CHAPTER 1

Overview

This chapter provides these topics about the IE 3000 switch software:

In this document, IP refers to IP Version 4 (IPv4).

Features

Some features described in this chapter are available only on the cryptographic (supports encryption) version of the software. You must obtain authorization to use this feature and to download the cryptographic version of the software from Cisco.com. For more information, see the release notes for this release.

The switch has these features:

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

The switch ships with these features to make the deployment and the use easier:

- Express Setup for quickly configuring a switch for the first time with basic IP information, contact information, switch and Telnet passwords, and Simple Network Management Protocol (SNMP) information through a browser-based program. For more information about Express Setup, see the getting started guide.
- User-defined and Cisco-default Smartports macros for creating custom switch configurations for simplified deployment across the network.
- A removable compact 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. Updated boot loader that has a secondary boot loader image that supports the compact flash file system driver to access the compact flash memory card. The switch boot loader contains a primary boot loader and a secondary boot loader that both reside in the boot flash.
- An embedded device manager GUI for configuring and monitoring a single switch through a web browser. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the switch online help.
- Cisco Network Assistant (hereafter referred to as *Network Assistant*) for

Note The Network Assistant must be downloaded from cisco.com/go/cna.

  - Managing communities, which are device groups like clusters, except that they can contain routers and access points and can be made more secure.
  - Simplifying and minimizing switch and switch cluster management from anywhere in your intranet.
  - Accomplishing multiple configuration tasks from a single graphical interface without needing to remember command-line interface (CLI) commands to accomplish specific tasks.
  - Interactive guide mode that guides you in configuring complex features such as VLANs, ACLs, and quality of service (QoS).
  - Configuration wizards that prompt you to provide only the minimum required information to configure complex features such as QoS priorities for traffic, priority levels for data applications, and security.
  - Downloading an image to a switch.
  - Applying actions to multiple ports and multiple switches at the same time, such as VLAN and QoS settings, inventory and statistic reports, link- and switch-level monitoring and troubleshooting, and multiple switch software upgrades.
  - Viewing a topology of interconnected devices to identify existing switch clusters and eligible switches that can join a cluster and to identify link information between switches.
  - Monitoring real-time status of a switch or multiple switches from the LEDs on the front-panel images. The system, redundant power system (RPS), and port LED colors on the images are similar to those used on the physical LEDs.

- Switch clustering technology for
  - Unified configuration, monitoring, authentication, and software upgrade of multiple, cluster-capable switches, regardless of their geographic proximity and interconnection media, including Ethernet, Fast Ethernet, Fast EtherChannel, small form-factor pluggable (SFP) modules, Gigabit Ethernet, and Gigabit EtherChannel connections. For a list of cluster-capable switches, see the release notes.
  - Automatic discovery of candidate switches and creation of clusters of up to 16 switches that can be managed through a single IP address.
  - Extended discovery of cluster candidates that are not directly connected to the command switch.

Performance Features

The switch ships with these performance features:

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports for optimizing bandwidth
- Automatic-medium-dependent interface crossover (auto-MDIX) capability on 10/100 and 10/100/1000 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 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)
- EtherChannel for enhanced fault tolerance and for providing up to 8 Gb/s (Gigabit EtherChannel) or 800 Mb/s (Fast EtherChannel) full-duplex bandwidth among switches, routers, and servers
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links
- Forwarding of 2 packets at Gigabit line rate
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown 2 unknown unicast, multicast, and bridged broadcast traffic
- Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3 for efficiently forwarding multimedia and multicast traffic
- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)
- IGMP snooping querier support to configure switch to generate periodic IGMP general query messages
- Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons
- IGMP filtering for controlling the set of multicast groups to which hosts on a switch port can belong
- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP leave timer for configuring the leave latency for the network
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features

- Support for Cisco IOS IP Service Level Agreements (SLAs) responder that allows the system to anticipate and respond to Cisco IOS IP SLAs request packets for monitoring network performance. See the release notes for responder configuration
- 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)
- Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure

Management Options

These are the options for configuring and managing the switch:

- An embedded device manager—The device manager is a GUI that is integrated in the software image. You use it to configure and to monitor a single switch. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the switch online help.
- Network Assistant—Network Assistant is a network management application that can be downloaded from Cisco.com. You use it to manage a single switch, a cluster of switches, or a community of devices. For more information about Network Assistant, see *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- CLI—The Cisco IOS software supports desktop- and multi-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 29, "Configuring SNMP."
- CNS—Cisco Networking Services is network management software that acts as a configuration service for automating 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 CNS Agents."
- CIP—Common Industrial Protocol (CIP) is a peer-to-peer application protocol that provides application level connections between the switch and industrial devices such as I/O controllers, sensors, relays, and so forth.You can manage the switch using CIP-based management tools, such as RSLogix. For more information about the CIP commands that the switch supports, see the Command Reference.

Manageability Features

These are the 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 a new image to a large number of switches
- Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding hostname and to a TFTP server for administering software upgrades from a TFTP server
- Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding MAC address
- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses
- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network
- Link 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
- 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
- Source Specific Multicast (SSM) mapping for multicast applications provides a mapping of source to group, allowing listeners to connect to multicast sources dynamically and reduces dependencies on the application
- Support for these IP services, making them VRF aware so that they can operate on multiple routing instances: HSRP, GLBP, uRPF, ARP, SNMP, IP SLA, TFTP, FTP, syslog, traceroute, and ping
- Configuration logging to log and to view changes to the switch configuration
- Unique device identifier to provide product identification information through a **show inventory** user EXEC command display
- In-band management access through the device manager over a Netscape Navigator or Microsoft Internet Explorer browser session
- In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic version of the software)
- 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 supports 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

Availability and Redundancy Features

These are the 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
  - UplinkFast and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately changing root and designated ports to the forwarding state
- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:
  - Port Fast for eliminating the forwarding delay by enabling a port to immediately change from the blocking state to the forwarding state
  - BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)
  - BPDU filtering for preventing a Port Fast-enabled port from sending or receiving BPDUs
  - Root guard for preventing switches outside the network core from becoming the spanning-tree root
  - Loop guard for preventing alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link
- Flex Link 2 interfaces to back up one another as an alternative to STP for basic link redundancy
- Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers, and to allow the failover of the server traffic to an operational link on another Cisco Ethernet switch.

VLAN Features

These are the 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 4094 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 Flex Link 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.

Security Features

The switch ships with these security features:

- IP Service Level Agreements (IP SLAs) responder support that allows the switch to be a target device for IP SLAs active traffic monitoring
- Web authentication to allow a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser
- 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
- 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 inbound security policies 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
- IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:
  - VLAN assignment for restricting IEEE 802.1x-authenticated users to a specified VLAN
  - Port security for controlling access to IEEE 802.1x ports
  - Voice VLAN to permit a Cisco IP Phone to access the voice VLAN regardless of the authorized or unauthorized state of the port
  - IP phone detection enhancement to detect and recognize a Cisco IP phone.
  - Guest VLAN to provide limited services to non-IEEE 802.1x-compliant users
  - Restricted VLAN to provide limited services to users who are IEEE 802.1x compliant, but do not have the credentials to authenticate via the standard IEEE 802.1x processes
  - IEEE 802.1x accounting to track network usage
  - IEEE 802.1x with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame
- IEEE 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch
- MAC authentication bypass to authorize clients based on the client MAC address.
- 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 10-38.
- 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 authentication, authorization, and accounting (AAA) services
- Secure Socket (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)

QoS and CoS Features

These are the QoS and CoS features:

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

  - IP ToS/DSCP and IEEE 802.1p CoS marking based on flow-based packet classification (classification based on information in the MAC, IP, and TCP/UDP headers) for high-performance quality of service at the network edge, allowing for differentiated service levels for different types of network traffic and for prioritizing mission-critical traffic in the network
  - Trusted port states (CoS, DSCP, and IP precedence) within a QoS domain and with a port bordering another QoS domain
  - Trusted boundary for detecting the presence of a Cisco IP Phone, trusting the CoS value received, and ensuring port security
- Policing
  - Traffic-policing policies on the switch port for managing how much of the port bandwidth should be allocated to a specific traffic flow
  - In Cisco IOS Release 12.2(25)SED and later, if you configure multiple class maps for a hierarchical policy map, each class map can be associated with its own port-level (second-level) policy map. Each second-level policy map can have a different policer.
  - Aggregate policing for policing traffic flows in aggregate to restrict specific applications or traffic flows to metered, predefined rates
- Out-of-Profile
  - Out-of-profile markdown for packets that exceed bandwidth utilization limits
- Ingress queueing and scheduling
  - Two configurable ingress queues for user traffic (one queue can be the priority queue)
  - Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
  - Shaped round robin (SRR) as the scheduling service for specifying the rate at which packets are sent to the internal 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

These are the monitoring features:

- Switch LEDs that provide port- and switch-level status
- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the switch has learned or removed
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN

- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations
- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- 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

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.

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

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

- Default switch IP address, subnet mask, and default gateway is 0.0.0.0. For more information, see Chapter 4, “Assigning the Switch IP Address and Default Gateway,” and Chapter 20, “Configuring DHCP Features.”
- Default domain name is not configured. For more information, see Chapter 4, “Assigning the Switch IP Address and Default Gateway.”
- DHCP client is enabled, the DHCP server is enabled (only if the device acting as a DHCP server is configured and is enabled), and the DHCP relay agent is enabled (only if the device is acting as a DHCP relay agent is configured and is enabled). For more information, see Chapter 4, “Assigning the Switch IP Address and Default Gateway,” and Chapter 20, “Configuring DHCP Features.”
- Switch cluster is disabled. For more information about switch clusters, see Chapter 6, “Clustering Switches,” and the *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- No passwords are defined. For more information, see Chapter 7, “Administering the Switch.”
- System name and prompt is *Switch.* For more information, see Chapter 7, “Administering the Switch.”
- NTP is enabled. For more information, see Chapter 7, “Administering the Switch.”
- DNS is enabled. For more information, see Chapter 7, “Administering the Switch.”

- TACACS+ is disabled. For more information, see Chapter 9, “Configuring Switch-Based Authentication.”
- RADIUS is disabled. For more information, see Chapter 9, “Configuring Switch-Based Authentication.”
- The standard HTTP server and Secure Socket (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
  - Interface speed and duplex mode is autonegotiate. For more information, see Chapter 11, “Configuring Interface Characteristics.”
  - Auto-MDIX is enabled. For more information, see Chapter 11, “Configuring Interface Characteristics.”
  - Flow control is off. For more information, see Chapter 11, “Configuring Interface Characteristics.”
- VLANs
  - Default VLAN is VLAN 1. For more information, see Chapter 13, “Configuring VLANs.”
  - VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 13, “Configuring VLANs.”
  - Trunk encapsulation is negotiate. For more information, see Chapter 13, “Configuring VLANs.”
  - VTP mode is server. For more information, see Chapter 14, “Configuring VTP.”
  - VTP version is Version 1. For more information, see Chapter 14, “Configuring VTP.”
  - Voice VLAN is disabled. For more information, see Chapter 15, “Configuring Voice VLAN.”
- STP, PVST+ is enabled on VLAN 1. For more information, see Chapter 16, “Configuring STP.”
- MSTP is disabled. For more information, see Chapter 17, “Configuring MSTP.”
- Optional spanning-tree features are disabled. For more information, see Chapter 18, “Configuring Optional Spanning-Tree Features.”
- Flex Links are not configured. For more information, see Chapter 19, “Configuring Flex Links and the MAC Address-Table Move Update Feature.”
- DHCP snooping is disabled. The DHCP snooping information option is enabled. For more information, see Chapter 20, “Configuring DHCP Features.”
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see Chapter 21, “Configuring IGMP Snooping and MVR.”
- IGMP throttling setting is deny. For more information, see Chapter 21, “Configuring IGMP Snooping and MVR.”
- The IGMP snooping querier feature is disabled. For more information, see Chapter 21, “Configuring IGMP Snooping and MVR.”
- MVR is disabled. For more information, see Chapter 21, “Configuring IGMP Snooping and MVR.”

- Port-based traffic
  - Broadcast, multicast, and unicast storm control is disabled. For more information, see Chapter 22, “Configuring Port-Based Traffic Control.”
  - No protected ports are defined. For more information, see Chapter 22, “Configuring Port-Based Traffic Control.”
  - Unicast and multicast traffic flooding is not blocked. For more information, see Chapter 22, “Configuring Port-Based Traffic Control.”
  - No secure ports are configured. For more information, see Chapter 22, “Configuring Port-Based Traffic Control.”
- CDP is enabled. For more information, see Chapter 24, “Configuring CDP.”
- UDLD is disabled. For more information, see Chapter 25, “Configuring UDLD.”
- SPAN and RSPAN are disabled. For more information, see Chapter 26, “Configuring SPAN and RSPAN.”
- RMON is disabled. For more information, see Chapter 27, “Configuring RMON.”
- Syslog messages are enabled and appear on the console. For more information, see Chapter 28, “Configuring System Message Logging.”
- SNMP is enabled (Version 1). For more information, see Chapter 29, “Configuring SNMP.”
- No ACLs are configured. For more information, see Chapter 30, “Configuring Network Security with ACLs.”
- QoS is disabled. For more information, see Chapter 32, “Configuring QoS.”
- No EtherChannels are configured. For more information, see Chapter 33, “Configuring EtherChannels and Link-State Tracking.”

Network Configuration Examples

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

Design Concepts for Using the Switch

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

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

Table 1-1 Increasing Network Performance

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

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

Table 1-2 Providing Network Services

Network Demands	Suggested Design Methods
Efficient bandwidth usage for multimedia applications and guaranteed bandwidth for critical applications	• Use IGMP snooping to efficiently forward multimedia and multicast traffic. • Use other QoS mechanisms such as packet classification, marking, scheduling, and congestion avoidance to classify traffic with the appropriate priority level, thereby providing maximum flexibility and support for mission-critical, unicast, and multicast and multimedia applications. • Use 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.
A growing demand for using existing infrastructure to transport data and voice from a home or office to the Internet or an intranet at higher speeds	Use the Catalyst Long-Reach Ethernet (LRE) switches to provide up to 15 Mb of IP connectivity over existing infrastructure, such as existing telephone lines. **Note** LRE is the technology used in the Catalyst 2900 LRE XL and Catalyst 2950 LRE switches. See the documentation sets specific to these switches for LRE information.

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://wwwin.cisco.com/enterprise/solutions/manufacturing/solutions/ettf.shtml

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.

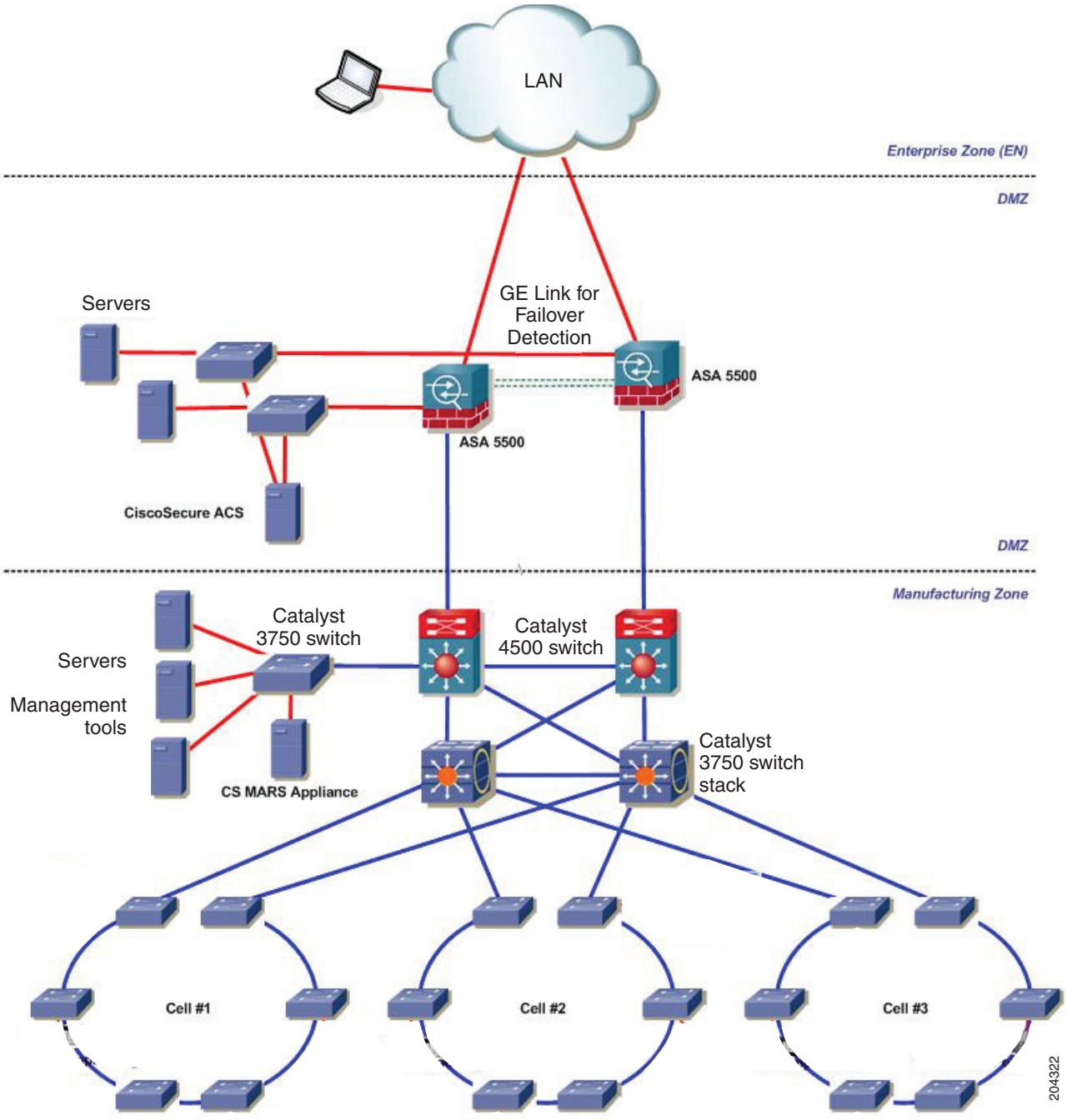
Manufacturing Zone

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:

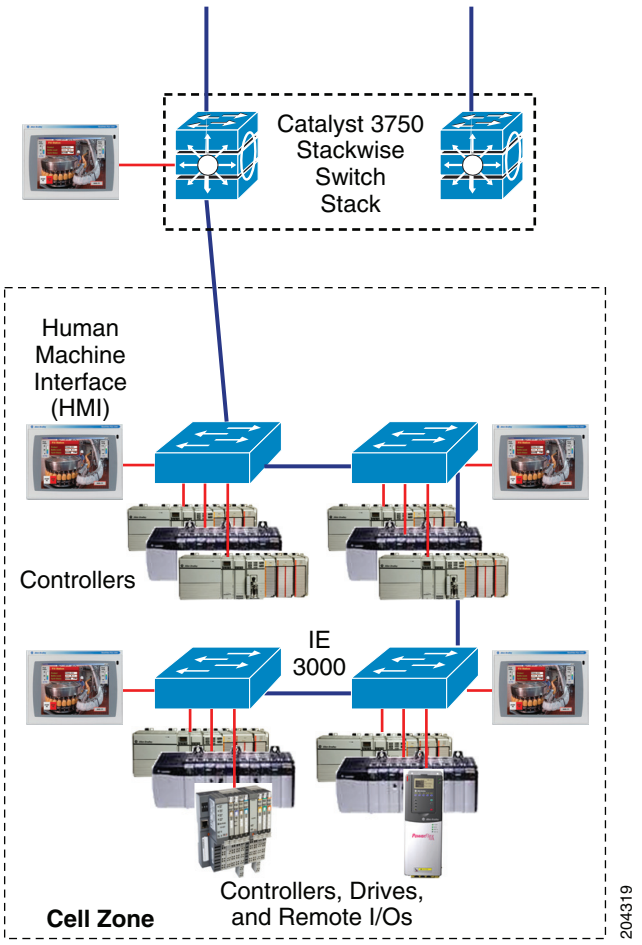
- Devices are connected to a switch through a single network connection or an IP-enabled I/O block or linking device if they do not support Ethernet. Most devices have no or limited failover capabilities and therefore cannot effectively use redundant network connections.
- Redundant connections can be 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

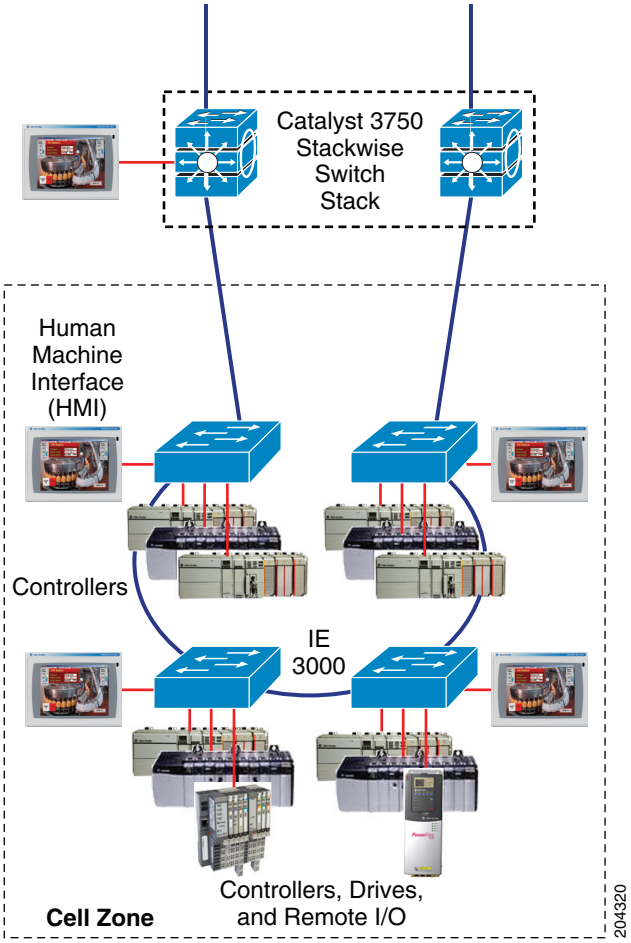


Cell Network—Ring Topology

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

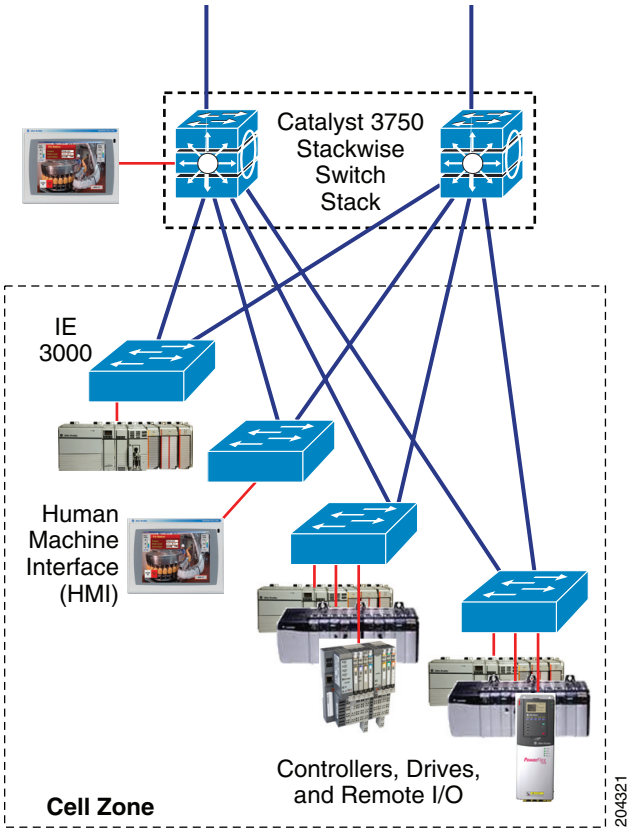


Cell Network—Redundant-Star Topology

In a redundant-star topology, every Layer 2 access switch has dual connections to a Layer 3 distribution switch. Devices are connected to the Layer2 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, “Assigning the Switch IP Address and Default Gateway”