PROFINET Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches

Cisco Catalyst IE9300 Rugged Series
Updated September 28, 2026

Topics included

1 Configure PROFINET....4
PROFINET protocol....5
Restrictions to configure PROFINET....5
Supported switch models....5
PROFINET device roles....6
PROFINET device data exchange....7
PROFINET configuration....8
PROFINET Netload-3 Robustness....8
Restrictions to configure PROFINET Netload-3 Robustness on IE9300....10
VLAN 0 priority tagging....10
Prepare and assign a switch for PROFINET network integration....11
Configure a switch for PROFINET integration using STEP7 or TIA....12
Enable PROFINET....14
Profinet connection configuration....15
Prevent default gateway and CDP loss during reloads and upgrades....16
Gateway IP address configuration scenarios....17
PROFINET monitoring and maintenance....18
PROFINET troubleshooting....19
Technical assistance....19
Feature history for PROFINET configuration....20

2 PROFINET System Redundancy....22
PROFINET system redundancy....23
Restrictions for PROFINET system redundancy....23
How PROFINET system redundancy modes work....23
Feature history for PROFINET System Redundancy....24

3 Read-only PROFINET....26
Read-only PROFINET....27
Configure read-only PROFINET....27
Feature history for Read-only PROFINET....28

1 Configure PROFINET

Topics:

- PROFINET protocol
- Restrictions to configure PROFINET
- Supported switch models
- PROFINET device roles
- PROFINET device data exchange
- PROFINET configuration
- PROFINET Netload-3 Robustness
- VLAN 0 priority tagging
- Prepare and assign a switch for PROFINET network integration
- Configure a switch for PROFINET integration using STEP7 or TIA
- Enable PROFINET
- Profinet connection configuration
- Prevent default gateway and CDP loss during reloads and upgrades
- Gateway IP address configuration scenarios
- PROFINET monitoring and maintenance
- PROFINET troubleshooting
- Technical assistance
- Feature history for PROFINET configuration

PROFINET protocol

Explains how the PROFINET protocol serves as an open industrial Ethernet standard for automation control, supporting scalable communication and modular frameworks for distributed automation applications.

PROFINET is the PROFIBUS international open industrial Ethernet standard that

- uses TCP/IP and IT standards for automation control
- enables scalable communication for industrial automation systems and process control networks, and
- emphasizes data exchange and defines communication paths to meet speed requirements.

PROFINET communication levels

PROFINET communication is scalable on three levels:

- Normal non-real-time communication that uses TCP/IP and enables bus cycle times of approximately 100 ms.
- Real-time communication which enables cycle times of approximately 10 ms.
- Isochronous real-time communication which enables cycle times of approximately 1 ms.

PROFINET I/O is a modular communication framework for distributed automation applications. It uses cyclic data transfer to exchange data, alarms, and diagnostic information with programmable controllers, input/output (I/O) devices, and other automation controllers such as motion controllers.

PROFINET I/O recognizes three classes of devices.

1. I/O devices
2. I/O controllers
3. I/O supervisors

Restrictions to configure PROFINET

Consider these restrictions when configuring the isco IOS XE IE9300 Rugged Series Switches.

- PROFINET feature set is available with Network-Essentials license.
- Cisco Catalyst IE9300 Rugged Series Switches support only PROFINET I/O, RT (Real-Time) but not IRT (isochronous real-time) communication.
- PROFINET can be enabled only on standalone IE-9300 series switches. PROFINET is not supported when Cisco IOS XE IE 9300 Rugged Series Switch are stacked.
- MRP-Client mode is supported from IOS XE Release 26.1.1.

Supported switch models

Lists the restrictions and guidelines for configuring PROFINET on Cisco Catalyst IE9300 Rugged Series Switches.

Cisco IOS XE IE9300 Rugged Series Switches are supported for PROFINET configuration with specific requirements and limitations that must be understood before implementation.

Supported switch models

Table 1: Cisco IOS XE IE9300 Rugged Series Switch support matrix

Switch model	Supported release
IE-9310-26S2C	17.8.1
IE-9320-26S2C	17.8.1
IE-9320-22S2C4X	17.11.1
Rest of the PIDs	17.12.1 and later

PROFINET device roles

Explains the different device roles in a PROFINET I/O system, including controllers, supervisors, and devices, and describes how they interact to manage automation and data exchange.

A PROFINET device role is a system component category that

- defines the function of each device in the PROFINET I/O system
- determines how devices exchange configuration, diagnostic, and I/O data, and
- enables communication and automation through Ethernet networking.

PROFINET device role reference information

The I/O controller detects the switch with the Discovery and Configuration Protocol (DCP), and sets the device name and IP address, so you do not need to enter Cisco IOS commands for the basic configuration. For advanced configurations (for example, QoS, DHCP, and similar features), you must use Cisco IOS commands on the switch because these features cannot be configured by using PROFINET.

- PROFINET I/O devices communicate over an Ethernet communication network to meet the automation industry requirement for bus cycle times of less than 100 ms.
- The network uses switches and full-duplex data exchange to avoid data collisions.

Note

If PROFINET DCP cannot detect the switch/PLC/IO MAC addresses, temporarily disable the firewall or virus scan from the Windows PC that installed the Siemens STEP7 or TIA Portal.

PROFINET device role examples

An I/O controller is a programmable logic controller (PLC) that controls I/O devices and exchanges data such as configuration, alarms, and I/O data through an automation program. The I/O controller and the I/O supervisor exchange diagnostic information. The I/O controller shares configuration and input/output information with the I/O device and receives alarms from the I/O device.

An I/O supervisor is an engineering station, such as a human machine interface (HMI) or PC, used for commissioning, monitoring, and diagnostic analysis. The I/O supervisor exchanges diagnostic, status, control, and parameter information with the I/O device.

An I/O device is a distributed input or output device such as a sensor, an actuator, or a motion controller.

PROFINET device data exchange

This topic explains how PROFINET devices exchange data after device discovery, including the use of GSD files and configuration attributes for switches and ports.

After PROFINET uses DCP to discover devices, including the switch, they establish application relationships (ARs) and communication relationships (CRs). After a connection is established and information about device parameters is exchanged, input and output data is exchanged.

The switch uses non-real-time CRs to exchange the data attributes listed in the tables.

Table 2: PROFINET I/O switch attributes

PROFINET I/O switch configuration attributes	Value or action
Device name	Configures a name for the device
TCP/IP	IP address, subnet mask, default gateway, SVI
Primary temperature alarm	Enables or disables monitoring for specified alarm
Secondary temperature alarm	Enables or disables monitoring for specified alarm
RPS failed alarm	Enables or disables monitoring for specified alarm
Relay major alarm	Enables or disables monitoring for specified alarm
Reset to factory defaults	Uses the PROFINET I/O controller to reset the switch to factory defaults. This action removes the startup configuration and reloads the switch.
Relay major configuration	Specifies the type of port alarm (for example, link fault) that triggers the major relay. Any port configured with the specified alarm type can trigger the major relay.

Table 3: PROFINET I/O port attributes

PROFINET I/O port configuration attributes	Value or action
Speed	10/100/1000/auto
Duplex	Half/full/auto
Port mode	Access/trunk
Link status	Shut down/no shut down
Configure rate limiting	Broadcast, unicast, multicast threshold exceeds configured levels
Port link fault alarm	Enables or disables monitoring for specified alarm
Port not forwarding alarm	Enables or disables monitoring for specified alarm
Port not operating alarm	Enables or disables monitoring for specified alarm

PROFINET I/O port configuration attributes	Value or action
Port FCS threshold alarm	Enables or disables monitoring for specified alarm
VLAN	VLAN Information

PROFINET devices are integrated by using a general station description (GSD) file that contains the data for engineering and data exchange between the I/O controller, the I/O supervisor, and the I/O devices, including the switch. Each PROFINET I/O field device must have an associated GSD file that describes the properties of the device and contains all this information required for configuration:

- Device identification information (device ID, vendor ID and name, product family, number of ports)
- Number and types of pluggable modules
- Error text for diagnostic information
- Communication parameters for I/O devices, including the minimum cycle time, the reduction ratio, and the watch dog time
- Configuration data for the I/O device modules, including speed, duplex, VLAN, port security information, alarms, and broadcast-rate-limiting thresholds
- Parameters configured for I/O device modules for the attributes listed in the **Profinet I/O Port Attributes** table.

The GSD file is on the switch, but the I/O supervisor uses this file.

Note

You must use the GSD file that is associated with the Cisco IOS release on the switch to manage your PROFINET network. Both the I/O supervisor and the Cisco IOS software alert you to a mismatch between the GSD file and the switch Cisco IOS software version.

PROFINET configuration

Provides configuration methods for PROFINET using either PROFINET software on the I/O supervisor or Cisco IOS software for basic switch configuration.

You can use either the PROFINET software on the I/O supervisor or the Cisco IOS software for basic switch configuration.

After you enable PROFINET, LLDP is automatically enabled on the switch because PROFINET relies on LLDP to fully function. If you disable PROFINET, you can enable or disable LLDP as needed.

PROFINET is enabled by default on all switches. The default configuration operates on VLAN 1, but you can assign it to another VLAN ID if required. By default, VLAN 1 is in a shutdown state when the switch is first powered on. To activate PROFINET on an out-of-the-box switch, you must unshut VLAN 1.

PROFINET Netload-3 Robustness

Learn how automatic traffic policing and source blocking protect PROFINET communication during abnormal network-load conditions.

PROFINET Netload-3 Robustness is an automatic, built-in traffic-protection feature. When PROFINET is enabled, the system automatically applies the protection mechanisms required to help maintain PROFINET communication during abnormal network-load conditions.

You do not configure or enable this feature separately. The system determines the applicable protection policy and automatically applies it to eligible interfaces associated with the PROFINET VLAN.

Netload-3 is different from PROFINET Conformance Class B. Netload-3 describes resistance to network load. Conformance Class B describes the PROFINET functions supported by a device.

The feature operates automatically when the PROFINET subsystem is enabled. No additional netload-specific commands or configurable thresholds are provided.

The switch performs the following functions:

- Examines incoming PROFINET packets to determine the Frame ID and traffic classification.
- Allows valid traffic associated with the expected Application Relationship (AR) to continue without invoking netload protection.
- Detects unexpected PROFINET Real-Time (RT) frames received from a source other than the expected I/O controller.
- Invokes dynamic MAC access control list processing to block the offending Layer 2 source.
- Applies a system-defined policing policy to incoming IP traffic directed to the PROFINET VLAN IP address.
- Applies the policing policy to eligible physical interfaces when the platform does not support policing directly on a switched virtual interface.

This feature is supported on the these switches from IOS XE 26.2.1:

- Cisco Catalyst IE9300 Rugged Series Switches

Packet-handling behavior

The switch performs the actions given in the table automatically.

Table 4: Packet-handling behavior

Traffic condition	Switch action
Valid traffic associated with the expected AR.	Forwards the traffic without invoking netload blocking.
Unexpected PROFINET RT traffic from a source other than the expected I/O controller	Identifies the ingress interface, invokes dynamic MAC ACL processing for the source, and generates diagnostic information.
Incoming IP traffic directed to the PROFINET VLAN IP address	Applies a fixed, system-defined policing policy.
SVI policing is not supported by the platform	Applies the policing policy to eligible physical interfaces that carry the PROFINET VLAN.

Eligible physical interfaces

When protection must be applied at the physical-interface level, the system identifies eligible interfaces automatically. No netload-specific user configuration is required. An eligible interface must meet all the following conditions:

- The interface is associated with the PROFINET VLAN.
- The interface is operationally up.

- The interface is an access port in the PROFINET VLAN or a trunk port that allows the PROFINET VLAN.

A MAC ACL or Layer 3 ACL is applied to the interface when the specified conditions are met.

Restrictions to configure PROFINET Netload-3 Robustness on IE9300

The following restrictions apply to IE9300 switches:

- This feature is available only when the IE9300 switch operates as a standalone switch.
- This feature is not supported when the IE9300 switch is part of a switch stack.
- This feature requires the Network Essentials license.
- IE9300 switches support PROFINET RT communication but do not support IRT communication.
- This does not change the existing IE9300 PROFINET PID and minimum-release requirements.

VLAN 0 priority tagging

Configure PROFINET settings to enable seamless communication in industrial automation networks. This task explains how to activate PROFINET on a switch by enabling the default VLAN 1 configuration.

You can prioritize traffic without assigning it to a specific VLAN.

Starting with Cisco IOS XE Release 17.18.1, the VLAN 0 priority tagging feature allows you to prioritize traffic without assigning it to a specific VLAN. This feature enables the transmission and reception of 802.1Q Ethernet frames with the VLAN ID set to zero, by retaining the 802.1P priority bits of the VLAN 0 Ethernet packets. These Ethernet frames are known as **priority tagged** frames. As a result, critical traffic receives higher processing priority.

Perform these steps to configure the default PROFINET settings on a switch:

Procedure

1. Use the **configure terminal** command to enter global configuration mode.

   Example

   ```
   Switch# configure terminal
   ```

2. Use the **interface vlan 1** command to access the VLAN 1 interface.

   Example

   ```
   Switch(config)# interface vlan 1
   ```

3. Use the **no shut** command to enable VLAN 1.

   Example

   ```
   Switch(config-if)# no shut
   ```

4. Use the **end** command to exit the configuration mode.

Example

```
Switch(config-if)#end
```

5. To enable PROFINET on the switch, refer to Enable PROFINET.

> **Note**
>
> Cisco devices undergo the Profinet Certification process to ensure compliance with industrial automation standards. During this process, the use of non-standard protocols such as CDP results in test failures, preventing certification. As a result, Cisco devices intended for Profinet environments must use IEEE standard LLDP instead of CDP.

Prepare and assign a switch for PROFINET network integration

Configure and assign switches with the correct GSD file to ensure seamless integration into a PROFINET network using TIA Portal or STEP7. This process helps guarantee compatibility and readiness for network deployment.

This task enables you to prepare and assign a Cisco switch for integration into a PROFINET network using TIA Portal or STEP7. Completing this ensures the switch is recognized and managed correctly within the automation environment.

Use this task to prepare the files for integrating a switch into a PROFINET network using TIA Portal or STEP7.

Before you begin

- Ensure that the GSD file version matches the one bundled with your Cisco IOS software.
- Verify the GSD file is available and accessible on your PC.

  For more information on what a GSD file is, what information it contains about PROFINET devices, where Cisco stores these files on its switches, how to load them, and how to verify that the correct GSD is in use, see General Station Description File.
- PROFINET is enabled by default on all switches. Hence, do not use the CLI to configure or modify the switch when PROFINET and TIA are in use.

Perform these steps to prepare and assign a switch for PROFINET network integration.

Procedure

1. Launch the latest version of the TIA Portal or STEP7.
2. Click **Create new project** and enter a name in the **Project name** field. Click **Create**.
3. From the STEP7/TIA dashboard, choose **Options** > **Manage general station description files**.
4. Browse to the latest version of the GSD file location on your PC and click **Install**.

   Wait for the **Hardware catalog** to update.
5. From the **Hardware catalog**, choose the PLC and the switch.

   The PLC and the switch appear in the **Devices & networks** window.
6. Assign the switch to the PLC.

Configure a switch for PROFINET integration using STEP7 or TIA

Configure a switch for integration into a PROFINET network using STEP7 or the TIA portal. This task enables communication between the switch and the PLC for seamless device discovery and assignment.

Configuring a switch for PROFINET integration allows it to communicate with the PLC and participate in the network. This task ensures the switch is properly set up for device discovery and assignment.

Use this task to configure a switch for integration into a PROFINET network using either STEP7 or the TIA portal.

Before you begin

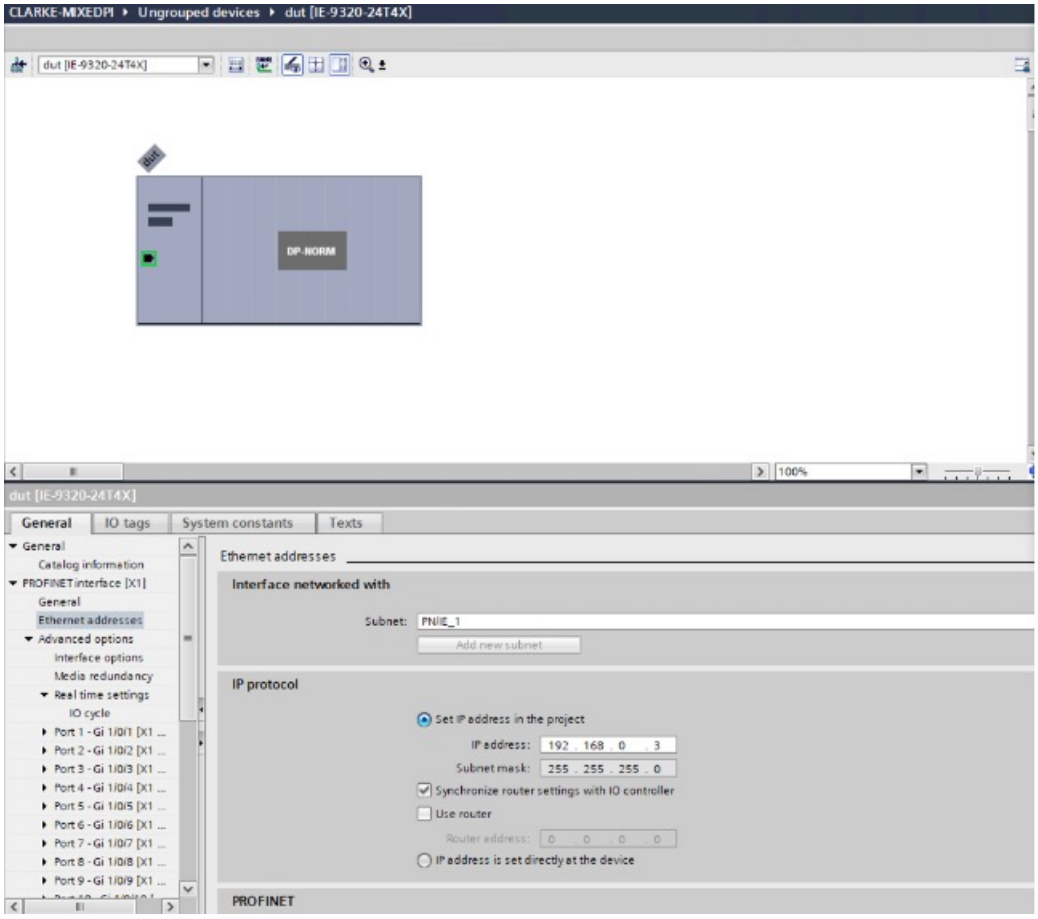
Ensure the GSD file is installed and the switch is assigned to the PLC.

Perform these steps to configure a switch for PROFINET integration using STEP7 or TIA:

Procedure

1. Double-click on the switch icon and assign the IP address and name.

Figure 1: Ethernet addresses

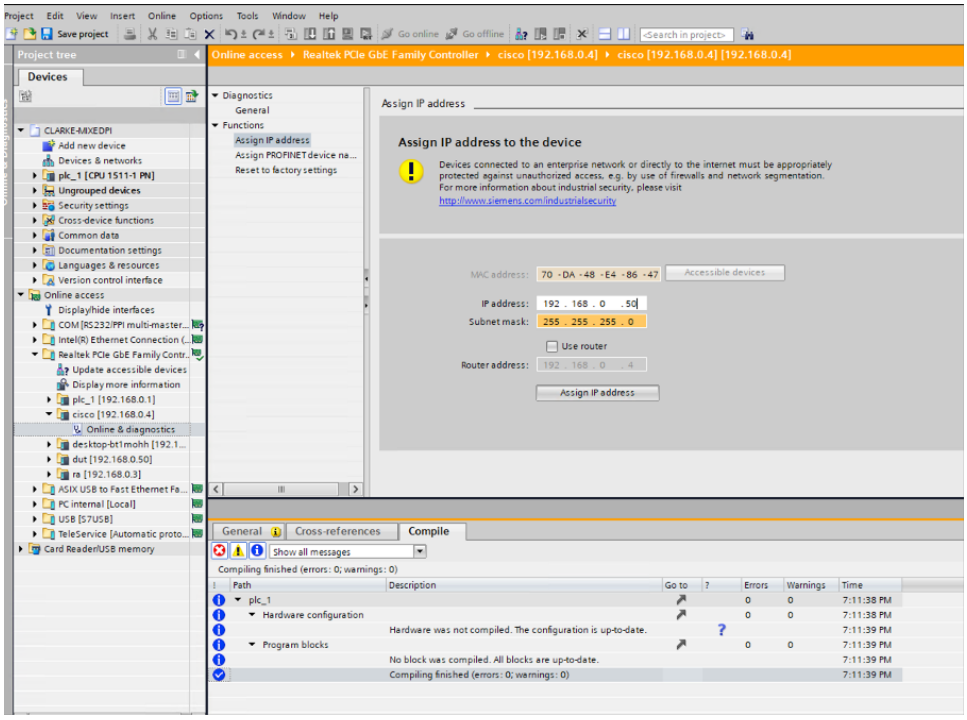


> **Note**
>
> These settings are for STEP7 or the TIA Portal only; the actual switch configuration occurs during discovery.

a) In the **General** tab, under the **Profinet interface**, choose **Ethernet addresses**.
b) In the **IP protocol** section, enter the IP address and click **Save**.
c) In the **General** tab, enter the name of the switch in the **Name** field.

2. From the **Hardware catalog**, add any required expansion or pluggable modules to the switch.
3. Discover the device on the network.
   a) From the main menu, choose **Online** > **Accessible devices**.
   b) From the **PG/PC interface** choose the PC which is connected to the PROFINET. This uses LLDP (enabled by default) and initiates the device discovery.
   c) Click **Show** to verify the switch appears in the **Accessible device** section with its MAC address listed.
4. Assign the IP address and device name to the switch.

Figure 2: Assign IP address



a) In the **Devices** pane, go to **Online & diagnostics**.
b) Locate **Assign IP address** in **Functions** and enter the IP address in the field.
c) In the **Assign PROFINET device name** and enter the name in the field.

5. Save, compile, and download the project.
   a) In the **General** tab, choose the **Devices & networks** and click **Save project** from the tool bar.
   b) From the tool bar, click **Compile**.
   c) From the tool bar, click **Download**. In the **Extended download to device** window, choose the correct interface from the **Connection to interface/subnet**.
   d) Choose **Show accessible devices** and from the **Select target device**, choose **PLC** and click **Load** and **Finish**.

6. Click **Go online** to establish a live connection.

Enable PROFINET

Configure PROFINET on the switch to enable industrial protocol support and optimize device communication. This task ensures proper setup of device ID, VLAN, and port access for PROFINET operation.

Enabling PROFINET allows the switch to support industrial automation protocols, facilitating communication between devices in a PROFINET network.

Before you begin

- Ensure you have access to the switch with the required privileges.
- Verify the switch is running Cisco IOS or IOS XE software that supports PROFINET.

Follow these steps to enable PROFINET on the switch:

Procedure

1. Use the **configure terminal** command to enable global configuration mode.

   Example

   ```
   Switch# configure terminal
   ```

2. Use the **profinet** command to enable PROFINET on the switch.

   Example

   ```
   Switch(config)# profinet
   ```

   After PROFINET is enabled, you can configure the device as described in Configure a switch for PROFINET integration using STEP7 or TIA on page 12 (recommended) or by using the Cisco IOS commands provided in the subsequent steps.

3. (Optional) Use the **profinet id** *id* command to set the PROFINET device identifier (ID) by using the Cisco IOS software.

   Example

   ```
   Switch(config)# profinet id Cisco
   ```

   The maximum length of the ID string can be 240 characters. The only special characters allowed are period (.) and hyphen (-), and they are allowed only in specific positions within the ID string. The ID can have multiple labels within the string. Each label can be from 1 to 63 characters, and labels must be separated by a period (.). The final character in the string must not be zero (0).

   For more details about configuring the PROFINET ID, see the PROFINET specification, document number TC2-06-0007a, filename PN-AL-protocol_2722_V22_Oct07, available at PROFIBUS .

   This step is optional and can be done through STEP7 or TIA PORTAL STEP 7 or the TIA Portal Automation application installed on the Supervisor (recommended).

4. (Optional) Use the **profinet vlan 10** command to change the VLAN number. The default VLAN number is 1. The VLAN ID range is from 1 to 4096. One PROFINET VLAN is supported per switch.

Example

```
Switch(config)# profinet vlan 10
```

> **Note**
>
> You must create a VLAN before assigning a new VLAN to PROFINET if you are using a non default VLAN.

5. Use the **interface** *interface_id* command to configure the port for PROFINET.

   Example

   ```
   Switch(config)# interface gi1/0/2
   ```

6. Use the **switchport access vlan** command to configure the access VLAN required for the port.

   Example

   ```
   Switch(config-if)# switchport access vlan 10
   ```

7. Use the **switchport mode access** command to assign a specific VLAN to a switch port configured in access mode.

   Example

   ```
   Switch(config-if)# switchport mode access
   ```

8. Use the **switchport voice vlan dot1p** command to the interface to allow VLAN 0 tagged packets.

   Example

   ```
   Switch(config-if)# switchport voice vlan dot1p
   ```

   This command applies to Cisco IOS XE release 17.17.1 and earlier versions. Starting with Cisco IOS XE release 17.18.1, the system enables the command by default.

   The **switchport voice vlan dot1p** command allows specified VLAN tagged packets along with the COS values of ingress frames.

9. Use the **end** command to return to privileged EXEC mode.

   Example

   ```
   Switch(config)# end
   ```

Profinet connection configuration

Lists the CLI configurations that are automatically applied and saved when a Profinet connection or session is established.

When a Profinet connection/session is established, the network device automatically applies and saves the CLI configurations (including SNMP) given in the table below.

Table 5: CLI for the PROFINET Configuration

CLI	Purpose
snmp-server community private RW **snmp-server community public RO**	Configure two Simple Network Management Protocol (SNMP) community strings, each with a read-write and read-only access.
LLDP **lldp timer 5** **lldp holdtime 20** **lldp run**	Enable the Link Layer Discovery Protocol (LLDP) with a frame transmission interval of 5 seconds and a holdtime of 20 seconds.
CDP **no cdp run**	Disable the Cisco Discovery Protocol (CDP).
Power-supply **power-supply dual**	Set up the device to manage dual power supplies, ensuring it can operate redundantly if one power supply fails.

Note

CDP is enabled by default in IOS XE 17.18.2 and later releases.

Prevent default gateway and CDP loss during reloads and upgrades

Configure Cisco IE switches to prevent the loss of default gateway and Cisco Discovery Protocol (CDP) configurations during reloads and upgrades on Cisco IOS XE 17.x.

This task ensures network connectivity remains intact by preventing the silent disappearance of default gateway and CDP configurations when Profinet interferes with running configuration persistence.

Cisco IE switches have Profinet (PN) enabled by default to facilitate management through the Siemens TIA application portal, similar to other I/O devices, Programmable Logic Controllers (PLCs), and I/O devices within the Local Area Network (LAN).

Upon reloading an Industrial Ethernet (IE) switch operating on Cisco IOS XE 17.x or performing an upgrade from version 16.x, you may experience unexpected network connectivity disruptions. This phenomenon arises because the default gateway configuration fails to persist in the running configuration, resulting in its silent disappearance. Moreover, the Cisco Discovery Protocol (CDP) may also be disabled during this process.

When the Profinet feature is active, the Profinet subsystem conducts several critical checks to ensure proper configuration:

- Non-Zero Values: The switch IP address configured on the Profinet VLAN, gateway address, and netmask must all be non-zero.
- Subnet Consistency: The IP address and gateway address must reside within the same subnet.
- Uniqueness: The IP address and gateway address must not be identical.

If any of these conditions are not met while the Profinet feature is enabled, the default gateway configuration is removed from the running configuration. Additionally, if you save this incomplete configuration to the startup configuration using the **write mem** command, the erroneous settings will persist through power cycles.

Before you begin

While both the default gateway and CDP configurations are retained in the startup configuration, they do not appear in the running configuration post-reload or upgrade.

Follow these steps to prevent default gateway and CDP loss during reloads and upgrades:

Procedure

1. Disable Profinet.

   Enter the **no profinet** command to disable the Profinet feature.

2. Reconfigure settings.

   Manually re-enter the CDP and default gateway configurations.

3. Save configuration.

   Use the **write mem** command to save the updated configuration.

4. Verify configuration.

   Optionally, reload the switch to confirm that the configurations are correctly reflected in the running configuration post-reload.

5. Check Profinet status.

   Use the **show profinet status** to ensure that Profinet is disabled.

Gateway IP address configuration scenarios

Understand how PROFINET controllers, the CLI, and management applications affect IP address, subnet mask, and gateway configuration across reloads and upgrades.

The configuration and persistence of the IP address, subnet mask, and default gateway depend on how PROFINET and the management system control the device.

Scenario 1: The device is managed by a PROFINET controller

When PROFINET is enabled and the device is actively managed by a PROFINET controller, such as a PLC or TIA Portal, the controller configures the IP address, subnet mask, and default gateway. The device receives these parameters after it connects to the controller.

The device does not retain these parameters across a software upgrade or reload. After the device reconnects to the PROFINET controller, the controller configures the parameters again. This behavior complies with the PROFINET specification.

The PROFINET requirements related to the IP address, subnet mask, and default gateway remain enforced.

Scenario 2: PROFINET is enabled, but the device is not managed by a PROFINET controller

When PROFINET is enabled but the device is not actively managed by a PROFINET controller, you can configure the IP address, subnet mask, and default gateway by using the CLI or another management application, such as Cisco Catalyst Center.

To prevent PROFINET from affecting the IP address, subnet mask, or default gateway configuration, disable PROFINET, save the running configuration, and reload the device:

```
Switch# configure terminal
Switch(config)# no profinet
Switch(config)# end
Switch# write memory
Switch# reload
```

After the device reloads, PROFINET no longer controls these parameters.

Scenario 3: The device is managed by both a PROFINET controller and Cisco Catalyst Center

In a converged network, the device may connect to an active PROFINET controller, and Cisco Catalyst Center or the CLI may manage its IP configuration. The IP address, subnet mask, and gateway information is not sourced from the PROFINET controller in this scenario.

Guidelines for managing IP configuration:

- Configure a default route instead of a default gateway to maintain gateway connectivity.

```
Switch# configure terminal
Switch(config)# ip routing
Switch(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.254
```

- The PROFINET requirements related to the IP address, subnet mask, and gateway remain enforced because PROFINET is active.
- After a software upgrade or reload, the PROFINET module clears the IP address, subnet mask, and gateway information unless they are provided by the PROFINET controller or TIA Portal. If the PROFINET controller or TIA Portal does not supply these parameters, Cisco Catalyst Center or another management application must reconfigure them.

PROFINET monitoring and maintenance

Lists commands for displaying PROFINET configuration and status information.

Use these commands to monitor PROFINET sessions, check subsystem status, and view adjacent interface information for maintaining PROFINET connectivity.

Table 6: Commands for displaying the PROFINET Configuration

Command	Purpose
show profinet session	Displays the currently connected PROFINET sessions.
show profinet status	Displays the status of the PROFINET subsystem.
show lldp neighbor interface-id detail	Displays information about the adjacent interface.

Example:

```
Switch#show profinet status
Profinet : Enabled
Connection Status : Connected
Vlan : 1
Profinet ID : Switch
```

```
GSD version : Match
Reduct Ratio : 128
```

PROFINET troubleshooting

Lists the debug commands and methods for troubleshooting PROFINET configuration issues.

The PLC has LEDs that display red for alarms, and the I/O supervisor software monitors those alarms.

To troubleshoot PROFINET use the **debug profinet** privileged EXEC command with the keywords shown in Commands for Troubleshooting the PROFINET Configuration. Be aware that the output of a debug command might cause a serial link to fail. You should use these commands only under the guidance of a Cisco Technical Support engineer. When you use this command, use Telnet to access the Cisco IOS command-line interface (CLI) by using Ethernet rather than a serial port.

Table 7: PROFINET troubleshooting commands

Command	Purpose
debug profinet alarm	Displays the alarm status (on or off) and content of PROFINET alarms.
debug profinet cyclic	Displays information about the time-cycle-based PROFINET Ethernet frames.
debug profinet error	Displays the PROFINET session errors.
debug profinet packet ethernet	Displays information about the PROFINET Ethernet packets.
debug profinet packet udp	Displays information about the PROFINET User Datagram Protocol (UDP) packets.
debug profinet platform	Displays information about the interaction between the Cisco IOS software and PROFINET.
debug profinet topology	Displays the PROFINET topology packets received.
debug profinet trace	Displays a group of traced debug output logs.

Technical assistance

Lists technical support resources and access information.

This reference provides access to technical support resources available through Cisco.

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature history for PROFINET configuration

Identify the Cisco IOS XE releases that introduced VLAN 0 priority tagging and PROFINET Netload-3 Robustness.

Table 8: Feature History Table

Feature	Release information	Feature description
VLAN 0 priority tagging	Cisco IOS XE Release 17.18.1	This feature enables prioritization of critical traffic using 802.1Q frames with a VLAN ID of zero, ensuring higher processing priority without VLAN assignment.
PROFINET Netload-3 Robustness	Cisco IOS XE Release 26.2.x	PROFINET NETLOAD Class III protection increases resilience to abnormal network traffic. The feature detects unexpected PROFINET Real-Time traffic, invokes Layer 2 source blocking, and rate-limits incoming Layer 3 traffic directed to the PROFINET VLAN IP address.

2 PROFINET System Redundancy

Topics:

- PROFINET system redundancy
- Restrictions for PROFINET system redundancy
- How PROFINET system redundancy modes work
- Feature history for PROFINET System Redundancy

PROFINET system redundancy

Use PROFINET S2 controller redundancy to maintain device communication through active and standby controller connections during a controller failure.

A PROFINET system redundancy is a communication architecture that

- allows IO devices and IO controllers to maintain communication in the event of device or connection failure, and
- ensures higher availability and reliability in industrial automation networks.

Starting from 26.1.1, Cisco Industrial Ethernet (IE) switches support only S2 controller redundancy as per the *PN-AL-Protocol_2722_V24MU5* and *PN-AL-Services_2712_V24Mu5* specifications.

> **Note**
>
> After you upgrade the software, download and install the updated Generic Station Description Markup Language (GSDML) configuration files to enable S2 redundancy.

Prerequisites to PROFINET system Reduncandy modes opration

- Enable S2 mode so that each PROFINET device forms two communication relationships (Application Relationships (ARs)) with two controllers.
- Ensure both the IO device and the controllers support S2 redundancy features.
- Ensure that the device is connected to both controllers through a single PROFINET interface (NAP).
- Maintain only one active controller connection at a time.

Restrictions for PROFINET system redundancy

Review supported PROFINET redundancy modes, including S2 support and the exclusion of R1 and R2 modes.

- Only S2 PROFINET redudandcy is supported. R1 and R2 PROFINET redudandcy modes are not supported.

How PROFINET system redundancy modes work

Understand how S2 redundancy uses two application relationships through a single network interface to switch communication to a standby controller when the primary connection fails.

Summary

PROFINET system redundancy modes ensure continuous communication between IO controllers and IO devices. This increases system availability by enabling failover paths if a controller or network component fails.

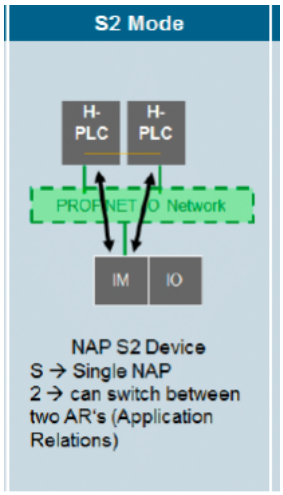
Table 9: key components of PROFINET system redundancy workflflow

Component	Function
PLC (Programmable Logic Controller)	Acts as the IO controller, managing the communication and control logic for the automation system.

Component	Function
IO device (IOD)	The field device (such as ET 200SP, Cisco IE switches) that connects to the controller and exchanges process data.
Network Access Point (NAP)	The PROFINET interface on the IO device, which may be single or provide redundancy.
Application Relationship (AR)	The logical connection for data exchange between a controller and an IO device.

Workflow

Figure 3: PROFINET system redundancy in S2 mode



The process involves these stages:

1. The IO device supports two ARs, each with a separate PLC, but has only a single NAP.
2. Only one AR is active for IO data exchange and the other AR is in standby.
3. If the primary connection fails, the IO device quickly switches to the backup AR, minimizing downtime.

Result

PROFINET system redundancy modes provide graded levels of redundancy to maintain process continuity in industrial networks. These modes range from no failover (S1 redundancy mode) to controller failover (S2 redundancy mode).

Feature history for PROFINET System Redundancy

Identify the Cisco IOS XE release that introduced PROFINET S2 controller redundancy for improved availability in industrial networks.

Table 10: Feature history

Feature Name	Releases	Description
PROFINET system redundancy	Cisco IOS XE 26.1.1	This feature enables Cisco Industrial Ethernet (IE) switches to interoperate with existing high available systems by providing robust controller failover using PROFINET S2 controller redundancy mode. It aims to minimize potential issues and downtime in the event of network or controller failures.

3 Read-only PROFINET

Topics:

- Read-only PROFINET
- Configure read-only PROFINET
- Feature history for Read-only PROFINET

Read-only PROFINET

Protect critical network settings from PROFINET changes while retaining device discovery, identification, and existing LLDP, SNMP, and CDP configurations.

The read-only PROFINET feature is a configuration mode that prevents modifications to critical network parameters, including IP address, subnet mask, gateway, device name, and factory reset settings. While write operations are restricted, the feature still allows read and identification functions. Additionally, it preserves existing configurations for LLDP, SNMP, and CDP, ensuring these services remain fully operational.

Configure read-only PROFINET

Enable or disable read-only PROFINET and verify its operational status using CLI commands.

Enable read-only PROFINET.

Procedure

1. Use the **configure terminal** command to enter configuration mode.

   Example

   ```
   Switch# configure terminal
   ```

2. Use the **profinet read-only** command to enable PROFINET as read-only.

   Example

   ```
   Switch(config)# profinet read-only
   ```

   Use the **no profinet read-only** command to disable this feature.

3. (Optional) Use the **Show profinet status** command to monitor PROFINET status.

   Example

   ```
   Switch# show profinet status
   Profinet                        : Enabled
   Connection Status               : Disconnected
   Vlan                            : 1
   Profinet ID                     :
   GSD version                     : Unknown
   Reduct Ratio                    : 128
   MRP                             : Enabled
   MRP License Status              : Not Applicable
   MRP Max Rings Allowed           : 3
   Profinet read-only              : Enabled
   ```

Feature history for Read-only PROFINET

Identify the Cisco IOS XE release that introduced read-only PROFINET to protect network settings while preserving discovery and identification functions.

Table 11: Feature history

Feature Name	Releases	Description
Read-only PROFINET	Cisco IOS XE 26.1.1	This feature increases device security and network flexibility by placing Discovery and Configuration Protocol (DCP) operations in read-only mode. It: • Protects the IP address, gateway, and device name from changes. • Protects critical network settings and prevents unexpected loss of connectivity. • Maintains compatibility with LLDP, SNMP, and CDP. • Allows devices to perform identification and basic network discovery.