CHAPTER 1

Overview

This chapter provides these topics about the switch software:

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

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

Features

Beginning with Cisco IOS Release 12.2(44)SE, the switch ships with the IP base image installed, which provides Layer 2+ features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), static routing, EIGRP and PIM stub routing, the Hot Standby Router Protocol (HSRP), the Routing Information Protocol (RIP), IPv6 host management, and IPv6 MLD snooping.

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

The switch has these features:

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

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

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

Performance Features

The switch ships with these performance features:

- Cisco EnergyWise manages the energy usage of power over Ethernet (PoE) entities

  For more information, see the *Cisco EnergyWise Version 2 Configuration Guide* on Cisco.com.
- 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 10/100/1000 Mb/s 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
- 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) 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
- 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 efficiently forwarding multimedia and multicast 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
- IGMP helper to allow the switch to forward a host request to join a multicast stream to a specific IP destination address
- Multicast Listener Discovery (MLD) snooping to enable efficient distribution of IP Version 6 (IPv6) multicast data to clients and routers in a switched network.
- 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
- Cisco IOS IP Service Level Agreements (SLAs), a part of Cisco IOS software that uses active traffic monitoring for measuring network performance
- 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)
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group
- 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.
- Multicast VLAN registration (MVR) enhancements include the ability to configure 2000 MVR groups when the switch is in dynamic MVR mode and a new command (**mvr ringmode flood**) to ensure that forwarding in a ring topology is limited to member ports.

Management Options

These are the options for configuring and managing the switch:

- An embedded device manager—The device manager is a GUI that is integrated in the software image. You use it to configure and to monitor a single switch. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the switch online help.
- CLI—The Cisco IOS software supports desktop- and multilayer-switching features. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station. For more information about the CLI, see Chapter 2, “Using the Command-Line Interface.”
- SNMP—SNMP management applications such as iscoWorks2000 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 31, “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, see Chapter 4, "Configuring Cisco IOS Configuration Engine."

Note For additional descriptions of the management interfaces, see the "Design Concepts for Using the Switch" section on page 1-14.

- FastEthernet 0 (fa0)—This interface is an internal connection to the HP Onboard Administrator that is only used for switch management traffic, not for data traffic. This interface is connected to the Onboard Administrator through the blade server backplane connector.

  For more information about the HP Onboard Administrator, see the HP c-Class BladeSystem documentation at http://www.hp.com/go/bladesystem/documentation.

Manageability Features

These are the manageability features:

- CNS embedded agents for automating switch management, configuration storage, and delivery
- DHCP for automating configuration of switch information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)
- DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients
- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts
- DHCP-based autoconfiguration and image update to download a specified configuration a new image to a large number of switches
- DHCP server port-based address allocation for the preassignment of an IP address to a switch port
- Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding hostname and to a TFTP server for administering software upgrades from a TFTP server
- Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding MAC address
- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses
- Disabling MAC address learning on a VLAN
- 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

- 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
- Wired location service sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE)
- Network Time Protocol (NTP) for providing a consistent time stamp to all switches from an external source
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch uses
- Configuration logging to log and to view changes to the switch configuration
- Unique device identifier to provide product identification information through a **show inventory** user EXEC command display
- In-band management access through the device manager over a Netscape Navigator or Microsoft Internet Explorer browser session
- In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic version of the software)
- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests
- Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem
- CPU utilization threshold trap monitors CPU utilization
- The internal Ethernet interface fa0, a Layer 3 interface that you can communicate with only through the HP Onboard Administrator
- 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)
- The HTTP client in Cisco IOS supports can send requests to both IPv4 and IPv6 HTTP servers, 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 supports stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses.
- 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.

Availability and Redundancy Features

These are the availability and redundancy features:

- HSRP for command switch and Layer 3 router redundancy
- 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 (Layer 2 trunk failover) to mirror the state of the external Ethernet links and to allow the failover of the processor blade traffic to an operational external link on a separate Cisco Ethernet switch

VLAN Features

These are the 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.
- 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.
- 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
- 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

The switch ships with these security features:

- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring
- Web authentication to allow a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser
- MAC authentication bypass (MAB) aging timer to detect inactive hosts that have authenticated after they have authenticated by using MAB
- Local web authentication banner so that custom banner or image file can be displayed at a web authentication login screen
- Password-protected access (read-only and read-write access) to management interfaces (device manager 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 shut down the VLAN on the port when a violation occurs, instead of shutting down the entire port.
- 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
- Port security aging to set the aging time for secure addresses on a port
- BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs

- Standard and extended IP access control lists (ACLs) for defining 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
- 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 with open access to allow a host to access the network before being authenticated
- Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host
- IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:
  - VLAN assignment for restricting IEEE 802.1x-authenticated users to a specified VLAN
  - Port security for controlling access to IEEE 802.1x ports
  - Voice VLAN to permit a Cisco IP Phone to access the voice VLAN regardless of the authorized or unauthorized state of the port
  - Guest VLAN to provide limited services to non-IEEE 802.1x-compliant users
  - Restricted VLAN to provide limited services to users who are IEEE 802.1x compliant, but do not have the credentials to authenticate via the standard IEEE 802.1x processes
  - IEEE 802.1x accounting to track network usage
  - IEEE 802.1x with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame
  - IEEE 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch
  - Voice aware IEEE 802.1x security to apply traffic violation actions only on the VLAN on which a security violation occurs
  - Voice aware IEEE 802.1x security to apply traffic violation actions only on the VLAN on which a security violation occurs
  - 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 authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch
  - Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port
- MAC authentication bypass to authorize clients based on the client MAC address
- Network Admission Control (NAC) features:
  - NAC Layer 2 IEEE 802.1x validation of the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access.

    For information about configuring NAC Layer 2 IEEE 802.1x validation, see the "Configuring NAC Layer 2 802.1x Validation" section on page 8-52.
  - 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 the Inaccessible Authentication Bypass Feature" section on page 8-47.
  - 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
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services
- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic version 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)
- 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

These are the QoS and CoS features:

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

Layer 3 Features

These are the Layer 3 features:

- 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, including RIP Versions 1 and 2
- 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
- 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
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients
- IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router
- IPv6 unicast host management
- The ability to exclude a port in a VLAN from the SVI line-state up or down calculation

Monitoring Features

These are the monitoring features:

- Switch LEDs that provide port- and switch-level status
- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the switch has learned or removed
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN (except for the fa0 interface)
- 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 10/100/1000 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.

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. The fa0 interface might receive an IP Address from the DHCP server. For more information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway,” and Chapter 21, “Configuring DHCP Features and IP Source Guard.”
- 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 21, “Configuring DHCP Features and IP Source Guard.”
- No passwords are defined. For more information, see Chapter 5, “Administering the Switch.”
- System name and prompt is *Switch.* For more information, see Chapter 5, “Administering the Switch.”
- NTP is enabled. For more information, see Chapter 5, “Administering the Switch.”
- DNS is enabled. For more information, see Chapter 5, “Administering the Switch.”
- TACACS+ is disabled. For more information, see Chapter 7, “Configuring Switch-Based Authentication.”
- RADIUS is disabled. For more information, see Chapter 7, “Configuring Switch-Based Authentication.”

- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see Chapter 7, "Configuring Switch-Based Authentication."
- IEEE 802.1x is disabled. For more information, see Chapter 8, "Configuring IEEE 802.1x Port-Based Authentication."
- Port parameters
  - Operating mode is Layer 2 (switchport). For more information, see Chapter 10, "Configuring Interface Characteristics."
  - Interface speed and duplex mode is autonegotiate. For more information, see Chapter 10, "Configuring Interface Characteristics."
  - Auto-MDIX is enabled. For more information, see Chapter 10, "Configuring Interface Characteristics."
  - Flow control is off. For more information, see Chapter 10, "Configuring Interface Characteristics."
  - PortFast is enabled on the sixteen internal Gigabit Ethernet ports. For more information, see Chapter 19, "Configuring Optional Spanning-Tree Features."
- No Smartports macros are defined. For more information, see Chapter 11, "Configuring Smartports Macros."
- VLANs
  - Default VLAN is VLAN 1. For more information, see Chapter 12, "Configuring VLANs."
  - VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 12, "Configuring VLANs."
  - Trunk encapsulation is negotiate. For more information, see Chapter 12, "Configuring VLANs."
  - VTP mode is server. For more information, see Chapter 13, "Configuring VTP."
  - VTP version is Version 1. For more information, see Chapter 13, "Configuring VTP."
  - No private VLANs are configured. For more information, see Chapter 15, "Configuring Private VLANs."
  - Voice VLAN is disabled. For more information, see Chapter 14, "Configuring Voice VLAN."
- IEEE 802.1Q tunneling and Layer 2 protocol tunneling are disabled. For more information, see Chapter 16, "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling."
- STP, PVST+ is enabled on VLAN 1. For more information, see Chapter 17, "Configuring STP."
- MSTP is disabled. For more information, see Chapter 18, "Configuring MSTP."
- Optional spanning-tree features are disabled. For more information, see Chapter 19, "Configuring Optional Spanning-Tree Features."
- Flex Links are not configured. For more information, see Chapter 20, "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 21, "Configuring DHCP Features and IP Source Guard."
- IP source guard is disabled. For more information, see Chapter 21, "Configuring DHCP Features and IP Source Guard."
- Dynamic ARP inspection is disabled on all VLANs. For more information, see Chapter 22, "Configuring Dynamic ARP Inspection."
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see Chapter 23, "Configuring IGMP Snooping and MVR."

- IGMP throttling setting is deny. For more information, see Chapter 23, “Configuring IGMP Snooping and MVR.”
- The IGMP snooping querier feature is disabled. For more information, see Chapter 23, “Configuring IGMP Snooping and MVR.”
- MVR is disabled. For more information, see Chapter 23, “Configuring IGMP Snooping and MVR.”
- Port-based traffic
  - Broadcast, multicast, and unicast storm control is disabled. For more information, see Chapter 24, “Configuring Port-Based Traffic Control.”
  - No protected ports are defined. For more information, see Chapter 24, “Configuring Port-Based Traffic Control.”
  - Unicast and multicast traffic flooding is not blocked. For more information, see Chapter 24, “Configuring Port-Based Traffic Control.”
  - No secure ports are configured. For more information, see Chapter 24, “Configuring Port-Based Traffic Control.”
- CDP is enabled. For more information, see Chapter 25, “Configuring CDP.”
- UDLD is disabled. For more information, see Chapter 27, “Configuring UDLD.”
- SPAN and RSPAN are disabled. For more information, see Chapter 28, “Configuring SPAN and RSPAN.”
- RMON is disabled. For more information, see Chapter 29, “Configuring RMON.”
- Syslog messages are enabled and appear on the console. For more information, see Chapter 30, “Configuring System Message Logging.”
- SNMP is enabled (Version 1). For more information, see Chapter 31, “Configuring SNMP.”
- No ACLs are configured. For more information, see Chapter 32, “Configuring Network Security with ACLs.”
- QoS is disabled. For more information, see Chapter 33, “Configuring QoS.”
- No EtherChannels are configured. For more information, see Chapter 34, “Configuring EtherChannels and Layer 2 Trunk Failover.”
- IP unicast routing is disabled. For more information, see Chapter 35, “Configuring IP Unicast Routing.”
- No HSRP groups are configured. For more information, see Chapter 39, “Configuring HSRP and Enhanced Object Tracking.”

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 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.
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.

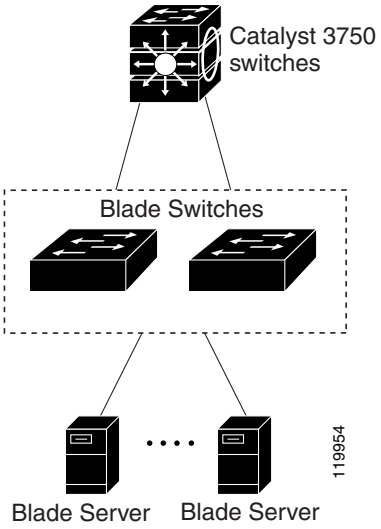
You can use the switches to create the following:

- Cost-effective Gigabit-to-the-blade server for high-performance workgroups (Figure 1-1)—For high-speed access to network resources, you can use the Cisco Catalyst Blade Switch 3020 for HP in the access layer to provide Gigabit Ethernet to the blade servers. 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 blade switches are connected to Catalyst 3750 switches in the distribution layer.

  Each blade 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-Blade Server)



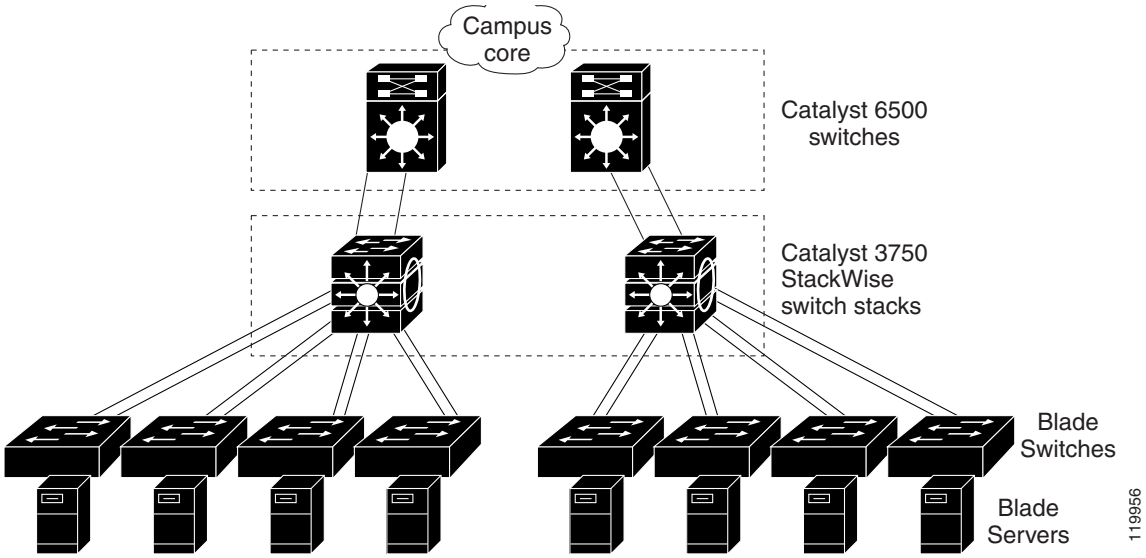
- Server aggregation (Figure 1-2)—You can use the switches to interconnect groups of servers, centralizing physical security and administration of your network. For high-speed IP forwarding at the distribution layer, connect the switches in the access layer to multilayer switches with routing capability.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

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

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

  Using dual SFP module uplinks from the blade 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



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"