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.

Features

The Catalyst 3750 switches are shipped with either of these software images installed:

- 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, and the Hot Standby Router Protocol (HSRP) and Routing Information Protocol (RIP). Switches with the SMI installed can be upgraded to the EMI.
- Enhanced multilayer image (EMI), which provides a richer set of enterprise-class intelligent services. It includes all SMI 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 EMI includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) Protocol.

  EMI-only features are noted in the "Layer 3 Features" section on page 1-8.

Note Unless otherwise noted, all features described in this chapter and in this guide are supported on both the SMI and EMI.

Note Some features noted in this chapter are available only on the cryptographic (that is, supports encryption) versions of the SMI and EMI. You must obtain authorization to use this feature and to download the cryptographic version of the software from Cisco.com. For more information, refer to the release notes for this release.

The Catalyst 3750 switches have these features:

Ease-of-Use and Ease-of-Deployment 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
- Cluster Management Suite (CMS) graphical user interface (GUI) for
  - Simplifying and minimizing switch, switch stack, and switch cluster management through a supported web browser from anywhere in your intranet.
  - Accomplishing multiple configuration tasks from a single CMS window 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).
  - Automated 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.
  - 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 Trivial File Transfer Protocol (TFTP) server.
  - Adding, removing, and replacing switches in the stack without disrupting the operation of the stack.
- 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. Refer to the release notes for a list of cluster-capable switches.
  - 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

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports for optimizing bandwidth
- Automatic-media-dependent interface crossover (Auto MDIX) capability on 10/100 and 10/100/1000 Mbps interfaces that enables the interface to automatically detect the required cable connection type (straight through or crossover) and configure the connection appropriately
- 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 of bandwidth between 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 and 2:
  - (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
- 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
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features

Management Options

- CMS—CMS is a graphical user interface that can be launched from anywhere in your network through a web browser such as Netscape Communicator or Microsoft Internet Explorer. CMS is already installed on the switch. For more information about CMS, see Chapter 3, "Getting Started with CMS."
- CLI—The Cisco IOS CLI software is enhanced to support 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 25, "Configuring SNMP."

Manageability Features

Note The encrypted Secure Shell (SSH) feature listed in this section is available only on the cryptographic (that is, supports encryption) versions of the SMI and EMI.

- Dynamic Host Configuration Protocol (DHCP) for automating configuration of switch information (such as IP address, default gateway, host name, and Domain Name System [DNS] and Trivial File Transfer Protocol (TFTP) server names)
- Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding host name 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 Media Access Control (MAC) address
- 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 timestamp 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
- In-band management access through CMS over a Netscape Communicator 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 [that is, supports encryption] versions of the SMI and EMI)
- In-band management access through SNMP versions 1 and 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

Note For additional descriptions of the management interfaces, see the "Network Configuration Examples" section on page 1-11.

Availability 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 balancing load across VLANs
  - Rapid PVST+ for balancing load 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 IEEE 802.1W Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately transitioning 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 transition 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
- RPS support through the Cisco RPS 300 and Cisco RPS 675 for enhancing power reliability

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 full 1 to 4094 range 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 (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
- VLAN1 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

Note The Kerberos feature listed in this section is available only on the cryptographic (that is, supports encryption) versions of the SMI and EMI.

- Password-protected access (read-only and read-write access) to management interfaces (CMS and 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/User Datagram Protocol (UDP) headers
- Source and destination MAC-based ACLs for filtering non-IP traffic
- IEEE 802.1X port-based authentication to prevent unauthorized devices (clients) from gaining access to the network
  - 802.1X with VLAN assignment for restricting 802.1X-authenticated users to a specified VLAN
  - 802.1X with port security for controlling access to 802.1X ports
  - 802.1X with voice VLAN to permit an IP phone access to the voice VLAN regardless of the authorized or unauthorized state of the port
  - 802.1X with guest VLAN to provide limited services to non-802.1X-compliant users
- Terminal Access Controller Access Control System Plus (TACACS+), a proprietary feature for managing network security through a TACACS server

- Remote Authentication Dial-In User Service (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 [that is, supports encryption] versions of the SMI and EMI)

QoS and CoS Features

- Automatic QoS (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues (voice over IP only)
- 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 802.1P CoS marking priorities on a per-port basis for protecting the performance of mission-critical applications
  - IP TOS/DSCP and 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
  - 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 determining the rate at which packets are dequeued 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 determining 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

Note Some features noted in this section are available only on the EMI.

- 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 EMI)
  - Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP) (requires the EMI)
  - Border Gateway Protocol (BGP) Version 4 (requires the EMI)
- 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
- Fallback bridging for forwarding non-IP traffic between two or more VLANs (requires the EMI)
- 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 EMI)
- Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains (requires the EMI)
- Distance Vector Multicast Routing Protocol (DVMRP) tunnelling for interconnecting two multicast-enabled networks across non-multicast networks (requires the EMI)
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients

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

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.

If you do not configure the switch at all, the switch operates with the default settings listed in Table 1-1. This table lists the key software features, their defaults, and where to find more information about the features.

For information about setting up the initial switch configuration and assigning basic IP information to the switch, refer to the hardware installation guide.

Table 1-1 Default Settings After Initial Switch Configuration

Feature	Default Setting	More information in...
Switch IP address, subnet mask, and default gateway	0.0.0.0	Chapter 4, "Assigning the Switch IP Address and Default Gateway"
Domain name	None	
DHCP	DHCP client enabled	
Switch stack	Enabled (not configurable)	Chapter 5, "Managing Switch Stacks"
Switch cluster	Disabled	Chapter 6, "Clustering Switches"
Passwords	None defined	Chapter 7, "Administering the Switch"
TACACS+	Disabled	
RADIUS	Disabled	
System name and prompt	*Switch*	
NTP	Enabled	
DNS	Enabled	
802.1X	Disabled	Chapter 10, "Configuring 802.1X Port-Based Authentication"
Port parameters		
Operating mode	Layer 2 (switchport)	Chapter 11, "Configuring Interface Characteristics"
Interface speed and duplex mode	Autonegotiate	
Auto MDIX	Disabled	
Flow control	Off	
VLANs		
Default VLAN	VLAN 1	Chapter 12, "Configuring VLANs"
VLAN trunking	Dynamic auto (DTP)	
Trunk encapsulation	Negotiate	
VTP mode	Server	Chapter 13, "Configuring VTP"
VTP version	1	
Voice VLAN	Disabled	Chapter 14, "Configuring Voice VLAN"
STP	PVST+ enabled on VLAN 1	Chapter 15, "Configuring STP"
MSTP	Disabled	Chapter 16, "Configuring MSTP"

Table 1-1 Default Settings After Initial Switch Configuration (continued)

Feature	Default Setting	More information in...
Optional spanning-tree features	Disabled	Chapter 17, "Configuring Optional Spanning-Tree Features"
IGMP snooping		
IGMP snooping	Enabled	Chapter 18, "Configuring IGMP Snooping and MVR"
IGMP filters	None applied	
MVR	Disabled	
Port-based Traffic		
Broadcast, multicast, and unicast storm control	Disabled	Chapter 19, "Configuring Port-Based Traffic Control"
Protected ports	None defined	
Unicast and multicast traffic flooding	Not blocked	
Secure ports	None configured	
CDP	Enabled	Chapter 20, "Configuring CDP"
UDLD	Disabled	Chapter 21, "Configuring UDLD"
SPAN and RSPAN	Disabled	Chapter 22, "Configuring SPAN and RSPAN"
RMON	Disabled	Chapter 23, "Configuring RMON"
Syslog messages	Enabled; displayed on the console	Chapter 24, "Configuring System Message Logging"
SNMP	Enabled; version 1	Chapter 25, "Configuring SNMP"
ACLs	None configured	Chapter 26, "Configuring Network Security with ACLs"
QoS	Disabled	Chapter 27, "Configuring QoS"
EtherChannels	None configured	Chapter 28, "Configuring EtherChannels"
IP unicast routing	Disabled	Chapter 29, "Configuring IP Unicast Routing"
HSRP groups	None configured	Chapter 30, "Configuring HSRP"
IP multicast routing	Disabled on all interfaces	Chapter 31, "Configuring IP Multicast Routing"
MSDP	Disabled	Chapter 32, "Configuring MSDP"
Fallback bridging	Not configured	Chapter 33, "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 they use.

Table 1-2 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 1-2 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 1-3 describes some network demands and how you can meet those demands.

Table 1-3 Providing Network Services

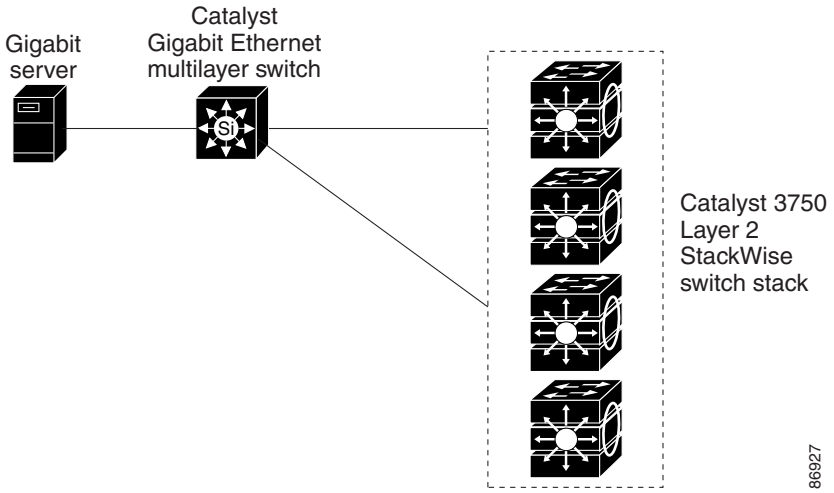
Network Demands	Suggested Design Methods
Efficient bandwidth usage for multimedia applications and guaranteed bandwidth for critical applications	• Use IGMP snooping to efficiently forward multimedia and multicast traffic. • Use other QoS mechanisms such as packet classification, marking, scheduling, 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. • Cross-stack EtherChannel 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 802.1P/Q. The Catalyst 3750 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. Refer to 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.

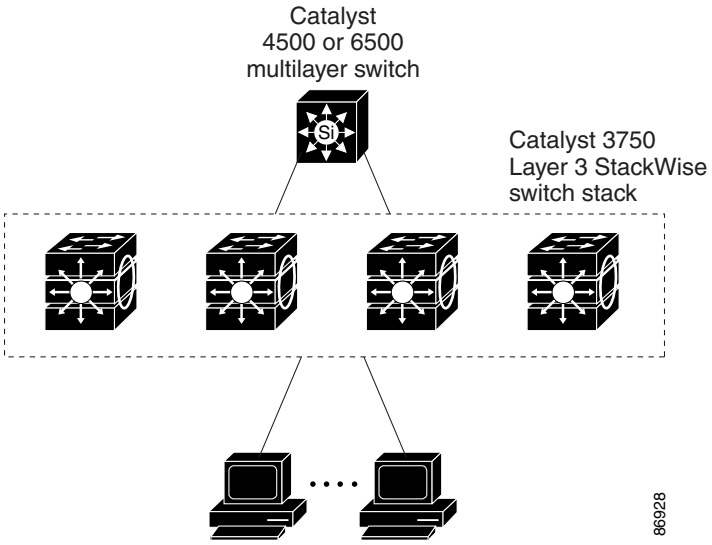
Figure 1-1 Cost-Effective Wiring Closet



- High-performance wiring closet (Figure 1-2) —For high-speed access to network resources, you can use Catalyst 3750 switches 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.

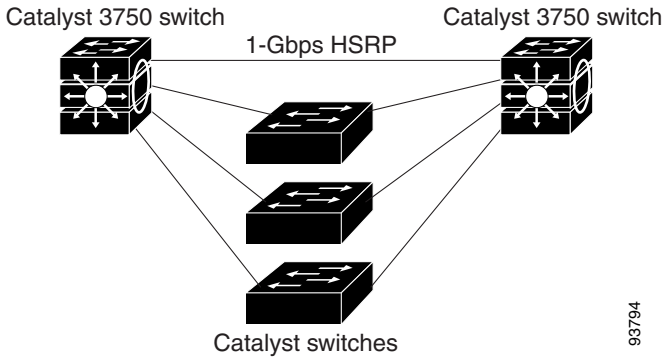
  Each switch in this configuration provides users with a dedicated 1-Gbps connection to network resources. Using SFP modules also provides flexibility in media and distance options through fiber-optic connections.

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 3750 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.

  Dual homing of servers to dual switch stacks with redundant Gigabit EtherChannel and cross-stack EtherChannel provide fault tolerance from the server racks to the core.

  Using dual SFP uplinks from the Catalyst 3750 switches provide 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

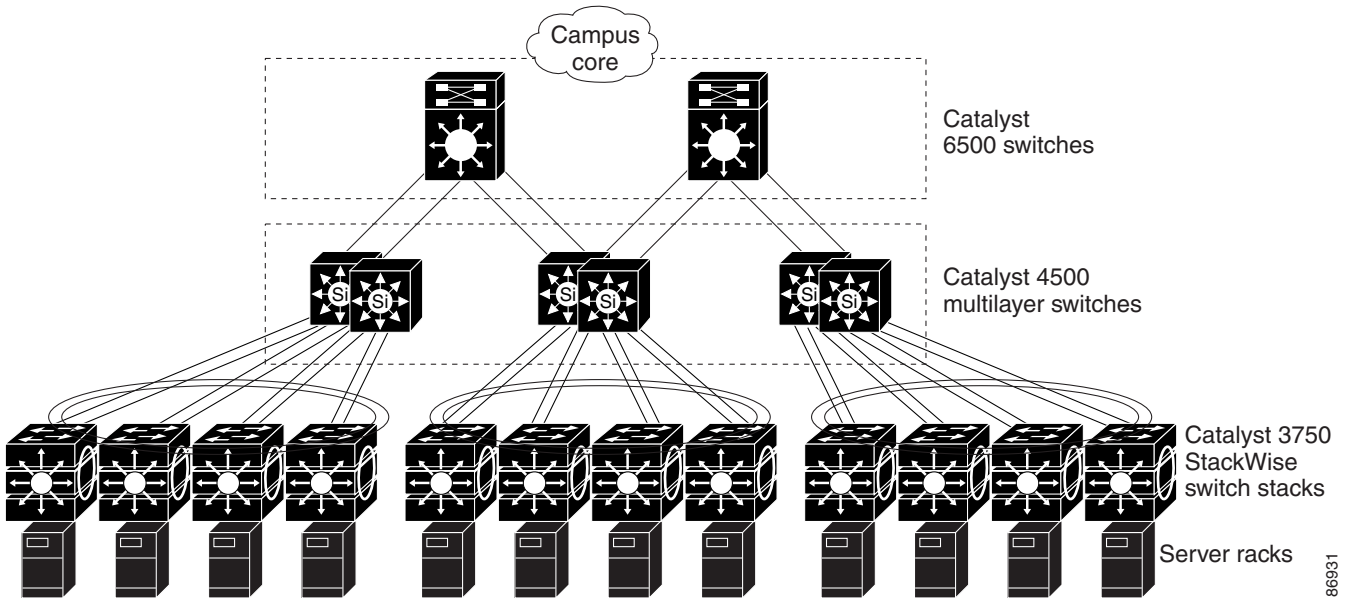
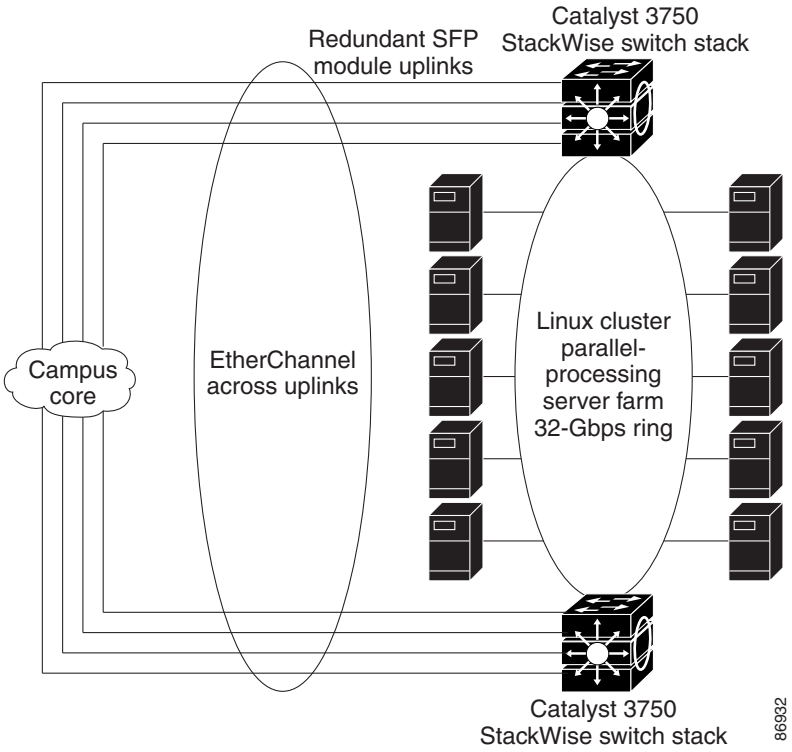


Figure 1-5 Linux Server Cluster



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

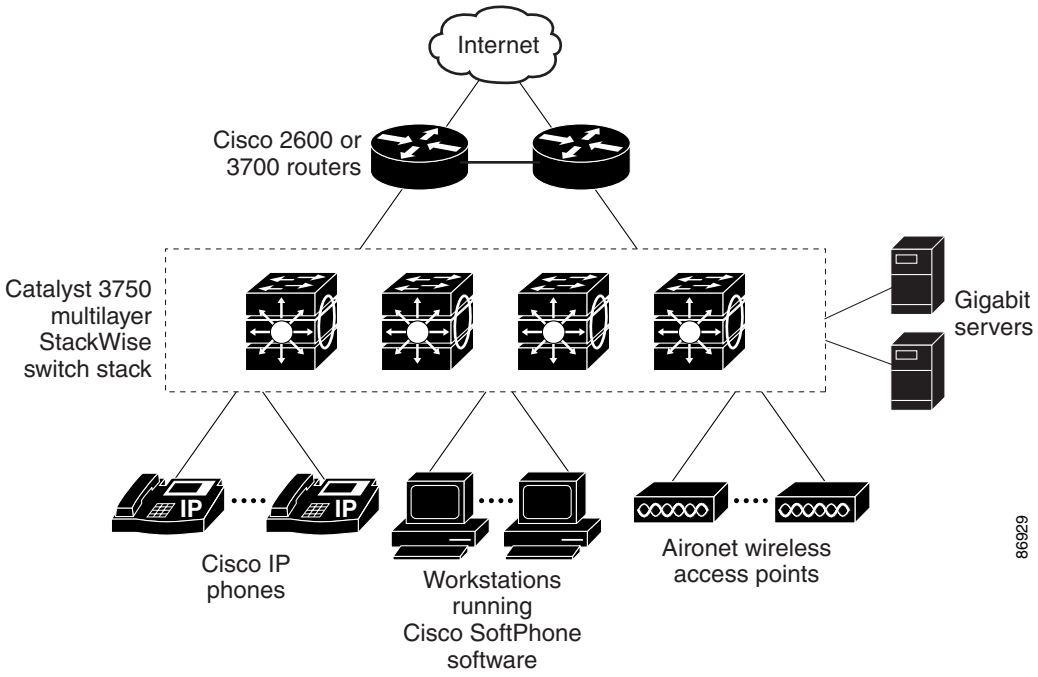
The switch stack is connected to workstations, Cisco IP Phones, and local servers. This network uses VLANs to logically segment the network into well-defined broadcast groups and for security management. Data and multimedia traffic are configured on the same VLAN. Voice traffic from the Cisco IP Phones 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. For any switch port connected to Cisco IP Phones, 802.1P/Q QoS gives voice traffic forwarding-priority over data traffic. Cisco IP Phones not connected to Catalyst inline-power switches must be connected to AC power sources to receive power.

When an end station in one VLAN needs to communicate with an end station in another VLAN, a router or multilayer switch routes the traffic to the appropriate 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 pieces of the network.

In addition to inter-VLAN routing, the switch stack provides QoS mechanisms such as DSCP priorities to prioritize the different types of network traffic and to deliver high-priority traffic in a predictable manner. If congestion occurs, QoS drops low-priority traffic to allow delivery of high-priority traffic.

With the switch stack 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

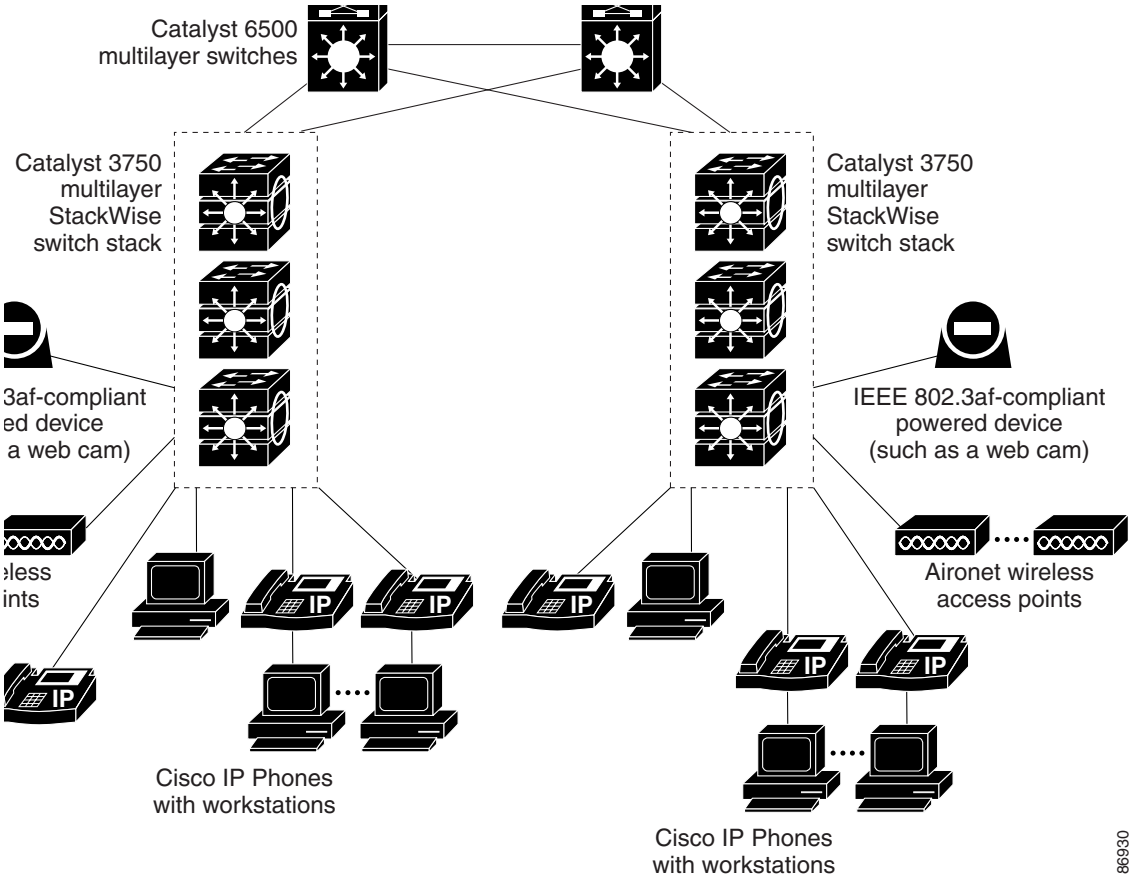
Switches in the wiring closet have traditionally been Layer 2-only devices, but as network traffic profiles evolve, switches in the wiring closet are increasingly employing multilayer services such as multicast management and traffic classification. Figure 1-7 shows a configuration for a network exclusively using multilayer switch stacks in the wiring closets and two backbone switches, such as the Catalyst 6000 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 determine 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

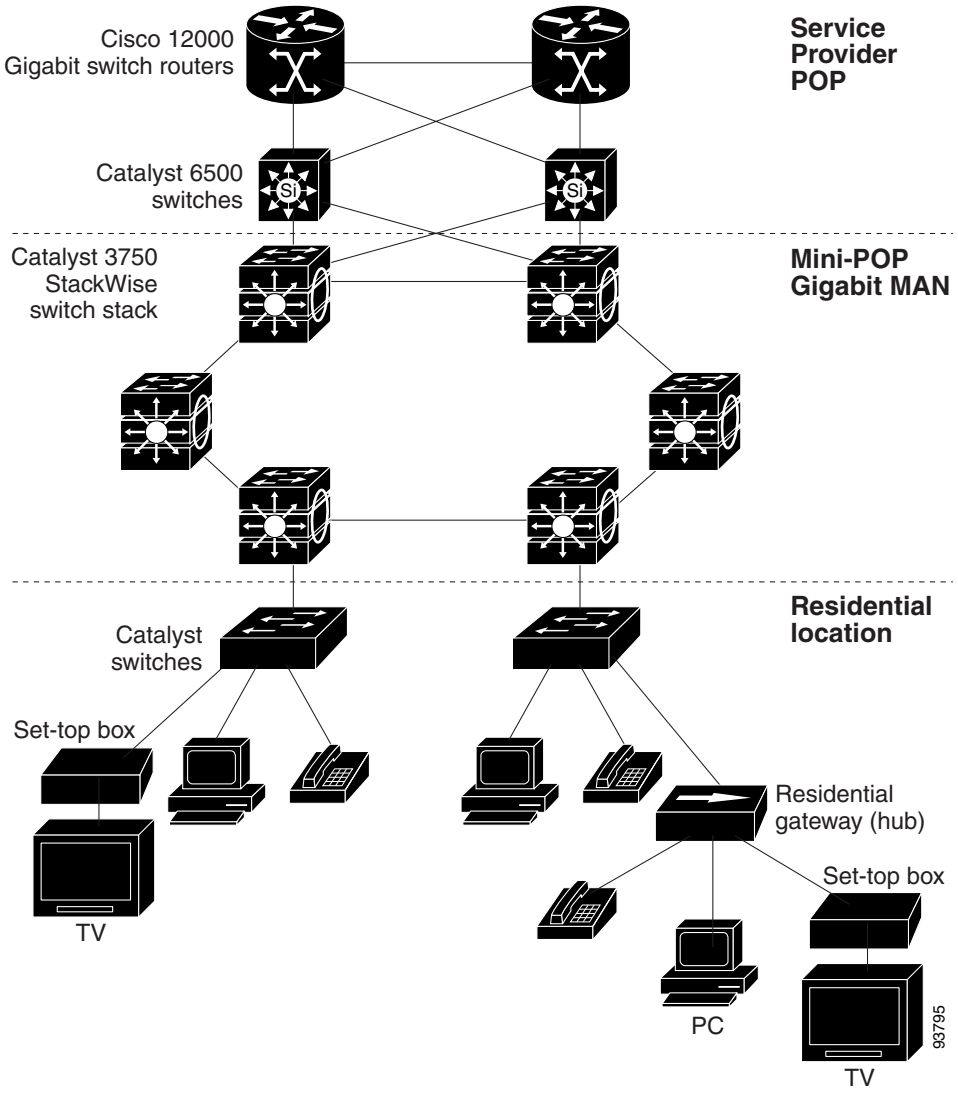
A growing segment of residential and commercial customers are requiring high-speed access to Ethernet metropolitan-area networks (MANs). Figure 1-8 shows a configuration for a Gigabit Ethernet MAN ring using Catalyst 3750 multilayer switches as aggregation switches in the mini-point-of-presence (POP) 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, refer to 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 802.1Q trunks with Private VLAN Edge (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 1-17 and "Large Network Using Catalyst 3750 Switches" section on page 1-18.

Figure 1-8 Catalyst 3750 Switches in a MAN Configuration



Where to Go Next

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

- Chapter 2, "Using the Command-Line Interface"
- Chapter 3, "Getting Started with CMS"
- Chapter 4, "Assigning the Switch IP Address and Default Gateway"