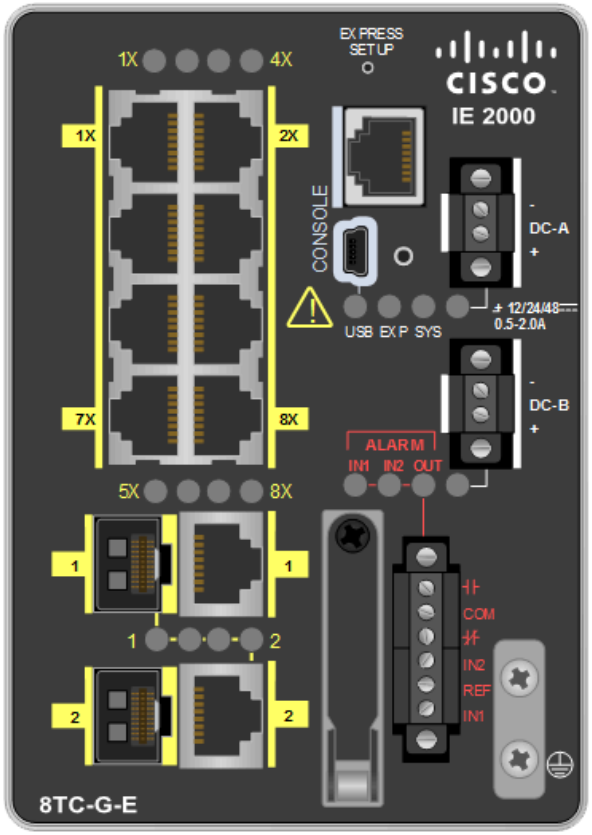
Cisco IE 2000 and IE 4010 Ethernet Switches for Metasys Networks Installation Instructions and Troubleshooting Guide



Building Technologies & Solutions

www.johnsoncontrols.com

2022-07-08

LIT-12013055

Release 12.0

Contents

Cisco® switch introduction

Cisco® industrial Ethernet (IE) switches use a fanless cooling system that allows operation in challenging environments where large amounts of dust, extreme temperature fluctuations, or vibrations may be present. This design allows the switch to operate in locations that may typically damage an IT-grade switch.

This document provides information on the Cisco IE 2000 switch and the Cisco IE 4010 switch. The two switches have different dimensions but have similar features. For additional information, refer to the Cisco proprietary documentation available from the *Support and Downloads* page of the Cisco website: https://www.cisco.com/c/en/us/support/index.html.

A label on the switch has two important pieces of information. The first is the serial number. This is needed for warranty claims and to associate the switch with a Cisco SmartNet® contract that enables additional Cisco support. The second is the MAC address of the switch. The value printed on the label is the chassis MAC address; the switch has additional MAC addresses for each physical port and switch virtual interface (logical port).

Summary of changes

The following information is new or revised:

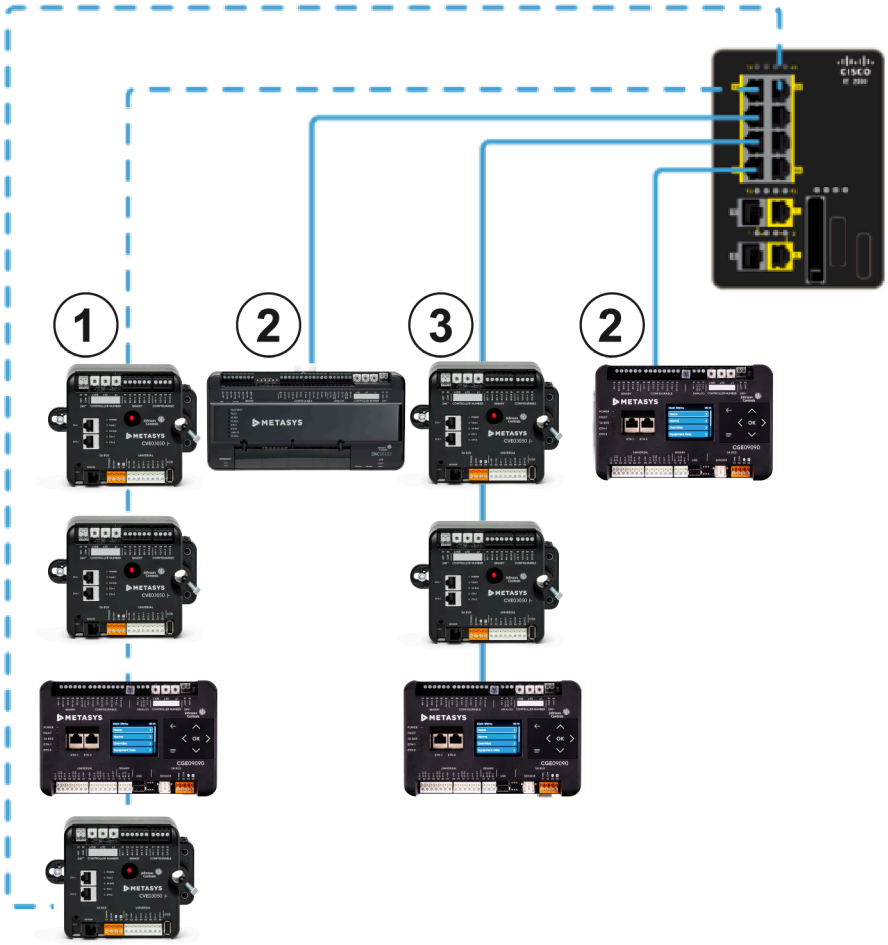
- Newer devices included in Figure 1, Figure 2, and Figure 9.
- Replaced mentions of VMA and NAE devices with CVE/CGE and network engine devices in Example network, Trivial network, and Troubleshooting.
- Replaced mentions of CVE devices with the more generic term IP-based field controller in Starting up the switch.
- New BACnet/IP and BACnet/SC sections in Network security.
- Added new note to Cisco IE 2000 switch termination diagram.

Cisco IE 2000 switch applications

The IE 2000 switches selected in the Johnson Controls® catalog as access switches can be configured to manage rings using Media Redundancy Protocol (MRP). See Figure 1 **label 1**.

A ring topology improves network availability. When the ring is closed it is in the normal state, and the switch sends data to the devices in the ring through only one of the two ring ports. The switch manages the physical ring as a single logical chain. However, if the ring opens it is in a failure state. When this occurs, the switch will detect the break and begin sending data over both switch ports. The switch then manages the physical ring as two logical chains. Therefore, the failure of a single device does not block communication to other devices, and the failure of a single cable does not block communication to any devices. You may also configure a port for a chain or home-run connection. When you design an IP network using the JCI IP Network Wizard, unused ports are configured for no access to the network.

Figure 1: Examples arrangements of controllers connected to a switch



Label	Description
1	Ring network.
2	Star network. Also known as a home-run network.
3	Chain network. Also known as a daisy-chain network.

The IE 2000 switch is a managed switch that has several traffic management features. However, you must enable these features in the switch configuration. The workflow for Johnson Controls systems is to use the Metasys IP Network Wizard to develop the switch configuration in the branch office, and then load the configuration onto the switch at the time of installation. This guide does not cover switch configuration. For information on switch configuration, refer to the *Cisco IE 2000 Software Configuration Guide* available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie2000/software/release/15-0_1_ey/configuration/guide/scg-ie2000.html

In some situations, the IP network Wizard supports another application for a Cisco IE 2000 switch. One switch can be given an additional role as a central router for the Metasys IP network. This can be an effective way to handle routing in networks that are not quite large enough to justify the cost of an aggregation switch. One possibility is for one access switch to serve both as an access switch and the central router. A second possibility is for one switch to serve as a dedicated central router. Note that when the IP Network Wizard specifies a Cisco IE 2000 as a dedicated router, it specifies a switch that does not support MRP.

Cisco IE 4010 switch applications

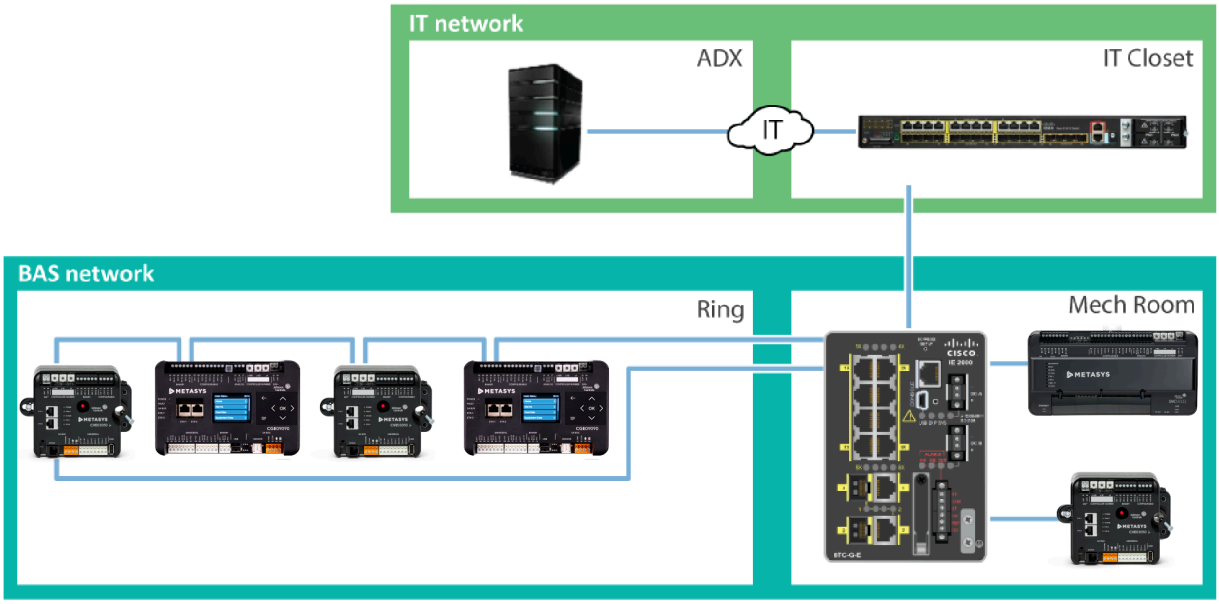
In a IP network designed using JCI's IP Network Wizard, the IE 4010 switch is specified as an aggregations switch. It is possible to use the IE 4010 as an access switch, but the architectures supported by the IP Network Wizard specify IE 2000 switches as access switches.

The IE 4010 switch is a managed switch that has several traffic management features. However, you must enable these features in the switch configuration. The workflow for Johnson Controls systems is to use the Metasys IP Network Wizard to develop the switch configuration in the branch office, and then load the configuration onto the switch at the time of installation. This guide does not cover switch configuration. For information on switch configuration, refer to the *Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration Guide* available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000.html

Example network

The following figure shows an example network in a building automation system.

Figure 2: Example IP network with Cisco switch



In this example, the physical wiring alone does not provide enough information to fully understand the network. The network engine supervises the controllers connected to the switch, to the CVE in the mechanical room, and to the CVEs and CGEs in the office area. The ADX is connected on the IT side of the network.

In a network of unmanaged switches, the wiring defines the network. A device can communicate with any other connected device on the network. The standard network designs for Metasys Release 10.0 or later use managed switches to impose design rules. These rules complicate and clarify the network, and are described in further detail below.

One goal of networking is to provide segmentation. BACnet uses broadcasts for device discovery. Before IP controllers, the scope of broadcasts was mostly limited to one MS/TP trunk. The limit was imposed by the physical configuration of the network. For IP networks, the limit is imposed logically instead of physically. Each device receives an IP address and a subnet mask; the address seen through the mask identifies the subnet. Defined this way, a subnet exists in OSI Layer 3. A VLAN is

defined in OSI Layer 2. For Metasys, you define VLANs and subnets so that they overlay exactly. If two devices are in the same subnet, they are also in the same VLAN; if two devices are in the same VLAN, they are also in the same subnet.

All the devices on a ring have to be in the same VLAN. A network engine can supervise devices in more than one VLAN. In the example shown in Figure 2, the simplest design is to place all of the controllers in the same VLAN, including the single controller that is connected to the switch but not part of the ring. There is no benefit in creating a second VLAN if it has only the one controller in the Mechanical Room.

The network engine can be in the same VLAN as the controllers, or in a separate VLAN. In the example in Figure 2, it is in a separate VLAN. In Metasys Release 9.0 networks, a BACnet/IP Broadcast Management Device (BBMD) may be required to rebroadcast communications between VLANs. In Release 10.0 you can configure a controller as a BBMD. Alternatively, you can configure the switches to forward BACnet broadcasts from the network engine to the subnet in which the IP controllers reside. You must consider the design of the network as a whole, and you can use the Metasys IP Network wizard to guide you as you make some of these decisions. For more information on the design of Metasys IP networks, refer to the *Metasys IP Networks for BACnet/IP Controllers Technical Bulletin (LIT-12012458).*

Cisco IE switch communication protocols

The Cisco IE 2000 and IE 4010 switches use Internet Protocol (IP) for Ethernet ports. The devices that connect to the switch must also use IP and Ethernet.

For reasons of cybersecurity, you can configure both the IE 2000 and IE 4010 switches to forward only those packets required for the application running on the network. For example, you can configure switches for Johnson Controls BAS systems to permit the BACnet protocol, but block other protocols.

Cisco IE switch compliance

The Cisco IE switches are compliant with many standards. For more information, refer to the Cisco proprietary documentation, such as model-specific data sheets, available from the *Support and Downloads* page of the Cisco website: https://www.cisco.com/c/en/us/support/index.html.

Cisco IE switch technical specifications

For more information on the technical specifications of the Cisco IE switches, refer to the Cisco proprietary documentation, such as the model-specific data sheets, available from the *Support and Downloads* page of the Cisco website (https://www.cisco.com/c/en/us/support/index.html).

Cisco IE 2000 switch installation

For detailed information regarding installation, safety and power requirements, and power connections, refer to the *Cisco IE 2000 Switch Hardware Installation Guide*, available at https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie2000/hardware/installation/guide/ie2000_hig.pdf.

Cisco IE 2000 switch installation materials and tools

In addition to the required materials and tools listed in the Cisco proprietary documentation, the following materials and tools are also required:

- Secure Digital (SD) flash memory module (SD card) preloaded with the IE 2000 software and switch configuration files

- Small Phillips-head screwdriver for opening the SD card slot
- Large slotted screwdriver for mounting the switch on a DIN rail
- DIN rail bracket. Optional: depends on mounting location

Note: For information on compatible SD cards, refer to the *Ring Manager IP Network System Catalog Page (LIT-1901096)*.

Inserting an SD card into a Cisco IE 2000 switch

1. Locate the SD card slot.
2. Loosen the captive screw at the top of the cover and pull the cover back to expose the SD card slot.
3. Insert an SD card that contains, at minimum, a `config.text` (case sensitive) configuration file and the desired version of IOS operating system. The IOS operating system is a `.bin` file.
4. Close the cover and tighten the screw.

Mounting the Cisco IE 2000 switch on a DIN rail

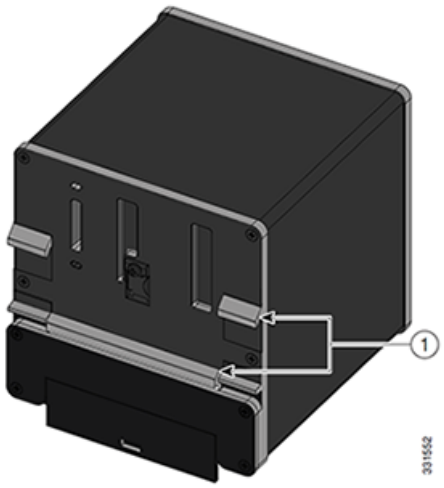
The Cisco IE 2000 switch may require extra depth when mounted in an enclosure. If the enclosure is shallow, you may need to rotate the switch 90 degrees horizontally in the enclosure. For ease of maintenance, mount the switch so that you can view the LED indicator forward-facing and the serial number on the side.

Mount the switch and the power supply on the DIN rail. The power supply includes a power cord for the local power receptacle. To connect power to the switch, use wire provided by the installer, and the power connectors that are shipped with the switch and power supply. For cooling purposes, ensure that there is a minimum clearance of two inches around the switch, with one inch either side.

Cisco IE 2000 switch DIN rail mounting application

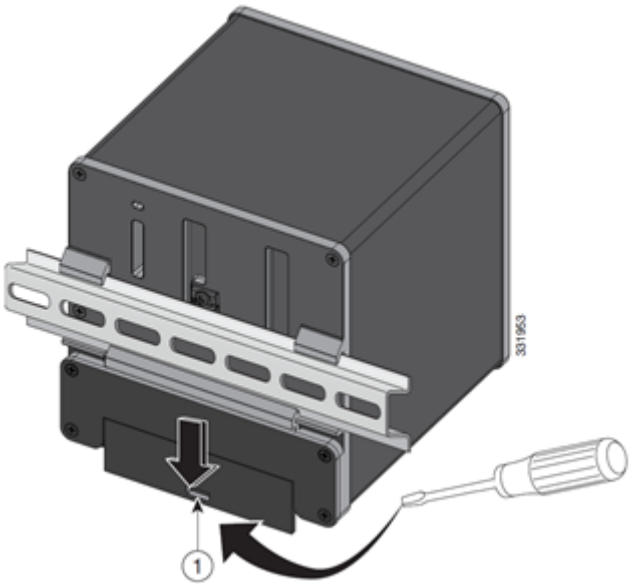
The following figure shows the rear of the Cisco IE 2000 Switch, and label 1 indicates the location of the DIN rail mounting clips.

Figure 3: Cisco IE 2000 switch DIN rail mount application



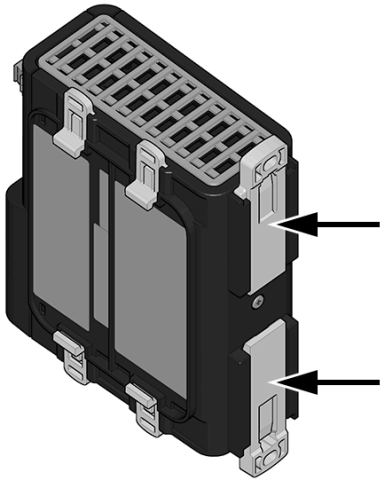
The following figure shows how to remove the Cisco IE 2000 Switch from the DIN rail mount application. To release the DIN rail, use a large slotted screw driver to push down the spring-loaded latch indicated by label 1.

Figure 4: Cisco IE 2000 switch DIN rail removal



The following figure shows the rear of the AC power module, and the location of the DIN rail mounting clips.

Figure 5: Cisco PWR-IE50W-AC-IEC DIN rail clip locations



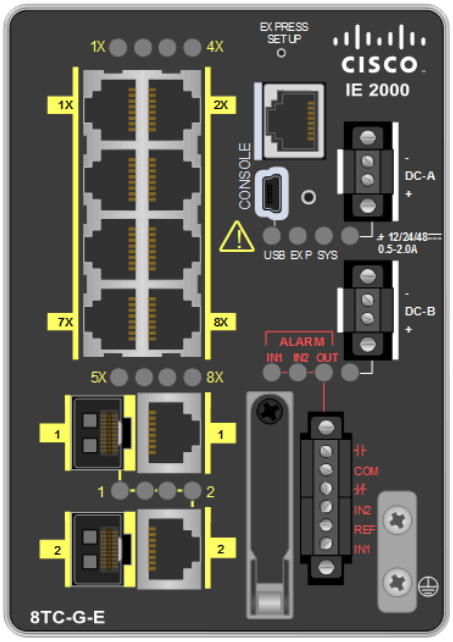
Wiring the Cisco IE 2000 switch

The IE 2000 family of switches includes various models which differ in the number of ports, the physical port types, and other features. The three models of the IE 2000 switch that you can use in the design of a Metasys IP network are listed below:

- IE-2000-4T-G-B: 4 access ports and 2 uplink ports; when this switch is specified, it is specified as a dedicated router and not for network access or as a ring manager.
- IE-2000-8TC-G-E: 8 access ports and 2 uplink ports

- IE-2000-16TC-G-E: 16 access ports and 2 uplink ports

Figure 6: Cisco IE 2000 switch



The ports that are labeled in yellow with X designations, for example, 1X, 2X, and 3X, are Fast Ethernet ports with connection speeds of 10/100 Mbits/sec. These ports accept RJ-45 connectors. You typically use Fast Ethernet ports as access ports, to connect controllers to a switch.

The ports that are labeled in yellow without X designations, for example, 1, 2, and 3, are Gigabit Ethernet ports with connection speeds of 1000 Mbits/sec. Depending on the network design, these ports accept either a copper-based RJ-45 connector or a small form factor pluggable (SFP) optical transceiver for terminating a fiber optic cable. You can use fiber optic cables to extend the reach of a connection. You typically use Gigabit Ethernet ports for uplink, to connect a switch to another switch.

The ports that are labeled in blue are console ports for local access. These ports are not connected during installation, or during regular operation.

How you use a particular port depends on switch configuration. For configuration files generated by the wizard, the default configuration for a port is to block traffic. You enable ports for purposes such as access or uplink, for a particular topology (ring or other types), and for specified subnets/VLANs. This means that the details of the switch wiring are specific to the network that you install. For information on how to connect a switch, refer to the accompanying installation sheet.

Powering the Cisco IE 2000 switch

If you are loading a new configuration file, see Starting up the switch. If you are loading a known good configuration file, you can connect the Ethernet cables before or after you apply power to the switch.

Note: Do not connect Ethernet cables to the switch ports until you verify the sucessful upload of the correct configuration file from the SD card. If you use the IP Network Wizard to create the switch configuration file, you need to verify the configuration of the switch. Once the system (SYS) and one or both power (PSU) LEDs on the switch appear steady green indicating the switch startup is complete, connect a laptop to the local maintenance port of the switch specified in the IP Network Wizard Installation Sheet. Configure the laptop to obtain its IP address via Dynamic Host Configuration Protocol (DHCP). Verify that the laptop is assigned the laptop IP address corresponding to the switch as specified in the Installation Sheet.

To connect power to the switch, refer to the *Connecting to Power* section in the *Cisco IE 2000 Switch Hardware Installation Guide*, available at https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie2000/hardware/installation/guide/ie2000_hig.pdf. The IE 2000 supports dual power supplies. Using the power supply specified in the *Ring Manager IP Network System Catalog Page (LIT-1901096)*, a single power supply is sufficient for normal operation. If a second power supply was previously configured, or if Cisco's Industrial Network Director (IND) is used to deploy the switch configuration, you can disable the status readback for the second supply. For more information, see Table 9. If the status LED is red, the second supply is not present. If the other power status LED is green, the switch is able to run normally.

When startup is complete, and the switch is operating normally, the system (SYS) and power (PSU) LED indicators are steady green. If the network is alive, the LED indicators for each Ethernet port appear steady green, or blinking green if there is an active device connected to the port.

When you configure two ports for MRP, you have the opportunity to note connection errors on the ring. If one LED indicator on one of the ports is steady green and the LED on the other port is blinking green, then the ring is closed and working correctly. If both LED indicators are blinking green, the ring is open and at least one device or cable is faulty.

Installing the Cisco IE 4010 switch

For detailed information regarding installation, safety and power requirements, and power connections, refer to the *Cisco IE 4010 Switch Hardware Installation Guide*, available at https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/hardware/installation/guide/ie4010_hig.html.

Cisco IE 4010 switch installation materials and tools

In addition to the required materials and tools listed in the Cisco proprietary documentation, you also require a Secure Digital (SD) flash memory module (SD card) preloaded with the Cisco IE 4010 software and switch configuration files.

Note: For information on compatible SD cards, refer to the *Ring Manager IP Network System Catalog Page (LIT-1901096)*.

Installing the power supply unit for the Cisco IE 4010 switch

The IE 4010 switch is supplied with a power supply installed. For information on how to install or replace a power supply, refer to the *Power Supply Installation* section in the *Cisco IE 4010 Switch Hardware Installation Guide*, available at https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/hardware/installation/guide/ie4010_hig/higpower.html

Inserting an SD card into the Cisco IE 4010 switch

1. Locate the SD card slot.
2. Loosen the captive screw at the top of the cover and pull the cover back to expose the SD card slot.

3. Insert an SD card that contains the `config.text` (case sensitive) configuration file and the desired version of IOS operating system. The IOS operating system is a `.bin` file.
4. Close the cover and tighten the screw.

Result

Note: For information on compatible SD cards, refer to the *Ring Manager IP Network System Catalog Page (LIT-1901096)*.

Mounting the Cisco IE 4010 switch

The Cisco IE 4010 switch has mounting brackets for rack mounting. Alternatively, you can order a wall mounting kit to mount the switch on the wall. When mounting the switch on a wall, ensure that you comply with the Cisco proprietary documentation guidelines for orientations that allow for adequate cooling.

Wiring the Cisco IE 4010 switch

The Cisco IE 4010 switch has two types of ports: ports for copper cables and ports for SFPs that support fiber optic cables. Fiber optic cables are specified where the distance between switches exceeds 100 m. For each connection, verify the type of cable, and then use the corresponding port. The ports labeled in blue are console ports for local access. The console ports are not connected during installation. The console ports accept copper cables with RJ-45 connectors.

How you use a particular port depends on switch configuration. For configuration files generated by the wizard, the default configuration for a port is to block traffic. You enable ports for purposes such as access or uplink, for a particular topology (ring or other types), and for specified subnets/VLANs. This means that the details of the switch wiring are specific to the network that you install. For information on how to connect a switch, refer to the accompanying installation sheet.

Figure 7: Cisco IE 4010 switch

Powering the Cisco IE 4010 switch

If you are loading a new configuration file, see Starting up the switch. If you are loading a known good configuration file, you can connect the Ethernet cables before or after you apply power to the switch.

Note: Do not connect Ethernet cables to the switch ports until you verify the sucessful upload of the correct configuration file from the SD card. If you use the IP Network Wizard to create the switch configuration file, you need to verify the configuration of the switch. Once the system (SYS) and one or both power (PSU) LEDs on the switch appear steady green indicating the switch startup is complete, connect a laptop to the local maintenance port of the switch specified in the IP Network Wizard Installation Sheet. Configure the laptop to obtain its IP address via Dynamic Host Configuration Protocol (DHCP). Verify that the laptop is assigned the laptop IP address corresponding to the switch as specified in the Installation Sheet.

To connect power to the switch, refer to the *Power Supply Installation* section in the *Cisco IE 4010 Switch Hardware Installation Guide*, available at https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/hardware/installation/guide/ie4010_hig/higpower.html.

When startup is complete, the system (SYS) and one or both power (PSU) LEDs appear steady green. The system LED blinks during the power-on self-test. If the network is alive, the LED indicators for each Ethernet connection appear steady green or blinking green if there is an active device connected to the port.

Configuring the switch

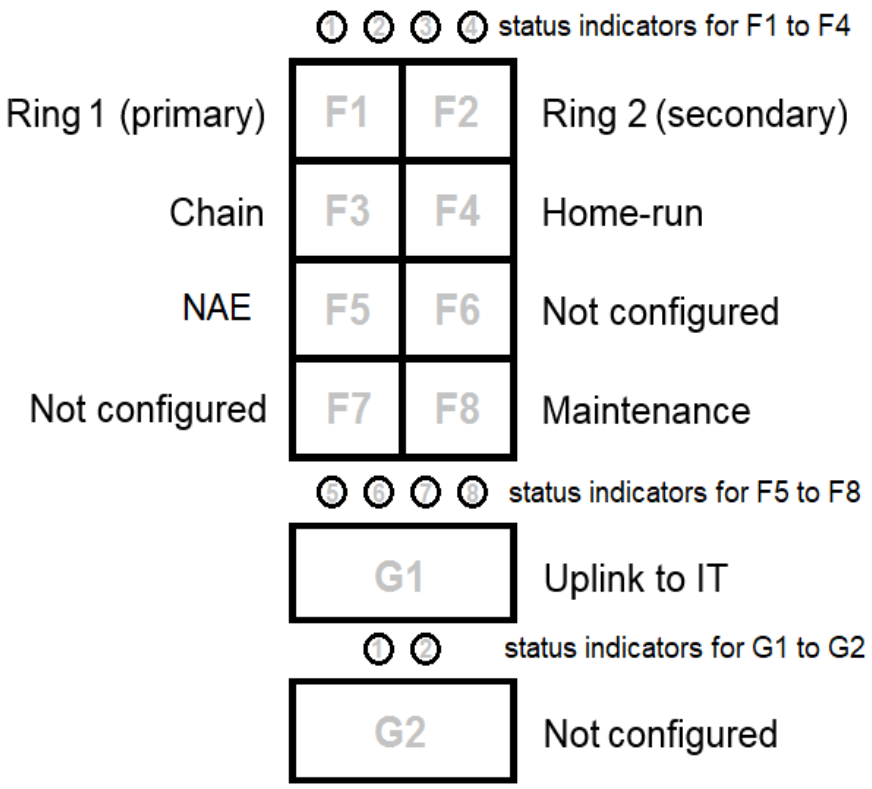
Configuration files

The network design is implemented by the switch configurations, so understanding the configurations is the key to understanding the network. The installation sheet generated by the Metasys IP Network Wizard provides an essential summary. It includes an overview of the configuration, and information about the rest of the system that you are required to configure.

The configuration file and installation sheet are usually delivered on an SD card. To understand the network better, remove the SD card from the slot on the switch, insert the card into the card slot on your laptop, and copy the Installation Sheet file. Then return the card to the slot on the switch and close the cover.

The Installation Sheet has network information such as an addressing plan that can confirm or correct presumptions made at the network design stage. It also has port assignments for all the switches. For example, Figure 8 shows the connection assignments for the ports of the switch shown in Figure 2 above.

Figure 8: Port assignment



FastEthernet ports 1 and 2 are for a ring of controllers that support MRP. Port 3 is for a daisy chain of controllers. A single controller is part of a chain of one, and can be connected to the port. Port 5 is for the network engine. Ports 6 and 7 are not used. Port 8 is for a service laptop, for example, a laptop running the Controller Configuration Tool (CCT). Gigabit Ethernet port 1 is the connection to the rest of the network. Gigabit Ethernet port 2 is not configured.

An actual configuration may differ from the example shown in Figure 8. For example, a switch may have up to three rings, up to two mirror ports, and an unlimited number of chain ports, subject to the overall limitation of the total number of ports. A chain of length one is also known as a home-run connection.

Connecting a service laptop

ⓘ **Note:** This step is not required for standard configuration using IP network wizard but, rather, as an optional step to verify communication is established.

In standard switch configurations, the last Fast Ethernet port is configured for a service laptop. You can use the port to connect your laptop to the network so that you can ping IP addresses and use the usual Metasys tools, such as the System Configuration Tool (SCT), the Site Management Portal (SMP), and the Controller Configuration Tool (CCT). Also, if you need to manage the switch, you can open a secure shell session on the switch's management interface specified in the Installation Sheet. To open a secure shell, use the `ssh` command, the IP address of the management interface, and the user name and password for the switch.

To connect a service laptop, complete the following steps:

1. Verify that your laptop is configured to use DHCP before you connect to the switch. If not, make a note of your static IP address, and then change the configuration. The switch assigns your laptop an address in a very small subnet that gives it the same connectivity profile as the network engine. The assigned DCHP address is listed in the Installation Sheet.
2. Connect an Ethernet cable between the laptop and maintenance port.

You are now able to ping the switch virtual interface (SVI), the network engine, all the controllers connected to the switch, all the network engines supervising controllers connected to the switch, and all the controllers that are supervised by the network engines that are connected to other switches.

Starting up the switch

To verify that the correct switch configuration file is successfully loaded into a Cisco IE 2000 or IE 4010 switch at a bench, complete the following steps:

1. Insert the SD card for the switch into the switch's SD card slot prior to connecting the Ethernet cables to the uplink ports of the switch. At minimum, the SD card must contain the following files:
    a. The switch-specific configuration file. You must name the switch configuration file `config.text`(case sensitive).
    b. A copy of the iOS .bin file for the switch. For example, the `IE2000-universalk9-mz.152-6.E2a.bin` for an IE 2000 switch.
    c. An empty ssh.enable file.
    d. Power cycle the switch.
2. Connect a laptop to the local maintenance port of the switch once the system (SYS) and one or both power (PSU) LEDs on the switch appear steady green. Steady green indicates the switch start-up is completed. Port 8 is always configured as the local maintenance port on the IE 2000 switches. Port 19 is always configured as the local maintenance port on the IE 4010 switches. Configure the laptop to obtain its IP address via Dynamic Host Configuration Protocol (DHCP).
3. Verify that the laptop is assigned the laptop IP address corresponding to the switch as specified in the Installation Sheet.
4. Connect a powered up IP-based field controller controller to FE1 and FE2. Confirm that there is one solid FE light and one blinking FE light.

    ⓘ **Note:** If the IP-based field controller is in the factory state, use CCT or SIS BACnet Explorer to locate the IP-based field controller by instance number range 2000001 to 2000999 or use the instance number downloaded into the controller.
5. Verify that the IP-based field controller is assigned an IP address corresponding to the switch and defined ring, as specified in the installation sheet.

Optional. Repeat steps 4-6 for each additional Ring, using FE3 and FE4 for Ring 2, and using FE5 and FE6 for Ring 3. You have to power cycle the IP-based field controller because the DHCP lease is of 10 minutes duration.

Network design reference

Starting with Metasys Release 9.0, it is possible to create a network for building automation that is based on Ethernet. Starting with Release 10.0, such a system includes IP controllers with redundant network connections that can support a Media Redundancy Protocol (MRP) enabled ring.

In an IP-based building automation system, Internet Protocol is the networking technology that connects the site manager, network engines, and controllers. If all controllers in a Metasys network are IP controllers, MS/TP networking persists only in the SA bus.

Trivial network

Not every network requires a network switch. If a communication connection is not required outside of the connected devices, the following network is adequate for commissioning and operation.

Figure 9: IP Network that does not require a switch

Figure 9 illustrates a simple network where the CVEs are connected as a chain. The chain is terminated on one end by an network engine and on the other end by a laptop running SCT or CCT. You can optionally run packet capture software on the laptop to monitor its Ethernet port. Configure the CVEs with DHCP enabled and temporarily configure the network engine to have a static IP address from the Automatic Private IP Addressing (APIPA) address range: `169.254.0.0/16`. When powered up, CVEs search for a DHCP server. If the CVEs do not find a DHCP server, they self-assign an IPv4 APIPA address. At this point, the laptop that is running SCT can discover them. Configure the laptop to obtain and assign an IP address via DHCP. The CVEs can forward packets along the chain in both directions, so SCT is able to discover all of the CVEs.

Segmentation

The idea of segmentation is closely related to addressing. For best practice in Metasys, assign static IP addresses to the ADX, network engines, and switches. These addresses are obtained from the IT address space. For best practice, assign each controller a dynamic IP address from an address space that is private with respect to IT. The use of private addresses allows Johnson Controls to install a large building automation and control network while consuming only a small amount of IT-assigned IP addresses.

If you extend a VLAN into the IE switches from the IT switch, you need a trunk port connection, as shown in Figure 2. Alternatively, if traffic is routed to and from the building's network, you can implement a routed port instead.

Network security

The switch configurations generated by the IP Network Wizard configuration tool apply the network security features. For example, an unconfigured port does nothing. Among the configured ports, the ring and chain ports have the most restrictive security settings. This is because, if we assume that the switch itself is in a locked closet or cabinet, the controller ports would have the less physical security. The service port has the least restrictive settings. Assuming that the network engine is also in a locked closet, the port to which it is connected also has more permissions than a chain or ring port.

BACnet/IP

Take a least privilege approach regarding network security in the Metasys BACnet/IP network. That is, only allow access to individuals, devices, and protocols that require access to the Metasys

BACnet/IP network. Access to the network infrastructure by individuals is restricted through the use of passwords. Access to the switching and routing functions of the network infrastructure is restricted by limiting the number of configured switch ports, and restricting devices and protocols through the use of ACLs.

BACnet/SC

BACnet Secure Connect (BACnet/SC) is a new BACnet datalink ASHRAE 135-2020 Annex AB that provides secure message transport by using the standard IP application protocol, Secure WebSocket, which is an extension to HTTPS and runs over Transport Layer Security (TLS). BACnet/SC thereby provides a secure mechanism to authenticate and authorize a device to use the network. From a cybersecurity standpoint, mixing BACnet/IP and BACnet/SC compromises the security of the network. It is best practice to use only BACnet/SC for the entire site to safeguard a site's security, if possible. If you must connect BACnet/IP devices to the network, it is best practice to minimize the number of BACnet/IP devices and isolate them to one engine.

Switching and routing

The switch needs to perform both switching and routing. Switching is done in OSI layer 2, and is therefore needed between the controller connected as a homerun, and the controllers connected as a ring. Switching is simple and fast. The switch can identify where to send packets within a VLAN. The only additional configuration that is required is to assign the switch's ports to VLANs.

Routing is done in OSI layer 3, and is therefore needed between the controllers and the network engine when the network engine resides in a VLAN different than the controllers it supervises, and between the network engine and ADS. Routing connects different subnets and usually needs more configuration than switching. For a Metasys network, important routes are defined in the switch configuration. For example, the configuration includes explicit routing statements that tell the switch how to send packets between the network engine and the controllers. Every device needs a default route. A default route tells the device where to send a packet if it does not have any other information about the destination of the packet. The controllers and network engine have the address of the switch for their default route. If configured correctly, the switch will know where to send the packet next.

Switches have addresses and default routes like any other device. They have one MAC address for every physical port and virtual port. The basic IP address is the Switch management Virtual Interface (SVI). It may also manage the virtual interface for one or more VLANs. These virtual interfaces are used to construct the routing rules.

Dynamic host control protocol

In older network configurations, all IP addresses were assigned statically. Computers never moved, so their subnet assignments were always correct. Also, the supply of 32-bit addresses seemed inexhaustible. In the present day, devices are more plentiful, and it is customary to allocate pools of addresses and let computers make the final assignments. The usual mechanism is dynamic host control protocol (DHCP). It is worth discussing DHCP in detail because it is useful in troubleshooting network issues.

The switches are configured as DHCP servers. The switch configurations on a site are unique so that each switch has a unique pool of addresses that it can assign to controllers. All IP addresses across the building network are unique. They may duplicate addresses in the customer’s IT network, but that is not a problem. The IE 2000 switches provide a layer 3 boundary between the controllers and the customer network. The switches have routing statements to forward every packet where it needs to go.

Configure all controllers so that the DHCP client software is enabled. When first powered up on the network, a controller sends a broadcast message soliciting a DHCP server. If, after retries, there is still no DHCP server, then the controller assigns itself an unused APIPA address beginning with

169.254. It continues indefinitely looking for a DHCP server, but in the meantime can communicate with other devices on the same network segment using its self-assigned address.

Alternatively, if the controller finds a DHCP server, the client and server exchange a series of messages, at the end of which, the controller is assigned an IP address from the server's pool of addresses, assigned a default gateway, and given other information. However, the assignment is a lease, not a permanent allocation. The switch configuration files generated by the configuration tool have the DHCP lease set to ten minutes. Half way through the lease period, the controller contacts the DHCP server and tries to renew the lease. If necessary, it tries again when the remaining time is only one quarter of the original term. When only one eighth of the original term remains, it broadcasts a request for DHCP. When the original term expires, it gives up its address and assigns itself a 169.254 address.

Because the lease term is short and controllers are not very mobile, the DHCP server is configured to respond to a renewal request by giving the client a new term on the address it already has. If a controller is power-cycled and tries to get a new address, the switch recognizes the MAC address and assigns the controller its previous address. The switch remembers assignments even when it is power-cycled. However abandoned addresses are available for reuse. When the there are no longer any previously unused addresses left in the DHCP pool of addresses, a new device is assigned to the oldest previously used address in the DHCP pool.

Cisco IE 2000 reference

Physical features of Cisco IE 2000 switch

Figure 10: Physical features of the Cisco IE 2000 switch (8-port model)

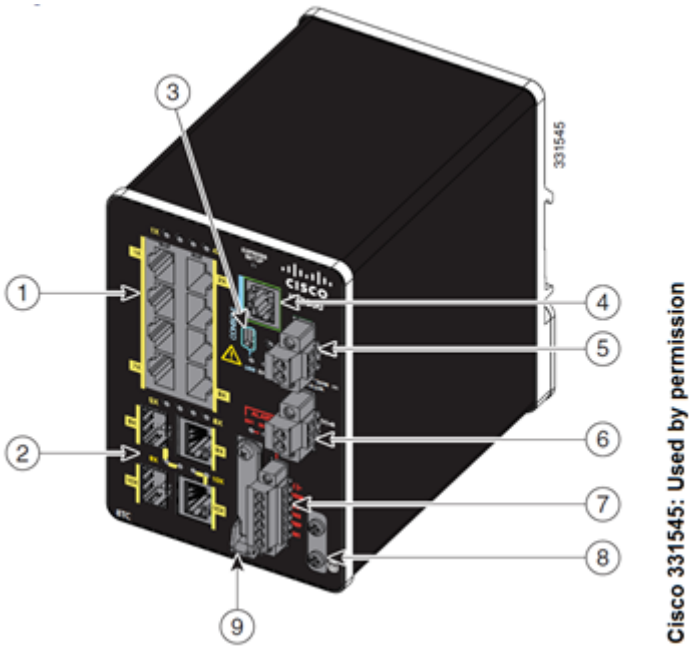


Table 1: Physical features of Cisco IE 2000 switch

Callout	Name	Description
1	10/100 Mbits/sec Ethernet Ports	Provides network access downlink. You can set these ports for speed and duplex autonegotiation. Use Cat5e cable or newer.
2	1000 Mbits/sec Ethernet Ports	Provides an uplink to an aggregation switch. Also provides an uplink to the IT network (segmented network architecture) or a isolated access switch (isolated or connected network architecture). If you do not need to use these ports for uplink, you can also use them for access. Use Cat5e cables or newer. You can convert these ports for optical connections using SFPs.
3	USB Mini-Type B Console Port	Connection for a desktop computer or laptop. To use this port, you must download the vendor specific Windows USB device driver to match the USB-to-Serial converter that you use, and install it on your laptop. Use only the 5-pin USB mini-type B. Other type B connectors are not compatible with the switch. Use a small Phillip screwdriver to loosen the cover.
4	Serial RJ-45 Console Port	Use to connect the switch to a desktop computer or laptop. To use this port, you must download the Cisco Windows USB device driver and install it on your laptop. Requires a USB to RJ45 cable such as the Cisco RJ-45-to-DB-9 female cable connected to a DB-9-male-to-USB cable.
5, 6	Power Connection, Dual DC	Provides primary and secondary DC power. Each power connector has an LED status indicator. If you use a single power supply, you can connect it to either power connection.
7	Alarm Connector	Provides six alarm wire connections. Includes Alarm Inputs and Output relay.
8	Protective Ground Connection	Provides grounding to the switch.
9	SD Card Slot	Use to deploy a switch configuration without opening a console session. You can also transfer the switch configuration from a failed switch to its replacement. Cisco recommends using a ruggedized 1GB Class 6 SD card. Use a small screwdriver to loosen the cover.

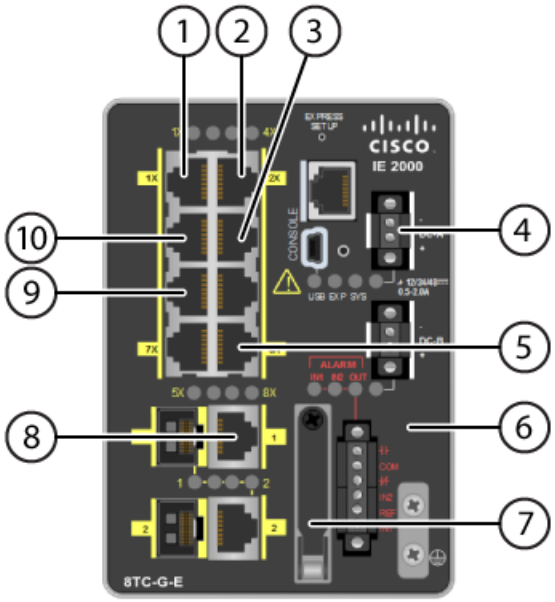
Cisco IE 2000 switch termination diagram

The diagram below is an example of the connections that may be used for a building automation system with one MRP ring and two Daisy Chains both supervised by one network engine.

Note: When using MRP ring configurations in the network, all engines must be at the same Metasys release.

The specific termination for a specific installation depends on the switch configuration. In the normal workflow it is summarized in an installation sheet.

Figure 11: Cisco IE 2000 switch example termination diagram (8-port model)



Label	Example use
1	MRP ring 1, port 1
2	MRP ring 1, port 2
3	Daisy chain port
4	DC power input
5	Maintenance port
6	Standard location for serial number
7	SD card slot
8	Uplink port
9	Network engine port
10	Daisy chain port

The configured ports are set for autonegotiation for speed and duplex.

If a destination port is connected to another active device, then LEDs indicate the port status. For more information, see Table 2.

LEDs of Cisco IE 2000 switch

Figure 12: LEDs indicators of Cisco IE 2000 switch (16-port model)

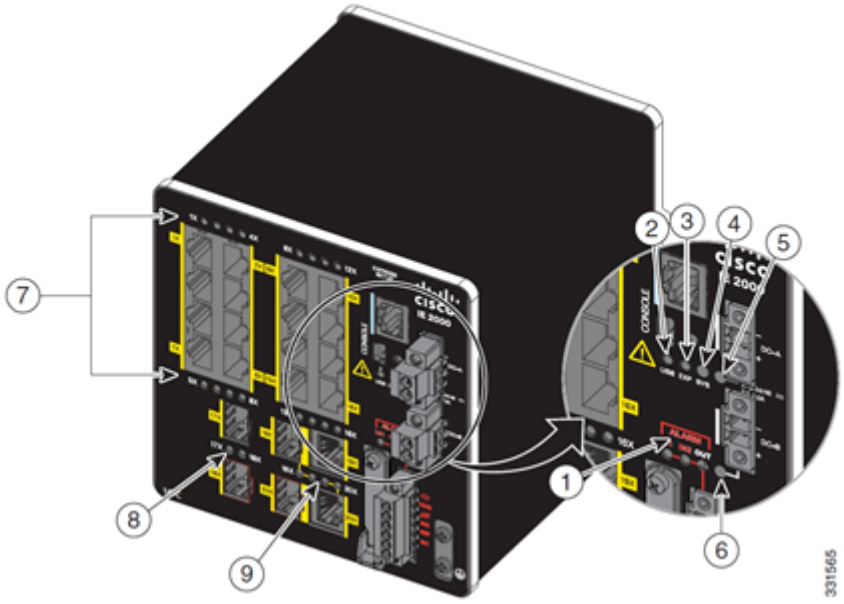


Table 2: Cisco IE 2000 LED indicators

Callout	LED name	Color	Normal	Description/other conditions
1	Alarm	Green or red	Off or green	Off/green: Alarm Out is not configured or the switch is off. Blinking red: major alarm detected. Red: minor alarm detected.
2	USB console port	Green	Green	Green: port is active. Off: port is inactive.
3	Express Setup	Green or red	Off	Displays the express setup mode, which is not described in this guide.
4	System	Green or red	Off or solid green	Off: powered off. Blinking green: booting in progress. Green: operating normally. Red: not functioning properly.
5, 6	Power connector	Green or red	Green	Green: power present, operating normally. Off: Power not present, system is not powered on. Red: Power not present, power supply alarm configured.

Table 2: Cisco IE 2000 LED indicators

Callout	LED name	Color	Normal	Description/other conditions
7	100/100BASE-T traffic	Green or amber	Off, solid green, or blinking green	Off: no link, port not configured. Solid green: link present. Blinking green: data sent or being received. Alternating green and amber: Link Fault. Solid amber: port is disabled and is not forwarding data. This condition can occur because of improperly terminated Ethernet cables. Specific to MRP ring ports: if both ends of a chain of devices are terminated back to the two designated MRP ring ports on a switch, the forwarding port displays blinking green and the blocked port displays solid green. This combination of LED light status signifies the ring is closed or in a healthy state. If both ring ports display blinking green, the MRP ring is open or in a faulty state. ⓘ **Note:** After a port is newly connected or reconfigured, this LED is amber for approximately 30 seconds while STP checks the switch for possible loops.
8	SFP module Ethernet	Green or amber	Off/solid green/ blinking green	Off: no link, port not configured. Solid green: link present. Blinking green: data sent or being received. Alternating green and amber: Link Fault. Solid Amber: port is disabled and is not forwarding data. ⓘ **Note:** After a port is newly connected or reconfigured, this LED is amber for approximately 30 seconds while STP checks the switch for possible loops.
9	Gigabit Ethernet traffic	Green or amber	Off, solid green, or blinking green	Off: no link, port not configured. Solid green: link present. Blinking green: data sent or being received. Alternating green and amber: Link Fault. Solid amber: port is disabled and is not forwarding data. ⓘ **Note:** After a port is newly connected or reconfigured, this LED is amber for approximately 30 seconds while STP checks the switch for possible loops.

Cisco IE 4010 reference

Physical features of Cisco IE-4010-4S24P switch

Figure 13: Physical features of Cisco IE-4010-4S24P switch

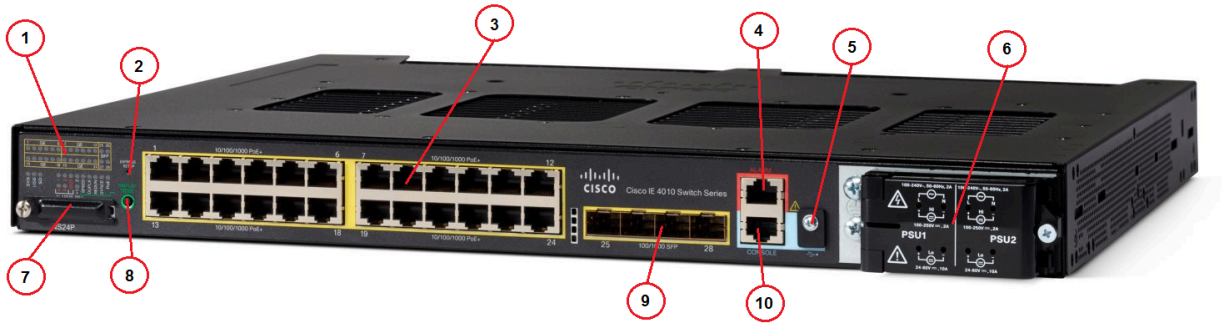


Table 3: Physical features of Cisco IE-4010-4S24P switch

Callout	Name	Description
1	LEDs	Monitors switch activity and performance.
2	Express Setup button	Use to start the express setup process, which is not described in this guide.
3	10/100/1000 Mbits/sec Power over Ethernet (PoE+) Ethernet Ports	Dual-purpose ports, for use as uplink or network access ports, with PoE/PoE+ support for devices. Use Cat5e cable or newer.
4	Alarm port	Four alarm inputs and one alarm output for integrating hardware alarms.
5	USB Mini-Type B console port	Use to connect the switch to a terminal server. To use this port, download the Cisco Windows USB device driver on to the switch and the server. Use only the 5-pin USB mini-type B. Other type B connectors are not compatible with the switch. Use a small Phillip screwdriver to loosen the cover.
6	Power input terminal	Screw terminals for the AC and DC power connections. The switch supports up to two power supplies.
7	SD Card Slot	Allows you to replace a failed switch without reconfiguring the switch. Cisco recommends using a ruggedized 1GB Class 6 SD card. Use a small Phillip screwdriver to loosen the cover.
8	Display Mode button	Use to choose the mode the port LEDs display.
9	100/1000 Mbits/sec SFP ports	Connections for other devices and downlink interfaces. SFP modules have local connectors for fiber-optic connections or RJ-45 connectors.
10	RJ-45 serial console port	Use to connect the switch to a terminal server. To use this port, download the vendor specific Windows USB device driver to match the USB-to-Serial converter that you use, and install it on your laptop. Requires a USB to RJ45 cable such as the Cisco RJ-45-to-DB-9 female cable connected to a DB-9 male-to-USB cable.

Cisco IE 4010 switch termination diagrams

If you use the Metasys IP Network wizard, which is a switch configuration tool, an Installation Sheet is generated at the time the switch configuration is generated.

LEDs of Cisco IE-4010-4S24P switch

Figure 14: LEDs indicators of Cisco IE-4010-4S24P switch

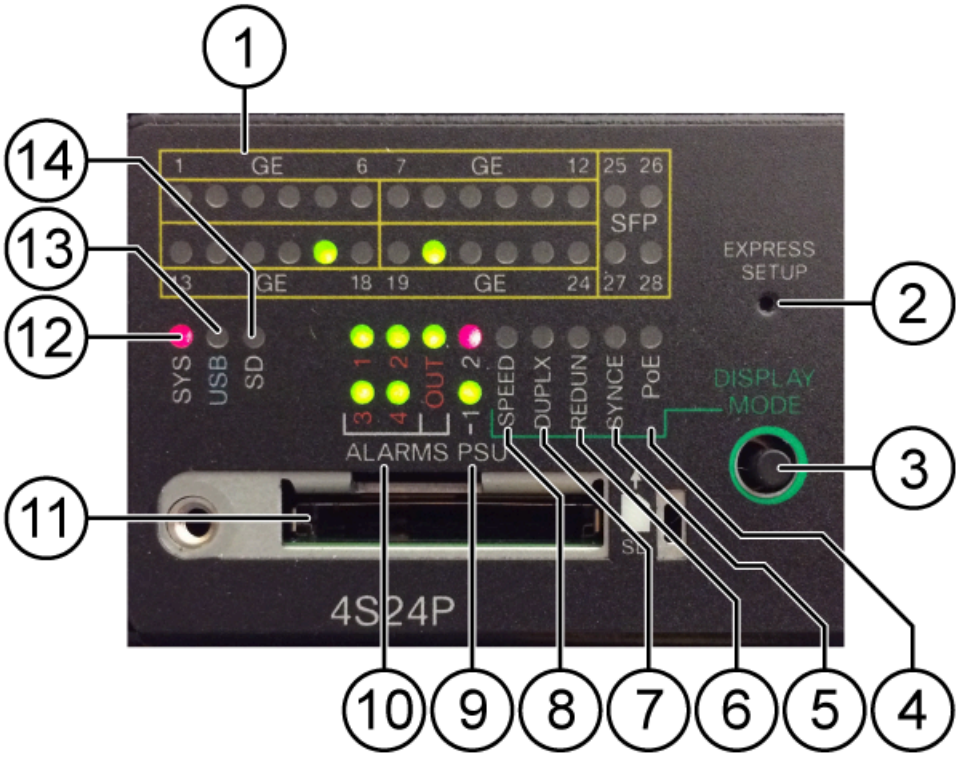


Table 4: Cisco IE-4010-4S24P LED indicators

Label	LED name	Color	Normal	Description/other conditions
1	Port status (1 through 28)	Green or amber	Off or green	Off: no link or port is shut down. Green: link is present, no activity. Blinking green: activity, port is sending or receiving data. Alternating green and amber: link fault. Amber: port is blocked and is not forwarding data. ⓘ **Note:** For further information, see Table 5.
2	Express Setup button	Not applicable	Not applicable	Use to start the express setup process, which is not described in this guide.
3	Display Mode switch	Not applicable	Not applicable	Press to cycle through display modes until LEDs labeled 4 through 8 are off.
4-8	Display mode indicators	Green, amber, or red	Green, amber, or red	Indicate the current display mode. See Table 5 for details.

Table 4: Cisco IE-4010-4S24P LED indicators

Label	LED name	Color	Normal	Description/other conditions
9	Power status	Green or red	Off or green	Off: power supply not installed. Green: valid input present and output operating within range. Red: valid input present, output is outside operating range or not present. Blinking red: power supply installed but valid input not present.
10	Alarm status 1–4 (input alarms) Output alarm	Green or red	Green	**For 1-4** Green: alarm not present. Red: minor alarm present. Blinking red: major alarm present. **Output Alarm** Green: alarm not present. Red alarm condition present.
11	SD Card slot and cover	Not applicable	Not applicable	Not applicable
12	System	Green or red	Off or blinking green	Off: powered off. Blinking green: booting in progress. Green: operating normally. Red: not functioning properly.
13	USB console port	Green	Off or green	Green: port is active. Off: port is inactive.
14	SD card activity	Green or amber	Green	Fast blinking amber: unsupported SD card is detected. Slow blinking amber: SD card is not present. Green: SD card is functioning. Blinking green: SD card transfer in progress.

Table 5: Display mode LEDs

Display mode LED	Display mode	Port status LED color and description
All off	Port status	This mode is default. Off: no link or port is shut down. Green: link present, no activity. Blinking green: activity, port is sending or receiving data. Alternating green and amber: link fault. Amber: port is blocked and not forwarding data. If a port is configured for spanning tree, the port LED can be amber for up to 30 seconds while the network is tested for possible loops.
SPEED	Port speed	**10/100/1000/SFP ports** Off: port is not operating. Amber: port is operating at 10 Mb/s. Green: port is operating at 100 Mb/s. Flashing green: port is operating at 1000 Mb/s. **Uplink ports** Green: port is operating at 1000 Mb/s.
DUPLX	Port duplex mode	Off: port is not operating. Amber: port is operating in half duplex. Green: port is operating in full duplex.

Table 5: Display mode LEDs

Display mode LED	Display mode	Port status LED color and description
REDUN	Redundancy status	Green: one or more redundancy protocols are configured and active. Blinking amber: one or more redundancy protocols are indicating a redundancy fault. Flash blinking green: displays that ports are in a redundancy protocol and the redundancy fault status.
SYNC	Synchronous Ethernet status	Not supported
PoE	PoE port power	Off: PoE is off. Green: PoE is on and all ports are functioning correctly. Alternating green and amber: PoE is on but one of the low priority ports power is disconnected or failed. Blinking amber: PoE is on but one of the high priority ports power is disconnected or failed. Amber: PoE is on with failures.

Cisco IOS reference

You **do not** need to use Cisco IOS® commands to configure typical installations. You can use the IP Network Wizard instead. The following sections are included to support advanced configuration and troubleshooting. For detailed descriptions of Cisco IOS commands, refer to the *Cisco IOS Configuration Fundamentals Command Reference*, available at https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html

To access the command line interface of the switch, use a remote terminal session, such as SSH, from a laptop connected to the terminal point. Alternatively, the two console ports on the switch also give access to the command line, through a serial interface. The two console ports have different form factors: one is RJ-45 and other is USB (5-pin mini-Type B connector).

The command prompt indicates the command mode. Most commands are available from only one mode. There are many command modes, including the following.

Table 6: IOS command line prompt modes

Prompt	Mode
>	This is the least privileged mode, and has the smallest command set.
#	This is the privileged mode, from which one can change the switch configuration.

The flavors of privileged mode include the following.

Table 7: IOS Command Line prompt modes in privileged mode

Prompt	Tasks completed in this mode
`(config)#`	Editing a switch configuration.
`(dhcp-config)#`	Editing the DHCP configuration of switch.
`(config-if)#`	Editing the configuration of a switch interface.

The switch ports are physical interfaces. Other interfaces, like switch virtual interfaces (SVIs), are logical interfaces. You configure logical interfaces at the same time that you create them.

When typing commands, it is helpful to know the following:

- Use the up arrow to retrieve previous commands.

- Use the tab key for command completion. There are abbreviated versions of most commands.
- Use a `?` to get help on options that could be typed at this point. For example, to view help on the show command, enter `show ?`.
- Use the tab key to auto-complete. For example, typing `sh`+TAB+SPACE+`run`+TAB fills the command line with `show running-config`.

IOS commands for gathering information

To run the commands that are of most use in configuration and troubleshooting, you must be in the privileged mode. For practical purposes, the switch owner is the person who has physical access to the switch and knows the passwords leading to the privileged mode.

There are two passwords. The first password is for logon; the second is for elevation of privileges, including editing the switch configuration. To edit the configuration using the command-line interface, log on to the switch, enter `enable`, then enter the password for elevation of privilege.

You can set most terminal servers to create a log file of your sessions. It is advisable to make a log of all your sessions. If you need to gather information, the easiest way is to start a log file, then use commands to display the needed information. The following commands are useful for gathering switch information.

Table 8: CISCO IOS Command Line Interface Commands

CLI command	Information displayed
`show version`	Hardware version, software version, MAC addresses, and so on. The switch serial number is indicated as `System serial number`, and is also marked on the front face and right side of the switch.
`show license`	LAN level, MRP
`show running-config`	The current, active configuration
`show mrp ring 1`	Ring status and ports for ring 1
`show mrp ports`	Shows the port status for all MRP ring ports
`show interface FastEthernet 1/1`	Information about port 1
`show interface status`	The port status. This is the same information that you can infer from the port status LEDs on the switch.
`show platform sdflash`	SD card information, including the total amount of memory on the card
`show file system`	Available file system details, including total size and the amount of free space
`show sdm prefer`	The active Switching Database Management (SDM) template
`show cdp neighbors`	Other Cisco devices that are neighbors on the network
`show ip interface brief`	Lists the interfaces configured on the switch
`show ip dhcp binding`	A table of IP addresses and lease status organized by MAC address
`show ip dhcp snooping binding`	Similar to the previous command, but with additional details. To use this command, DHCP snooping must be enabled. The lease status is one of the following: • Active: lease is current and term has not expired • Terminated: the term expired without being renewed • Terminated + Remembered: the term expired, but the address is still available if the device tries to renew; it returns to the pool if the pool becomes exhausted
`show mac address-table`	The switch's table of which MAC addresses are associated with each switch port.
`show vlan`	VLAN number, name, status, and port assignments.

Modifying the configuration

Changing the switch configuration is not difficult, but can negatively impact the operation of the switch if done incorrectly. Use caution and make a backup of the existing configuration to minimize the risk. Changes take effect immediately, but are not automatically saved to nonvolatile memory, which is required for changes to persist through a restart. This document does not provide complete instructions. For more details about network architecture, refer to the *Metasys IP Networks for BACnet/IP Controllers Technical Bulletin (LIT-12012458)* and standard Cisco switch configuration documentation.

For small changes, use physical access to the switch. Eject the SD card, put it in your laptop, create a backup copy of the file, and edit the original file directly. You need to restart the switch after you re-insert the updated SD card in order for the changes to the configuration file to take effect. This approach is suitable for tasks including changing the hostname. With care, you can edit the configuration file to complete more complicated tasks, including changing the BACnet UDP port number. However, it may be easier to run the configuration tool again.

Remember that the default security setting is to report all changes to switch configuration and all removal and insertion of SD cards.

There are two passwords. The first password is for logon; the second is for elevation of privileges, including editing the switch configuration. Use the console port on the switch to connect to the command line. To change the configuration, complete the following steps:

1. Log on to the switch.
2. Enter `enable`
3. Enter the password for elevation of privilege.
4. Enter `config terminal`, to set the console to take configuration commands from terminal.

From this point on, you are manually configuring the switch and need to exercise caution.

Table 9: CISCO IOS command line commands for configuring a switch

CLI command	Explanation
`config terminal`	Enter configuration mode
`hostname mySwitch`	Change the name of the switch to `mySwitch`
`no power-supply dual`	Disable the status indicator for the second power supply on an IE 2000 when operating with a single power supply.
`end`	Leave current mode and return to previous mode
`exit`	Leave current mode and return to command prompt

Mirroring a port for packet capture

Use the following commands to set up a monitor session, so that you can capture packets crossing a physical switch interface. The idea is to reconfigure the switch so that a copy of activity on a live port is sent to the maintenance port. The configuration commands are the following:

- `monitor session 1 source interface Fa1/1`
- `monitor session 1 destination interface Fa1/8 encapsulation replicate`

If you enter these two lines, you set up a monitoring session, session 1. The first line specifies that the source is FastEthernet1/1, which is the port labeled 1X on the switch. The second line specifies that the destination port FastEthernet1/8, which is the port labeled 8X on the port. By convention, the last port is the maintenance port. Because port 1 is a ring port, all of the management frames are replicated, making the capture file very large. On the other hand, most packet capture programs have a way to filter out packets during the capture.monitor session 1 destination interface Fa1/8 encapsulation replicate

ⓘ **Note:** If you wish to ignore the MRP test frame messages, you can exclude `encapsulation replicate` from the CLI command line on the monitor session of an MRP port. Doing so significantly reduces the resultant capture file.

To leave the session, return to the configuration mode, enter `no monitor session 1` and save the configuration file if necessary. If you do not save the configuration after creating the session, you can use the `reload` command to restart the switch and kill the session.

In many cases, it is more useful to monitor the forwarding port, indicated by a blinking LED, than the blocked port, indicated by a solid LED. To force the ports to change roles, disconnect and reconnect the wires. For example, disconnect both cables, then reconnect the cable to the port that is mirrored, then reconnect the cable to the port that is not mirrored. It is also possible to change the switch configuration so that the mirror port mirrors both ring ports. This gives a more complete picture of what is happening, but also means that there are more packets to try to understand.

To check your work after exiting configuration mode, enter the following IOS command: `show monitor session all`.

Additional IOS commands

Table 10: CISCO IOS command line commands available in unprivileged mode

Command	Explanation
`enable`	Enter privileged mode
`ping 192.168.3.1`	Check for communication between the switch and IP address `192.168.3.1`

The following useful commands are available in privileged modes. If you ssh into the switch from the maintenance port, you are automatically placed in the first privileged mode.

Table 11: CISCO IOS Command Line Commands Available in Privileged Mode

Command	Explanation
`cd`	Change working directory
`pwd`	Show working directory
`copy config.text config_Jan01.text`	Make a copy of a `config.text` file
`delete config_Jan01.text`	Delete the file that has the name `config_Jan01.text`. To confirm the deletion, press the Enter key.
`dir sdflash:`	List the files on the SD card
`copy running-config flash:config.text`	Copy configuration from memory to switch flash. It takes effect after you restart the switch. ⓘ **Note:** If you use an SD card, copy the running config to the SD card so that the SD card has the current configuration running on the switch. To copy the running config to the SD card, enter `copy running-config sdflash:config.text`. You can use the copy to restore the running configuration if the switch is restarted, or if the current switch fails and the SD card is moved to the replacement switch. If the `config.text` file is present on the SD card, the switch boots using this file.
`reload`	Restart the switch, loading the configuration from the last saved version
`show clock`	Check the time setting
`clock set hh:mm:ss dd mm yyyy`	Change the time setting
`copy sdflash:config.text config.text`	Copy the SD card to switch flash
`sync sdflash: flash:`	Copies all of flash card to switch memory
`locate-switch`	Command the EXP indicator LED to blink green. This is useful when you log on to a switch over the network, and need to identify the physical switch.

Troubleshooting and repair

Cisco IE switch repair information

If a switch needs to be removed, label each Ethernet cable with the port to which it is connected before you disconnect it.

If a switch needs to be replaced, remember to remove the SD card. The SD cards contains all of the information needed to set up and configure a replacement switch.

If you need to replace a switch that is experiencing problems, note the switch serial number. You require this serial number to obtain support from Cisco's SmartNet support program.

Troubleshooting

Use a copy of the Installation Sheet to assist you in troubleshooting. For more information, see Configuration files. If the contents do not seem obvious, sketch out a network diagram like the one drawn for the Example network section. You can mark physical connections, VLAN/subnet boundaries, static IP addresses, points where security features are applied, the paths over which you can ping devices, and so on.

Use the following actions to troubleshoot the Cisco IE 2000 switch:

- For general failures, check the LED indicators.
- If the switch indicates that it is not configured, check the SD card slot for the SD card. Verify the SD card contains a configuration file named `config.text` (case sensitive), and an operating system. The operating system is a large `.bin` file. For further information, see Table 4, Table 5, and Table 12.
- Inspect the cables and connectors for damage or loose connections.
- If the switch is a remote device, verify the device is powered on and operating correctly.
- If the switch does not boot on, the switch may need to be replaced.

To reset a switch to the factory default setting, refer to https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie2000/hardware/installation/guide/ie2000_hig.pdf.

Table 12: Troubleshooting problems and solutions

Problem	Solution
The LEDs on the port for the controller chain is unlit.	Look at the installation sheet and verify that the switch port is configured for a chain. Make sure that the one end of the chain is plugged into the switch. Make sure that at least the first of the controllers is powered and connected. Attempt a discovery or ping to force traffic on the network. Make sure that the controllers' ETH1 and ETH2 LEDs are blinking green, which indicates active communication.
The LEDs on the switch indicate that the ring is open. **Closed:** one ring port blinking green, one port solid green. **Open:** both ring ports blinking green.	Make sure that the two ends of the ring are plugged into two ring ports of the same ring. Verify port numbers on the installation sheet. For best practice use different color coded Ethernet cables for the different rings. Make sure that the cables are connected all the way around the ring. Make sure that all the controllers are powered. Make sure that the controllers' ETH1 and ETH2 LEDs are blinking green. Blinking green indicates active communication. If a controller is connected on a port, the LED always shows an indication of traffic. Even if the controller is not sending anything, traffic is generated by the ring manager, which sends test messages into the ring ports. The MRP manager may not be configured on the switch. On the switch's command line interface, enter: `show license`. The expected status of the manager is `License State: Active, In Use`. The expected status of the client is `License State: Active, Not in Use, EULA not accepted`. If the manager is present but not accepted, enter the command: `license right-to-use activate mrp-manager acceptEULA`. However, the ordering system is set up to order the license with the switch.
The network engine cannot discover any controllers.	Verify that the BACnet port used in the switch Access Control Lists (ACLs) matches that specified in the wizard, is configured in the network engine, and is configured in the IP controllers. For example, all ports can be 47808, which is the standard port, or all can be a non-standard port, for example 47818, but all port settings must use the same value. ⓘ **Note:** The switch ACLs always allow 47808 because it is used when commissioning a new IP controller. However, the switch ACLs may additionally allow a non-standard BACnet port value. Verify that the network engines IP address and network mask match the values that were specified in wizard input and installation sheet. For example, if the network mask is `255.255.255.248`, then an input `255.255.248.0`, or a similar number, is incorrect. Ping the network engines to verify that the address matches the Installation Sheet. If the network engine is on a network segment containing many other third party BACnet/IP devices, the network engine may not be able to process the high number of broadcast replies. To determine the number of broadcast replies, use the Wireshark application to capture traffic on the network engine port.
I see IP controllers with IP addresses which do not match the subnets listed in the Installation Sheet.	You may be able to discover the controllers at a `169.254` address, but not ping them at the expected address, for example a `172.x.x.x` address. This means that the controllers' generated a self-assigned addresses, instead of obtaining them through DHCP. If the switch is running, wait five minutes. The controllers may renew their lease and obtain accurate IP addresses. To force another round of DHCP requests, cycle power to the controllers. If the controllers are configured to use static addresses, configure the controllers to use DHCP.
My laptop cannot see anything.	Verify that your laptop is connected to the maintenance port specified in the installation sheet. Verify that the laptop is configured for DHCP. Verify your laptop is assigned the laptop address specified for the switch in the Installation Sheet, and not a self-assigned address, for example one starting with 169.254. Verify that the LED on the switch port blinks green when you do something. If you connect a different laptop to the switch maintenance port shortly after disconnecting the previous one, wait 10 minutes for the previous DHCP lease to expire.
I cannot access the switch.	Check the installation sheet and verify that you specified the IP address of the switch's management interface in your ssh session. Use the switch console log on. the switch console uses a serial connection instead of an Ethernet connection.

Table 12: Troubleshooting problems and solutions

Problem	Solution
The network engine cannot discover all of the controllers.	To verify that all of the controllers have received DHCP addresses, in the switch's command line interface, enter the following commands: `show ip dhcp snooping bind`, which shows the number of IP address leased.
I cannot move off the switch to reach other devices on the network.	You are not expected not have access to the full network, but you are expected to be able to access some other parts. To see neighboring switches, in the switch's command line interface, enter the following command : `show cdp neighbor`. Draw a map showing how the switches are interconnected. Add information about the Metasys devices. Additionally, refer to the installation sheet saved to the SD cards. If IND is installed and configured to manage the BAS network, you can also refer to the Network Topology view in IND.
The switch is powered but does not perform any switching.	The switch may have an old version of the operating system, which is missing an important feature. From the switch's command line interface, enter the following command: `show version`. The required version for an IE 2000 is `15.2(6)E1` or newer. The required version for an IE 41010 is `15.2(4)EC2` or newer. It is possible that a newer release may contain a bug. If you suspect that the operating system is the cause of the problem, ask the Field Support Center for the latest IOS version that has been tested with Metasys. Look at the log files on the switch. From the switch's command line interface, enter the following command: `show log`. Retention of the log data depends on the size of the buffer that is allocated. If it is too small, set up a syslog server on a computer with a large amount of free of disk space. You can use the wizard to redirect logging to a syslog server. The switch my not have loaded the `config.text` file from the SD card. Connect a laptop to the local maintenance port of the switch specified in the IP Network Wizard Installation Sheet. Configure the laptop to obtain its IP address via Dynamic Host Configuration Protocol (DHCP). Verify that the laptop is assigned the laptop IP address corresponding to the switch as specified in the Installation Sheet, indicating that the switch has the correct `config.text` file loaded. Learn how to use the switch's debug facility. The command is `debug [debug options]`, and to get a list of the options, enter `debug ?`.
Something is wrong on the aggregation switch.	We use the Rapid Spanning Tree Protocol (RSTP) to create a redundant path between the access switches and the aggregation switch. From the switch's command line interface, enter this command: `show spanning-tree` to see everything, or `show spanning-tree vlan number` to limit the scope to a particular VLAN, for example the BAS VLAN listed in the Installation Sheet. The expected response from the command is `This bridge is the root`, with a priority value of 8000 or lower.
The switch has intermittent problems.	It may be helpful to install network monitoring software, for example Cisco's Industrial Network Director (IND). IND has capabilities that include mapping the physical connections between switches, reporting network statistics, and logging switch errors. IND runs on a network server and collects switch information using protocols including SNMP.

Product warranty

This product is covered by a limited warranty, details of which can be found at www.johnsoncontrols.com/buildingswarranty.

Software terms

Use of the software that is in (or constitutes) this product, or access to the cloud, or hosted services applicable to this product, if any, is subject to applicable end-user license, open-source software information, and other terms set forth at www.johnsoncontrols.com/techterms. Your use of this product constitutes an agreement to such terms.

Single point of contact

APAC	EU	UK	NA/SA
JOHNSON CONTROLS C/O CONTROLS PRODUCT MANAGEMENT NO. 32 CHANGJIANG RD NEW DISTRICT WUXI JIANGSU PROVINCE 214028 CHINA	JOHNSON CONTROLS VOLTAWEG 20 6101 XK ECHT THE NETHERLANDS	JOHNSON CONTROLS TYCO PARK GRIMSHAW LANE MANCHESTER M40 2WL UNITED KINGDOM	JOHNSON CONTROLS 5757 N GREEN BAY AVE. GLENDALE, WI 53209 USA

Contact information

Contact your local branch office: www.johnsoncontrols.com/locations

Contact Johnson Controls: www.johnsoncontrols.com/contact-us