Release Notes for the Industrial Ethernet 1000 Switch (Software Release 1.7)

First Published: 2018-05-08

Hardware Supported

Table 1: Switch Models Supported

Model	FE Uplink (copper	Gig Uplink (SFP)	FE Downlink (Copper)	POE(+) - Downlink	Description
IE-1000-4T1T-LM	1	0	4	0	IE1K with total of 5 FE ports 10/100
IE-1000-6T2T-LM	2	0	6	0	IE1K with total of 8 FE ports 10/100
IE-1000-4P2S-LM	0	2	0	4	IE1K with 2 GE SFP, 4 PoE 10/100 with total of 6 ports
IE-1000-8P2S-LM	0	2	0	8	IE1K with 2 GE SFP, 8 PoE 10/100 with total of 10 ports

SFP Modules Supported

The SFP modules are switch Ethernet SFP modules that provide connections to other devices. Depending on the switch model, these field-replaceable transceiver modules provide uplink interfaces. The modules have LC connectors for fiber-optic connections. For a complete list of supported SFP modules refer to the Data Sheet.

Express Setup Requirements

You need this equipment to set up the switch:

- Computer with Windows 7/Windows 10/Mac
- A Web browser (IE 11, Firefox 46.01 and 47.0) with JavaScript enabled (disable pop-up blockers and proxy settings).
- A straight-through or crossover Category 5 Ethernet cable to connect your computer to the switch port.
- A small paper clip to reach the express setup button.

Note Before running Express Setup, disable any wireless client running on your computer.

Installation Notes

You can assign IP information to your switch by using these methods:

- Express Setup program, as described in the Hardware Installation Guide.
- DHCP-based setup

Note If the switch fails to acquire the IP address from the DHCP server, it may fall back to default IP 192.168.1.254. Please ensure the server is connected then reboot the switch.

Note If the Express Setup failed in the Web Browser, press and hold the Express Setup button for 15-20 seconds to reset the switch to factory default

New Features in this Release

TACACS+ and RADIUS AAA Client

TACACS+ and RADIUS are two security protocols used to control access into networks. RADIUS uses UDP while TACACS+ uses TCP. Both can provide Authentication, Authorization and Accounting. In Saturn Phase III, Authentication and Authorization are supported.

User access to the switch through Telnet/SSH/DM can be controlled by TACACS+/RADIUS Authentication/Authorization.

IEEE 802.1x security

IEEE 802.1x is an IEEE standard for port-based network access control, which provides an authentication mechanism to devices wishing to attach to a LAN. When 802.1x authentication is enabled, ports are authenticated before any other Layer 2 features are enabled.

Single host mode with MAC authentication bypass is supported in this release.

BootP server with per-port support

BootP protocol is supported in this release. With BootP support, when client sends a BootP request, the server responds with BootP response based on same DHCP pool configuration.

DHCP snooping ease-of-use enhancement

A Device Manager page has been added to display the following:

- DHCP snooping table lists IP address, DHCP server and related port if DHCP snooping is enabled

Ping Support
A page has been provided in the Device Manager to initiate ping request and display the ping response statistics.

Linux IPTables security enhancement
IPTables will block all incoming traffic except Telnet/SSH/SNMP if they are enabled in the default configuration of the device.

CSRF Enhancement
The anti-CSRF, token based approach is supported in this release.

Sticky-MAC
An attribute of port-security, the Sticky-MAC feature enables the web interface to retain MAC addresses it dynamically learns. Sticky-MAC addresses form part of running configuration.

Software Features

Smartports Macros
Smartports macros provide port configurations that customer can manually apply based on the device connected to the port.

Port Mirroring
Port mirroring copies traffic from a source port on the switch to a destination port on the same switch for analysis.

Error Disable Event
If a specific error occurs on a port, the switch automatically disables the port so that it does not send or receive traffic. Current support error event: link flap, DHCP rate limit.

Storm Control
Provide configuration of storm control policy, rate to prevent LAN ports from being disrupted by excessive traffic.

Syslog
Syslog displays a record of events that occurred on the device and its ports. Syslog entries can be viewed on Web GUI or forward to a remote syslog server.

Common Industrial Protocol (CIP)
CIP is an industrial control protocol. It provides a comprehensive suite of messages and services for the collection of industrial automation applications. IE 1000 natively support CIP without any configuration needed, it passed ODVA CIP conformance testing and can be integrated into industrial automation environment.

Web GUI interface only
Through a user-friendly web device manager, the Cisco IE 1000 provides easy out-of-the-box configuration and simplified operational manageability to deliver advanced and secure industrial networks.

BPDU Guard
The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has PortFast configured. The BPDU guard transitions the port into errdisable state, and a message appears on the console.

DHCP Server
The DHCP Server feature is a full DHCP Server implementation that assigns and manages IP addresses from specified address pools within the switch to DHCP clients.

Ether Channel LACP
Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad.

IGMP

IGMP is an IPv4 protocol that a host uses to request multicast data for a particular group. Using the information obtained through IGMP, the software maintains a list of multicast group or channel memberships on a per-interface basis. The systems that receive these IGMP packets send multicast data that they receive for requested groups or channels out the network segment of the known receivers.

HTTP/HTTPs, SSH, and Telnet

The Cisco IE 1000 Switch provides connectivity via HTTP/HTTPs, SSH and Telnet.

MST spanning tree mode

MST maps multiple VLANs into a spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of STP instances required to support a large number of VLANs. MST improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

MST provides rapid convergence through explicit handshaking as each MST instance uses the IEEE 802.1w standard, which eliminates the 802.1D forwarding delay and quickly transitions root bridge ports and designated ports to the forwarding state.

QOS Priority port

The Priority Port feature allows the end user to specify a port which is connected to high priority end devices (eg: IP phone, or PLC), as a Priority Port. Once the Priority Port is configured, all the Ethernet packets received from that end device will have higher priority than packets received from other end devices connected to the IE1000.

PoE Management

PoE Management Modes:

- Auto-LLDP: use LLDP for max power draw; reserves what is negotiated
- Auto-PD Class: PD class determines max power draw; reserves the class max
- Static: max power determined by value in ‘max power field’; reserves based on max power field

Port-security

Port Security limits the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, only the specified maximum number of users are allowed on the port. If this number is exceeded, an action is taken (described below). Port Security works together with MAC address learning to restrict access to a port.

SNMP v2/v3, trap

The switch supports SNMPv2 and SNMPv3 traps.

SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message.

STP port fast

Port Fast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states.

You can use Port Fast on interfaces connected to a single end device or server, to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge.

Interfaces connected to a single end device or server should not receive bridge protocol data units (BPDUs). An interface with Port Fast enabled goes through the normal cycle of spanning-tree status changes when the switch is restarted.

Virtual LAN (VLAN)

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.

Alarm

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.

The Cisco IE 1000 PoE(+) switches have one external alarm port and supports one output relay.

Caveats

Table 2: Open Caveats

ID	Description
CSCvi10667	Secure Mac entries are not getting deleted when interface is in shutdown state
CSCvh19579	Device manager takes approximately ~20 seconds to show the Dashboard page after a software uprade image swap or reloaded with clearing cookies.
CSCvh74894	IE1000 does not transmit AAA request to ISE server if username is 'root', 'daemon' , 'bin' , 'sys' , 'sync', 'mail' , 'www-data' , 'operator' , 'nobody'
CSCvi04968	DNS Secondary Server IP overwritten by Primary server IP from the DHCP Server options response
CSCvg90472	Mac Aging 2x longer than configured
CSCvg50157	The successful message is not shown to user after an ImageUpgrade

Related Documentation

Installation, Configuration, Maintenance, and Operation Guides

http://www.cisco.com/c/en/us/support/switches/industrial-ethernet-1000-series-switches/tsd-products-support-series-home.html

Online Help (available on the switch)

Device Manager online help

SFP Information

- Compatibility Information:http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html
- Installation Notes:http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html