CHAPTER 1

Overview

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

- Features, page 1-1
- Default Settings After Initial Switch Configuration, page 1-6
- Where to Go Next, page 1-8

Features

The switch supports the IP base feature set, which provides Layer 2+ features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), and basic IPv6 management.

- Deployment Features, page 1-1
- Performance Features, page 1-2
- Management Options, page 1-3
- Manageability Features, page 1-3
- Availability and Redundancy Features, page 1-4
- VLAN Features, page 1-5
- Security Features, page 1-5
- QoS and CoS Features, page 1-6
- Monitoring Features, page 1-6
- Default Settings After Initial Switch Configuration, page 1-6

Deployment 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 information about Express Setup, see the getting started guide.
- An embedded device manager GUI for configuring and monitoring a single switch through a web browser. For information about starting the device manager, see the getting started guide. For information about the device manager, see the switch online help.

- 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, Gigabit Ethernet, Gigabit EtherChannel, 10-Gigabit Ethernet, and 10-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

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports to optimize bandwidth
- Automatic medium-dependent interface crossover (auto-MDIX) capability on 10/100/1000-Mb/s interfaces and on 10/100/1000 BASE-TX small form-format pluggable (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
- SFP+ support for 10 Gigabit speeds
- Support for up to 9216 bytes [the maximum packet size or maximum transmission unit (MTU) size] for frames that are bridged in hardware and software through Gigabit Ethernet ports and 10-Gigabit Ethernet ports
- 802.3x flow control on all ports (The switch does not send pause frames.)
- EtherChannel for enhanced fault tolerance and to provide up to 4 Gb/s (Gigabit EtherChannel) or 40 Gb/s (10-Gigabit EtherChannel) full-duplex bandwidth among switches, routers, and servers
- Port Aggregation Protocol (PAgP) for automatic creation of EtherChannel links
- Forwarding of Layer 2 packets at Gigabit line rate
- Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3. For IGMP devices, IGMP snooping for efficiently forwarding multimedia and multicast traffic
- IGMP snooping querier support for configuring 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 throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP leave timer for configuring the network leave latency
- 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)

Management Options

- An embedded device manager—The device manager is a GUI that is embedded in the software image. You use it to configure and to monitor a single switch. For information about starting the device manager, see the getting started guide. For information about the device manager, see the switch online help.
- CLI—The Cisco IOS software supports desktop and multilayer switching features. You can access the CLI by connecting your management station directly to the switch console port, by connecting your PC directly to the Ethernet management port, or by using Telnet from a remote management station or PC. For information about the CLI, see Chapter 2, "Using the Command-Line Interface."
- SNMP—SNMP management applications such as CiscoWorks LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station or a PC 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 information about using SNMP, see Chapter 23, "Configuring SNMP."

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 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 to disable MAC address learning on a VLAN to limit the size of the MAC address table
- Disabling MAC address learning on a VLAN
- 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
- 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
- Configuration logging to log and to view changes to the switch configuration
- Configuration replacement and rollback to replace the running configuration on a switch with any saved Cisco IOS configuration file

- 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 software image)
- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests
- Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem
- Out-of-band management access through the Ethernet management port to a PC
- Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying switch configuration or switch image files (requires the cryptographic software image)
- The HTTP client in Cisco IOS sends requests to both IPv4 and IPv6 HTTP servers, and the HTTP server in Cisco IOS services HTTP requests from both IPv4 and IPv6 HTTP clients
- IPv6 supports stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses.
- DHCP server port-based address allocation for the preassignment of an IP address to a switch port.
- Wired location service sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE).
- CPU threshold trap monitors CPU use.
- 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.
- USB mini-Type B console port in addition to the RJ-45 console port. Console input is active on only one port at a time.
- USB Type A port for external Cisco USB flash memory devices (thumb drives or USB keys). You can use Cisco CLI commands to read, write, erase, copy, or boot from the flash memory.

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
- 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:
  - Up to 128 supported spanning-tree instances
  - Per-VLAN spanning-tree plus (PVST+) for load-balancing across VLANs
  - Rapid PVST+ for load-balancing across VLANs and for rapid convergence of spanning-tree instances
  - UplinkFast and BackboneFast for fast convergence after a spanning-tree topology change and to achieve load-balancing between redundant uplinks, including Gigabit uplinks

- 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and to provide multiple forwarding paths for data traffic and load-balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+)
- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:
  - Port Fast to eliminate the forwarding delay by enabling a port to immediately change from the blocking state to the forwarding state
  - BPDU guard to shut down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)
  - BPDU filtering to prevent a Port Fast-enabled port from sending or receiving BPDUs
  - Root guard to prevent switches outside the network core from becoming the spanning-tree root
  - Loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link

VLAN Features

- Support for up to 64 VLANs for assigning users to VLANs associated with resources, traffic patterns, and bandwidth
- Support for VLAN IDs in the 1 to 4094 range
- 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) to negotiate trunking on a link between two devices and to negotiate the type of trunking encapsulation (802.1Q) to be used
- VLAN Trunking Protocol (VTP) and VTP pruning to reduce network traffic by restricting flooded traffic to links for stations receiving the traffic
- VLAN 1 minimization to reduce the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. When enabled, no user traffic is sent or received on the trunk. The switch CPU contiinues to send and receive control protocol frames.

Security Features

- Password-protected access (read-only and read-write access) to management interfaces (device manager, and the CLI) to protect against unauthorized configuration changes
- Multilevel security for a choice of security level, notification, and resulting actions
- Static MAC addressing to ensure security
- BPDU guard to shut down a Port Fast-configured port when an invalid configuration occurs
- Extended MAC access control lists to define security policies in the inbound direction on Layer 2 interfaces
- MAC authentication bypass to authorize clients based on the client MAC address
- TACACS+ to manage 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

- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic software image)
- 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 software image)

QoS and CoS Features

- Classification
  - 802.1p class of service marking priorities on a per-port basis to protect the performance of mission-critical applications
- Egress queues and scheduling
  - Four egress queues per port

Monitoring Features

- Switch LEDs provide port and switch status
- MAC address notification traps and RADIUS accounting to track users on a network, storing the MAC addresses that the switch has learned or removed
- Switched Port Analyzer (SPAN) to traffic monitor on any port or VLAN
- SPAN 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
- Online diagnostics to test the hardware functionality of the supervisor engine, modules, and switch while the switch is connected to a network

Default Settings After Initial Switch Configuration

You only need to assign basic IP information to the switch and connect it to other network devices.

Note To assign an IP address by using the browser-based Express Setup program, see the getting started guide. To assign an IP address by using the CLI-based setup program, see the hardware installation guide.

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

- Default switch IP address, subnet mask, and default gateway is 0.0.0.0. For information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway,” and Chapter 14, “Configuring DHCP Features.”
- Default domain name is not configured. For information, see Chapter 3, “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 information, see Chapter 3, "Assigning the Switch IP Address and Default Gateway," and Chapter 14, "Configuring DHCP Features."
- Switch cluster is disabled. For information, see Chapter 4, "Clustering Switches," and the *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- No passwords are defined. For information, see Chapter 5, "Administering the Switch."
- System name and prompt is *Switch.* For information, see Chapter 5, "Administering the Switch."
- NTP is enabled. For information, see Chapter 5, "Administering the Switch."
- DNS is enabled. For information, see Chapter 5, "Administering the Switch."
- TACACS+ is disabled. For information, see Chapter 7, "Configuring Switch-Based Authentication."
- RADIUS is disabled. For information, see Chapter 7, "Configuring Switch-Based Authentication."
- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For information, see Chapter 7, "Configuring Switch-Based Authentication."
- Port parameters
  - Operating mode is Layer 2 (switchport). For information, see Chapter 8, "Configuring Interface Characteristics."
  - Interface speed and duplex mode is autonegotiate. For information, see Chapter 8, "Configuring Interface Characteristics."
  - Auto-MDIX is enabled. For information, see Chapter 8, "Configuring Interface Characteristics."
  - Flow control is off. For information, see Chapter 8, "Configuring Interface Characteristics."
- VLANs
  - Default VLAN is VLAN 1. For information, see Chapter 9, "Configuring VLANs."
  - VLAN trunking setting is dynamic auto (DTP). For information, see Chapter 9, "Configuring VLANs."
  - Trunk encapsulation is negotiate. For information, see Chapter 9, "Configuring VLANs."
  - VTP mode is server. For information, see Chapter 10, "Configuring VTP."
  - VTP version is Version 1. For information, see Chapter 10, "Configuring VTP."
- STP, PVST+ is enabled on VLAN 1. For information, see Chapter 11, "Configuring STP."
- MSTP is disabled. For information, see Chapter 12, "Configuring MSTP."
- Optional spanning-tree features are disabled. For information, see Chapter 13, "Configuring Optional Spanning-Tree Features."
- IGMP snooping is enabled. No IGMP filters are applied. For information, see Chapter 15, "Configuring IGMP Snooping."
- IGMP throttling setting is deny. For information, see Chapter 15, "Configuring IGMP Snooping."
- The IGMP snooping querier feature is disabled. For information, see Chapter 15, "Configuring IGMP Snooping."
- CDP is enabled. For information, see Chapter 17, "Configuring CDP."
- UDLD is disabled. For information, see Chapter 19, "Configuring UDLD."
- SPAN are disabled. For information, see Chapter 20, "Configuring SPAN and RSPAN."

- RMON is disabled. For information, see Chapter 21, “Configuring RMON.”
- Syslog messages are enabled and appear on the console. For information, see Chapter 22, “Configuring System Message Logging.”
- SNMP is enabled (Version 1). For information, see Chapter 23, “Configuring SNMP.”
- QoS is disabled. For information, see Chapter 25, “Configuring QoS.”
- No EtherChannels are configured. For information, see Chapter 26, “Configuring EtherChannels and Link-State Tracking.”

Where to Go Next

- Chapter 2, “Using the Command-Line Interface”
- Chapter 3, “Assigning the Switch IP Address and Default Gateway”