Configuration Overview

Feature Software Licensing

Software Licensing for the IE5000 is now simplified with the introduction of right-to-use (RTU) licensing. This allows you to order and activate a specific license type and level via command line. Uploading an extra license file is no longer necessary.

Note: Upgrading to the IP Services feature set requires the purchase of one of the following licenses (product IDs listed):
- **L-IE5000-RTU**

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.
- 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 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 10 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 such as lanbase-routing, ipv6 routing.
- 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 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 at software.cisco.com/download/.
- Prime Infrastructure—Cisco Prime Infrastructure simplifies the management of wireless and wired networks. It offers Day 0 and 1 provisioning, as well as Day N assurance from the branch to the data center. We call it One Management. With this single view and point of control, you can reap the benefits of One Management across both network and compute.
- 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.
- 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 Configuring SNMP, page 539

- 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 Configuring Cisco IOS Configuration Engine, page 79

Industrial Application

- 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 RSlogix/RSlinx then monitor the CIP functionality via IOS command lines or Web based Device Manager.
- Profinet Version 2—Support for PROFINET IO, a modular communication framework for distributed automation applications. The embedded Profinet GSD file allows user to bring up Cisco IE switch using Siemens STEP7 or TIA Portal software then monitor the functionality via command line or Web based Device Manger.

Feature Availability

Feature availability varies depending on your license. For more information about licenses and available features, refer to the datasheet:
http://www.cisco.com/c/en/us/products/switches/industrial-ethernet-5000-series-switches/datasheet-listing.html

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 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:

Note: For more information about the following default settings, see the corresponding sections of this guide.

- Default switch IP address, subnet mask, and default gateway is 0.0.0.0.
- Default domain name is not configured.
- DHCP client is enabled, the DHCP server is enabled, and the DHCP relay agent is enabled.
- Switch cluster is disabled.
- No passwords are defined.
- System name and prompt is Switch.
- NTP is enabled.
- DNS is enabled.
- TACACS+ is disabled.
- RADIUS is disabled.

- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled.
- IEEE 802.1x is disabled.
- Port parameters
  - Interface speed and duplex mode is autonegotiate.
  - Auto-MDIX is enabled.
  - Flow control is off.
- VLANs
  - Default VLAN is VLAN 1.
  - VLAN trunking setting is dynamic auto (DTP).
  - Trunk encapsulation is negotiate.
  - VTP mode is server.
  - VTP version is Version 1.
  - Voice VLAN is disabled.
- STP, PVST+ is enabled on VLAN 1.
- MSTP is disabled.
- Optional spanning-tree features are disabled.
- FlexLinks are not configured.
- DHCP snooping is disabled.
- IP source guard is disabled.
- DHCP server port-based address allocation is disabled.
- Dynamic ARP inspection is disabled on all VLANs.
- IGMP snooping is enabled. No IGMP filters are applied.
- IGMP throttling setting is deny.
- The IGMP snooping querier feature is disabled.
- MVR is disabled.
- Port-based traffic
  - Broadcast, multicast, and unicast storm control is disabled.
  - No protected ports are defined.
  - Unicast and multicast traffic flooding is not blocked.
  - No secure ports are configured.
- CDP is enabled.
- UDLD is disabled.

- LLDP is disabled.
- SPAN and RSPAN are disabled.
- RMON is disabled.
- Syslog messages are enabled and appear on the console.
- SNMP is enabled (Version 1).
- No ACLs are configured.
- QoS is enabled.
- No EtherChannels are configured.
- IP unicast routing is disabled.

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 on page 5 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 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 2 on page 6 describes some network demands and how you can meet them.

Table 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, 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.

Where to Go Next

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

- Performing Switch Setup Configuration, page 59

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.