



Overview

This chapter provides these topics about the Catalyst 2940 switch software:

- [Features, page 1-1](#)
- [Management Options, page 1-5](#)
- [Network Configuration Examples, page 1-7](#)
- [Where to Go Next, page 1-11](#)



Note

In this document, IP refers to IP version 4 (IPv4). Layer 3 IP version 6 (IPv6) packets are treated as non-IP packets.

Features

This section describes the features supported in this release:

Ease of Use and Ease of Deployment

- 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
- User-defined SmartPort macros for creating custom switch configurations for simplified deployment across the network
- Cluster Management Suite (CMS) software for simplifying switch and switch cluster management through a web browser, such as Netscape Communicator or Microsoft Internet Explorer, from anywhere in your intranet
- Switch clustering technology used with CMS for
 - Unified configuration, monitoring, authentication, and software upgrade of multiple switches (refer to the release notes for a list of eligible cluster members).
 - 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.
- Hot Standby Router Protocol (HSRP) for command-switch redundancy. The redundant command switches used for HSRP must have compatible software releases.



Note

See the [“Advantages of Using CMS and Clustering Switches”](#) section on page 1-6.



Note Refer to the release notes for the list of Catalyst switches eligible for switch clustering, including which ones can be command switches and which ones can only be member switches. See [Chapter 5, “Clustering Switches,”](#) for the required software versions and browser and Java plug-in configurations.

Performance

- Autosensing of speed on the 10/100 and 10/100/1000 ports and autonegotiation of duplex mode on the 10/100 ports for optimizing bandwidth
- Automatic medium-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



Note Auto-MDIX is not supported on 1000BASE-SX or -LX Small Form-Factor Pluggable (SFP) interfaces.

- Fast EtherChannel for enhanced fault tolerance and increased bandwidth between switches, routers, and servers
- Per-port broadcast storm control for preventing faulty end stations from degrading overall system performance with broadcast storms
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links
- Internet Group Management Protocol (IGMP) snooping for IGMP versions 1, 2, and 3 to limit flooding of IP 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)
- Multicast VLAN regitime-stamptime-stampstration (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
- Dynamic address learning for enhanced security
- Protected port (Private VLAN Edge) option for restricting the forwarding of traffic to designated ports on the same switch

Manageability

- Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding 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
- Directed unicast requests to a Trivial File Transfer Protocol (TFTP) server for obtaining software upgrades from a TFTP server

- Default configuration storage in Flash memory to ensure that the switch can be connected to a network and can forward traffic with minimal user intervention
- In-band management access through a CMS web-based session
- In-band command-line interface (CLI) management using Telnet connections
- 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 and a modem



Note For additional descriptions of the management interfaces, see the [“Management Options” section on page 1-5](#).

Redundancy

- HSRP for command-switch redundancy
- UniDirectional link detection (UDLD) on all Ethernet ports 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:
 - Per-VLAN spanning-tree plus (PVST+) for balancing load across LANs
 - UplinkFast and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks
- VLAN 1 minimization to reduce 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. The switch CPU continues to send and receive control protocol frames
- Optional spanning-tree features available in the PVST+ 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 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



Note The switch supports up to four spanning-tree instances.

VLAN Support

- The Catalyst 2940 switch supports 4 port-based VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
- IEEE 802.1Q trunking protocol 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
- VLAN Membership Policy Server (VMPS) for dynamic VLAN membership

- VLAN Trunking Protocol (VTP) for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic.
- Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (802.1Q) to be used
- Voice VLAN for creating subnets for voice traffic from Cisco IP Phones
- VLAN 1 minimization to reduce 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. The switch CPU continues to send and receive control protocol frames

Security

- Bridge protocol data unit (BPDU) guard for shutting down a Port Fast-configured port when an invalid configuration occurs
- Protected port option for restricting the forwarding of traffic to designated ports on the same switch
- Password-protected access (read-only and read-write access) to management interfaces (CMS and CLI) for protection against unauthorized configuration changes
- 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
- Multilevel security for a choice of security level, notification, and resulting actions
- Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) support that requires network administrators to login with a user name and password before they can access a switch
- VLAN 1 minimization to reduce 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. The switch CPU continues to send and receive control protocol frames.
- IEEE 802.1X port-based authentication to prevent unauthorized devices from gaining access to the network
- IEEE 802.1X port-based authentication with voice VLAN to permit an IP phone access to the voice VLAN irrespective of the authorized or unauthorized state of the port
- Access control lists (ACLs) for defining security policies on management interfaces, which can be a management VLAN or any traffic that is going directly to the CPU, such as SNMP, Telnet, or web traffic.

For instructions about applying ACLs to management interfaces, refer to the “Configuring IP Services” section of the *Cisco IOS IP and IP Routing Configuration Guide, Cisco IOS Release 12.1* and to the *Cisco IOS IP and IP Routing Command Reference, Cisco IOS Release 12.1*.



Note The switch does not support ACLs on physical interfaces.

Quality of Service and Class of Service

- Support for IEEE 802.1P class of service (CoS) scheduling for classification and preferential treatment of high-priority voice traffic
- Trusted boundary (detect the presence of a Cisco IP Phone, trust the CoS value received, and ensure port security. If the IP phone is not detected, disable the trusted setting on the port and prevent misuse of a high-priority queue.)

- Scheduling of egress queues—Four egress queues on all switch ports. Support for strict priority and weighted round-robin (WRR) CoS policies

Monitoring

- Switch LEDs that provide visual port and switch status
- Switched Port Analyzer (SPAN) for traffic monitoring on any port or VLAN
- SPAN support of intrusion detection systems (IDSs) to monitor, repel, and report network security violations
- MAC address notification for tracking the MAC addresses that the switch has learned or removed
- 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

Management Options

The switches are designed for plug-and-play operation: you only need to 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 configure and monitor the switch—on an individual basis or as part of a switch cluster—through its various management interfaces.

This section discusses these topics:

- [Management Interface Options, page 1-6](#)
- [Advantages of Using CMS and Clustering Switches, page 1-6](#)

Management Options

The switches are designed for plug-and-play operation: you can install the switch in your network without any configuration. To manage the switch remotely, you only need to 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 configure and monitor the switch—on an individual basis or as part of a switch cluster—through its various management interfaces.



Note

To assign an IP address by using the browser-based Express Setup program, refer to Chapter 1, “Quick Setup”, in the hardware installation guide.

This section discusses these topics:

- [Management Interface Options, page 1-6](#)
- [Advantages of Using CMS and Clustering Switches, page 1-6](#)

Management Interface Options

You can configure and monitor individual switches and switch clusters by using these interfaces:

- **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. Using CMS, you can configure and monitor a standalone switch, a specific cluster member, or an entire switch cluster. You can also display network topologies to gather link information and display switch images to modify switch and port level settings.

For more information about CMS, see [Chapter 3, “Getting Started with CMS.”](#)

- **CLI**—The switch Cisco IOS CLI software is enhanced to support desktop-switching features. You can configure and monitor the switch and switch cluster members from the CLI. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station.

For more information about the CLI, see [Chapter 2, “Using the Command-Line Interface.”](#)

- **SNMP**—SNMP provides a means to monitor and control the switch and switch cluster members. You can manage switch configuration settings, performance, and security and collect statistics by using SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView.

You can manage the switch 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 RMON groups.

For more information about using SNMP, see the [Chapter 23, “Configuring SNMP.”](#)

Advantages of Using CMS and Clustering Switches

Using CMS and switch clusters can simplify and minimize your configuration and monitoring tasks. You can use Cisco switch clustering technology to manage up to 16 interconnected and supported Catalyst switches through one IP address as if they were a single entity. This can conserve IP addresses if you have a limited number of them. CMS is the easiest interface to use and makes switch and switch cluster management accessible to authorized users from any PC on your network.

By using switch clusters and CMS, you can:

- Manage and monitor interconnected Catalyst switches (refer to the release notes for a list of supported switches), regardless of their geographic proximity and interconnection media, including Small Form-Factor Pluggable (SFP), Ethernet, Fast Ethernet, Fast EtherChannel, Gigabit Ethernet, and Gigabit EtherChannel connections.
- Accomplish multiple configuration tasks from a single CMS window without needing to remember CLI commands to accomplish specific tasks.
- Apply actions from CMS to multiple ports and multiple switches at the same time to avoid re-entering the same commands for each individual port or switch. Here are some examples of globally setting and managing multiple ports and switches:
 - Port configuration such as speed and duplex settings
 - Port and console port security settings
 - NTP, STP, and VLAN configurations
 - Inventory and statistic reporting and link and switch-level monitoring and troubleshooting
 - Group software upgrades

- View a topology of interconnected devices to identify existing switch clusters and eligible switches that can join a cluster. You can also use the topology to quickly identify link information between switches.
- Monitor real-time status of a switch or multiple switches from the LEDs on the front-panel images. The port LED colors on the images are similar to those on the physical LEDs.
- Use an interactive mode that takes you step-by-step through configuring complex features such as VLANs.

For more information about CMS, see [Chapter 3, “Getting Started with CMS.”](#) For more information about switch clusters, see [Chapter 5, “Clustering Switches.”](#)

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 1-1](#) 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	<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Increased power of new PCs, workstations, and servers • High demand from networked applications (such as e-mail with large attached files) and from bandwidth-intensive applications (such as multimedia) 	<ul style="list-style-type: none"> • Connect global resources—such as servers and routers to which network users require equal access—directly to the Fast Ethernet or Gigabit Ethernet switch ports so that they have their own Fast Ethernet or Gigabit Ethernet segment. • Use the Fast EtherChannel or Gigabit 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 such as voice and data integration 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
High demand for multimedia support	<ul style="list-style-type: none"> Use IGMP and MVR to efficiently forward multicast traffic.
High demand for protecting mission-critical applications	<ul style="list-style-type: none"> Use VLANs and protected ports to provide security and port isolation. 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	<ul style="list-style-type: none"> Use quality of service (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.
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.	<ul style="list-style-type: none"> Use the Catalyst 2900 LRE XL or Catalyst 2950 LRE switches to provide up to 15 Mb of IP connectivity over existing infrastructure (existing telephone lines).

Small Network Configuration

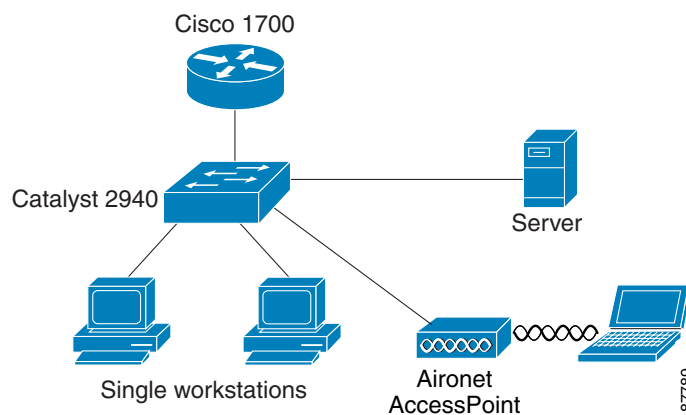
Figure 1-1 shows a configuration for a network that has up to 25 users. Users in this network require e-mail, file-sharing, database, and Internet access.



Note

An external power supply is required for the Cisco Aironet access point.

Figure 1-1 Small to Medium-Sized Network Configuration



You optimize network performance by placing workstations on the same logical segment (VLAN) as the servers they access most often. This in turn reduces access point processing and improves performance and throughput.

Workstations are connected directly to the 10/100 switch ports for their own 10- or 100-Mbps access to network resources (such as web and mail servers). When a workstation is configured for full-duplex operation, it receives up to 200 Mbps of dedicated bandwidth from the switch. The Cisco Aironet

Wireless Access Point provides network connectivity for mobile users. Although the wireless access provides less bandwidth, it allows users to have network connectivity regardless of their location in the office.

A server is connected to the Gigabit ports on the switch, allowing 1-Gbps throughput to users when needed. When the switch and server ports are configured for full-duplex operation, the links provide 2 Gbps of bandwidth. For networks that do not require Gigabit performance from a server, connect the server to a Fast Ethernet or Fast EtherChannel switch port.

Connecting a router to a Fast Ethernet switch port provides multiple, simultaneous access to the Internet through one line.

Collapsed Backbone and Switch Cluster Configuration

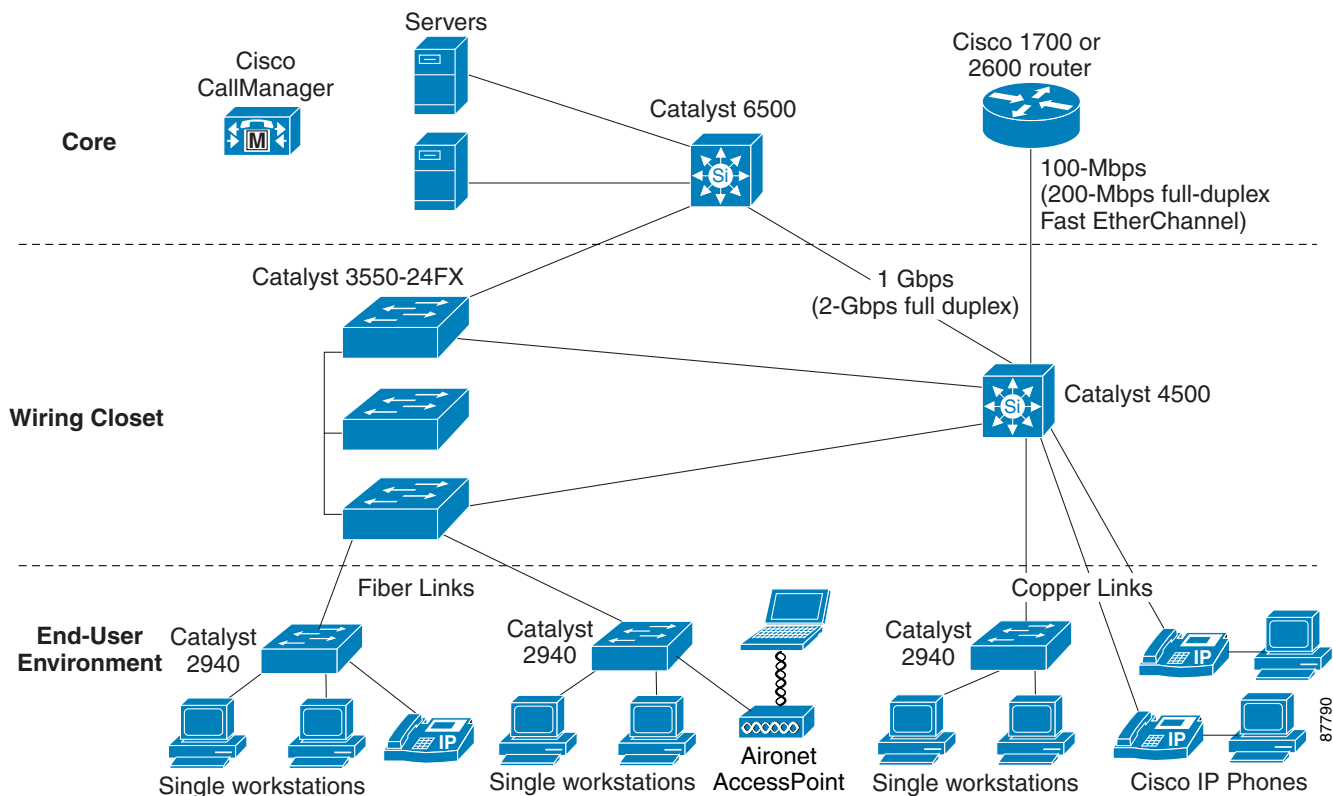
Figure 1-2 shows a configuration for a network of up to 500 employees. This network uses a collapsed backbone and switch clusters. A collapsed backbone has high-bandwidth uplinks from all segments and subnetworks to a single device, such as a Gigabit switch, that serves as a single point for monitoring and controlling the network. You can use a Catalyst 6500 switch, as shown, or other Gigabit switch to create a Gigabit backbone. A Layer 3 backbone switch provides the benefits of inter-VLAN routing and allows the router to focus on WAN access.



Note

An external power supply is required for IP phones and the Cisco Aironet access point.

Figure 1-2 Collapsed Backbone and Switch Cluster Configuration



The workgroups are created by clustering all the Catalyst switches except the Catalyst 4500 switch. Using CMS and Cisco switch clustering technology, you can group the switches into multiple clusters, as shown, or into a single cluster. You can manage a cluster through the IP address of its active and standby command switches, regardless of the geographic location of the cluster members.

Workgroups that require fiber connectivity can be connected to the network by the 2940-8TF-S with its fixed 100-FX uplink. Multiple 100-FX links can be aggregated to a 3550-24FX or Catalyst 4500. As an alternative, a Catalyst 2940-8TF with a 1000Base-SX SFP can be used to provide Gigabit connectivity to a Catalyst 3550-12G or Catalyst 4500.

This network uses VLANs to segment the network logically into well-defined broadcast groups and for security management. You can configure up to four VLANs on the Catalyst 2940 switch. Data and multimedia traffic are configured on the same VLAN. Voice traffic from the Cisco IP Phones are configured on separate voice VLAN IDs (VVIDs), or you can combine voice, multimedia, and data on a single VLAN. For any switch port connected to Cisco IP Phones, 802.1P/Q QoS gives forwarding priority to voice traffic over data traffic.

Grouping servers in a centralized location provides benefits such as security and easier maintenance. The Gigabit connections to a server farm provide the workgroups full access to the network resources (such as a call-processing server running Cisco CallManager software, a DHCP server, or an IP/TV multicast server).

Cisco IP Phones are connected—using standard straight-through, twisted-pair cable with RJ-45 connectors—to the 10/100 inline-power ports on the Catalyst 4500 switches and to the 10/100 ports on the Catalyst 2940 switches. These multiservice switch ports automatically detect any IP phones that are connected. Cisco CallManager controls call processing, routing, and 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.

Each 10/100 inline-power port on the Catalyst 4500 switches provides –48 VDC power to the Cisco IP Phone. The IP phone can receive redundant power when it is also connected to an AC power source. IP phones not connected to an inline power switch receive power from an AC power source.

Large Campus Configuration

Figure 1-3 shows a configuration for a network of more than 1000 users. Because it can aggregate up to 142 nonblocking Gigabit connections, a Catalyst 6500 multilayer switch is used as the distribution layer switch.

You can use the workgroup configurations shown in previous examples to create workgroups with Gigabit uplinks to the Catalyst 6500 switch. For example, you can use switch clusters that have a mix of Catalyst 3550 and 2950 switches. Catalyst 2940 switches are used outside of the wiring closet in the user environment to add managed ports if pulling additional wiring from the wiring closet is unfeasible or not cost efficient.

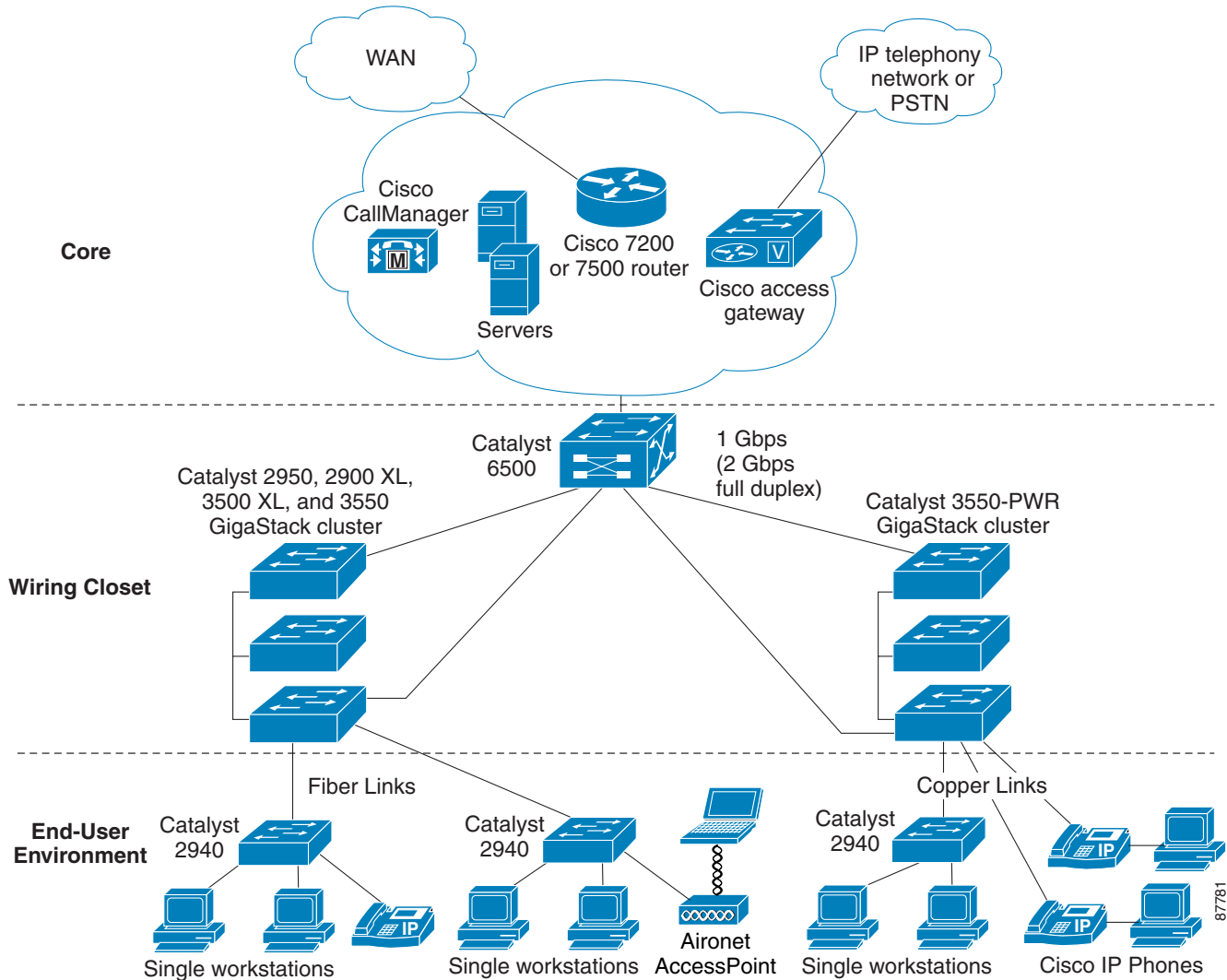
The Catalyst 6500 switch provides the workgroups with Gigabit access to core resources:

- Cisco 7000 series router for access to the WAN and the Internet.
- Server farm that includes a call-processing server running Cisco CallManager software. Cisco CallManager controls call processing, routing, and IP phone features and configuration.
- Cisco Access gateway (such as Cisco Access Digital Trunk Gateway or Cisco Access Analog Trunk Gateway) that connects the IP network to the Public Switched Telephone Network (PSTN) or to users in an IP telephony network.

**Note**

An external power supply is required for IP phones and the Cisco Aironet access point.

Figure 1-3 Large Campus Configuration



Where to Go Next

Before configuring the switch, review these sections for start-up information:

- [Chapter 2, “Using the Command-Line Interface”](#)
- [Chapter 3, “Getting Started with CMS”](#)
- [Chapter 4, “Assigning the Switch IP Address and Default Gateway”](#)

