Overview

This document describes how to configure system management features on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. The switch can be managed through one of the following methods:

- Command Line Interface (CLI) over a serial connection to the switch console or over a telnet session
- Web management interface through a browser (Network Management)
- Network Management Application through SNMP

This document describes managing the switch using the CLI. The CLI interface supports the standard IOS commands.

Features

The switch ships with one of these software images installed:

- The LAN Base image includes advanced quality of service (QoS), flexible VLAN handling, supervisory control and data acquisition (SCADA) protocol classification support, resilient Ethernet protocol (REP) for improved convergence time in ring topologies, Flexlink for fast failover in hub-and-spoke topologies, and comprehensive security features.
- The IP Services image adds advanced Layer 3 features such as support for advanced IP routing protocols, Multi-VPN Routing and Forwarding Customer Edge (Multi-VRF CE/VRF-Lite), and Policy Based Routing (PBR).

Some features noted in this chapter are available only on the cryptographic (that is, supports encryption) version of the switch software image. 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 two different types of interfaces by default: network node interfaces (NNIs) to connect to the service provider network and user network interfaces (UNIs) to connect to customer networks. Some features are supported only on one of these port types. You can also configure enhanced network interfaces (ENIs). An ENI is typically a user-network facing interface and has the same default configuration and functionality as UNIs, but can be configured to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), and EtherChannel Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP).

This chapter provides a summary of the following system management features:

DHCP

The initial switch configuration (for example, assigning the switch IP address and default gateway information) can be performed through the switch setup program, manually, or through a Dynamic Host Configuration Protocol (DHCP) server.

- Use the switch setup program if you want to be prompted for specific IP information.

  For more information about the setup program, see the "Configuring the Switch with the CLI-Based Setup Program" appendix in the *Cisco 1E 2000U Switch Hardware Installation Guide*.

- If you are an experienced user familiar with the switch configuration steps, use the CLI to manually configure the switch. Otherwise, use the switch setup program.
- Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device, and the other is a mechanism for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices. The switch can act as both a DHCP client and a DHCP server.

You can use the DHCP image upgrade features to configure a DHCP server to download both a new image and a new configuration file to one or more switches in a network. This helps ensure that each new switch added to a network receives the same image and configuration.

Related Topics

Chapter 2, "Assigning the Switch IP Address and Default Gateway"

Switch Boot Optimization

You can configure the switch to minimize the time it takes to boot. When switch boot optimization is enabled, the switch disables the memory test, file system check (FSCK), and power-on self-test (POST) that occur during the normal boot process.

Related Topics

Chapter 3, "Configuring Switch Boot Optimization"

NTP

You can manage the system time and date on your switch using automatic configuration, such as the Network Time Protocol (NTP), or manual configuration methods.

NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Related Topics

Chapter 4, "Administering the Switch"

MAC Address Table

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports.

With multiple MAC addresses supported on all ports, you can connect any port on the switch to individual workstations, repeaters, switches, routers, or other network devices. The switch provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As stations are added or removed from the network, the switch updates the address table, adding new dynamic addresses and aging out those that are not in use.

You can control MAC address learning on a VLAN and manage the MAC address table space that is available on the switch by controlling which VLANs, and therefore which ports, can learn MAC addresses.

Related Topics

Chapter 4, "Administering the Switch"

DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on your switch, you can substitute the hostname for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

Related Topics

Chapter 4, "Administering the Switch"

Switch Alarms

The switch software monitors switch conditions on a per-port or a switch basis. If the conditions present on the switch or a port do not match the set parameters, the switch software triggers an alarm or a system message. By default, the switch software sends the system messages to a system message logging facility, or a *syslog* facility. You can also configure the switch to send Simple Network Management Protocol (SNMP) traps to an SNMP server. You can configure the switch to trigger an external alarm device by using the alarm relay.

Related Topics

Chapter 5, "Configuring the Switch Alarms"

SDM Templates

If the switch is running the IP services image, you can use SDM templates to optimize system resources in the switch to support specific features, depending on how the switch is used in the network. The SDM templates allocate Ternary Content Addressable Memory (TCAM) resources to support different features. You can use the SDM templates for IP Version 4 (IPv4) and select the default template to balance system resources or select the layer-2 template to support only Layer 2 features in hardware.

Note Switches running the LAN Base image support only the layer-2 template

The dual IPv4 and IPv6 templates also enable a dual stack environment.

Related Topics

Chapter 6, "Configuring SDM Templates"

Smartports Macros

Smartports macros provide a convenient way to save and share common configurations. You can use Smartports macros to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network.

Each Smartports macro is a set of CLI commands. The switch software has a set of default macros (which cannot be edited by user). You can also create your own macros. Smartports macros do not contain new CLI commands; they are simply a group of existing CLI commands.

Related Topics

Chapter 7, "Configuring Smartports Macros"

LLDP and LLDP-MED

To support non-Cisco devices and to allow for interoperability between other devices, the switch supports the IEEE 802.1AB Link Layer Discovery Protocol (LLDP). LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet (PoE), and inventory management.

Related Topics

Chapter 8, "Configuring LLDP and LLDP-MED"

Port-Based Traffic Control

The switch has the following features for controlling traffic on an interface:

- Storm control—Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces
- Protected ports—Ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch
- Port blocking—Blocks a port (protected or nonprotected) from flooding unknown unicast or multicast packets to other ports
- Port security—Restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port

Related Topics

Chapter 9, "Configuring Port-Based Traffic Control"

CDP

CDP is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

Related Topics

Chapter 10, “Configuring CDP”

SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Related Topics

Chapter 11, “Configuring SPAN and RSPAN”

RMON

Remote Network Monitoring (RMON) is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments.

Related Topics

Chapter 12, “Configuring RMON”

System Message Logging

By default, a switch sends the output from system messages and **debug** privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console. You can use system message logging in the following ways:

- Set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations.
- Time-stamp log messages or set the syslog source address to enhance real-time debugging and management.
- Access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer.
- Remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet or through the console port.

Related Topics

Chapter 13, "Configuring System Message Logging"

SNMP

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

Related Topics

Chapter 14, "Configuring SNMP"

Cisco IOS IP SLAs

Cisco IP SLAs is a part of Cisco IOS software that allows Cisco customers to analyze IP service levels for IP applications and services by using active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. With Cisco IOS IP SLAs, service provider customers can measure and provide service level agreements, and enterprise customers can verify service levels, verify outsourced service level agreements, and understand network performance. Cisco IOS IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist with network troubleshooting.

Related Topics

Chapter 16, "Configuring Cisco IOS IP SLAs Operations"

Embedded Event Manager

Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery within a Cisco IOS device. EEM offers the ability to monitor events and take informational, corrective, or any other EEM action when the monitored events occur or when a threshold is reached. An EEM policy defines an event and the actions to be taken when that event occurs.

This policy is a programmed script that you can use to customize a script to invoke an action based on a given set of events occurring. The script generates actions such as generating custom syslog or Simple Network Management Protocol (SNMP) traps, invoking CLI commands, forcing a failover, and so forth. The event management capabilities of EEM are useful because not all event management can be

managed from the switch and because some problems compromise communication between the switch and the external network management device. Network availability is improved if automatic recovery actions are performed without rebooting the switch.

Related Topics

Chapter 15, "Configuring Embedded Event Manager"

Ethernet OAM, CFM, and E-LMI

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet networks to increase management capability within the context of the overall Ethernet infrastructure. The switch supports IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Local Management Interface (E-LMI), and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback. It also supports IP Service Level Agreements (SLAs) for CFM, and ITU-T Y.1731 fault management. Ethernet OAM manager controls the interworking between any two of the protocols (CFM, E-LMI, and OAM).

Related Topics

Chapter 17, "Configuring Ethernet OAM, CFM, and E-LMI"

Online Diagnostics

With online diagnostics, you can test and verify the hardware functionality of the switch while the switch is connected to a live network. The online diagnostics contain packet switching tests that monitor different hardware components and verify the data path and the control signals.

The online diagnostics detect problems in these areas:

- Hardware components
- Interfaces (Ethernet ports and so forth)
- Solder joints

Online diagnostics are categorized as on-demand, scheduled, or health-monitoring diagnostics.

- On-demand diagnostics run from the CLI.
- Scheduled diagnostics run at user-designated intervals or at specified times when the switch is connected to a live network.
- Health monitoring runs in the background.

Related Topics

Chapter 18, "Configuring Online Diagnostics"

Supported MIBs

See Appendix A, "Supported MIBs" for the list of supported management information bases (MIBs) for this release.