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).

Features

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

The switch has these features:

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:

- 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 Mbps interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately
- Support for up to 9000 bytes for frames that are bridged in hardware and up to 2000 bytes for frames that are bridged by software
- IEEE 802.3x flow control on all ports (the switch does not send pause frames)
- EtherChannel for enhanced fault tolerance and for providing up to 8 Gbps (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 packets at Gigabit line rate
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic
- Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3 for efficiently forwarding multimedia and multicast traffic
- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)
- IGMP snooping querier support to configure switch to generate periodic IGMP General Query messages
- 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

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 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 25, "Configuring SNMP."
- IE2100—Cisco Intelligence Engine 2100 Series Configuration Registrar is a network management device that works with embedded Cisco Networking Services (CNS) agents in the switch software. 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 IE2100, see Chapter 4, "Configuring Cisco IOS CNS Agents."
- 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:

- Cisco IE2100 Series 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
- 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

- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network
- 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
- The internal Ethernet interface fa0, a Layer 3 interface that you can communicate with only through the HP Onboard Administrator

Note For additional descriptions of the management interfaces, see the "Design Concepts for Using the Switch" section on page 1-10.

Availability and Redundancy Features

These are the availability and redundancy features:

- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
- IEEE 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:
  - Up to 128 spanning-tree instances supported
  - Per-VLAN spanning-tree plus (PVST+) for load balancing across VLANs
  - Rapid PVST+ for load balancing across VLANs and providing rapid convergence of spanning-tree instances
  - UplinkFast and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately changing root and designated ports to the forwarding state

- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:
  - Port Fast for eliminating the forwarding delay by enabling a port to immediately change from the blocking state to the forwarding state
  - BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)
  - BPDU filtering for preventing a Port Fast-enabled port from sending or receiving BPDUs
  - Root guard for preventing switches outside the network core from becoming the spanning-tree root
  - Loop guard for preventing alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link
- Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy
- 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 1024 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.

Security Features

The switch ships with these security features:

- Web authentication to allow a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser.
- 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
- Port security aging to set the aging time for secure addresses on a port
- BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs
- Standard and extended IP access control lists (ACLs) for defining inbound security policies on Layer 2 interfaces (port ACLs)
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces
- 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
- 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
- MAC authentication bypass to authorize clients based on the client MAC address.
- 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)

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.

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

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 17, “Configuring DHCP Features.”
- Default domain name is not configured. For more information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway.”
- DHCP client is enabled, the DHCP server is enabled (only if the device acting as a DHCP server is configured and is enabled), and the DHCP relay agent is enabled (only if the device is acting as a DHCP relay agent is configured and is enabled). For more information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway,” and Chapter 17, “Configuring DHCP Features.”
- 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 6, "Configuring Switch-Based Authentication."
- RADIUS is disabled. For more information, see Chapter 6, "Configuring Switch-Based Authentication."
- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see Chapter 6, "Configuring Switch-Based Authentication."
- IEEE 802.1x is disabled. For more information, see Chapter 7, "Configuring IEEE 802.1x Port-Based Authentication."
- Port parameters
  - Interface speed and duplex mode is autonegotiate. For more information, see Chapter 8, "Configuring Interface Characteristics."
  - Auto-MDIX is enabled. For more information, see Chapter 8, "Configuring Interface Characteristics."
  - Flow control is off. For more information, see Chapter 8, "Configuring Interface Characteristics."
  - PortFast is enabled on the sixteen internal Gigabit Ethernet ports. For more information, see Chapter 15, "Configuring Optional Spanning-Tree Features."
- No Smartports macros are defined. For more information, see Chapter 9, "Configuring Smartports Macros."
- VLANs
  - Default VLAN is VLAN 1. For more information, see Chapter 10, "Configuring VLANs."
  - VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 10, "Configuring VLANs."
  - Trunk encapsulation is negotiate. For more information, see Chapter 10, "Configuring VLANs."
  - VTP mode is server. For more information, see Chapter 11, "Configuring VTP."
  - VTP version is Version 1. For more information, see Chapter 11, "Configuring VTP."
  - Voice VLAN is disabled. For more information, see Chapter 12, "Configuring Voice VLAN."
- STP, PVST+ is enabled on VLAN 1. For more information, see Chapter 13, "Configuring STP."
- MSTP is disabled. For more information, see Chapter 14, "Configuring MSTP."
- Optional spanning-tree features are disabled. For more information, see Chapter 15, "Configuring Optional Spanning-Tree Features."
- Flex Links are not configured. For more information, see Chapter 16, "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 17, "Configuring DHCP Features."
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see Chapter 18, "Configuring IGMP Snooping and MVR."
- IGMP throttling setting is deny. For more information, see Chapter 18, "Configuring IGMP Snooping and MVR."

- The IGMP snooping querier feature is disabled. For more information, see Chapter 18, "Configuring IGMP Snooping and MVR."
- MVR is disabled. For more information, see Chapter 18, "Configuring IGMP Snooping and MVR."
- Port-based traffic
  - Broadcast, multicast, and unicast storm control is disabled. For more information, see Chapter 19, "Configuring Port-Based Traffic Control."
  - No protected ports are defined. For more information, see Chapter 19, "Configuring Port-Based Traffic Control."
  - Unicast and multicast traffic flooding is not blocked. For more information, see Chapter 19, "Configuring Port-Based Traffic Control."
  - No secure ports are configured. For more information, see Chapter 19, "Configuring Port-Based Traffic Control."
- CDP is enabled. For more information, see Chapter 20, "Configuring CDP."
- UDLD is disabled. For more information, see Chapter 21, "Configuring UDLD."
- SPAN and RSPAN are disabled. For more information, see Chapter 22, "Configuring SPAN and RSPAN."
- RMON is disabled. For more information, see Chapter 23, "Configuring RMON."
- Syslog messages are enabled and appear on the console. For more information, see Chapter 24, "Configuring System Message Logging."
- SNMP is enabled (Version 1). For more information, see Chapter 25, "Configuring SNMP."
- No ACLs are configured. For more information, see Chapter 26, "Configuring Network Security with ACLs."
- QoS is disabled. For more information, see Chapter 27, "Configuring QoS."
- No EtherChannels are configured. For more information, see Chapter 28, "Configuring EtherChannels and Layer 2 Trunk Failover."

Design Concepts for Using the Switch

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

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

Table 1-1 Increasing Network Performance

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

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

Table 1-2 Providing Network Services

Network Demands	Suggested Design Methods
Efficient bandwidth usage for multimedia applications and guaranteed bandwidth for critical applications	• Use IGMP snooping to efficiently forward multimedia and multicast traffic. • Use other QoS mechanisms such as packet classification, marking, scheduling, and congestion avoidance to classify traffic with the appropriate priority level, thereby providing maximum flexibility and support for mission-critical, unicast, and multicast and multimedia applications. • Use MVR to continuously send multicast streams in a multicast VLAN but to isolate the streams from subscriber VLANs for bandwidth and security reasons.
High demand on network redundancy and availability to provide *always on* mission-critical applications	• Use VLAN trunks and BackboneFast for traffic-load balancing on the uplink ports so that the uplink port with a lower relative port cost is selected to carry the VLAN traffic.
An evolving demand for IP telephony	• Use QoS to prioritize applications such as IP telephony during congestion and to help control both delay and jitter within the network. • Use switches that support at least two queues per port to prioritize voice and data traffic as either high- or low-priority, based on IEEE 802.1p/Q. The switch supports at least four queues per port. • Use voice VLAN IDs (VVIDs) to provide separate VLANs for voice traffic.

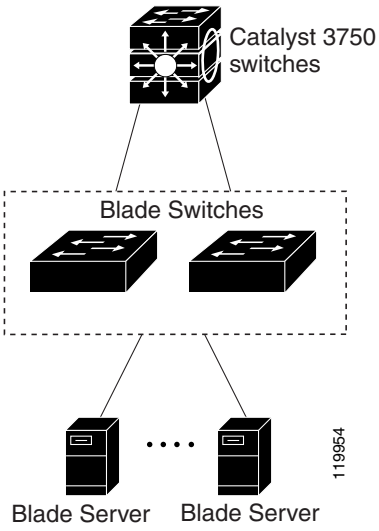
You can use the switches to create the following:

- 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-Gbps 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)



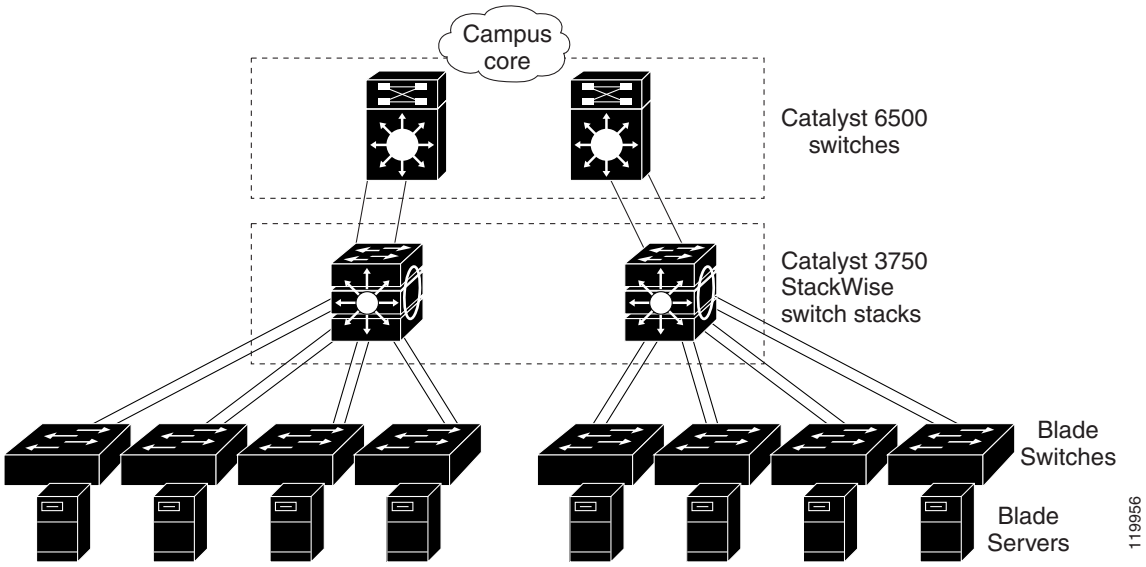
- Server aggregation (Figure 1-2)—You can use the switches to interconnect groups of servers, centralizing physical security and administration of your network. For high-speed IP forwarding at the distribution layer, connect the switches in the access layer to multilayer switches with routing capability.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