
- Support for the Built-in Traffic Simulator using Cisco IOS IP SLAs video operations to generate synthetic traffic for a variety of video applications, such as Telepresence, IPTV and IP video surveillance camera. You can use the simulator tool:
  - for network assessment before deploying applications that have stringent network performance requirements.
  - along with the Cisco Mediatrace for post-deployment troubleshooting for any network related performance issues.

The traffic simulator includes a sophisticated scheduler that allows the user to run several tests simultaneously or periodically and over extended time periods. For information, see the *Configuring Cisco IOS IP SLAs Video Operations* document at:
http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/12-2se/Configuring_IP_SLAs_Video_Operations.html

- Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications. One of the services of Medianet is auto provisioning for Cisco Digital Media Players and Cisco IP Video Surveillance cameras through Auto Smartports.
- Cisco Mediatrace and performance monitor
  - Cisco Mediatrace to troubleshoot and isolate network or application issues in traffic streams. It helps drill down to analyze one-way delay, one-way packet loss, one-way jitter, and connectivity in IPv4 networks that carry video traffic. This tool can be used for any UDP-based video or non-video traffic stream.

For information:
http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/15_1m_and_t/mm_15_1m_and_t.html

– Cisco Application Performance Monitor to track the video packet flow and to troubleshoot and isolate performance degradation in traffic streams. You can use the performance monitor for both video and nonvideo traffic.

  For information:
  http://www.cisco.com/en/US/docs/ios/media_monitoring/command/reference/mm_book.html

– Configuration guidelines for Mediatrace and performance monitor:

  Video monitoring is supported only on physical ports. It is not supported on EtherChannels.

  When a switch receives excessive traffic, packets are dropped.

  The switch supports policy maps and port-based trust only on ingress ports.

– Limitations for Mediatrace and performance monitor:

  You cannot configure video monitoring and a router or VLAN ACL on the same interface.
  If you configure video monitoring before configuring the ACL, the ACL settings override the video monitoring settings, and a message appears.
  If you configure the ACL before configuring video monitoring, the switch rejects the video monitoring commands, and a message appears.

  As video monitoring packets pass through the network queues, they can be dropped.

  The switch cannot apply QoS settings to packets forwarded in software.

  The switch cannot match lost or dropped packets to a specific traffic or data flow. For information about these packets, see the ingress and egress QoS counters.

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 25, “Configuring DHCP and IP Source Guard 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 25, "Configuring DHCP and IP Source Guard Features."
- Switch cluster is disabled. For more information about switch clusters, see Chapter 6, "Clustering Switches," and the *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- No passwords are defined. For more information, see Chapter 7, "Administering the Switch."
- System name and prompt is *Switch.* For more information, see Chapter 7, "Administering the Switch."
- NTP is enabled. For more information, see Chapter 7, "Administering the Switch."
- DNS is enabled. For more information, see Chapter 7, "Administering the Switch."
- TACACS+ is disabled. For more information, see Chapter 9, "Configuring Switch-Based Authentication."
- RADIUS is disabled. For more information, see Chapter 9, "Configuring Switch-Based Authentication."
- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see Chapter 9, "Configuring Switch-Based Authentication."
- IEEE 802.1x is disabled. For more information, see Chapter 10, "Configuring IEEE 802.1x Port-Based Authentication."
- Port parameters
  - Operating mode is Layer 2 (switchport). For more information, see Chapter 14, "Configuring Interface Characteristics."
  - Interface speed and duplex mode is autonegotiate. For more information, see Chapter 14, "Configuring Interface Characteristics."
  - Auto-MDIX is enabled. For more information, see Chapter 14, "Configuring Interface Characteristics."
  - Flow control is off. For more information, see Chapter 14, "Configuring Interface Characteristics."
  - PoE is autonegotiate. For more information, see Chapter 14, "Configuring Interface Characteristics."
- VLANs
  - Default VLAN is VLAN 1. For more information, see Chapter 15, "Configuring VLANs."
  - VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 15, "Configuring VLANs."
  - Trunk encapsulation is negotiate. For more information, see Chapter 15, "Configuring VLANs."
  - VTP mode is server. For more information, see Chapter 16, "Configuring VTP."
  - VTP version is Version 1. For more information, see Chapter 16, "Configuring VTP."
  - No private VLANs are configured. For more information, see Chapter 18, "Configuring Private VLANs."
  - Voice VLAN is disabled. For more information, see Chapter 17, "Configuring Voice VLAN."
- IEEE 802.1Q tunneling and Layer 2 protocol tunneling are disabled. For more information, see Chapter 19, "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling."

- STP, PVST+ is enabled on VLAN 1. For more information, see Chapter 20, "Configuring STP."
- MSTP is disabled. For more information, see Chapter 21, "Configuring MSTP."
- Optional spanning-tree features are disabled. For more information, see Chapter 22, "Configuring Optional Spanning-Tree Features."
- Flex Links are not configured. For more information, see Chapter 24, "Configuring Flex Links and the MAC Address-Table Move Update Feature."
- DHCP snooping is disabled. The DHCP snooping information option is enabled. For more information, see Chapter 25, "Configuring DHCP and IP Source Guard Features."
- IP source guard is disabled. For more information, see Chapter 25, "Configuring DHCP and IP Source Guard Features."
- DHCP server port-based address allocation is disabled. For more information, see Chapter 25, "Configuring DHCP and IP Source Guard Features."
- Dynamic ARP inspection is disabled on all VLANs. For more information, see Chapter 26, "Configuring Dynamic ARP Inspection."
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see Chapter 27, "Configuring IGMP Snooping and MVR."
- IGMP throttling setting is deny. For more information, see Chapter 27, "Configuring IGMP Snooping and MVR."
- The IGMP snooping querier feature is disabled. For more information, see Chapter 27, "Configuring IGMP Snooping and MVR."
- MVR is disabled. For more information, see Chapter 27, "Configuring IGMP Snooping and MVR."
- Port-based traffic
  - Broadcast, multicast, and unicast storm control is disabled. For more information, see Chapter 28, "Configuring Port-Based Traffic Control."
  - No protected ports are defined. For more information, see Chapter 28, "Configuring Port-Based Traffic Control."
  - Unicast and multicast traffic flooding is not blocked. For more information, see Chapter 28, "Configuring Port-Based Traffic Control."
  - No secure ports are configured. For more information, see Chapter 28, "Configuring Port-Based Traffic Control."
- CDP is enabled. For more information, see Chapter 29, "Configuring CDP."
- UDLD is disabled. For more information, see Chapter 31, "Configuring UDLD."
- SPAN and RSPAN are disabled. For more information, see Chapter 32, "Configuring SPAN and RSPAN."
- RMON is disabled. For more information, see Chapter 33, "Configuring RMON."
- Syslog messages are enabled and appear on the console. For more information, see Chapter 34, "Configuring System Message Logging and Smart Logging."
- SNMP is enabled (Version 1). For more information, see Chapter 35, "Configuring SNMP."
- No ACLs are configured. For more information, see Chapter 37, "Configuring Network Security with ACLs."
- QoS is disabled. For more information, see Chapter 38, "Configuring QoS."
- No EtherChannels are configured. For more information, see Chapter 39, "Configuring EtherChannels and Link-State Tracking."

- IP unicast routing is disabled. For more information, see Chapter 41, "Configuring IP Unicast Routing."
- IPv6 unicast routing is disabled. For more information, see Chapter 42, "Configuring IPv6 Unicast Routing."
- No HSRP groups are configured. For more information, see Chapter 45, "Configuring HSRP and VRRP."
- IP multicast routing is disabled on all interfaces. For more information, see Chapter 49, "Configuring IP Multicast Routing."
- MSDP is disabled. For more information, see Chapter 50, "Configuring MSDP."
- Fallback bridging is not configured. For more information, see Chapter 51, "Configuring Fallback Bridging."

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 1-21
- "Small to Medium-Sized Network Using Catalyst 3560 and 3560-C Switches" section on page 1-24
- "Large Network Using Catalyst 3560 Switches" section on page 1-25
- "Long-Distance, High-Bandwidth Transport Configuration" section on page 1-27

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 optional IP multicast routing to design networks better suited for multicast traffic. • 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 Hot Standby Router Protocol (HSRP) for cluster command switch and router redundancy. • 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.

Table 1-2 Providing Network Services (continued)

Network Demands	Suggested Design Methods
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** 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.

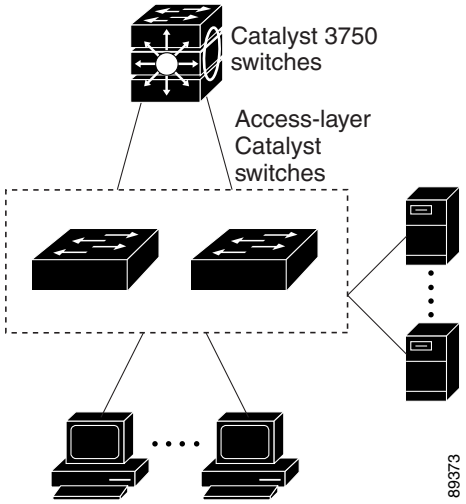
You can use the switches to create the following:

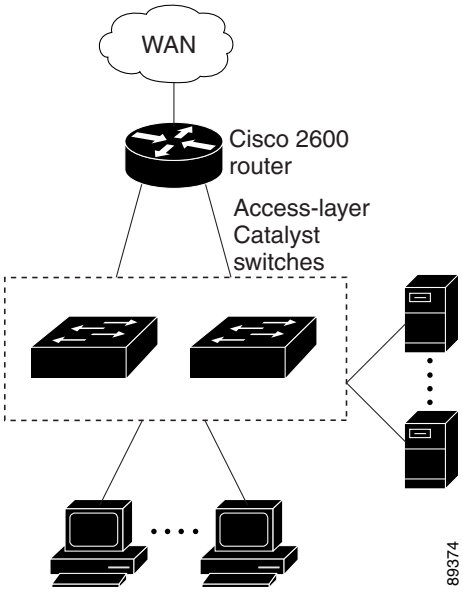
- Cost-effective Gigabit-to-the-desktop for high-performance workgroups (Figure 1-1)—For high-speed access to network resources, you can use the 3560 switches in the access layer to provide Gigabit Ethernet to the desktop. To prevent congestion, use QoS DSCP marking priorities on these switches. For 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 3560 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 3560 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)





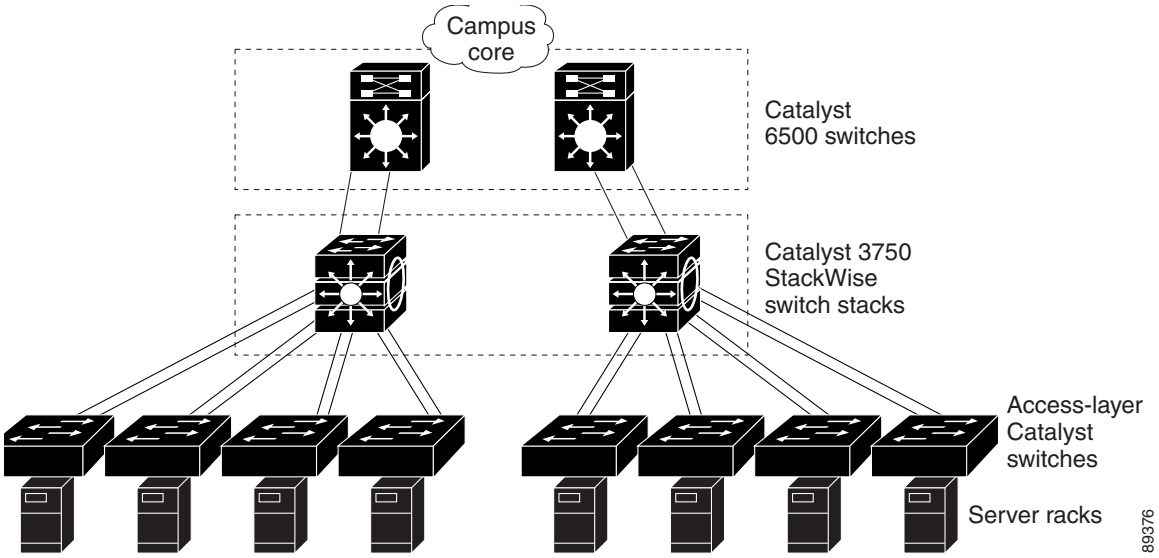
- Server aggregation (Figure 1-2)—You can use the switches to interconnect groups of servers, centralizing physical security and administration of your network. For high-speed IP forwarding at the distribution layer, connect the switches in the access layer to multilayer switches with routing capability. 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 3560 and 3560-C Switches

Figure 1-3 shows a configuration for a network of up to 500 employees. This network uses Catalyst 3560 Layer 3 switches with high-speed connections to two routers. For network reliability and load balancing, this network has HSRP enabled on the routers and on the switches. This ensures connectivity to the Internet, WAN, and mission-critical network resources if one of the routers or switches fails. The switches are using routed uplinks for faster failover. They are also configured with equal-cost routing for load sharing and redundancy.

The switches are connected to workstations, local servers, and IEEE 802.3af compliant and noncompliant powered devices (such as Cisco IP Phones). 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 switches 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 multilayer switches or 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.

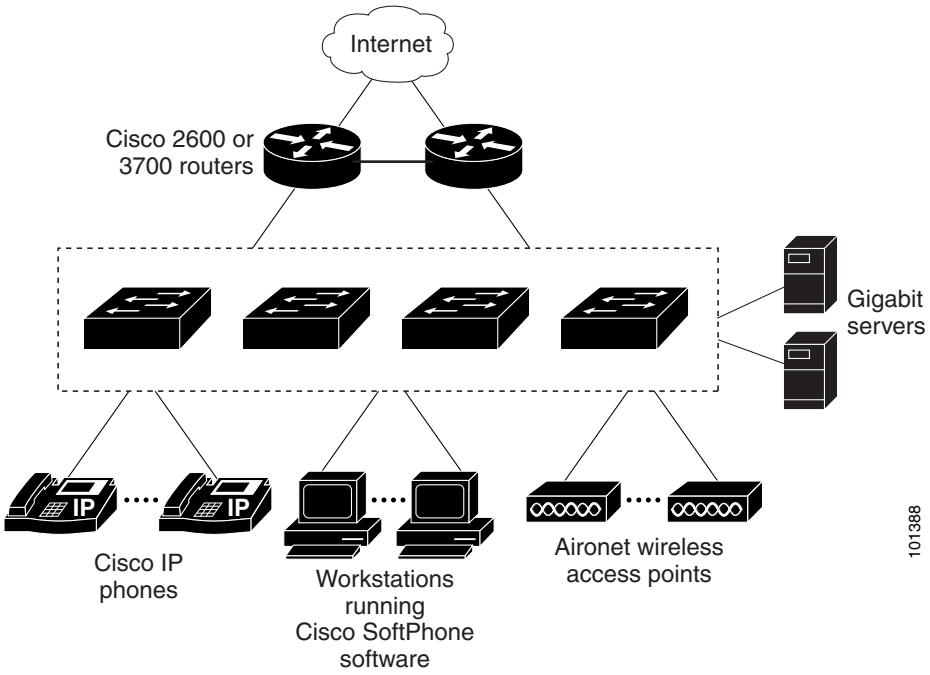
For prestandard and IEEE 802.3af-compliant powered devices connected to Catalyst PoE switches, IEEE 802.1p/Q QoS gives voice traffic forwarding-priority over data traffic.

Catalyst PoE switch ports automatically detect any Cisco pre-standard and IEEE 802.3af-compliant powered devices that are connected. Each PoE switch port provides 15.4 W of power per port. The powered device, such as a Cisco IP Phone, can receive redundant power when it is also connected to an AC power source. Powered devices not connected to Catalyst PoE switches must be connected to AC power sources to receive power.

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.

With the multilayer switches providing inter-VLAN routing and other network services, the routers focus on firewall services, Network Address Translation (NAT) services, voice-over-IP (VoIP) gateway services, and WAN and Internet access.

Figure 1-3 Collapsed Backbone Configuration



Large Network Using Catalyst 3560 Switches

Switches in the wiring closet have traditionally been only Layer 2 devices, but as network traffic profiles evolve, switches in the wiring closet are increasingly employing multilayer services such as multicast management and traffic classification. Figure 1-4 shows a configuration for a network that only use Catalyst 3560 multilayer switches in the wiring closets and two backbone switches, such as the Catalyst 6500 switches, to aggregate up to ten wiring closets.

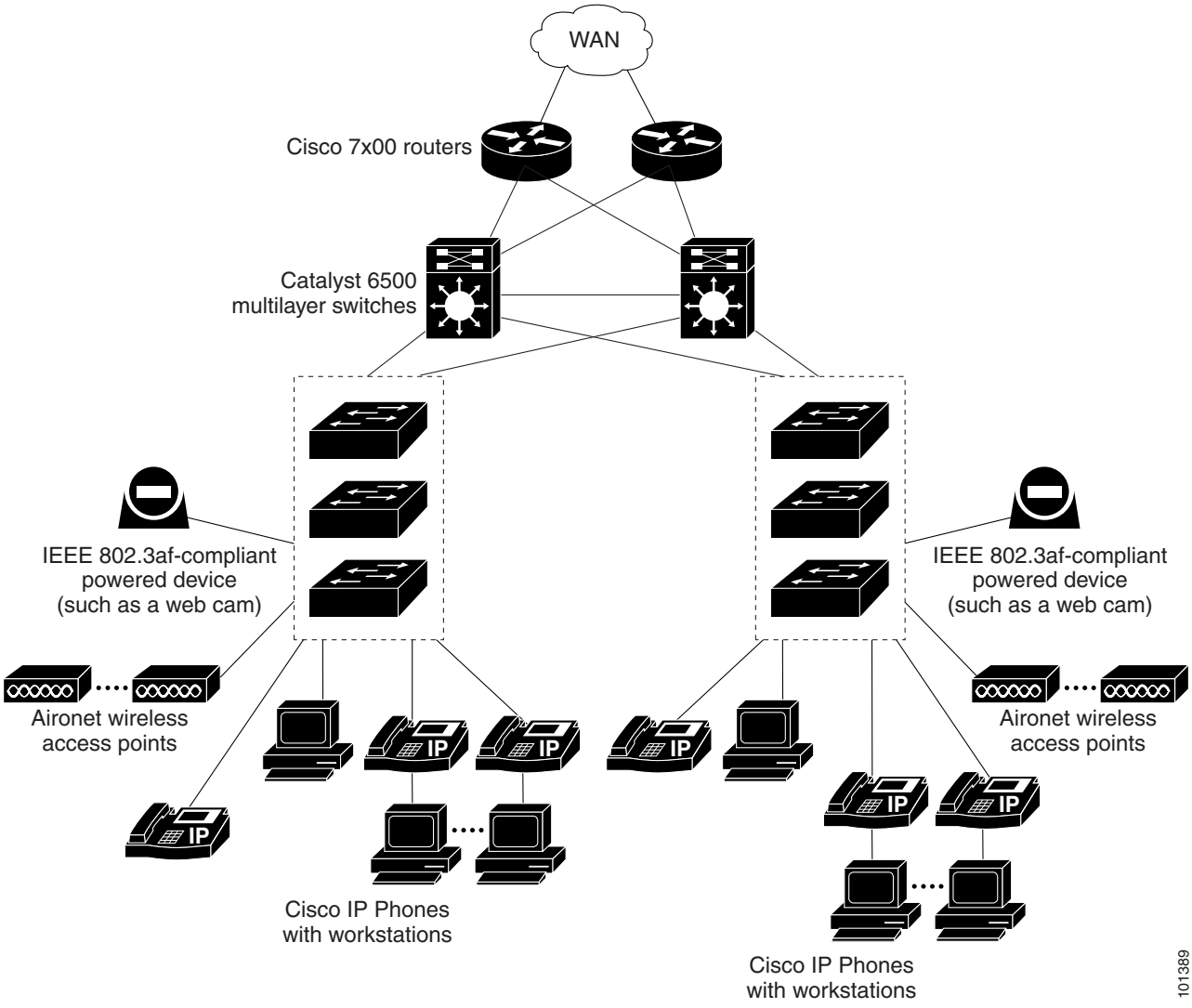
In the wiring closet, each switch has IGMP snooping enabled to efficiently forward multimedia and multicast traffic. QoS ACLs that either drop or mark nonconforming traffic based on bandwidth limits are also configured on each switch. VLAN maps provide intra-VLAN security and prevent unauthorized users from accessing critical pieces of the network. QoS features can limit bandwidth on a per-port or

per-user basis. The switch ports are configured as either trusted or untrusted. You can configure a trusted port to trust the CoS value, the DSCP value, or the IP precedence. If you configure the port as untrusted, you can use an ACL to mark the frame in accordance with the network policy.

Each switch provides inter-VLAN routing. They provide proxy ARP services to get IP and MAC address mapping, thereby removing this task from the routers and decreasing this type of traffic on the WAN links. These switches also have redundant uplink connections to the backbone switches, with each uplink port configured as a trusted routed uplink to provide faster convergence in case of an uplink failure.

The routers and backbone switches have HSRP enabled for load balancing and redundant connectivity to guarantee mission-critical traffic.

Figure 1-4 Switches in Wiring Closets in a Backbone Configuration



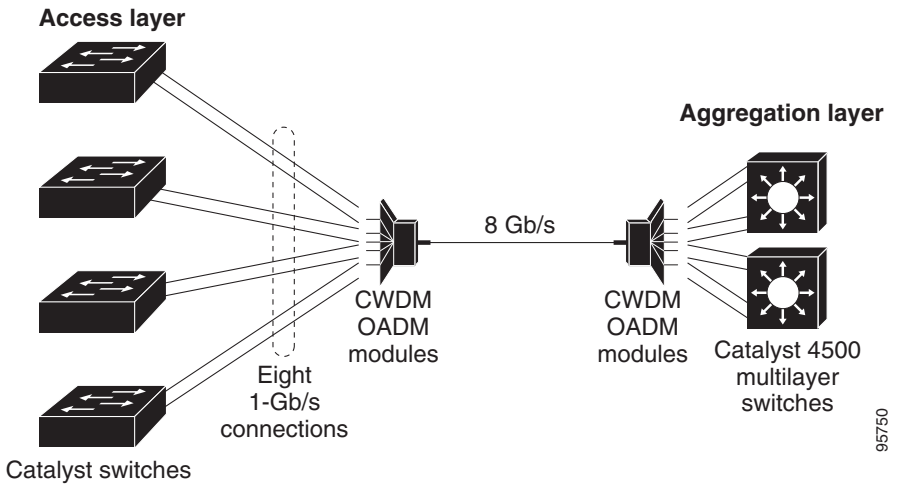
Long-Distance, High-Bandwidth Transport Configuration

Figure 1-5 shows a configuration for sending 8 Gigabits of data over a single fiber-optic cable. The Catalyst 3560 or 3560-C 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 1-5 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"

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.