Overview

This chapter provides these topics about the Catalyst 3750 switch software:

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

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

Features

The switch ships with either of these software images installed:

- IP base image (formerly known as the standard multilayer image [SMI]), which provides Layer 2+ features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), static routing, EIGRP stub routing, the Hot Standby Router Protocol (HSRP), and the Routing Information Protocol (RIP). Switches with the IP base image installed can be upgraded to IP services image (formerly known as the enhanced multilayer image [EMI].)

- IP services image, which provides a richer set of enterprise-class intelligent services. It includes all IP base image features plus full Layer 3 routing (IP unicast routing, IP multicast routing, and fallback bridging). To distinguish it from the Layer 2+ static routing and RIP, the IP services image includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and the Open Shortest Path First (OSPF) Protocol.

  IP services image-only Layer 3 features are described in the "Layer 3 Features" section on page 1-11.

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

IPv6 Multicast Listener Discovery (MLD) snooping is supported in all Catalyst 3560 and 3750 images; for more information, see Chapter 37, "Configuring IPv6 MLD Snooping." For full IPv6 support, including IPv6 routing and access control lists (ACLs), the advanced IP services image is required; upgrade licenses for this image can be ordered from Cisco. For more information on IPv6 routing, see Chapter 36, "Configuring IPv6 Unicast Routing." For more information on IPv6 ACLs, see Chapter 38, "Configuring IPv6 ACLs."

Some features described in this chapter are available only on the cryptographic (supports encryption) versions of the software IP base and IP services images. 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, page 1-2

- Performance Features, page 1-4

- Management Options, page 1-5

- Manageability Features, page 1-5 (includes a feature requiring the cryptographic versions of the software IP base and IP services images)

- Availability and Redundancy Features, page 1-6

- VLAN Features, page 1-7

- Security Features, page 1-8 (includes a feature requiring the cryptographic versions of the software IP base and IP services images)

- QoS and CoS Features, page 1-9

- Layer 3 Features, page 1-11 (includes features requiring the IP services image)

- Power over Ethernet Features, page 1-12

- Monitoring Features, page 1-12

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.

- User-defined and Cisco-default Smartports macros for creating custom switch configurations for simplified deployment across the network.

- An embedded device manager GUI for configuring and monitoring a single switch through a web browser. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the switch online help.

- Cisco Network Assistant (hereafter referred to as *Network Assistant*) for

  - Managing communities, which are device groups like clusters, except that they can contain routers and access points and can be made more secure.

  - Simplifying and minimizing switch, switch stack, and switch cluster management from anywhere in your intranet.

- 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 system, redundant power system (RPS), and port LED colors on the images are similar to those used on the physical LEDs.

- Cisco StackWise technology for

  - Connecting up to nine switches through their StackWise ports and operating as a single switch or switch-router in the network.

  - Creating a bidirectional 32-Gbps switching fabric across the switch stack, where all stack members have full access to the system bandwidth.

  - Using a single IP address and configuration file to manage the entire switch stack.

  - Automatic Cisco IOS version-check of new stack members with the option to automatically load images from the stack master or from a TFTP server.

  - Adding, removing, and replacing switches in the stack without disrupting the operation of the stack.

  - Provisioning a new member for a switch stack with the offline configuration feature. You can configure in advance the interface configuration for a specific stack member number and for a specific switch type of a new switch that is not part of the stack. The switch stack retains this information across stack reloads whether or not the provisioned switch is part of the stack.

  - Displaying stack-ring activity statistics (the number of frames sent by each stack member to the ring).

- Switch clustering technology for

  - Unified configuration, monitoring, authentication, and software upgrade of multiple, cluster-capable switches, regardless of their geographic proximity and interconnection media, including Ethernet, Fast Ethernet, Fast EtherChannel, small form-factor pluggable (SFP) modules, Gigabit Ethernet, and Gigabit EtherChannel connections. For a list of cluster-capable switches, see the release notes.

  - Automatic discovery of candidate switches and creation of clusters of up to 16 switches that can be managed through a single IP address.

  - Extended discovery of cluster candidates that are not directly connected to the command switch.

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 and 10/100/1000 Mbps interfaces and on 10/100/1000 BASE-TX SFP module interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately

- Support for up to 1546 bytes routed frames, up to 9000 bytes for frames that are bridged in hardware and up to 2000 bytes for frames that are bridged by software

- IEEE 802.3x flow control on all ports (the switch does not send pause frames)

- Up to 32 Gbps of forwarding rates in a switch stack

- EtherChannel for enhanced fault tolerance and for providing up to 8 Gbps (Gigabit EtherChannel) or 800 Mbps (Fast EtherChannel) full-duplex bandwidth among switches, routers, and servers

- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links

- Forwarding of Layer 2 and Layer 3 packets at Gigabit line rate across the switches in the stack

- 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

- 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 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

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.

- 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 either by connecting your management station directly to the switch console port or by using Telnet from a remote management station. You can manage the switch stack by connecting to the console port of any stack member. 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 31, "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."

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 versions of the software IP base and IP services images)

- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests

- Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem

- Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying switch configuration or switch image files (requires the cryptographic versions of the software IP base and IP services images)

> **Note**   For additional descriptions of the management interfaces, see the "This section provides network configuration concepts and includes examples of using the switch to create dedicated network segments and interconnecting the segments through Fast Ethernet and Gigabit Ethernet connections." section on page 1-15.

Availability and Redundancy Features

These are the availability and redundancy features:

- HSRP for command switch and Layer 3 router redundancy

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

    The newly elected stack master begins accepting Layer 2 traffic in less than 1 second and Layer 3 traffic between 3 to 5 seconds.

- Cross-stack EtherChannel for providing redundant links across the switch stack

- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults

- IEEE 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:

    – Up to 128 spanning-tree instances supported

    – Per-VLAN spanning-tree plus (PVST+) for load balancing across VLANs

- Rapid PVST+ for load balancing across VLANs and providing rapid convergence of spanning-tree instances

- UplinkFast, cross-stack UplinkFast, and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks and cross-stack Gigabit uplinks

- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately changing root and designated ports to the forwarding state

- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:

  - Port Fast for eliminating the forwarding delay by enabling a port to immediately change from the blocking state to the forwarding state

  - BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)

  - BPDU filtering for preventing a Port Fast-enabled port from sending or receiving BPDUs

  - Root guard for preventing switches outside the network core from becoming the spanning-tree root

  - Loop guard for preventing alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link

- Equal-cost routing for link-level and switch-level redundancy

- Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy

- Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers, and to allow the failover of the server traffic to an operational link on another Cisco Ethernet switch.

- RPS support through the Cisco RPS 300 and Cisco RPS 675 for enhancing power reliability

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.

- 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

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, 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 security policies in both directions on routed interfaces (router ACLs) and VLANs and inbound on Layer 2 interfaces (port ACLs)

- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces

- VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/UDP headers

- Source and destination MAC-based ACLs for filtering non-IP traffic

- IPv6 ACLs to be applied to interfaces to filter IPv6 traffic:

- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers

- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings

- Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN

- IEEE 802.1Q tunneling so that customers with users at remote sites across a service-provider network can keep VLANs segregated from other customers and Layer 2 protocol tunneling to ensure that the customer's network has complete STP, CDP, and VTP information about all users

- Layer 2 point-to-point tunneling to facilitate the automatic creation of EtherChannels

- Layer 2 protocol tunneling bypass feature to provide interoperability with third-party vendors

- IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:

  - 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

- 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 IEEE 802.1x Validation" section on page 10-39.

  - 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 10-36.

  - 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 AAA services

- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic versions of the software (IP base and IP services images)

- 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 versions of the software IP base and IP services images)

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

- Cross-stack QoS for configuring QoS features to all switches in a switch stack rather than on an individual-switch basis

- 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

    - In Cisco IOS Release 12.2(25)SED and later, 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 stack 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.

Layer 3 Features

These are the Layer 3 features:

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

- HSRP for Layer 3 router redundancy

- IP routing protocols for load balancing and for constructing scalable, routed backbones:

    - RIP Versions 1 and 2

    - OSPF (requires the IP services image)

    - Enhanced IGRP (EIGRP) (requires the IP services image)

    - Border Gateway Protocol (BGP) Version 4 (requires the IP services image)

- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain

- Policy-based routing (PBR) for configuring defined policies for traffic flows

- Multiple VPN routing/forwarding (multi-VRF) instances in customer edge devices to allow service providers to support multiple virtual private networks (VPNs) and overlap IP addresses between VPNs (requires the IP services image)

- Fallback bridging for forwarding non-IP traffic between two or more VLANs (requires the IP services image)

- Static IP routing for manually building a routing table of network path information

- Equal-cost routing for load balancing and redundancy

- Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and router solicitation messages to discover the addresses of routers on directly attached subnets

- Protocol-Independent Multicast (PIM) for multicast routing within the network, allowing for devices in the network to receive the multicast feed requested and for switches not participating in the multicast to be pruned. Includes support for PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode (requires the IP services image)

- Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains (requires the IP services image)

- Distance Vector Multicast Routing Protocol (DVMRP) tunneling for interconnecting two multicast-enabled networks across nonmulticast networks (requires the IP services image)

- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients

- IPv6 unicast routing capability for forwarding IPv6 traffic through configured interfaces (requires the advanced IP services image)

- Nonstop forwarding (NSF) awareness to enable the Layer 3 switch to continue forwarding packets from an NSF-capable neighboring router when the primary route processor (RP) is failing and the backup RP is taking over, or when the primary RP is manually reloaded for a nondisruptive software upgrade (requires the IP services image)

Power over Ethernet Features

These are the Power over Ethernet (PoE) features:

- Ability to provide power to connected Cisco pre-standard and IEEE 802.3af-compliant powered devices from Power over Ethernet (PoE)-capable ports if the switch detects that there is no power on the circuit.

- Support for CDP with power consumption. The powered device notifies the switch of the amount of power it is consuming.

- Support for Cisco intelligent power management. The powered device and the switch negotiate through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-power Cisco powered device to operate at its highest power mode.

- Automatic detection and power budgeting; the switch maintains a power budget, monitors and tracks requests for power, and grants power only when it is available.

Monitoring Features

These are the monitoring features:

- Switch LEDs that provide port-, switch-, and stack-level status

- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the switch has learned or removed

- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN

- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations

- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis

- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events

- Layer 2 traceroute to identify the physical path that a packet takes from a source device to a destination device

- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on 10/100/1000 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.

Default Settings After Initial Switch Configuration

The switch is designed for plug-and-play operation, requiring only that you assign basic IP information to the switch and connect it to the other devices in your network. If you have specific network needs, you can change the interface-specific and system- and stack-wide settings.

> **Note** For information about assigning an IP address by using the browser-based Express Setup program, see the getting started guide. For information about assigning an IP address by using the CLI-based setup program, see the hardware installation guide.

If you do not configure the switch at all, the switch operates with these default settings:

- Default switch IP address, subnet mask, and default gateway is 0.0.0.0. For more information, see Chapter 3, "Assigning the Switch IP Address and Default Gateway," and Chapter 22, "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 22, "Configuring DHCP Features and IP Source Guard."

- Switch stack is enabled (not configurable). For more information, see Chapter 5, "Managing Switch Stacks."

- Switch cluster is disabled. For more information about switch clusters, see Chapter 6, "Clustering Switches," and the *Getting Started with Cisco Network Assistant*, available on Cisco.com.

- No passwords are defined. For more information, see Chapter 7, "Administering the Switch."

- System name and prompt is *Switch.* For more information, see Chapter 7, "Administering the Switch."

- NTP is enabled. For more information, see Chapter 7, "Administering the Switch."

- DNS is enabled. For more information, see Chapter 7, "Administering the Switch."

- TACACS+ is disabled. For more information, see Chapter 9, "Configuring Switch-Based Authentication."

- RADIUS is disabled. For more information, see Chapter 9, "Configuring Switch-Based Authentication."

- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see Chapter 9, "Configuring Switch-Based Authentication."

- IEEE 802.1x is disabled. For more information, see Chapter 10, "Configuring IEEE 802.1x Port-Based Authentication."

- Port parameters

    - Operating mode is Layer 2 (switchport). For more information, see Chapter 11, "Configuring Interface Characteristics."

    - Interface speed and duplex mode is autonegotiate. For more information, see Chapter 11, "Configuring Interface Characteristics."

– Auto-MDIX is enabled. For more information, see Chapter 11, "Configuring Interface Characteristics."

> **Note** In releases earlier than Cisco IOS Release 12.2(18)SE, the default setting for auto-MDIX is disabled.

– Flow control is off. For more information, see Chapter 11, "Configuring Interface Characteristics."

– PoE is autonegotiate. For more information, see Chapter 11, "Configuring Interface Characteristics."

- No Smartports macros are defined. For more information, see Chapter 12, "Configuring Smartports Macros."

- VLANs

  – Default VLAN is VLAN 1. For more information, see Chapter 13, "Configuring VLANs."

  – VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 13, "Configuring VLANs."

  – Trunk encapsulation is negotiate. For more information, see Chapter 13, "Configuring VLANs."

  – VTP mode is server. For more information, see Chapter 14, "Configuring VTP."

  – VTP version is Version 1. For more information, see Chapter 14, "Configuring VTP."

  – No private VLANs are configured. For more information, see Chapter 16, "Configuring Private VLANs."

  – Voice VLAN is disabled. For more information, see Chapter 15, "Configuring Voice VLAN."

- IEEE 802.1Q tunneling and Layer 2 protocol tunneling are disabled. For more information, see Chapter 17, "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling."

- For STP, PVST+ is enabled on VLAN 1. For more information, see Chapter 18, "Configuring STP."

- MSTP is disabled. For more information, see Chapter 19, "Configuring MSTP."

- Optional spanning-tree features are disabled. For more information, see Chapter 20, "Configuring Optional Spanning-Tree Features."

- Flex Links are not configured. For more information, see Chapter 21, "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 22, "Configuring DHCP Features and IP Source Guard."

- IP source guard is disabled. For more information, see Chapter 22, "Configuring DHCP Features and IP Source Guard."

- Dynamic ARP inspection is disabled on all VLANs. For more information, see Chapter 23, "Configuring Dynamic ARP Inspection."

- IGMP snooping is enabled. No IGMP filters are applied. For more information, see Chapter 24, "Configuring IGMP Snooping and MVR."

- IGMP throttling setting is deny. For more information, see Chapter 24, "Configuring IGMP Snooping and MVR."

- The IGMP snooping querier feature is disabled. For more information, see Chapter 24, "Configuring IGMP Snooping and MVR."

- MVR is disabled. For more information, see Chapter 24, "Configuring IGMP Snooping and MVR."

- Port-based traffic

  - Broadcast, multicast, and unicast storm control is disabled. For more information, see Chapter 25, "Configuring Port-Based Traffic Control."

  - No protected ports are defined. For more information, see Chapter 25, "Configuring Port-Based Traffic Control."

  - Unicast and multicast traffic flooding is not blocked. For more information, see Chapter 25, "Configuring Port-Based Traffic Control."

  - No secure ports are configured. For more information, see Chapter 25, "Configuring Port-Based Traffic Control."

- CDP is enabled. For more information, see Chapter 26, "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 Link-State Tracking."

- 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."

- IP multicast routing is disabled on all interfaces. For more information, see Chapter 40, "Configuring IP Multicast Routing."

- MSDP is disabled. For more information, see Chapter 41, "Configuring MSDP."

- Fallback bridging is not configured. For more information, see Chapter 42, "Configuring Fallback Bridging."

Network Configuration Examples

This section provides network configuration concepts and includes examples of using the switch to create dedicated network segments and interconnecting the segments through Fast Ethernet and Gigabit Ethernet connections.

Design Concepts for Using the Switch

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

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

Table 1-1   Increasing Network Performance

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

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

Table 1-2   Providing Network Services

Network Demands	Suggested Design Methods
Efficient bandwidth usage for multimedia applications and guaranteed bandwidth for critical applications	• Use IGMP snooping to efficiently forward multimedia and multicast traffic. • Use other QoS mechanisms such as packet classification, marking, scheduling, and congestion avoidance to classify traffic with the appropriate priority level, thereby providing maximum flexibility and support for mission-critical, unicast, and multicast and multimedia applications. • Use optional IP multicast routing to design networks better suited for multicast traffic. • Use MVR to continuously send multicast streams in a multicast VLAN but to isolate the streams from subscriber VLANs for bandwidth and security reasons.
High demand on network redundancy and availability to provide *always on* mission-critical applications	• Use switch stacks, where all stack members are eligible stack masters in case of stack-master failure. All stack members have synchronized copies of the saved and running configuration files of the switch stack. • Use cross-stack EtherChannels for providing redundant links across the switch stack. • Use Hot Standby Router Protocol (HSRP) for cluster command switch and router redundancy. • Use VLAN trunks, cross-stack UplinkFast, and BackboneFast for traffic-load balancing on the uplink ports so that the uplink port with a lower relative port cost is selected to carry the VLAN traffic.
An evolving demand for IP telephony	• Use QoS to prioritize applications such as IP telephony during congestion and to help control both delay and jitter within the network. • Use switches that support at least two queues per port to prioritize voice and data traffic as either high- or low-priority, based on IEEE 802.1p/Q. The switch supports at least four queues per port. • Use voice VLAN IDs (VVIDs) to provide separate VLANs for voice traffic.
A growing demand for using existing infrastructure to transport data and voice from a home or office to the Internet or an intranet at higher speeds	Use the Catalyst Long-Reach Ethernet (LRE) switches to provide up to 15 Mb of IP connectivity over existing infrastructure, such as existing telephone lines. **Note** LRE is the technology used in the Catalyst 2900 LRE XL and Catalyst 2950 LRE switches. See the documentation sets specific to these switches for LRE information.

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

• Cost-effective wiring closet (Figure 1-1)—A cost-effective way to connect many users to the wiring closet is to have a switch stack of up to nine Catalyst 3750 switches. To preserve switch connectivity if one switch in the stack fails, connect the switches as recommended in the hardware installation guide, and enable either cross-stack Etherchannel or cross-stack UplinkFast.

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

Figure 1-1   Cost-Effective Wiring Closet
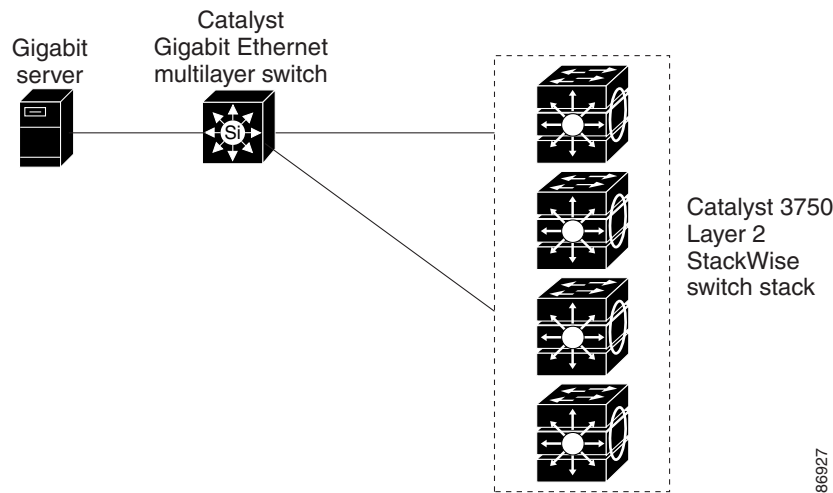
• High-performance wiring closet (Figure 1-2)—For high-speed access to network resources, you can use Catalyst 3750switches and switch stacks in the access layer to provide Gigabit Ethernet to the desktop. To prevent congestion, use QoS DSCP marking priorities on these switches. For high-speed IP forwarding at the distribution layer, connect the switches in the access layer to a Gigabit multilayer switch in the backbone, such as a Catalyst 4500 Gigabit switch or Catalyst 6500 Gigabit switch.

Each 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 1-2   High-Performance Wiring Closet
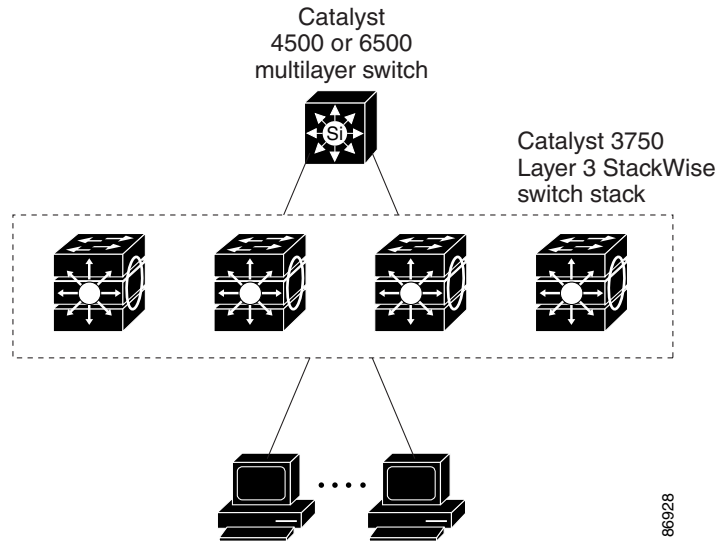
- Redundant Gigabit backbone—Using HSRP, you can create backup paths between two Catalyst 3750G multilayer Gigabit switches to enhance network reliability and load balancing for different VLANs and subnets. Using HSRP also provides faster network convergence if any network failure occurs. You can connect the Catalyst switches, again in a star configuration, to two Catalyst 3750G multilayer backbone switches. If one of the backbone switches fails, the second backbone switch preserves connectivity between the switches and network resources.

Figure 1-3   Redundant Gigabit Backbone
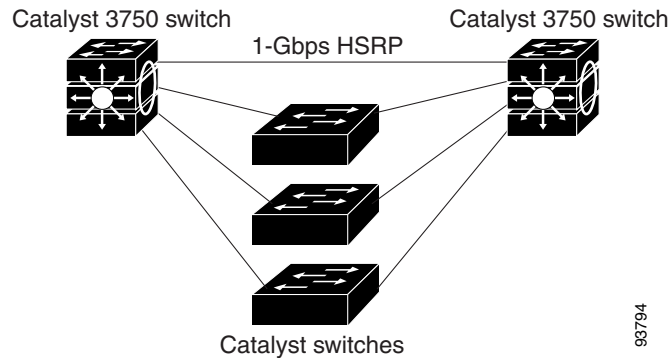
- Server aggregation (Figure 1-4) and Linux server cluster (Figure 1-5)—You can use the switches and switch stacks to interconnect groups of servers, centralizing physical security and administration of your network. For high-speed IP forwarding at the distribution layer, connect the switches in the 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, if required. 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 dual switch stacks, which have redundant Gigabit EtherChannels and cross-stack EtherChannels.

Using dual SFP module uplinks from the switches provides redundant uplinks to the network core. Using SFP modules provides flexibility in media and distance options through fiber-optic connections.

The various lengths of stack cable available, ranging from 0.5 meter to 3 meters provide extended connections to the switch stacks across multiple server racks, for multiple stack aggregation.
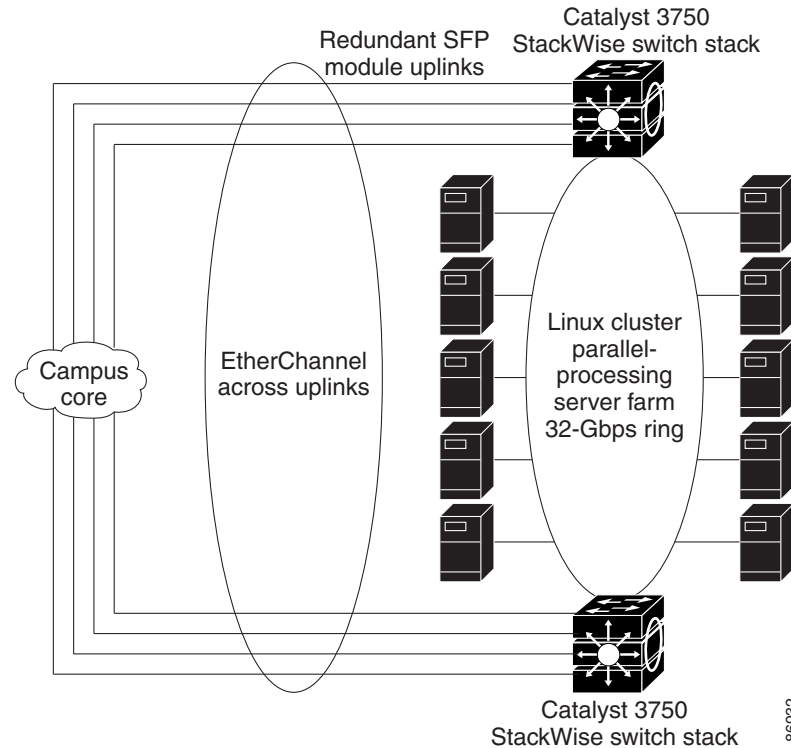
Figure 1-4   Server Aggregation
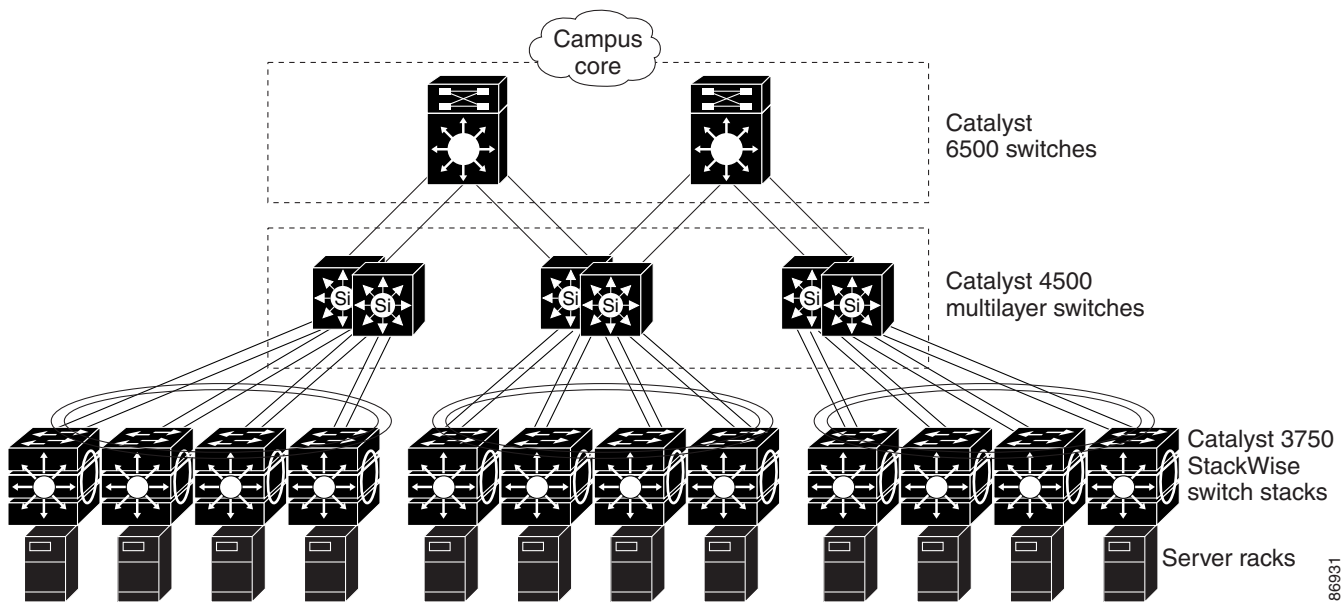
Figure 1-5   Linux Server Cluster

Small to Medium-Sized Network Using Catalyst 3750 Switches

Figure 1-6 shows a configuration for a network of up to 500 employees. This network uses a Catalyst 3750 Layer 3 switch stack with high-speed connections to two routers. For network reliability and load balancing, this network has HSRP enabled on the routers and on the switches. This ensures connectivity to the Internet, WAN, and mission-critical network resources in case one of the routers or switches fails. The switches are using routed uplinks for faster failover. They are also configured with equal-cost routing for load sharing and redundancy. (A Layer 2 switch stack can use cross-stack EtherChannel for load sharing.)

The switches are connected to workstations, local servers, and IEEE 802.3af compliant and noncompliant powered devices (such as Cisco IP Phones). The server farm includes a call-processing server running Cisco CallManager software. Cisco CallManager controls call processing, routing, and Cisco IP Phone features and configuration. The switches are interconnected through Gigabit interfaces.

This network uses VLANs to logically segment the network into well-defined broadcast groups and for security management. Data and multimedia traffic are configured on the same VLAN. Voice traffic from the Cisco IP Phones are configured on separate VVIDs. If data, multimedia, and voice traffic are assigned to the same VLAN, only one VLAN can be configured per wiring closet.

When an end station in one VLAN needs to communicate with an end station in another VLAN, a router or Layer 3 switch routes the traffic to the destination VLAN. In this network, the switch stack is providing inter-VLAN routing. VLAN access control lists (VLAN maps) on the switch stack provide intra-VLAN security and prevent unauthorized users from accessing critical areas of the network.

In addition to inter-VLAN routing, the multilayer switches provide QoS mechanisms such as DSCP priorities to prioritize the different types of network traffic and to deliver high-priority traffic. If congestion occurs, QoS drops low-priority traffic to allow delivery of high-priority traffic.

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

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

Cisco CallManager controls call processing, routing, and Cisco IP Phone features and configuration. Users with workstations running Cisco SoftPhone software can place, receive, and control calls from their PCs. Using Cisco IP Phones, Cisco CallManager software, and Cisco SoftPhone software integrates telephony and IP networks, and the IP network supports both voice and data.

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

Figure 1-6   Catalyst 3750 Switch Stack in a Collapsed Backbone Configuration
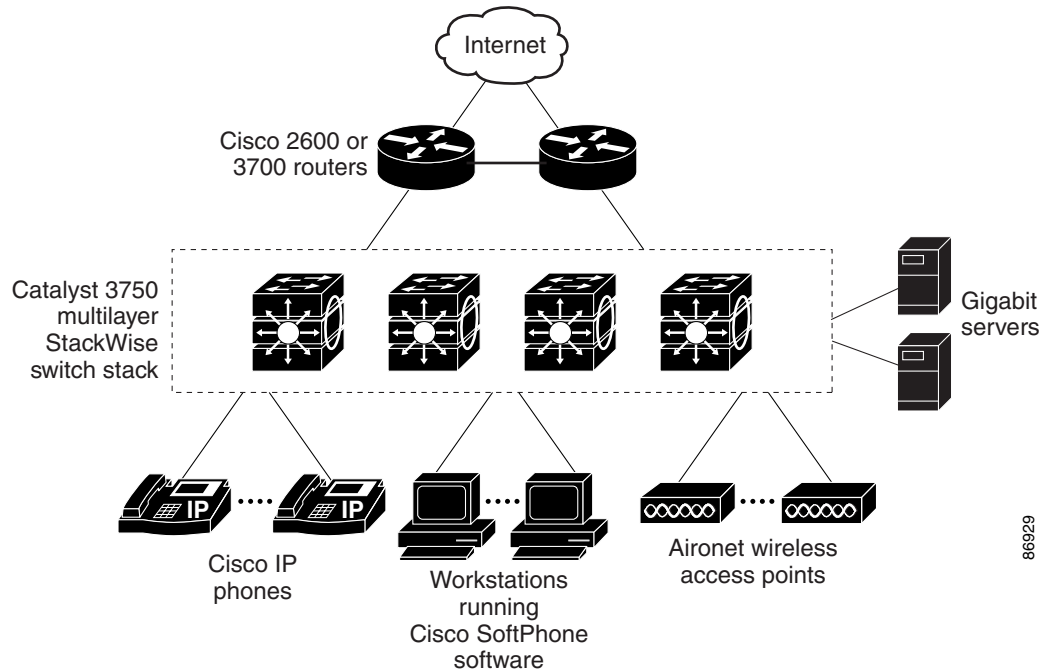
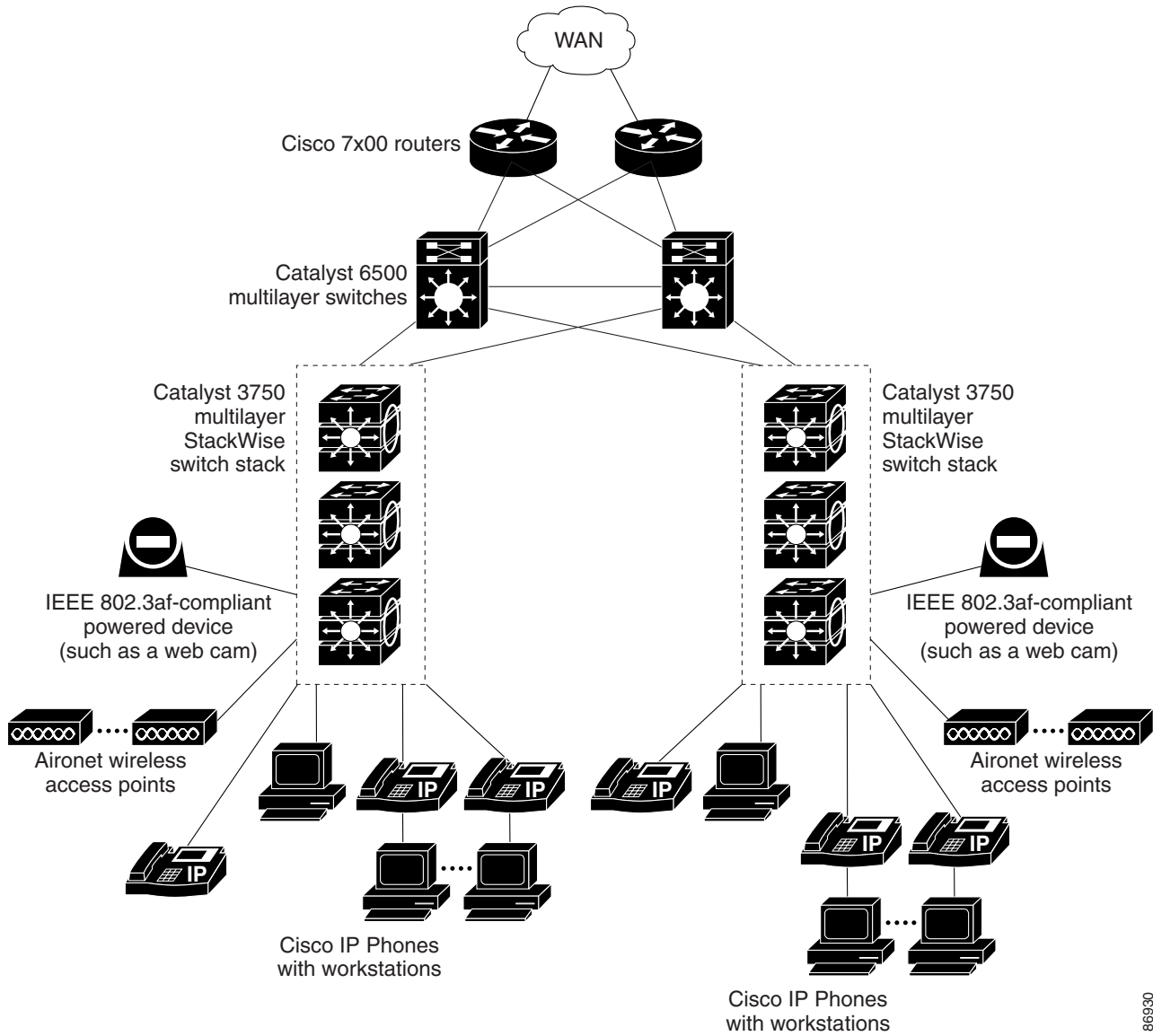# Large Network Using Catalyst 3750 Switches

Switches in the wiring closet have traditionally been only Layer 2 devices, but as network traffic profiles evolve, switches in the wiring closet are increasingly employing multilayer services such as multicast management and traffic classification. Figure 1-7 shows a configuration for a network that only use Catalyst 3750 multilayer switch stacks in the wiring closets and two backbone switches, such as the Catalyst 6500 switches, to aggregate up to ten wiring closets.

In the wiring closet, each switch stack has IGMP snooping enabled to efficiently forward multimedia and multicast traffic. QoS ACLs that either drop or mark nonconforming traffic based on bandwidth limits are also configured on each switch stack. VLAN maps provide intra-VLAN security and prevent unauthorized users from accessing critical pieces of the network. QoS features can limit bandwidth on a per-port or per-user basis. The switch ports are configured as either trusted or untrusted. You can configure a trusted port to trust the CoS value, the DSCP value, or the IP precedence. If you configure the port as untrusted, you can use an ACL to mark the frame in accordance with the network policy.

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

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

Figure 1-7   *Catalyst 3750 Switch Stacks in Wiring Closets in a Backbone Configuration*

Multidwelling Network Using Catalyst 3750 Switches

A growing segment of residential and commercial customers are requiring high-speed access to Ethernet metropolitan-area networks (MANs). Figure 1-8 shows a configuration for a Gigabit Ethernet MAN ring using multilayer switch stacks as aggregation switches in the mini-point-of-presence (POP) location. These switches are connected through 1000BASE-X SFP module ports.

The resident switches can be Catalyst 3750 switches, providing customers with high-speed connections to the MAN. Catalyst 2900 LRE XL and Catalyst 2950 LRE switches also can be used as residential switches for customers requiring connectivity through existing phone lines. The Catalyst 2900 LRE XL and Catalyst 2950 LRE switches can then connect to another residential switch or to a Catalyst 3750 aggregation switch. For more information about the Catalyst Long-Reach Ethernet (LRE) switches, see the documentation sets specific to these switches for LRE information.

All ports on the residential Catalyst 3750 switches (and Catalyst 2950 LRE switches if they are included) are configured as IEEE 802.1Q trunks with protected port and STP root guard features enabled. The protected port feature provides security and isolation between ports on the switch, ensuring that subscribers cannot view packets destined for other subscribers. STP root guard prevents unauthorized devices from becoming the STP root switch. All ports have IGMP snooping or CGMP enabled for multicast traffic management. ACLs on the uplink ports to the aggregating Catalyst 3750 multilayer switches provide security and bandwidth management.

The aggregating switches and routers provide services such as those described in the examples in the "Small to Medium-Sized Network Using Catalyst 3750 Switches" section on page 1-21 and the "Large Network Using Catalyst 3750 Switches" section on page 1-23.

*Figure 1-8   Catalyst 3750 Switches in a MAN Configuration*
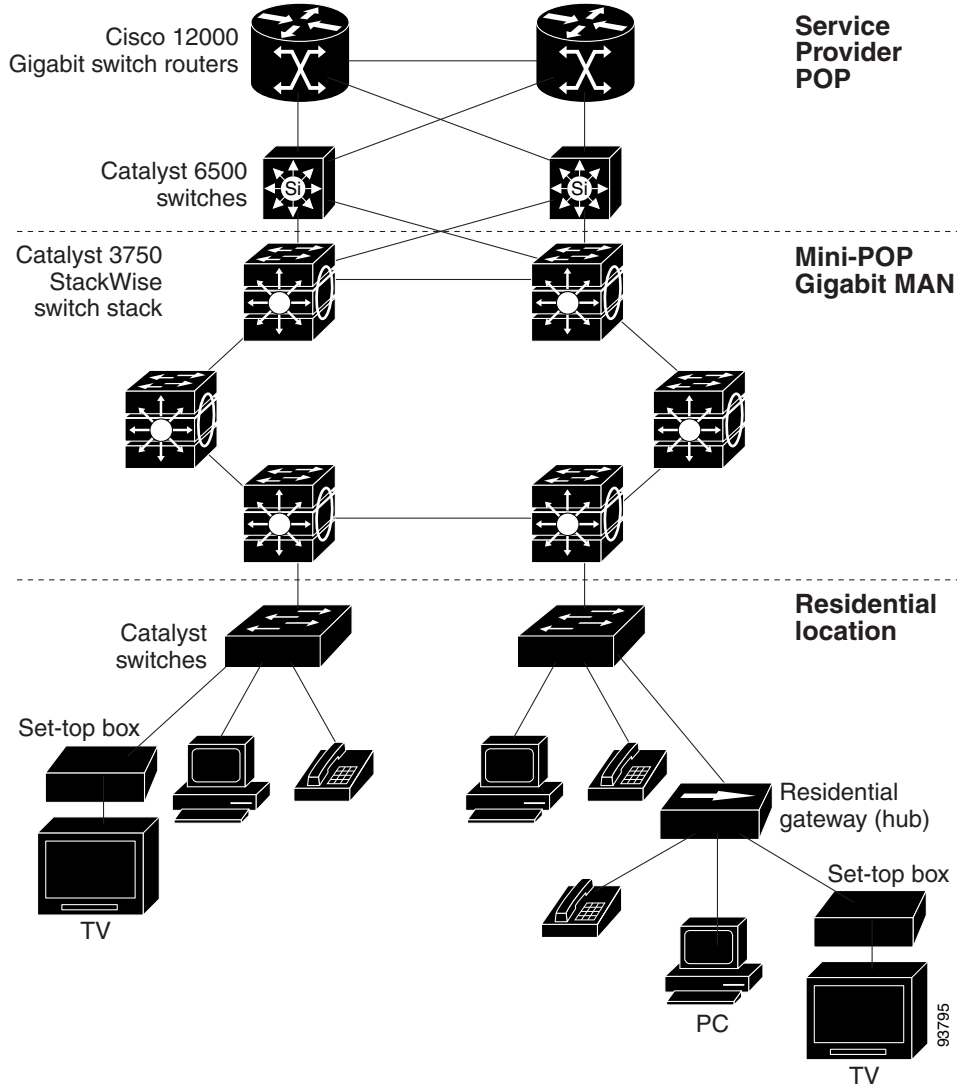
Long-Distance, High-Bandwidth Transport Configuration

Figure 1-9 shows a configuration for sending 8 Gigabits of data over a single fiber-optic cable. The Catalyst 3750 switches have coarse wavelength-division multiplexing (CWDM) fiber-optic SFP modules installed. Depending on the CWDM SFP module, data is sent at wavelengths from 1470 to 1610 nm. The higher the wavelength, the farther the transmission can travel. A common wavelength used for long-distance transmissions is 1550 nm.

The CWDM SFP modules connect to CWDM optical add/drop multiplexer (OADM) modules over distances of up to 393,701 feet (74.5 miles or 120 km). The CWDM OADM modules combine (or *multiplex*) the different CWDM wavelengths, allowing them to travel simultaneously on the same fiber-optic cable. The CWDM OADM modules on the receiving end separate (or *demultiplex*) the different wavelengths.

For more information about the CWDM SFP modules and CWDM OADM modules, see the *Cisco CWDM GBIC and CWDM SFP Installation Note*.

Figure 1-9   Long-Distance, High-Bandwidth Transport Configuration
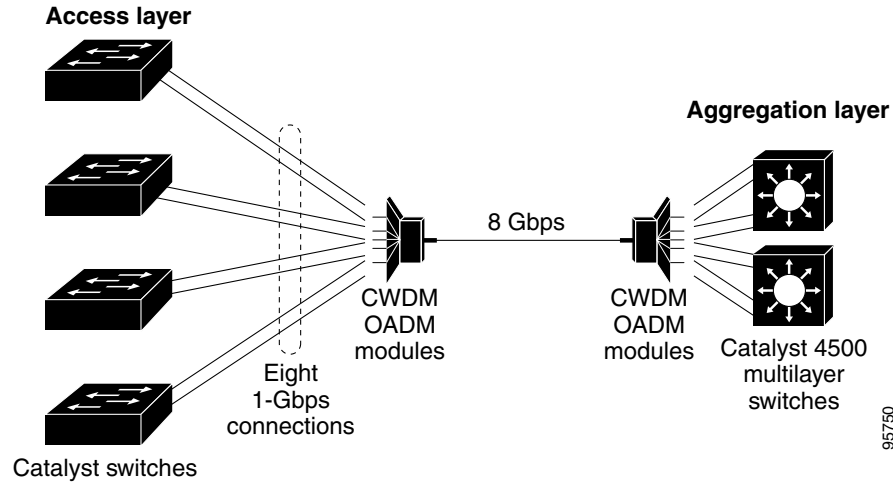
Where to Go Next

Before configuring the switch, review these sections for startup information:

- Chapter 2, "Using the Command-Line Interface"
- Chapter 3, "Assigning the Switch IP Address and Default Gateway"