CHAPTER 1

Configuration Overview

Features

Your switch uses the Cisco IOS software licensing (CISL) architecture to support a single universal cryptographic image (supports encryption). This image implements the LAN Base or LAN Lite features depending on your switch model:

- The LAN Base image provides quality of service (QoS), port security, and static routing features.
- The LAN Lite image provides reduced Layer 2 functionality without the loss of critical security features such as SSH and SNMPv3.

Feature Software Licensing

A feature license is supported on a single universal image that implements the LAN Base or LAN Lite features depending on your software license:

- The LAN Base features include quality of service (QoS), port security, and static routing.
- The LAN Lite features provide Layer 2 functionality without losing critical security features such as SSH and SNMPv3.

Cryptographic functionality is included on the universal image.

These guidelines can help you determine what image is running on your switch:

- Enter the **show version** privileged EXEC command. For example, IE-2000-8TC-G-E runs the LAN Base image by default and the IE-2000-4T-G-L runs the LAN Lite image by default.
- Enter the **show license** privileged EXEC command, to see which is the active image:

```
Switch# show license
Index 1 Feature: lanbase
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Priority: Medium
        License Count: Non-Counted

Index 2 Feature: lanlite
        Period left: 0  minute  0  second
```

Ease-of-Deployment and Ease-of-Use Features

- Express Setup for quickly configuring a switch for the first time with basic IP information, contact information, switch and Telnet passwords, and Simple Network Management Protocol (SNMP) information through a browser-based program. For more information about Express Setup, see the getting started guide.
- User-defined and Cisco-default Smartports macros for creating custom switch configurations for simplified deployment across the network.
- A removable SD flash card that stores the Cisco IOS software image and configuration files for the switch. You can replace and upgrade the switch without reconfiguring the software features.
- An embedded Device Manager GUI for configuring and monitoring a single switch through a web browser. For information about launching Device Manager, see the getting started guide. For more information about Device Manager, see the switch online help.

Performance Features

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports for optimizing bandwidth
- Automatic medium-dependent interface crossover (auto-MDIX) capability on 10/100 and 10/100/1000 Mb/s interfaces and on 10/100/1000 BASE-TX SFP module interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately
- Support for up to 1546 bytes routed frames, up to 9000 bytes for frames that are bridged in hardware, and up to 2000 bytes for frames that are bridged by software
- IEEE 802.3x flow control on all ports (the switch does not send pause frames)
- Support for up to 6 EtherChannel groups
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic
- Cisco Group Management Protocol (CGMP) server support and Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3:
  - (For CGMP devices) CGMP for limiting multicast traffic to specified end stations and reducing overall network traffic
  - (For IGMP devices) IGMP snooping for forwarding multimedia and multicast traffic
- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)
- IGMP snooping querier support to configure switch to generate periodic IGMP general query messages
- IGMP helper to allow the switch to forward a host request to join a multicast stream to a specific IP destination address
- IGMP filtering for controlling the set of multicast groups to which hosts on a switch port can belong

- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP leave timer for configuring the leave latency for the network
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features
- Cisco IOS IP Service Level Agreements (SLAs), a part of Cisco IOS software that uses active traffic monitoring for measuring network performance
- Configurable small-frame arrival threshold to prevent storm control when small frames (64 bytes or less) arrive on an interface at a specified rate (the threshold)
- FlexLink Multicast Fast Convergence to reduce the multicast traffic convergence time after a FlexLink failure
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group
- Support for QoS marking of CPU-generated traffic and queue CPU-generated traffic on the egress network ports

Management Options

- An embedded Device Manager—Device Manager is a GUI application that is integrated in the software image. You use it to configure and to monitor a single switch. For information about launching Device Manager, see the getting started guide. For more information about Device Manager, see the switch online help.
- Network Assistant—Network Assistant is a network management application that can be downloaded from Cisco.com. You use it to manage a single switch, a cluster of switches, or a community of devices. For more information about Network Assistant, see *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- CLI—The Cisco IOS software supports desktop- and multilayer-switching features. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station. 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 33, "Configuring SNMP."
- Cisco IOS Configuration Engine (previously known as the Cisco IOS CNS agent)—Configuration service automates the deployment and management of network devices and services. 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 CNS, see Chapter 5, "Configuring Cisco IOS Configuration Engine."

Manageability Features

- CNS embedded agents for automating switch management, configuration storage, and delivery.

- DHCP for automating configuration of switch information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names).
- DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients.
- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts.
- DHCP-based autoconfiguration and image update to download a specified configuration of a new image to a large number of switches.
- DHCPv6 bulk-lease query to support new bulk lease query type (as defined in RFC5460).
- DHCPv6 Relay Source Configuration feature to configure a source address for DHCPv6 relay agent.
- DHCP server port-based address allocation for the preassignment of an IP address to a switch port.
- Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding hostname and to a TFTP server for administering software upgrades from a TFTP server.
- Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding MAC address.
- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses.
- Configurable MAC address scaling that allows disabling MAC address learning on a VLAN to limit the size of the MAC address table.
- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network.
- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones.
- LLDP media extensions (LLDP-MED) location TLV that provides location information from the switch to the endpoint device.
- Network Time Protocol (NTP) for providing a consistent time stamp to all switches from an external source.
- Network Time Protocol version 4 (NTPv4) to support both IPv4 and IPv6 and compatibility with NTPv3.
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch uses.
- Support for the SSM PIM protocol to optimize multicast applications, such as video.
- Configuration logging to log and to view changes to the switch configuration.
- Unique device identifier to provide product identification information through a **show inventory** user EXEC command display.
- In-band management access through Device Manager over a Netscape Navigator or Microsoft Internet Explorer browser session.
- In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network.
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network.
- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests.
- Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem.

- Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying switch configuration or switch image files (requires the cryptographic version of the software).
- Configuration replacement and rollback to replace the running configuration on a switch with any saved Cisco IOS configuration file.
- The HTTP client in Cisco IOS can send requests to both IPv4 and IPv6 HTTP server, and the HTTP server in Cisco IOS can service HTTP requests from both IPv4 and IPv6 HTTP clients.
- Simple Network and Management Protocol (SNMP) can be configured over IPv6 transport so that an IPv6 host can send SNMP queries and receive SNMP notifications from a device running IPv6.
- IPv6 stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses.
- Disabling MAC address learning on a VLAN.
- DHCP server port-based address allocation for the preassignment of an IP address to a switch port.
- CPU utilization threshold trap monitors CPU utilization.
- LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.
- Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol.
- DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.

Availability and Redundancy Features

- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
- IEEE 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:
  - Up to 128 spanning-tree instances supported
  - Per-VLAN spanning-tree plus (PVST+) for load balancing across VLANs
  - Rapid PVST+ for load balancing across VLANs and providing rapid convergence of spanning-tree instances
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately changing root and designated ports to the forwarding state
- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:
  - Port Fast for eliminating the forwarding delay by enabling a port to immediately change from the blocking state to the forwarding state
  - BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)
  - BPDU filtering for preventing a Port Fast-enabled port from sending or receiving BPDUs

  - Root guard for preventing switches outside the network core from becoming the spanning-tree root
  - Loop guard for preventing alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link
- FlexLink Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy (requires the LAN Base image)
- Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers, and to allow the failover of the server traffic to an operational link on another Cisco Ethernet switch.

VLAN Features

- Support for up to 255 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth.
- Support for VLAN IDs in the 1 to 4096 range as allowed by the IEEE 802.1Q standard.
- VLAN Query Protocol (VQP) for dynamic VLAN membership.
- IEEE 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources.
- Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (IEEE 802.1Q) to be used.
- VLAN Trunking Protocol (VTP) and VTP pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic.
- Voice VLAN for creating subnets for voice traffic from Cisco IP phones.
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The switch CPU continues to send and receive control protocol frames.
- VLAN FlexLink load balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.
- Support for 802.1x authentication with restricted VLANs (also known as *authentication failed VLANs*).
- Support for VTP version 3 that includes support for configuring extended range VLANs (VLANs 1006 to 4096) in any VTP mode, enhanced authentication (hidden or secret passwords), propagation of other databases in addition to VTP, VTP primary and secondary servers, and the option to turn VTP on or off by port.

Security Features

- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring
- IP SLAs EOT to use the output from IP SLAs tracking operations triggered by an action such as latency, jitter, or packet loss for a standby router failover takeover (requires the LAN Base image)

- Web authentication to allow a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser
- Local web authentication banner so that a custom banner or an image file can be displayed at a web authentication login screen
- MAC authentication bypass (MAB) aging timer to detect inactive hosts that have authenticated after they have authenticated by using MAB
- Password-protected access (read-only and read-write access) to management interfaces (Device Manager, Network Assistant, and the CLI) for protection against unauthorized configuration changes
- Multilevel security for a choice of security level, notification, and resulting actions
- Static MAC addressing for ensuring security
- 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
- VLAN-aware port security option to shut down the VLAN on the port when a violation occurs, instead of shutting down the entire port
- Port security aging to set the aging time for secure addresses on a port
- Protocol storm protection to control the rate of incoming protocol traffic to a switch by dropping packets that exceed a specified ingress rate
- 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
- Source and destination MAC-based ACLs for filtering non-IP traffic
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers
- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings
- Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN
- Layer 2 protocol tunneling bypass feature to provide interoperability with third-party vendors
- IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:
  - Multidomain authentication (MDA) to allow both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), to independently authenticate on the same IEEE 802.1x-enabled switch port
  - Dynamic voice virtual LAN (VLAN) for MDA to allow a dynamic voice VLAN on an MDA-enabled port
  - VLAN assignment for restricting 802.1x-authenticated users to a specified VLAN
  - Port security for controlling access to 802.1x ports
  - Voice VLAN to permit a Cisco IP Phone to access the voice VLAN regardless of the authorized or unauthorized state of the port
  - IP phone detection enhancement to detect and recognize a Cisco IP phone

  - Guest VLAN to provide limited services to non-802.1x-compliant users
  - Restricted VLAN to provide limited services to users who are 802.1x compliant, but do not have the credentials to authenticate via the standard 802.1x processes
  - 802.1x accounting to track network usage
  - 802.1x with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame
  - 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch
  - Voice-aware 802.1x security to apply traffic violation actions only on the VLAN on which a security violation occurs
  - MAC authentication bypass to authorize clients based on the client MAC address
  - Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enable to authenticate a switch outside a wiring closet as a supplicant to another switch
  - IEEE 802.1x with open access to allow a host to access the network before being authenticated
  - IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch
  - Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host
  - Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port
- Network Admission Control (NAC) features:
  - NAC Layer 2 802.1x validation of the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access

    For information about configuring NAC Layer 2 802.1x validation, see the "Configuring NAC Layer 2 802.1x Validation" section on page 10-46
  - NAC Layer 2 IP validation of the posture of endpoint systems or clients before granting the devices network access

    For information about configuring NAC Layer 2 IP validation, see the *Network Admission Control Software Configuration Guide*
  - IEEE 802.1x inaccessible authentication bypass

    For information about configuring this feature, see the "Configuring Inaccessible Authentication Bypass" section on page 10-44
  - Authentication, authorization, and accounting (AAA) down policy for a NAC Layer 2 IP validation of a host if the AAA server is not available when the posture validation occurs

    For information about this feature, see the *Network Admission Control Software Configuration Guide.*
- TACACS+, a proprietary feature for managing network security through a TACACS server
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through AAA services
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6
- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic versions of the software)

- Secure Socket Layer (SSL) Version 3.0 support for the HTTP 1.1 server authentication, encryption, and message integrity and HTTP client authentication to allow secure HTTP communications (requires the cryptographic version of the software)
- Voice-aware IEEE 802.1x and MAC authentication bypass (MAB) security violation to shut down only the data VLAN on a port when a security violation occurs
- Support for IP source guard on static hosts
- RADIUS change of authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Secure ACS to reinitialize authentication, and apply to the new policies.
- IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
- Support for critical VLAN with multiple-host authentication so that when a port is configured for multi-authentication, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources
- Customizable web authentication enhancement to allow the creation of user-defined *login*, *success*, *failure* and *expire* web pages for local web authentication
- Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port
- VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs
- MAC move to allow hosts (including the hosts connected behind an IP phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port in the same way as a completely new MAC address.
- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.

QoS and CoS Features

Note These features require the LAN Base image.

- Automatic QoS (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues
- Automatic quality of service (QoS) Voice over IP (VoIP) enhancement for port-based trust of DSCP and priority queuing for egress traffic
- Classification
  - IP type-of-service/Differentiated Services Code Point (IP ToS/DSCP) and IEEE 802.1p CoS marking priorities on a per-port basis for protecting the performance of mission-critical applications

  - IP ToS/DSCP and IEEE 802.1p CoS marking based on flow-based packet classification (classification based on information in the MAC, IP, and TCP/UDP headers) for high-performance quality of service at the network edge, allowing for differentiated service levels for different types of network traffic and for prioritizing mission-critical traffic in the network
  - Trusted port states (CoS, DSCP, and IP precedence) within a QoS domain and with a port bordering another QoS domain
  - Trusted boundary for detecting the presence of a Cisco IP Phone, trusting the CoS value received, and ensuring port security
- Policing
  - Traffic-policing policies on the switch port for managing how much of the port bandwidth should be allocated to a specific traffic flow.
  - If you configure multiple class maps for a hierarchical policy map, each class map can be associated with its own port-level (second-level) policy map. Each second-level policy map can have a different policer.
  - Aggregate policing for policing traffic flows in aggregate to restrict specific applications or traffic flows to metered, predefined rates.
- Out-of-profile
  - Out-of-profile markdown for packets that exceed bandwidth utilization limits
- Ingress queueing and scheduling
  - Two configurable ingress queues for user traffic (one queue can be the priority queue)
  - Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
  - Shaped round robin (SRR) as the scheduling service for specifying the rate at which packets are sent to the ring (sharing is the only supported mode on ingress queues)
- Egress queues and scheduling
  - Four egress queues per port.
  - WTD as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications.
  - SRR as the scheduling service for specifying the rate at which packets are dequeued to the egress interface (shaping or sharing is supported on egress queues). Shaped egress queues are guaranteed but limited to using a share of port bandwidth. Shared egress queues are also guaranteed a configured share of bandwidth, but can use more than the guarantee if other queues become empty and do not use their share of the bandwidth.

Monitoring Features

- EOT and IP SLAs EOT static route support identify when a preconfigured static route or a DHCP route goes down
- 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 (RSPAN requires LAN Base image)

- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations (RSPAN requires LAN Base image)
- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Layer 2 traceroute to identify the physical path that a packet takes from a source device to a destination device
- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on 10/100 and 10/100/1000 copper Ethernet ports
- SFP module diagnostic management interface to monitor physical or operational status of an SFP module
- Facilities for processing alarms related to temperature, power-supply conditions, and the status of the Ethernet ports
- Alarm relay contacts that can be used for an external relay system
- Digital optical monitoring (DOM) to check status of X2 small form-factor pluggable (SFP) modules

Default Settings After Initial Switch Configuration

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

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

- Default switch IP address, subnet mask, and default gateway is 0.0.0.0. For more information, see Chapter 4, “Performing Switch Setup Configuration,” and Chapter 22, “Configuring DHCP.”
- Default domain name is not configured. For more information, see Chapter 4, “Performing Switch Setup Configuration.”
- DHCP client is enabled, the DHCP server is enabled (only if the device acting as a DHCP server is configured and is enabled), and the DHCP relay agent is enabled (only if the device is acting as a DHCP relay agent is configured and is enabled). For more information, see Chapter 4, “Performing Switch Setup Configuration,” and Chapter 22, “Configuring DHCP.”
- Switch cluster is disabled. For more information about switch clusters, see Chapter 6, “Configuring Switch Clusters,” and the *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- No passwords are defined. For more information, see Chapter 7, “Performing Switch Administration.”
- System name and prompt is Switch. For more information, see Chapter 7, “Performing Switch Administration.”
- NTP is enabled. For more information, see Chapter 7, “Performing Switch Administration.”
- DNS is enabled. For more information, see Chapter 7, “Performing Switch Administration.”
- TACACS+ is disabled. For more information, see Chapter 9, “Configuring Switch-Based Authentication.”
- RADIUS is disabled. For more information, see Chapter 9, “Configuring Switch-Based Authentication.”

- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see Chapter 9, “Configuring Switch-Based Authentication.”
- IEEE 802.1x is disabled. For more information, see Chapter 10, “Configuring IEEE 802.1x Port-Based Authentication.”
- Port parameters
  - Operating mode is Layer 2 (switch port). For more information, see Chapter 12, “Configuring Interface Characteristics.”
  - Interface speed and duplex mode is autonegotiate. For more information, see Chapter 12, “Configuring Interface Characteristics.”
  - Auto-MDIX is enabled. For more information, see Chapter 12, “Configuring Interface Characteristics.”
  - Flow control is off. For more information, see Chapter 12, “Configuring Interface Characteristics.”
- VLANs
  - Default VLAN is VLAN 1. For more information, see Chapter 14, “Configuring VLANs.”
  - VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 14, “Configuring VLANs.”
  - Trunk encapsulation is negotiate. For more information, see Chapter 14, “Configuring VLANs.”
  - VTP mode is server. For more information, see Chapter 15, “Configuring VTP.”
  - VTP version is Version 1. For more information, see Chapter 15, “Configuring VTP.”
  - Voice VLAN is disabled. For more information, see Chapter 16, “Configuring Voice VLAN.”
- STP, PVST+ is enabled on VLAN 1. For more information, see Chapter 17, “Configuring STP.”
- MSTP is disabled. For more information, see Chapter 18, “Configuring MSTP.”
- Optional spanning-tree features are disabled. For more information, see Chapter 19, “Configuring Optional Spanning-Tree Features.”
- FlexLinks are not configured. For more information, see Chapter 21, “Configuring FlexLinks and the MAC Address-Table Move Update.”
- DHCP snooping is disabled. The DHCP snooping information option is enabled. For more information, see Chapter 22, “Configuring DHCP.”
- IP source guard is disabled. For more information, see Chapter 22, “Configuring DHCP.”
- DHCP server port-based address allocation is disabled. For more information, see Chapter 22, “Configuring DHCP.”
- Dynamic ARP inspection is disabled on all VLANs. For more information, see Chapter 23, “Configuring Dynamic ARP Inspection.”
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see Chapter 25, “Configuring IGMP Snooping and MVR.”
- IGMP throttling setting is deny. For more information, see Chapter 25, “Configuring IGMP Snooping and MVR.”
- The IGMP snooping querier feature is disabled. For more information, see Chapter 25, “Configuring IGMP Snooping and MVR.”
- MVR is disabled. For more information, see Chapter 25, “Configuring IGMP Snooping and MVR.”

- Port-based traffic
  - Broadcast, multicast, and unicast storm control is disabled. For more information, see Chapter 26, "Configuring Port-Based Traffic Control."
  - No protected ports are defined. For more information, see Chapter 26, "Configuring Port-Based Traffic Control."
  - Unicast and multicast traffic flooding is not blocked. For more information, see Chapter 26, "Configuring Port-Based Traffic Control."
  - No secure ports are configured. For more information, see Chapter 26, "Configuring Port-Based Traffic Control."
- CDP is enabled. For more information, see Chapter 29, "Configuring CDP."
- UDLD is disabled. For more information, see Chapter 30, "Configuring UDLD."
- SPAN and RSPAN are disabled. For more information, see Chapter 27, "Configuring SPAN and RSPAN."
- RMON is disabled. For more information, see Chapter 31, "Configuring RMON."
- Syslog messages are enabled and appear on the console. For more information, see Chapter 32, "Configuring System Message Logging."
- SNMP is enabled (Version 1). For more information, see Chapter 33, "Configuring SNMP."
- No ACLs are configured. For more information, see Chapter 34, "Configuring Network Security with ACLs."
- QoS is disabled. For more information, see Chapter 35, "Configuring Standard QoS."
- No EtherChannels are configured. For more information, see Chapter 37, "Configuring EtherChannels."
- IP unicast routing is disabled. For more information, see Chapter 38, "Configuring Static IP Unicast Routing."

Factory Default Feature

To enable the factory default feature for the Cisco ESS-2020, the **service-declassify** command must be configured to one of the two enabled states. The factory default feature is disabled by default. Table 1-1 lists the settings and completion times for the factory default capability option.

Table 1-1 Settings and Completion Time for Factory Default Capability Options

Option	Action	Typical Completion Time
erase-config	Removes all configuration files from the device. This option leaves other non-configuration files intact.	Variable (less than 2 minutes)
erase-flash	Completely formats the flash filesystem. This also removes any IOS images present.[1]	Variable[2]

1. For the unit to function normally, the IOS needs to be reloaded by using xmodem from the bootloader prompt. Typical image load time is 20 to 25 minutes using a 115.2 kbaud console link (slower console links will increase the load time).
2. The erase time is between 12 and 14 minutes, depending on the flash memory vendor.

To initiate factory default, the signal FACTORY_DEFAULT_INPUT_L located on the main board connector P15, pin 50 must be grounded. While the process is executing, the FactoryDef_Gr LED flashes green. When the factory default process is complete, the FactoryDef_Yel LED lights indicating that the system is rebooting. The system stops at the bootloader prompt with the FactoryDef_Gr LED lit green indicating that the default procedure has successfully completed.

Note After the factory default procedure completes, there will be an empty file in the filesystem. This file is deleted the next time that IOS is booted.

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, page 1-14
- Ethernet-to-the-Factory Architecture, page 1-15

Design Concepts for Using the Switch

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

Table 1-2 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 them.

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, which provides maximum flexibility and support for mission-critical, unicast, and multicast and multimedia applications. • 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 VLAN trunks and BackboneFast for traffic-load balancing on the uplink ports so that the uplink port with a lower relative port cost is selected to carry the VLAN traffic.
An evolving demand for IP telephony	• Use QoS to prioritize applications such as IP telephony during congestion and to help control both delay and jitter within the network. • Use switches that support at least two queues per port to prioritize voice and data traffic as either high- or low-priority, based on IEEE 802.1p/Q. The switch supports at least four queues per port. • Use voice VLAN IDs (VVIDs) to provide separate VLANs for voice traffic.

Ethernet-to-the-Factory Architecture

This section is an overview of the Ethernet-to-the-Factory (EttF) architecture that provides network and security services to the devices and applications in automation and control systems. It then integrates those into the wider enterprise network.

EttF architecture applies to many types of manufacturing environments, but it must be tailored to the industry type, the manufacturing type, and the production-facility size. Deployments can range from small networks (less than 50 devices), to medium-sized networks (less than 200 devices), and to large networks (up to and more than 1000 devices).

Within the EttF architecture are conceptual structures called *zones* that separate the various functions, from the highest-level enterprise switches and processes to the smallest devices that control more detailed processes and devices on the factory floor. See Figure 1-1.

For more information about EttF architecture, see this URL:

http://www.cisco.com/web/strategy/manufacturing/ettf_overview.html

Enterprise Zone

The *enterprise zone* comprises the centralized IT systems and functions. Wired and wireless access is available to enterprise network services, such as enterprise resource management, business-to-business, and business-to-customer services.The basic business administration tasks, such as site business planning and logistics, are performed here and rely on standard IT services. Guest access systems are often located here, although it is not uncommon to find them in lower levels of the framework to gain flexibility that might be difficult to achieve at the enterprise level.

Demilitarized Zone

The *demilitarized zone* (DMZ) provides a buffer for sharing of data and services between the enterprise and manufacturing zones. The DMZ maintains availability, addresses security vulnerabilities, and abiding by regulatory compliance mandates. The DMZ provides segmentation of organizational control, for example, between the IT and production organizations. Different policies for each organization can be applied and contained. For example, the production organization might apply security policies to the manufacturing zone that are different than those applied to the IT organization.

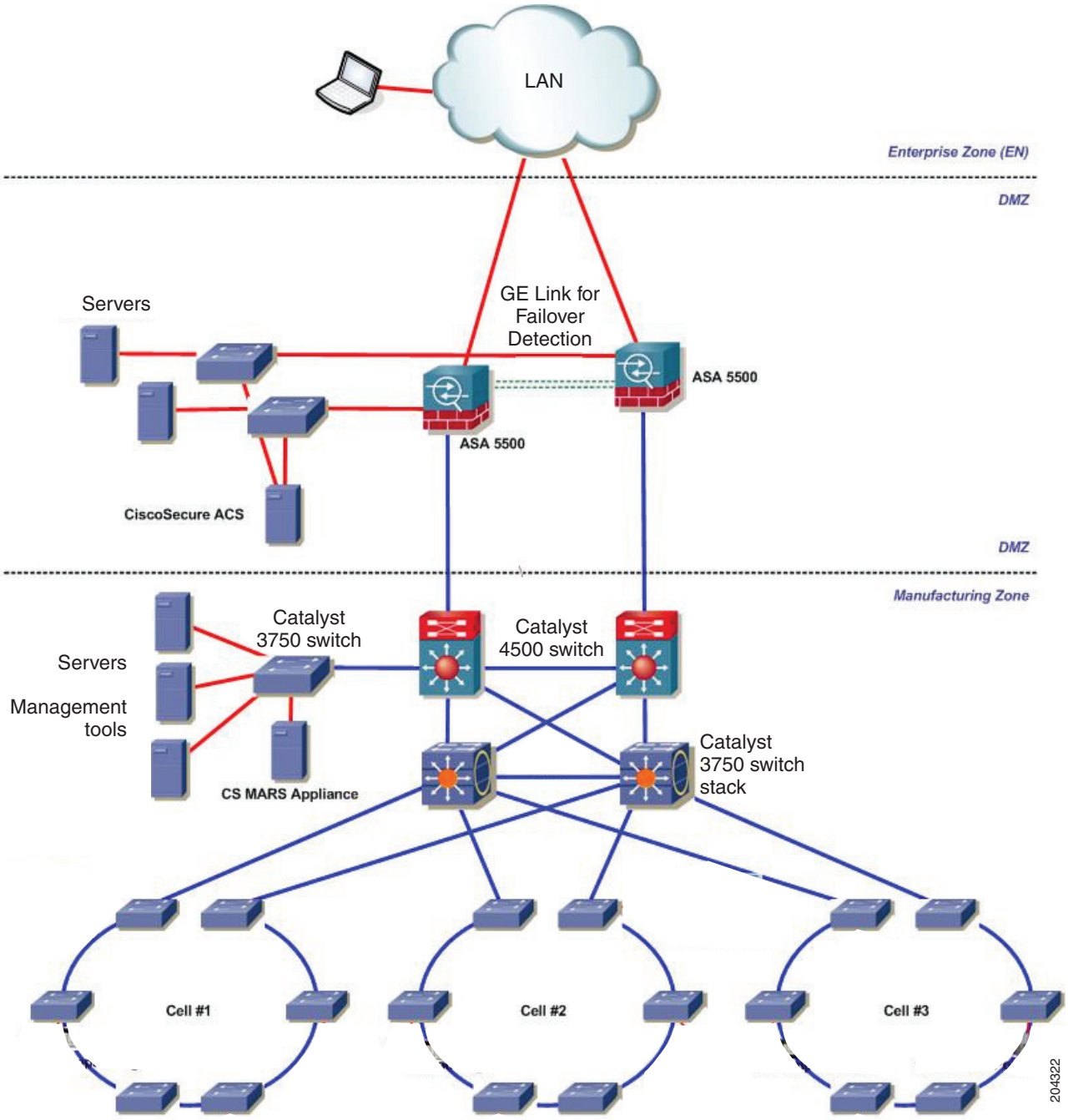
Manufacturing Zone

The *manufacturing zone* comprises the cell networks and site-level activities. All the systems, devices, and controllers that monitor the plant operations are in this zone. The cell zone is a functional area within a production facility.

The cell zone is a set of devices, controllers, and so on, that provide the real-time control of a functional aspect of the automation process. They are all in real-time communication with each other. This zone requires clear isolation and protection from the other levels of plant or enterprise operations.

Figure 1-1 shows the EttF architecture.

Figure 1-1 Ethernet-to-the-Factory Architecture



Topology Options

Topology design starts with considering how devices are connected to the network. The cell network also requires physical topologies that meet the physical constraints of the production floor. This section provides guidelines for topology designs and describes the trunk-drop, ring, and redundant-star topologies.

- Physical layout—The layout of the production environment drives the topology design. For example, a trunk-drop or ring topology is a good choice for a long conveyor-belt system, but a redundant-star configuration is not a good choice.
- Real-time communications—Latency and jitter are primarily caused by the amount of traffic and number of hops a packet must make to reach its destination. The amount of traffic in a Layer 2 network is driven by various factors, but the number of devices is important. Follow these guidelines for real-time communications:
  - The amount of latency introduced per Layer 2 hop should be considered. For instance, there is a higher latency with 100 Mb interfaces than there is with 1 Gigabit interfaces.
  - Bandwidth should not consistently exceed 50 percent of the interface capacity on any switch.
  - The CPU should not consistently exceed 50 to 70 percent utilization. Above this level, the switch might not properly process control packets and might behave abnormally.

These are the key connectivity considerations:

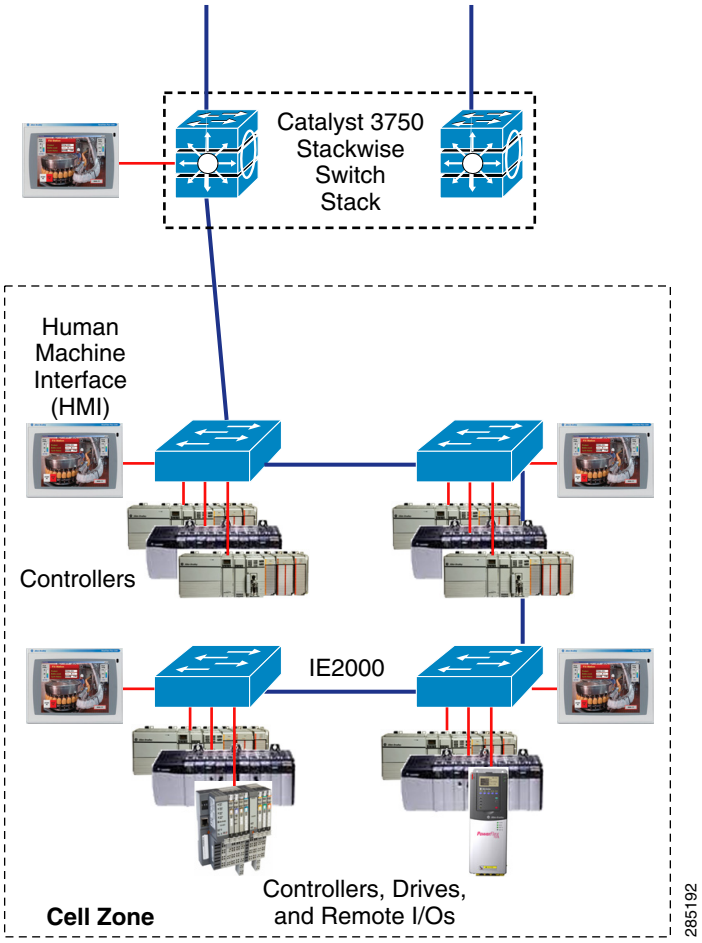
- Devices are connected to a switch through a single network connection or an IP-enabled I/O block or linking device if they do not support Ethernet. Most devices have no or limited failover capabilities and therefore cannot effectively use redundant network connections.
- Redundant connections can be used in certain industries and applications, such as process-related industries that are applied to critical infrastructure.

Cell Network—Trunk-Drop Topology

Switches are connected to each other to form a chain of switches in a *trunk-drop* topology (also known as a *cascaded* topology). See Figure 1-2.

- The connection between the Layer 3 switch and the first Layer 2 switch is very susceptible to oversubscription, which can degrade network performance.
- There is no redundancy to the loss of a connection.

Figure 1-2 Cell Network–Trunk-Drop Topology

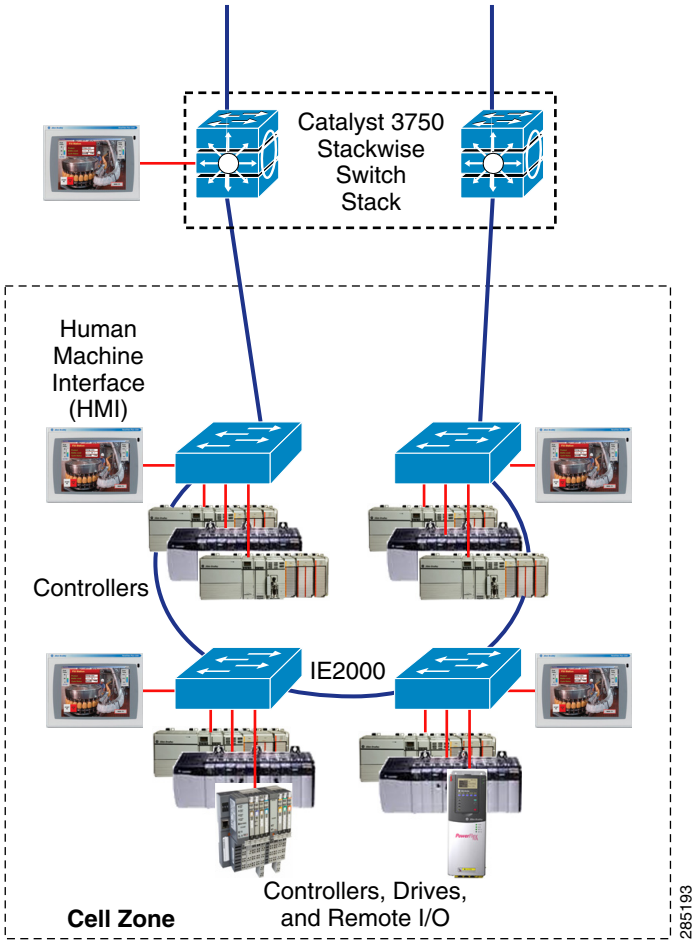


Cell Network—Ring Topology

A ring topology is similar to a trunk-drop topology except that the last switch in the chain is connected to the Layer 3 switch that forms a network ring. If a connection is lost in a ring, each switch maintains connectivity to the other switches. See Figure 1-3.

- The network can only recover from the loss of a single connection.
- It is more difficult to implement because it requires additional protocol implementation and Rapid Spanning Tree Protocol (RSTP).
- Although better than the trunk-drop, the top of the ring (connections to the Layer 3 switches) can become a bottleneck and is susceptible to oversubscription, which can degrade network performance.

Figure 1-3 Cell Network–Ring Topology

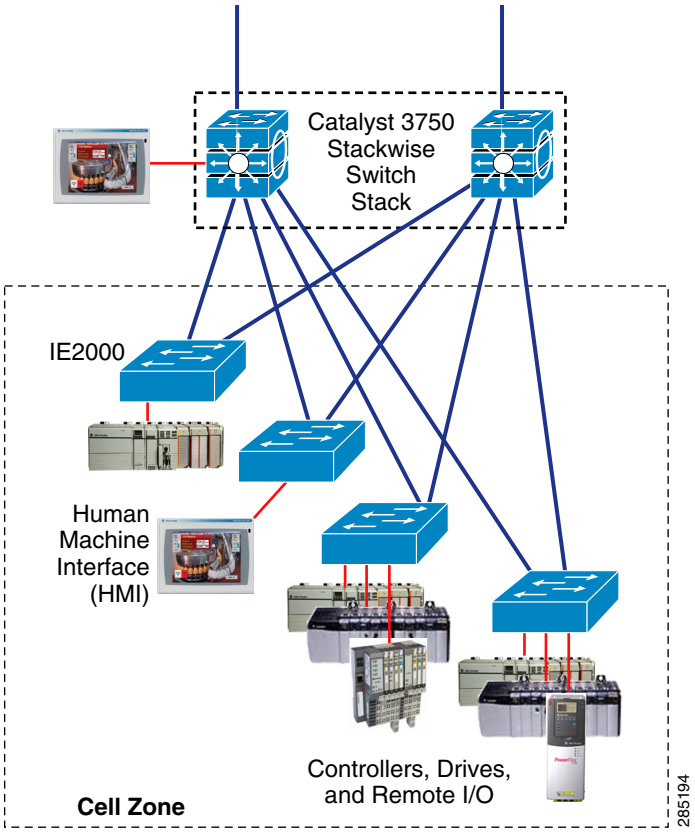


Cell Network—Redundant-Star Topology

In a redundant-star topology, every Layer 2 access switch has dual connections to a Layer 3 distribution switch. Devices are connected to the Layer 2 switches. See Figure 1-4.

- Any Layer 2 switch is always only two hops to another Layer 2 switch.
- In the Layer 2 network, each switch has dual connections to the Layer 3 devices.
- The Layer 2 network is maintained even if multiple connections are lost.

Figure 1-4 Cell Network–Redundant Star Topology



Where to Go Next

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

- Chapter 2, "Using the Command-Line Interface"
- Chapter 4, "Performing Switch Setup Configuration"

To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.