CHAPTER 1

Overview

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

In this document, IP refers to IP Version 4 (IPv4) unless there is a specific reference to IP Version 6 (IPv6).

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.

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

-
-
-
-
- *Network Assistant*
  -
  -
  -
  -
  -
  -
  -
  -
  - 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.

Note cisco.com/go/cna.

- 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.

–

–

Performance Features

•

•

- 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 Layer 2 packets at Gigabit line rate

  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

  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

  IPv6 host support for basic IPv6 management

  Multicast Listener Discovery (MLD) snooping to enable efficient distribution of IP version 6 (IPv6) multicast data to clients and routers in a switched network

  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

Management Options

- 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*

"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 to 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 6, "Configuring Cisco IOS Configuration Engine."

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

-
-

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

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

Precision Time Protocol (PTP) as defined in the IEEE 1588 standard to synchronize with nanosecond accuracy the real-time clocks of the devices in a network

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 Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 to utilize IPv6 transport, communicate with IPv6 peers, and advertise IPv6 routes

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**

Availability and Redundancy Features

-
-

  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

–

–

–

–

–

VLAN Features

•

•

•

- 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.
- Support for 802.1x authentication with restricted VLANs (also known as *authentication failed VLANs*

Security Features

–

–

–

–

–

–

posture

QoS and CoS Features

•

•

Monitoring Features

-
-
-
-

Default Settings After Initial Switch Configuration

Note

-
-
-
-
-
- *Switch.*
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

Network Configuration Examples

Design Concepts for Using the Switch

Table 1-1 Increasing Network Performance

Network Demands	Suggested Design Methods

Table 1-2 Providing Network Services

always on	

Ethernet-to-the-Factory Architecture

zones

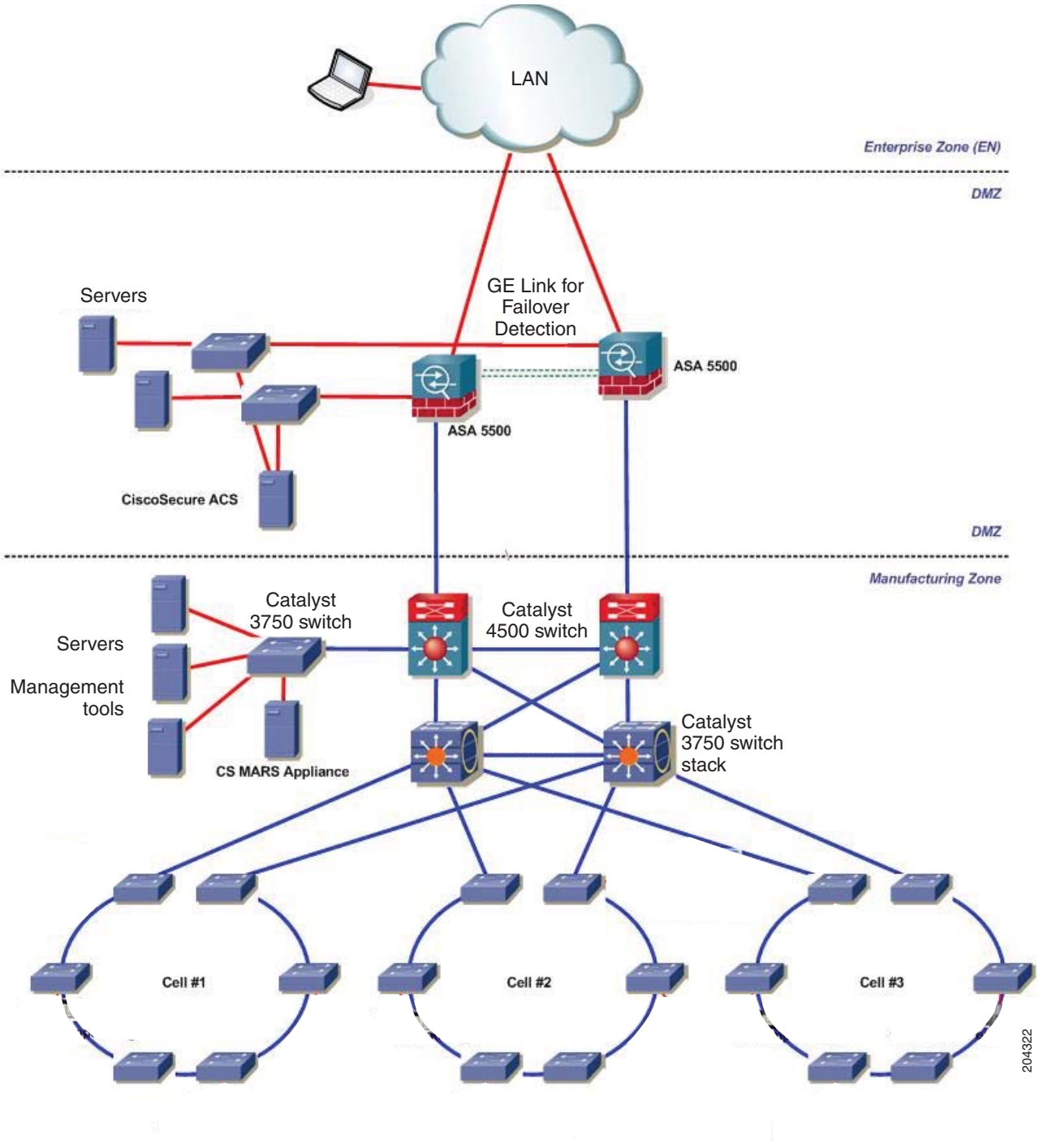
Enterprise Zone

Demilitarized Zone

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

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



Topology Options

-
-
-
-

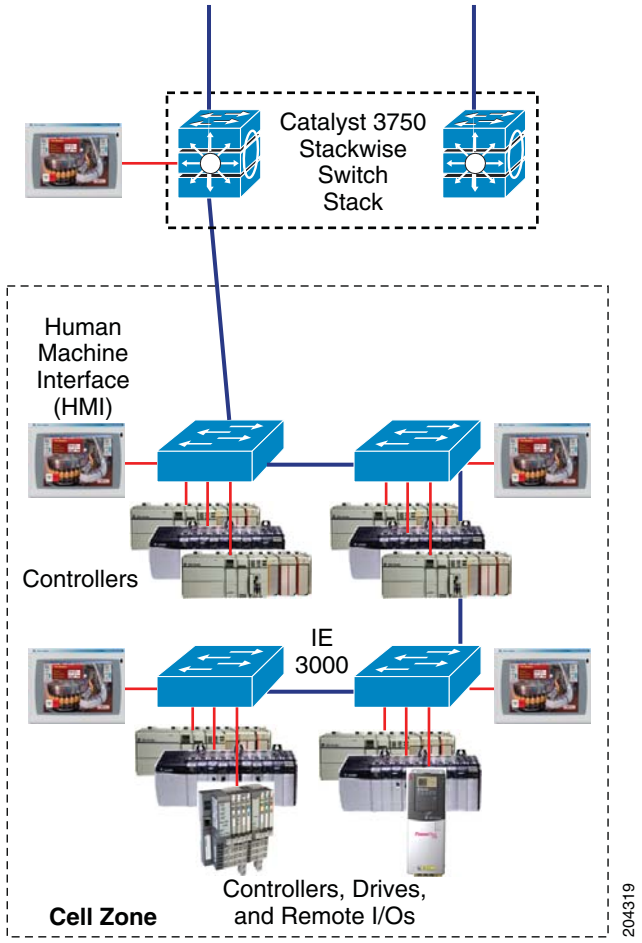
Cell Network—Trunk-Drop Topology

trunk-drop

cascaded

-
-

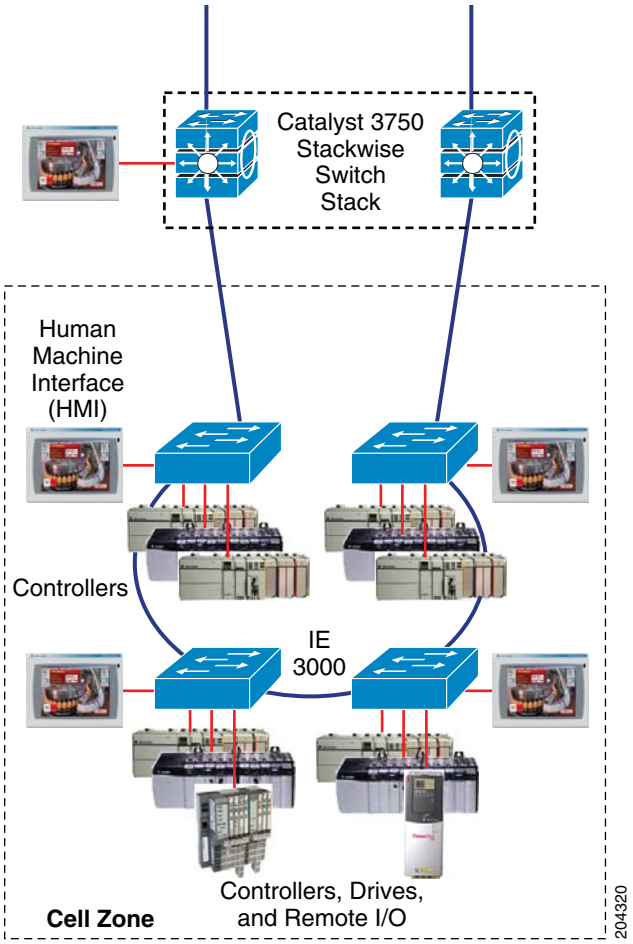
Cell Network–Trunk-Drop Topology



Cell Network—Ring Topology

-
-
-

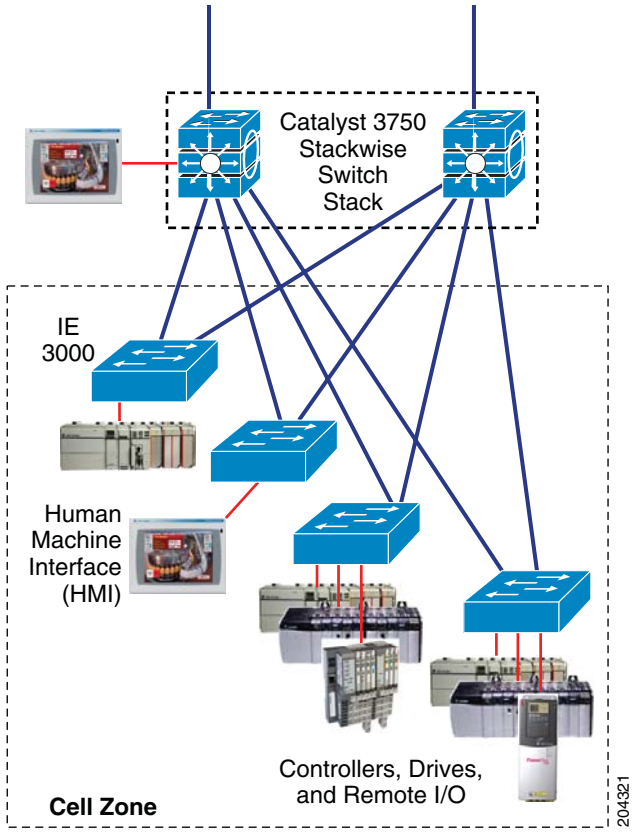
Figure 1-3 Cell Network–Ring Topology



Cell Network—Redundant-Star Topology

-
-
-

Figure 1-4 Cell Network–Redundant Star Topology



Where to Go Next

-
-