CHAPTER 1

Overview

This chapter provides these topics about the Catalyst 2350 switch software:

In this document, *IP* refers to IP Version 4 (IPv4).

Features

The switch supports either the cryptographic (supports encryption) or the noncryptographic software image.

Some features described in this chapter are only available on the cryptographic software image. You must obtain authorization to use these features and to download the cryptographic software from Cisco.com. For more information, see the release notes for this release.

The switch supports the IP base feature set, which provides Layer 2+ features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), and basic IPv6 management.

The switch has these features:

Deployment Features

The switch ships with these 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.
- An embedded device manager GUI for configuring and monitoring a single switch through a web browser. For information about starting the device manager, see the getting started guide. For more information about the device manager, see the switch online help.
- Cisco Network Assistant (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.
  - 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 video 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 colors of the system LED and system and port LEDs on the images are similar to those used on the physical LEDs.
- 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, Gigabit Ethernet, Gigabit EtherChannel, 10-Gigabit Ethernet, and 10-Gigabit EtherChannel connections. For a list of cluster-capable switches, see the release notes.
  - Automatic discovery of candidate switches and creation of clusters of up to 16 switches that can be managed through a single IP address.
  - Extended discovery of cluster candidates that are not directly connected to the command switch.

Performance Features

The switch ships with these performance features:

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports for optimizing bandwidth
- Automatic-medium-dependent interface crossover (auto-MDIX) capability on 10/100/1000-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 9216 bytes [the maximum packet size or maximum transmission unit (MTU) size] for frames that are bridged in hardware and software through Gigabit Ethernet ports and 10-Gigabit Ethernet ports
- 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 80 Gb/s (10-Gigabit EtherChannel) full-duplex bandwidth among switches, routers, and servers
- Port Aggregation Protocol (PAgP) for automatic creation of EtherChannel links
- Forwarding of Layer 2 packets at Gigabit line rate
- Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3. For IGMP devices, IGMP snooping for efficiently forwarding multimedia and multicast traffic
- IGMP snooping querier support to configure switch to generate periodic IGMP General Query messages
- IIGMP Helper to allow the switch to forward a host request to join a multicast stream to a specific IP destination address
- 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
- 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)

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 starting 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 or a PC 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 23, "Configuring SNMP."

Manageability Features

These are the manageability features:

- 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
- 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
- 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
- Disabling MAC address learning on a VLAN
- 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
- Support for the LLDP-MED location TLV that provides location information from the switch to the endpoint device
- Network Time Protocol (NTP) for providing a consistent time stamp to all switches from an external source
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch uses
- Configuration logging to log and to view changes to the switch configuration
- Configuration replacement and rollback to replace the running configuration on a switch with any saved Cisco IOS configuration file
- 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 software image)
- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests
- Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem
- Out-of-band management access through the Ethernet management port to a PC
- Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying switch configuration or switch image files (requires the cryptographic software image)
- DHCP-based autoconfiguration and image update to download a specified configuration a new image to a large number of switches
- 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
- IPv6 supports stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses.

Note For additional descriptions of the management interfaces, see the "Network Configuration Examples" 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
- 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

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
- IEEE 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
- Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (IEEE 802.1Q) to be used
- VLAN Trunking Protocol (VTP) and VTP pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic
- 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:

- 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
- BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces
- 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 AAA services

- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic software image)
- 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 software image)

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–both IPv4) within a QoS domain and with a port bordering another QoS domain
  - Trusted boundary for detecting the presence of a Cisco IP Phone and for trusting the CoS value received
- 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 on the switches
- 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
- Online diagnostics to test the hardware functionality of the supervisor engine, modules, and switch while the switch is connected to a live network

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 14, “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 14, "Configuring DHCP Features."
- Switch cluster is disabled. For more information about switch clusters, see Chapter 4, "Clustering Switches," and the *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- 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."
- Port parameters
  - Operating mode is Layer 2 (switchport). For more information, see Chapter 8, "Configuring Interface Characteristics."
  - 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."
- VLANs
  - Default VLAN is VLAN 1. For more information, see Chapter 9, "Configuring VLANs."
  - VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 9, "Configuring VLANs."
  - Trunk encapsulation is negotiate. For more information, see Chapter 9, "Configuring VLANs."
  - VTP mode is server. For more information, see Chapter 10, "Configuring VTP."
  - VTP version is Version 1. For more information, see Chapter 10, "Configuring VTP."
- STP, PVST+ is enabled on VLAN 1. For more information, see Chapter 11, "Configuring STP."
- MSTP is disabled. For more information, see Chapter 12, "Configuring MSTP."
- Optional spanning-tree features are disabled. For more information, see Chapter 13, "Configuring Optional Spanning-Tree Features."
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see Chapter 15, "Configuring IGMP Snooping."
- IGMP throttling setting is deny. For more information, see Chapter 15, "Configuring IGMP Snooping."
- The IGMP snooping querier feature is disabled. For more information, see Chapter 15, "Configuring IGMP Snooping."

- CDP is enabled. For more information, see Chapter 17, "Configuring CDP."
- UDLD is disabled. For more information, see Chapter 19, "Configuring UDLD."
- SPAN and RSPAN are disabled. For more information, see Chapter 20, "Configuring SPAN and RSPAN."
- RMON is disabled. For more information, see Chapter 21, "Configuring RMON."
- Syslog messages are enabled and appear on the console. For more information, see Chapter 22, "Configuring System Message Logging."
- SNMP is enabled (Version 1). For more information, see Chapter 23, "Configuring SNMP."
- QoS is disabled. For more information, see Chapter 25, "Configuring QoS."
- No EtherChannels are configured. For more information, see Chapter 26, "Configuring EtherChannels and Link-State Tracking."

Network Configuration Examples

The "Design Concepts for Using the Switch" section on page 1-10 provides network configuration concepts and includes examples of using the switch to create dedicated network segments and interconnecting the segments through Gigabit Ethernet and 10-Gigabit Ethernet connections.

Design Concepts for Using the Switch

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

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

Table 1-1 Increasing Network Performance

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

Bandwidth alone is not the only consideration when designing your network. As your network traffic profiles evolve, consider providing network services that can support applications for 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.
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.
A growing demand for using existing infrastructure to transport data 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 2950 LRE switch. See the documentation sets specific to this switch for LRE information.

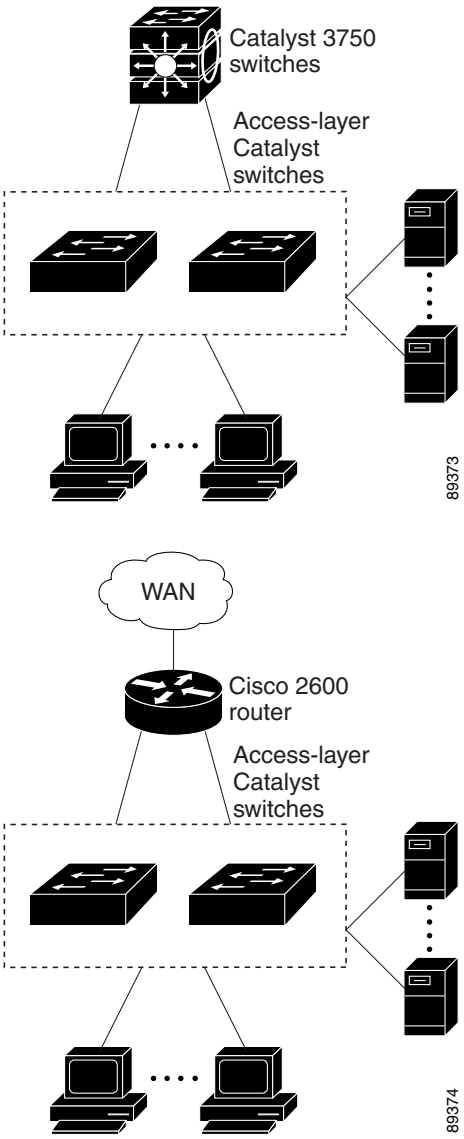
You can use the switches to create the following:

- High-performance wiring closet—For high-speed access to network resources, you can use the switches in the access layer to provide Gigabit Ethernet access 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 in the backbone, such as a Catalyst 4500 Gigabit switch or Catalyst 6500 Gigabit switch.
- Cost-effective Gigabit-to-the-desktop (GTD) access for high-performance workgroups—For high-speed access to network resources, you can use the 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 in Figure 1-1 is of an isolated high-performance workgroup, where the switches are connected to Catalyst 3750 switches in the distribution layer. The second illustration is of a high-performance workgroup in the branch office, where the 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)



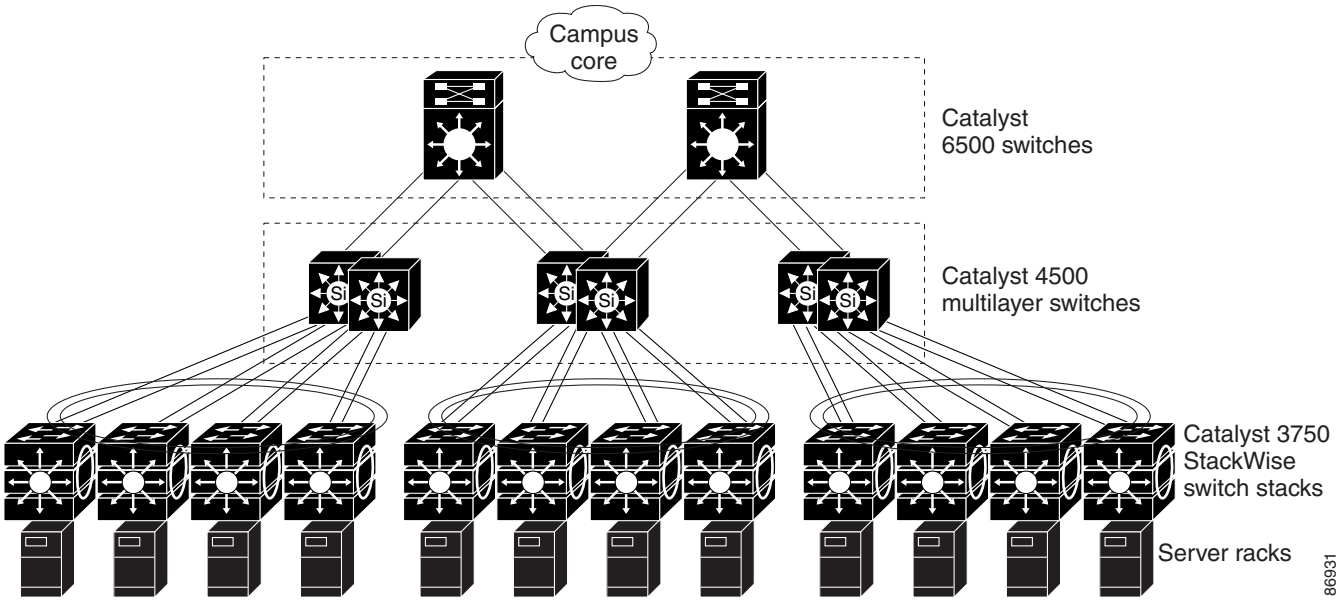
- Server aggregation (Figure 1-2)—You can use the switches and Catalyst 3750 switch stacks to interconnect groups of servers, centralizing physical security and administration of your network. For high-speed IP forwarding at the distribution layer, connect the switches in the access layer to multilayer 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 the 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



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"