



CHAPTER 1

Overview

This chapter provides these topics about the Catalyst 2950 and Catalyst 2955 switch software:

- [Features, page 1-1](#)
- [Management Options, page 1-9](#)
- [Network Configuration Examples, page 1-11](#)
- [Where to Go Next, page 1-25](#)



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

The switch software supports the switches listed in [Table 1-1](#) and in the release notes.

Table 1-1 **Switches Supported**

Switch	Software Image
Catalyst 2950-12	SI ¹
Catalyst 2950-24	SI
Catalyst 2950C-24	EI ²
Catalyst 2950G-12-EI	EI
Catalyst 2950G-24-EI	EI
Catalyst 2950G-24-EI-DC	EI
Catalyst 2950G-48-EI	EI
Catalyst 2950ST-8 LRE	EI
Catalyst 2950ST-24 LRE	EI
Catalyst 2950ST-24 LRE 997	EI
Catalyst 2950SX-24	SI
Catalyst 2950SX-48-SI	SI
Catalyst 2950T-24	EI

Table 1-1 Switches Supported (continued)

Switch	Software Image
Catalyst 2950T-48-SI	SI
Catalyst 2955C-12	EI
Catalyst 2955S-12	EI
Catalyst 2955T-12	EI

1. SI = standard software image
2. EI = enhanced software image

Certain Cisco Long-Reach Ethernet (LRE) customer premises equipment (CPE) devices are not supported by certain Catalyst 2950 LRE switches. In [Table 1-2](#), *Yes* means that the CPE is supported by the switch; *No* means that the CPE is not supported by the switch.

Table 1-2 LRE Switch and CPE Compatibility Matrix

LRE Devices	Catalyst 2950ST-8 LRE switch	Catalyst 2950ST-24 LRE switch	Catalyst 2950ST-24 LRE 997 switch
Cisco 575 LRE CPE	Yes	Yes	No
Cisco 576 LRE 997 CPE	No	No	Yes
Cisco 585 LRE CPE	Yes	Yes	No

This section describes the features supported in this release:

**Note**

Some features require that you have the EI installed on your switch. For a list of the switches that support the EI, see [Table 1-1](#), or see the release notes for this release.

Ease of Deployment and Ease of Use

The switch ships with these features to make the deployment and 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.
- User-defined Smartports macros for creating custom switch configurations for simplified deployment across the network.
- 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.
- Network Assistant application for
 - Simplifying and minimizing switch and switch cluster management from anywhere in your intranet.

- Accomplishing multiple configuration tasks from a single 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.
- Downloading an image to a switch by using TFTP.
- 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.
- Real-time status monitoring of a switch or multiple switches from the LEDs on the front-panel images from the device manager and from Network Assistant.
- Switch clustering technology for
 - Unified configuration, monitoring, authentication, and software upgrade of multiple switches (see 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.



Note For the Network Assistant software requirements, and for more information about clustering, see the *Getting Started with Cisco Network Assistant*, available on Cisco.com. For clustering requirements, including supported Cisco IOS releases, see the release notes for this release.

- Hot Standby Router Protocol (HSRP) for command-switch redundancy. The redundant command switches used for HSRP must have compatible software releases.
- DHCP-base autoconfiguration automatically configures a switch at startup with an IP address.

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
- IEEE 802.3x flow control on Gigabit Ethernet ports operating in full-duplex mode
- Fast EtherChannel and Gigabit EtherChannel for enhanced fault tolerance and for providing up to 2 Gbps of bandwidth among switches, routers, and servers
- Support for frames larger than 1500 bytes. These switches support frame sizes from 1500 to 1530 bytes:
 - Catalyst 2950G-12-EI, 2950G-24-EI, 2950G-24-EI-DC, and 2950G-48-EI switches running Cisco IOS Release 12.1(6)EA2 or later
 - Catalyst 2950 LRE switches
 - Catalyst 2955 switches

- Port blocking on forwarding unknown unicast and multicast traffic (available only on the Catalyst LRE switches and on the Catalyst 2950G-12-EI, 2950G-24-EI, 2950G-24-EI-DC, 2950G-48-EI, and 2955 switches)
- 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 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
- Protected port (private VLAN edge port) option for restricting the forwarding of traffic to designated ports on the same switch
- Dynamic address learning for enhanced security

Manageability

- Cisco Intelligence Engine 2100 (IE2100) Series Cisco Networking Services (CNS) embedded agents for automating switch management, configuration storage and delivery (available only with the EI)
- DHCP-based autoconfiguration for automatically configuring the switch during startup with IP address information and a configuration file that it receives during DHCP-based autoconfiguration



Note DHCP replaces the Bootstrap Protocol (BOOTP) feature autoconfiguration to ensure retrieval of configuration files by unicast TFTP messages. BOOTP is available in earlier software releases for this switch.

- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts (available only on the Catalyst 2955 switch)
- DHCP-Based Autoconfiguration with a saved file
- 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 (available only with the EI)
- 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
- Directed unicast requests to a 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 the embedded device manager through a Netscape Navigator or Internet Explorer session or through Network Assistant
- In-band management access through up to 16 simultaneous Telnet connections for multiple command-line interface (CLI)-based sessions over the network
- In-band management access through up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (only available in the enhanced cryptographic software image)
- In-band management access through SNMP versions 1, 2c, and 3 get and set requests
- Out-of-band management access through the switch console port to a directly-attached terminal or to a remote terminal through a serial connection and a modem



Note For additional descriptions of the management interfaces, see the [“Management Options” section on page 1-9](#).

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.
 - Up to 64 spanning-tree instances supported
 - Per-VLAN spanning-tree plus (PVST+) for load balancing across VLANs
 - Rapid PVST+ for load balancing across VLANs
 - UplinkFast, cross-stack UplinkFast, and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing among 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 transitioning root and designated ports to the forwarding state
- Optional spanning-tree features available in the PVST+, rapid PVST+, and MSTP modes:
 - 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

VLAN Support

- The switches support 250 port-based VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth



Note The Catalyst 2950-12, Catalyst 2950-24, Catalyst 2950SX-24, Catalyst 2950SX-48-SI, and Catalyst 2950T-48-SI switches support only 128 port-based VLANs.

- The switch supports up to 4094 VLAN IDs to allow service provider networks to support the number of VLANs allowed by the IEEE 802.1Q standard
- 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) pruning 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 (IEEE 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 (device manager, Network Assistant, 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
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers (available only with the EI)
- Multilevel security for a choice of security level, notification, and resulting actions
- MAC-based port-level security for restricting the use of a switch port to a specific group of source addresses and preventing switch access from unauthorized stations
- TACACS+, a proprietary feature for managing network security through a TACACS server
- IEEE 802.1x port-based authentication to prevent unauthorized devices from gaining access to the network
- 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
- IEEE 802.1x with 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.
- Network Admission Control (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 9-27.
- Standard and extended IP access control lists (ACLs) for defining security policies (available only with the EI)

Quality of Service and Class of Service

- Automatic quality of service (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues (only available in the EI)
- Classification
 - IEEE 802.1p class of service (CoS) with four priority queues on the switch 10/100 and LRE ports and eight priority queues on the Gigabit ports for prioritizing mission-critical and time-sensitive traffic from data, voice, and telephony applications
 - IP Differentiated Services Code Point (IP DSCP) and CoS marking priorities on a per-port basis for protecting the performance of mission-critical applications (only available with the EI)
 - 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 (only available in the EI)
 - Support for IEEE 802.1p 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.)
- Policing
 - Traffic-policing policies on the switch port for allocating the amount of the port bandwidth to a specific traffic flow
 - Policing traffic flows to restrict specific applications or traffic flows to metered, predefined rates
 - Up to 60 policers on ingress Gigabit-capable Ethernet ports
Up to six policers on ingress 10/100 ports
Granularity of 1 Mbps on 10/100 ports and 8 Mbps on 10/100/1000 ports
 - Out-of-profile markdown for packets that exceed bandwidth utilization limits



Note Policing is available only in the EI.

- Egress Policing and 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 show port and switch status
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN



Note RSPAN is available only in the EI.

- SPAN support of Intrusion Detection Systems (IDSs) to monitor, repel, and report network security violations
- Four groups (history, statistics, alarms, and events) of embedded remote monitoring (RMON) agents for network monitoring and traffic analysis
- 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
- Facilities for processing alarms related to temperature, power-supply conditions, and the status of the Ethernet ports (available only on the Catalyst 2955 switch)

LRE Features (available only on Catalyst 2950 LRE switches)

- Data, voice, and video transmission through categorized and noncategorized unshielded twisted-pair cable (Category 1, 2, and 3 structured and unstructured cable, such as existing telephone lines) in multi-unit, multidwelling, and multitenant buildings
- Up to 15 Mbps of bandwidth to remote Ethernet devices at distances of up to 4921 feet (1500 meters) on each switch LRE port
- Compliance with American National Standards Institute (ANSI) and European Telecommunication Standards Institute (ETSI) standards for spectral-mode compatibility with asymmetric digital subscriber line (ADSL), Integrated Services Digital Network (ISDN), and digital telephone networks
- Configuration and monitoring of connections between:
 - Switch LRE ports and the Ethernet ports on remote LRE customer premises equipment (CPE) devices, such as the Cisco 575 LRE CPE or the Cisco 585 LRE CPE
 - CPE Ethernet ports and remote Ethernet devices, such as a PC
- Support for connecting to the public switched telephone network (PSTN) through plain old telephone service (POTS) splitters such as the Cisco LRE 48 POTS Splitter
- Support for the rate selection, a utility that allows for automatic selection of transmission rates through sequences
- Support for Reed-Solomon error correction
- Support for a protected port on Cisco 585 CPE devices
- Support for small form-factor pluggable (SFP) modules instead of Gigabit Interface Converter (GBIC) modules

- Support for configuring the interleave delay feature
- Support for DC-input power and compliance with the VDSL 997 band plan on Catalyst 2950ST-24 LRE 997 switches
- Upstream power back-off mechanism for normalization of the upstream receive power levels by requiring the CPE devices on shorter lines to transmit at a lower power level than the CPEs on longer lines
- Support for sending LRE debugging messages to the LRE message logging process and to the system message logging process

Management Options

The switch is 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.



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.

This section discusses these topics:

- [Management Interface Options, page 1-9](#)
- [Advantages of Using Network Assistant and Clustering Switches, page 1-10](#)

Management Interface Options

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

- An embedded device manager—The device manager is a GUI that is integrated in the software image. You use it to can configure and to monitor a single switch through a web browser. For more information about the device manager, see the switch online help.
- Network Assistant—Network Assistant is a GUI that can be downloaded from Cisco.com. You use it to manage a single switch or a cluster of switches. For more information about Network Assistant, see the *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- CLI—The switch Cisco IOS software supports desktop-switching features. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet or SSH from a remote management station.

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

- IE2100—Cisco Intelligence Engine 2100 Series Configuration Registrar is a network management device that works with embedded 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 5, “Configuring Cisco IOS CNS Agents.”](#)

- **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 27, “Configuring SNMP.”](#)

Advantages of Using Network Assistant and Clustering Switches

Using Network Assistant 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. Network Assistant 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 Network Assistant, you can:

- Manage and monitor interconnected Catalyst switches (see the release notes for a list of supported switches), regardless of their geographic proximity and interconnection media, including Ethernet, Fast Ethernet, Fast EtherChannel, Cisco GigaStack GBIC, Gigabit Ethernet, and Gigabit EtherChannel connections.
- Accomplish multiple configuration tasks from a single Network Assistant window without needing to remember CLI commands to accomplish specific tasks.
- Apply actions from Network Assistant 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, VLAN, and quality of service (QoS) 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 system, redundant power system (RPS), and 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, ACLs, and QoS.
- Use a wizard that prompts you to provide the minimum required information to configure complex features such as QoS priorities for video traffic, priority levels for data applications, and security.

For more information about Network Assistant and clustering, see the *Getting Started with Cisco Network Assistant*, available on Cisco.com.

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” section on page 1-11
- “Small to Medium-Sized Network Configuration” section on page 1-14
- “Collapsed Backbone and Switch Cluster Configuration” section on page 1-15
- “Hotel Network Configuration” section on page 1-17
- “Service-Provider Central-Office Configuration” section on page 1-19
- “Large Campus Configuration” section on page 1-21
- “Multidwelling Network Using Catalyst 2950 Switches” section on page 1-22
- “Long-Distance, High-Bandwidth Transport Configuration” section on page 1-24

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 1-3 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 1-3 *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 1-4 describes some network demands and how you can meet those demands.

Table 1-4 *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 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 or 802.1Q.
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).

Figure 1-1 shows configuration examples of using the Catalyst switches to create these networks:

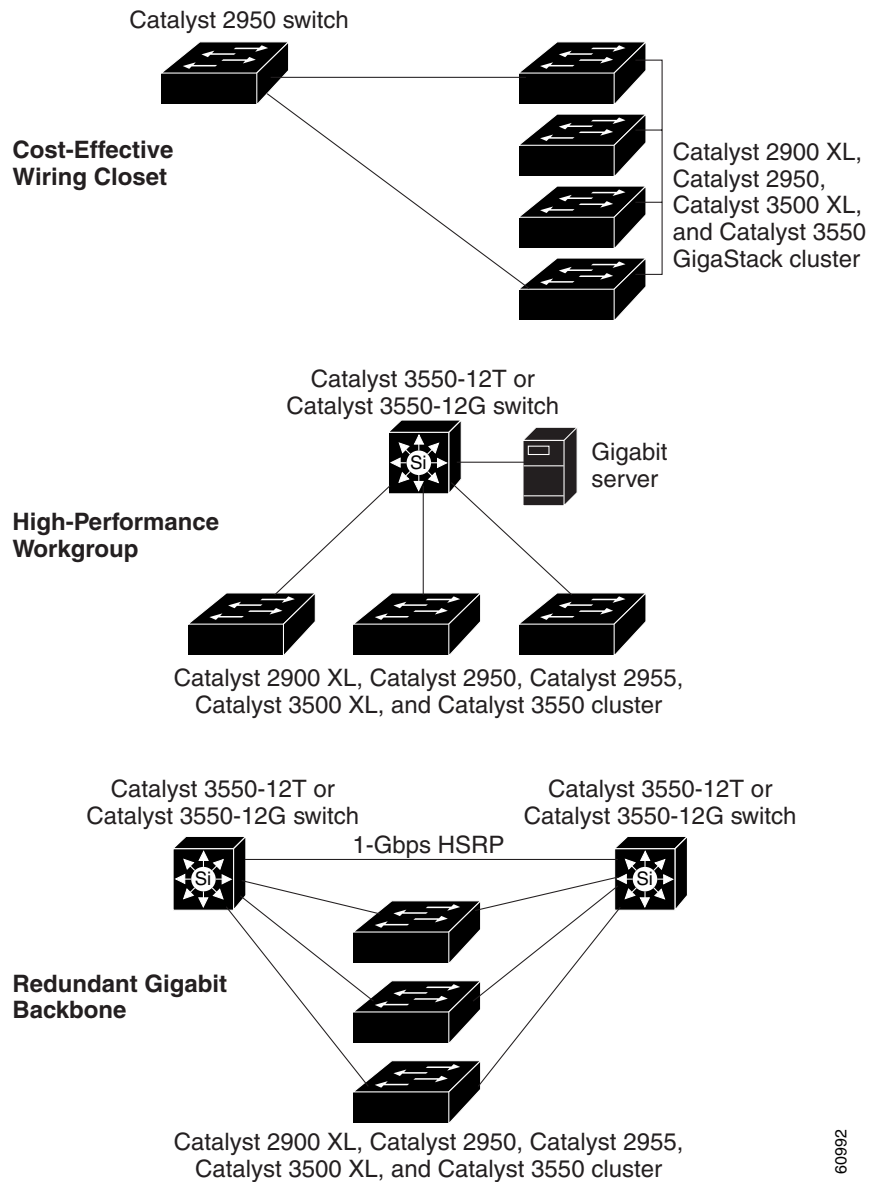
- **Cost-effective wiring closet**—A cost-effective way to connect many users to the wiring closet is to connect up to nine Catalyst 2900 XL, Catalyst 2950, Catalyst 3500 XL, and Catalyst 3550 switches through GigaStack GBIC connections. When you use a stack of Catalyst 2950G-48 switches, you can connect up to 432 users. To preserve switch connectivity if one switch in the stack fails, connect the bottom switch to the top switch to create a GigaStack loopback, and enable cross-stack UplinkFast on the cross-stack Gigabit uplinks.

You can create backup paths by using Fast Ethernet, Gigabit, Fast EtherChannel, or Gigabit EtherChannel links. Using Gigabit modules on two of the switches, you can have redundant uplink connections to a Gigabit backbone switch such as the Catalyst 3550-12G switch. If one of the redundant connections fails, the other can serve as a backup path. You can configure the stack members and the Catalyst 3550-12G switch as a switch cluster to manage them through a single IP address.

- **High-performance workgroup**—For users who require high-speed access to network resources, use Gigabit modules to connect the switches directly to a backbone switch in a star configuration. Each switch in this configuration provides users with a dedicated 1-Gbps connection to network resources in the backbone. Compare this with the switches in a GigaStack configuration, where the 1-Gbps connection is shared among the switches. With the high speed uplink to the distribution server, the user can efficiently obtain and store data from servers. Using these Gigabit Ethernet modules also provides flexibility in media and distance options:
 - 1000BASE-T GBIC: copper connections of up to 328 feet (100 meters)
 - 1000BASE-SX GBIC: fiber connections of up to 1804 feet (550 meters)
 - 1000BASE-LX/LH GBIC: fiber connections of up to 32,808 feet (10 kilometers)
 - 1000BASE-ZX GBIC: fiber connections of up to 328,084 feet (100 kilometers)

- GigaStack GBIC module for creating a 1-Gbps stack configuration of up to nine supported switches. The GigaStack GBIC supports one full-duplex link (in a point-to-point configuration) or up to nine half-duplex links (in a stack configuration) to other Gigabit Ethernet devices. Using the required Cisco proprietary signaling and cabling, the GigaStack GBIC-to-GigaStack GBIC connection cannot exceed 3 feet (1 meter).
- SFP modules: fiber and copper connections of up to 32,808 feet (10 kilometers) (supported only on the Catalyst 2950 LRE switches)
- Redundant Gigabit backbone—Using HSRP, you can create backup paths between Catalyst 3550-12T-L3 switches. To enhance network reliability and load balancing for different VLANs and subnets, you can connect the Catalyst 2950 switches, again in a star configuration, to two backbone switches. If one of the backbone switches fails, the second backbone switch preserves connectivity between the switches and network resources.

Figure 1-1 Example Configurations

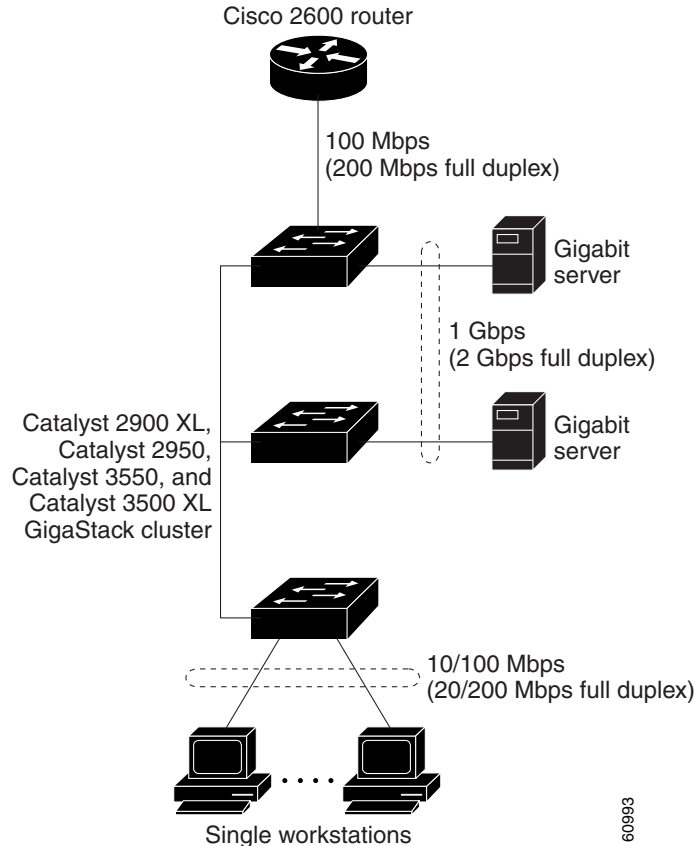


60992

Small to Medium-Sized Network Configuration

Figure 1-2 shows a configuration for a network that has up to 250 users. Users in this network require e-mail, file-sharing, database, and Internet access.

You optimize network performance by placing workstations on the same logical segment as the servers they access most often. This divides the network into smaller segments (or workgroups) and reduces the amount of traffic that travels over a network backbone, thereby increasing the bandwidth available to each user and improving server response time.

Figure 1-2 Small to Medium-Sized Network Configuration

A *network backbone* is a high-bandwidth connection (such as Fast Ethernet or Gigabit Ethernet) that interconnects segments and network resources. It is required if numerous segments require access to the servers. The Catalyst 2900 XL, Catalyst 2950, Catalyst 3500 XL, and Catalyst 3550 switches in this network are connected through a GigaStack GBIC on each switch to form a 1-Gbps network backbone. This GigaStack can also be configured as a switch cluster, with primary and secondary command switches for redundant cluster management.

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.

Servers are connected to the GBIC module ports on the switches, 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 1-3 shows a configuration for a network of approximately 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 3550-12T-L3 switch, as shown, or a Catalyst 3508G XL switch to create a Gigabit backbone. A Catalyst 3550-12T-L3 backbone switch provides the benefits of inter-VLAN routing and allows the router to focus on WAN access.

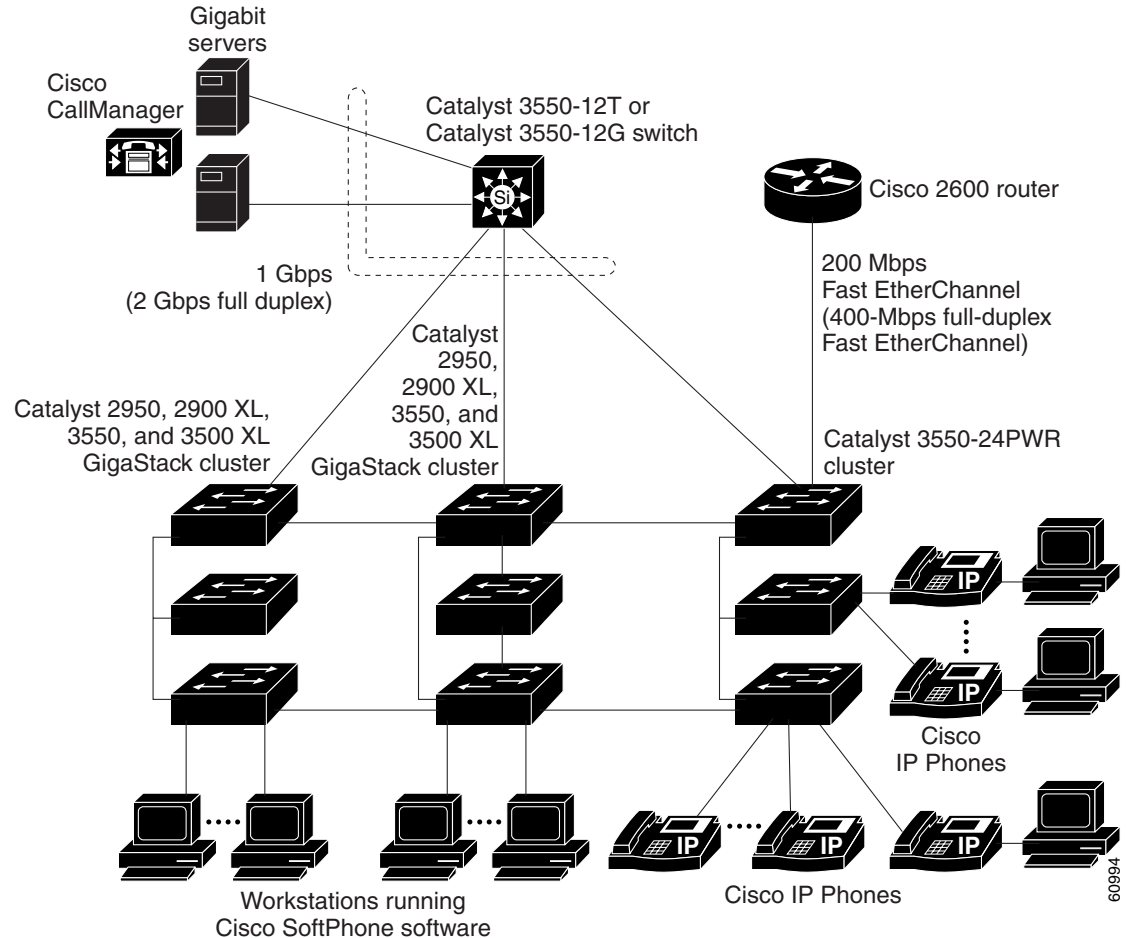
The workgroups are created by clustering all the Catalyst switches except the Catalyst 4908G-L3 switch. Using Network Assistant and Cisco switch clustering technology, you can group the switches into multiple clusters, as shown, or into a single cluster. You can manage a cluster through the IP address of its active and standby command switches, regardless of the geographic location of the cluster members.

This network uses VLANs to segment the network logically 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 voice VLAN IDs (VVIDs). You can have up to four VVIDs per wiring closet. 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 or 802.1Q 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 3550-24PWR switches and to the 10/100 ports on the Catalyst 2950 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 3550-24PWR 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 the Catalyst 3550-24PWR switches receive power from an AC power source.

Figure 1-3 Collapsed Backbone and Switch Cluster Configuration

Hotel Network Configuration

Figure 1-4 shows Catalyst 2950ST-8 LRE and 2950ST-24 LRE switches in a hotel network environment with approximately 200 rooms. This network includes a PBX switchboard, a router, and high-speed servers.

Connected to the telephone line in each hotel room is an LRE CPE device, such as a Cisco LRE CPE device. The LRE CPE device provides:

- Two RJ-11 ports, one for connecting to the telephone jack on the wall and one for connecting to a POTS telephone.
- One or more RJ-45 Ethernet ports for connecting to devices such as a customer's laptop, the room IP phone, the television set-top box, or a room environmental control device. A Cisco 575 LRE CPE provides one Ethernet connection; a Cisco 585 LRE CPE provides four.

When connected to the CPE device, the Ethernet devices and room telephone share the same telephone line.

**Note**

All telephones not directly connected to the hotel room CPE device require microfilters with a 300-ohm termination. Microfilters improve voice call quality when voice and data equipment are using the same telephone line. They also prevent nonfiltered telephone rings and nonfiltered telephone transitions (such as on-hook to off-hook) from interrupting the Ethernet connection.

Through a patch panel, the telephone line from each room connects to a nonhomologated POTS splitter, such as the Cisco LRE 48 POTS Splitter. The splitter routes data (high-frequency) and voice (low-frequency) traffic from the telephone line to a Catalyst 2950 LRE switch and digital private branch exchange (PBX). The PBX routes voice traffic to the PSTN.

If a PBX is not on-site, a homologated POTS splitter is required to connect directly to the PSTN.

**Note**

Consult the regulations for connecting to the PSTN in your area.

If a connection to a phone network is not required at all, a splitter is not needed, and the switch can connect directly to the patch panel.

**Note**

Cisco LRE products can share lines with analog telephones, Integrated Services Digital Network (ISDN) telephone network, and PBX switches that use the 0 to 700 kHz frequency range.

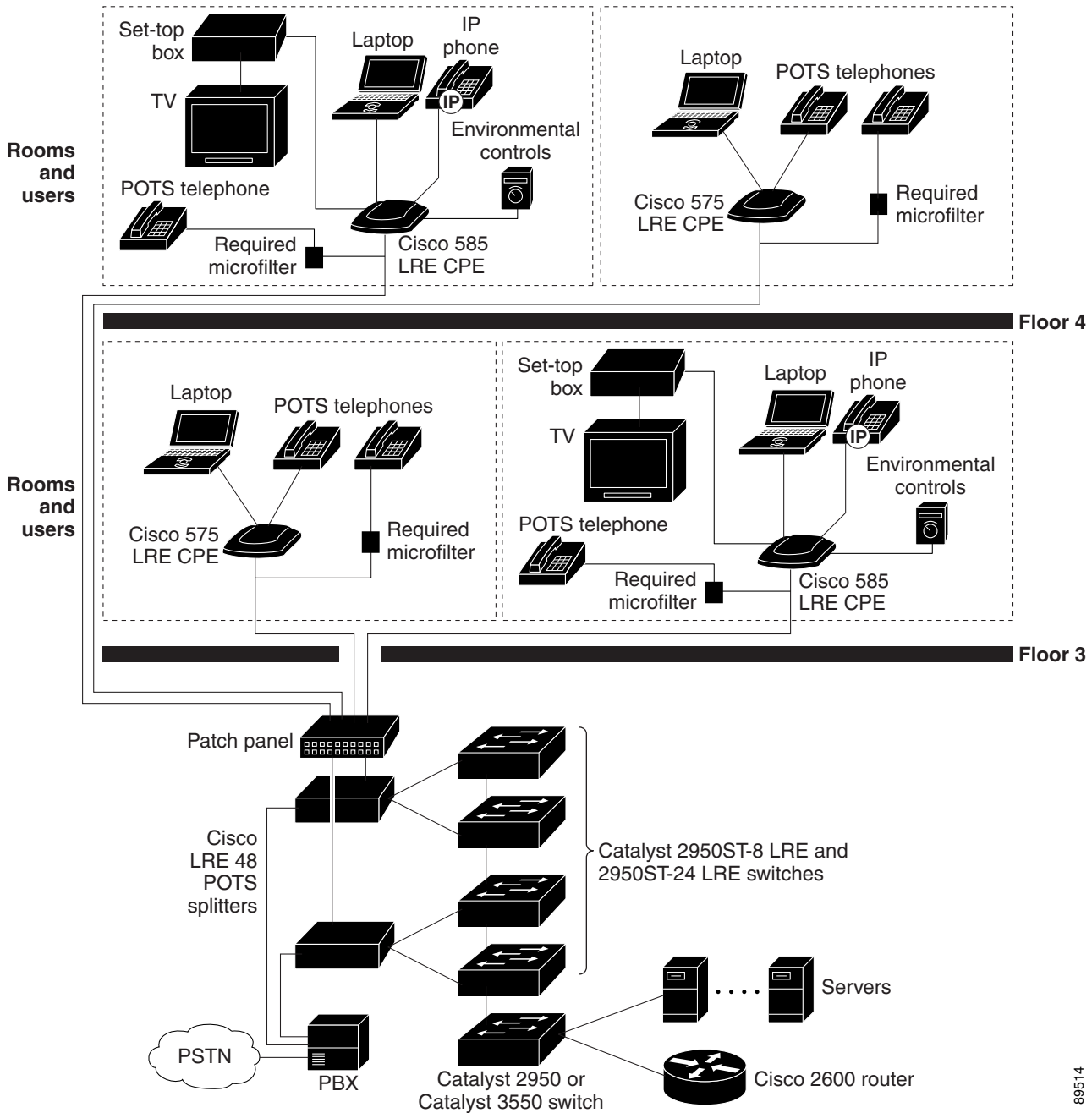
Data to and from the room devices (such as e-mail for the laptop and IP multicast traffic for the television) are transferred through the LRE link, which is established between the CPE RJ-11 wall port and the LRE port on an LRE switch. The upstream and downstream rates on the LRE link are controlled by a profile configured on each LRE port. If the LRE switch was connected to the PSTN through a homologated POTS splitter, all LRE ports would use an ANSI-compliant LRE profile named *LRE-998-15-4*.

The Catalyst 2950 LRE switches are cascaded through their 10/100/1000 switch ports. Each switch also has a 10/100/1000 connection to an aggregation switch, such as a Catalyst 3550-12G switch. The aggregation switch can connect to these devices:

- Accounting, billing, and provisioning servers
- A router that provides Internet access to the premises

You can manage the switches as a switch cluster and through Network Assistant. You can also manage and monitor the individual CPE devices from the LRE switches to which they are connected. The Catalyst 2950 LRE switch ports support the same software features as 10/100/1000 switch ports. For example, you can configure port-based VLANs on the LRE ports to provide individual port security and protected ports to further prevent unwanted broadcasts within the VLANs.

Figure 1-4 Network Hotel Configuration



89514

Service-Provider Central-Office Configuration

Figure 1-5 shows the Catalyst 2950ST-24 LRE 997 switches in a service-provider central-office network environment. The Catalyst 2950ST-24 LRE 997 switches have DC-input power supply and are compliant with the VDSL 997 band plan. The Catalyst 2950 LRE switches are located in a central office and are connected to the Cisco 576 LRE 997 CPE devices located in different buildings. The switches also connect to a Cisco 7500 router.

You can use a POTS splitter to connect the switches to the CPE devices. The splitter routes data (high-frequency) to a Catalyst 2950 LRE switch and voice (low-frequency) traffic from the telephone line to a PSTN.

Connected to the telephone line in each office is an Cisco 576 LRE 997 CPE device. The LRE CPE device provides:

- Two RJ-11 ports, one for connecting to the telephone jack on the wall and one for connecting to a POTS telephone.
- One RJ-45 Ethernet port for connecting to devices such as a customer's laptop, the office's IP phone, the television set-top box, or a office environmental control device. A Cisco 576 LRE 997 provides one Ethernet connection.

When connected to the CPE device, the Ethernet devices and office telephone share the same telephone line.

**Note**

All telephones not directly connected to the office CPE device require microfilters with a 300-ohm termination. Microfilters improve voice call quality when voice and data equipment are using the same telephone line. They also prevent nonfiltered telephone rings and nonfiltered telephone transitions (such as on-hook to off-hook) from interrupting the Ethernet connection.

**Note**

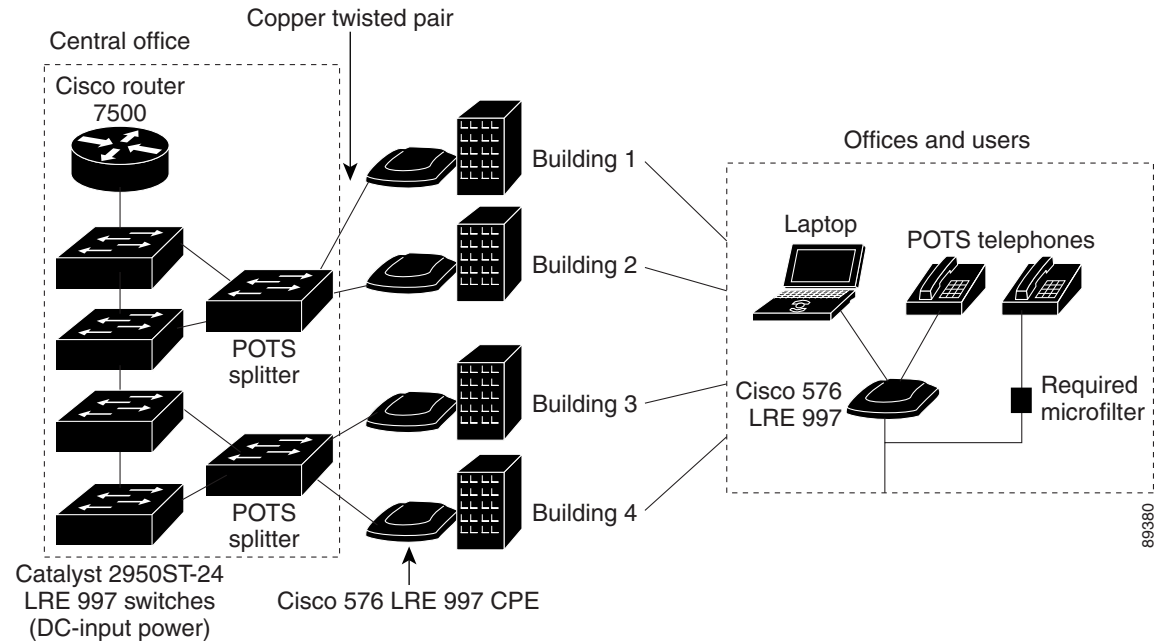
Cisco LRE products can share lines with analog telephones and Integrated Services Digital Network (ISDN) telephone network that use the 0 to 120 kHz frequency range.

Data to and from the office devices (such as e-mail for the laptop and IP multicast traffic for the television) are transferred through the LRE link, which is established between the CPE RJ-11 wall port and the LRE port on an LRE switch. The upstream and downstream rates on the LRE link are controlled by a profile configured on each LRE port.

The Catalyst 2950 LRE switches are cascaded through their 10/100/1000 switch ports. Each switch also has a 10/100/1000 connection to an aggregation switch, such as a Catalyst 3550-12G switch or Cisco 7600 router.

You can manage the switches as a switch cluster and through Network Assistant. You can also manage and monitor the individual CPE devices from the LRE switches to which they are connected. The Catalyst 2950 LRE switch ports support the same software features as 10/100/1000 switch ports. For example, you can configure port-based VLANs on the LRE ports to provide individual port security and protected ports to further prevent unwanted broadcasts within the VLANs.

Figure 1-5 Service Provider Central Office Configuration



Large Campus Configuration

Figure 1-6 shows a configuration for a network of more than 1000 users. Because it can aggregate up to 130 Gigabit connections, a Catalyst 6500 multilayer switch is used as the backbone 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 2950 and Catalyst 2955 switches.

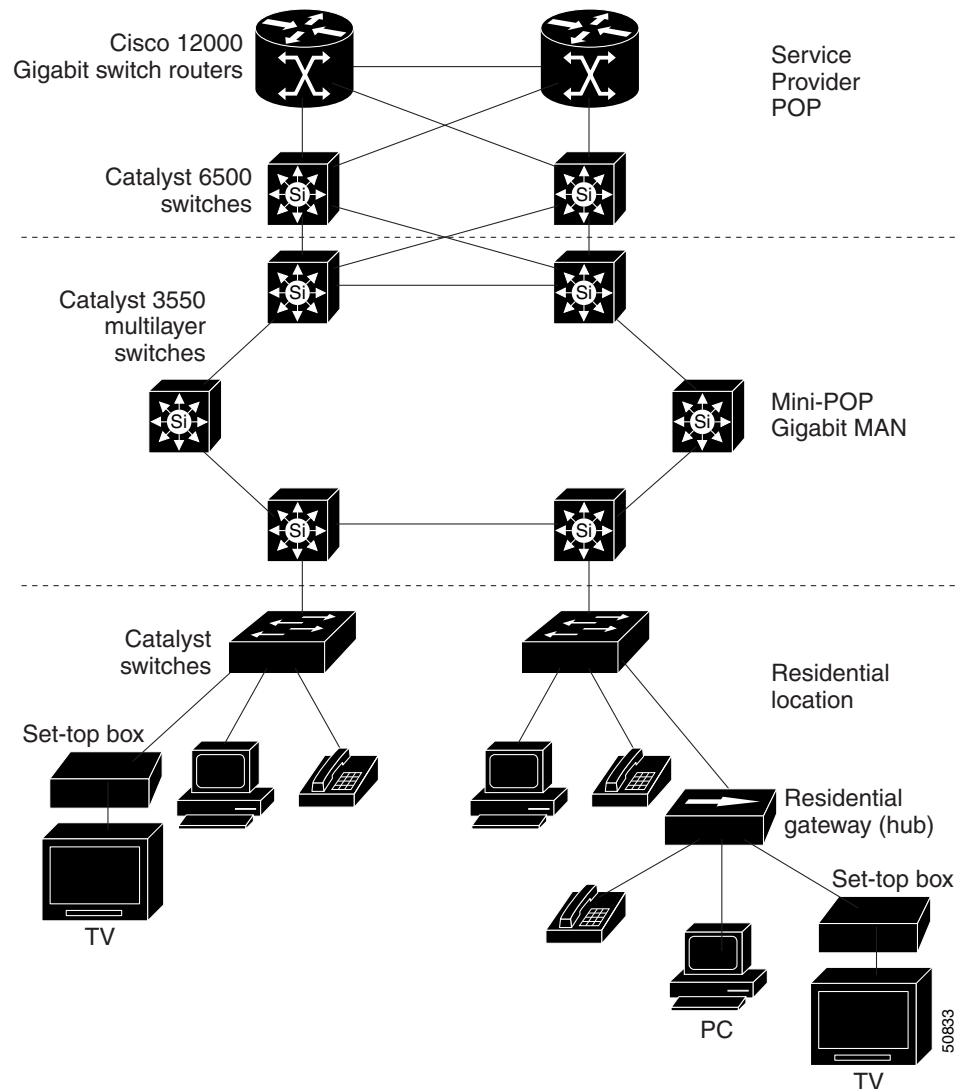
The Catalyst 6500 switch provides the workgroups with Gigabit access to core resources:

- 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.

All ports on the residential Catalyst 2950 and 2955 switches (and Catalyst LRE switches if they are included) are configured as 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 3550 multilayer switches provide security and bandwidth management.

The aggregating switches and routers provide services such as those described in the previous examples, “[Small to Medium-Sized Network Configuration](#)” and “[Large Campus Configuration](#).”

Figure 1-7 Catalyst 2950 Switches in a MAN Configuration



Long-Distance, High-Bandwidth Transport Configuration



Note

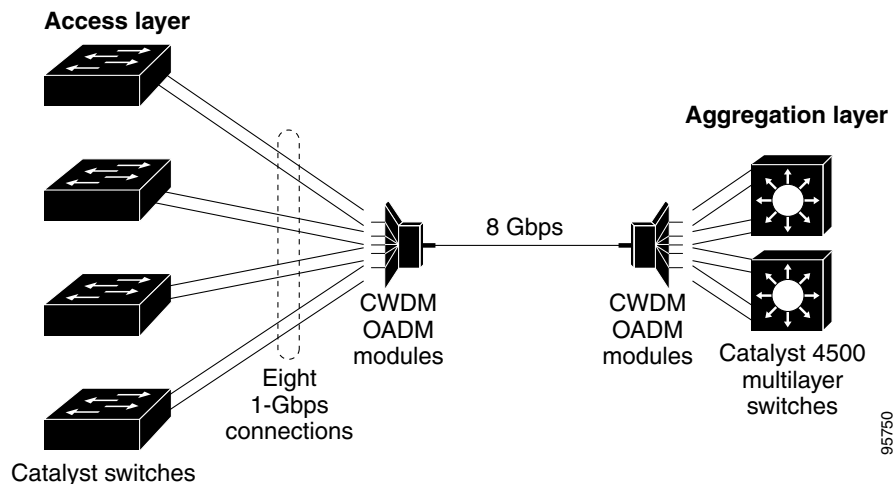
To use the feature described in this section, you must have the EI installed on your switch.

Figure 1-8 shows a configuration for transporting 8 Gigabits of data over a single fiber-optic cable. The Catalyst switches have Coarse Wave Division Multiplexer (CWDM) fiber-optic GBIC modules installed. Depending on the CWDM GBIC module, data is sent at wavelengths from 1470 nm 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 GBIC 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 GBIC modules and CWDM OADM modules, see the *Cisco CWDM GBIC and CWDM SFP Installation Note*.

Figure 1-8 Long-Distance, High-Bandwidth Transport Configuration



Where to Go Next

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

- [Chapter 2, “Using the Command-Line Interface”](#)
- [Chapter 4, “Assigning the Switch IP Address and Default Gateway”](#)
- [Chapter 5, “Configuring Cisco IOS CNS Agents”](#)

