Configure Industrial Asset Discovery

Industrial asset discovery

The Industrial Asset Discovery (IAD) feature provides enhanced visibility into directly connected end devices within an industrial network. IAD leverages discovery messages that are inherent to standard industrial protocols, such as Common Industrial Protocol (CIP) and Profinet, to identify and collect detailed information about these devices. Cisco Industrial Ethernet (IE) switches utilize the same protocol messages as CIP and Profinet devices to ensure that there is no operational impact on end devices. The devices continue to respond as expected within the network.

How IAD works

IAD sends and processes discovery messages from CIP and Profinet protocols. These messages allow the switch to identify connected industrial devices, such as programmable logic controllers (PLCs) and intelligent electronic devices (IEDs), and to gather detailed information about their network connectivity. Since IAD uses the same protocol messages as the connected devices, it does not disrupt normal device communication.

IAD collects layer 2 network connectivity details, such as the switch, interface, and VLAN assignments, for each discovered device. This information is processed and maintained in a local inventory database on the switch. IAD collects information from IP Device Tracking (IPDT) and device discovery protocols such as Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP), to provide a comprehensive view of all connected assets.

Key benefits

- **Enhanced device visibility:** Provides granular information about connected industrial devices, switch port, and VLAN assignment.

- **Improved network segmentation:** Supports identification of unauthorized devices, which helps network administrators identify misconnection and misconfiguration, and assist with their network segmentation policies.
- **Automated data export:** Enables export of device inventory data using JSON syslog integration for external monitoring or asset management.
- **Non-intrusive operation:** Uses standard protocol messages, ensuring no impact to end device behavior or network performance.

Supported protocols

IAD collects and correlates device information using these protocols:

- CIP
- Profinet
- IPDT
- CDP
- LLDP

Industrial asset discovery operation

After the switch boots and you enable IAD, the system waits for a period before sending discovery messages to the enabled industrial protocols. The system sends subsequent notifications at periodic intervals.

You can:

- Configure the interval to send notifications by using **iad refresh-interval** command.
- Enable and disable discovery for any, or all of the supported protocols in IAD.

Each access switch maintains a local IAD database to store collated device information collected from the supported protocols. The system refreshes the local database dynamically according to the configured timer values.

The system automatically refreshes the database when an interface state changes from *down* to *up*. During a link flap event, IAD sends a discovery message, waits for a predefined interval, and then sends the next discovery message to prevent excessive traffic.

IAD discovery gathers and stores these details about each end device.

- Status of connected physical port in **Up** or **Down** state
- IP address
- MAC address
- Serial number
- Device PID
- Vendor

- Device type

Device code	Device
R	Router
B	Source route bridge
T	Telephone
H	Host
C	DOCSIS cable device
W	WLAN access point
P	Repeater
G	Trans bridge
F	Switch
I	IGMP
E	Phone
S	Station
D	Remote
A	CVTA
M	Two-port Mac relay
O	Other

- Software version
- Protocol
- Timestamp
- Physical port
- Port mode

Code	Port mode
ACC	Access
TR	Trunk
RO	Routed

- VLAN
- Reported time

The device details stored by IAD and displayed in the console can vary based on the network configuration and device characteristics.

Guidelines and Limitations

Consider these guidelines and limitations when configuring IAD:

- For CIP and Profinet protocols, it is assumed that the end devices are connected through access ports, while switch-to-switch peer links use trunk ports. The system does not record end devices detected on trunk interfaces in the local database.
- When an interface goes down, the system updates the Interface Status for all related records to **down**. When the interface comes up, the system sends discovery messages, refreshes the records, and updates the Interface Status to **up**.
- For CIP and Profinet discovery messages, assign an IP address to the Switched Virtual Interface (SVI) for the VLAN. Use the same VLAN for Profinet or CIP devices.
- The IAD database supports a maximum of 100 records (devices). No limit exists for the number of records an interface can receive.
- Enable at least one protocol—Profinet, CIP, LLDP, IPDT, or CDP— for IAD operation. For instructions, see Enable PROFINET, Enable CIP, Enable LLDP, Enable IPDT, and Enable CDP.

Default configuration

IAD is disabled by default. When you enable IAD, the system applies specific default settings for protocol discovery and database updates.

The system uses these default settings:

- Sends discovery messages for CIP and Profinet.
- Receives device records from CDP, LLDP, and IPDT.
- Sets the default refresh interval for protocol discovery notifications as 6 hours (21,600 seconds).

Configure industrial asset discovery

Perform this task to enable IAD and set the discovery packet refresh interval.

Before you begin

Ensure that the protocols you want to enable for IAD are active at the switch level.

Procedure

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

Example:

```
Device# configure terminal
```

Step 2 Use the **iad enable {cdp | cip | ipdt | lldp | profinet}** command to enable IAD for a specific protocol.

Example:

```
Device(config)# iad enable cip
```

Note
If you do not specify a protocol, the system enables IAD for all supported protocols.

Step 3 Use the **iad refresh-interval** *seconds* command to specify the rate at which CIP or Profinet discovery packets are sent in seconds.

Example:

```
Device(config)# iad refresh-interval 10800
```

Example:

Note
The **refresh-interval** range is 10 to 86400 seconds. The default value is 21600 seconds (6 hours).

Export IAD records to syslog server

IAD can periodically export inventory records as syslog JSON strings to a syslog server. To enable this feature, you must configure IAD export and a syslog session using a logging discriminator and a TCP session for asset discovery events.

Configure IAD export

Perform this task to enable the periodic export of IAD inventory records.

Procedure

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

Example:

```
Device# configure terminal
```

Step 2 Use the **iad export enable** command to enable IAD export.

Example:

```
Device(config)# iad export enable
```

Step 3 Use the **iad export export-interval** *seconds* command to set the export frequency in seconds.

Example:

```
Device(config)# iad export export-interval 300
```

The **export-interval** range is 1 to 1440 seconds.

Configure syslog session for IAD

Perform this task to configure a syslog session using logging discriminators and TCP transport to filter and export asset discovery messages in JSON format.

Before you begin

Ensure you have:

- Administrative privileges to access the device CLI.
- Network connectivity to the syslog server.
- The IP address and TCP port of the syslog server.

Procedure

Step 1 Use the **logging discriminator** *discriminator-name* [**severity includes** *severity-level*] [**facility includes** *facility-name*] [**mnemonics includes** *mnemonic-string*] [**rate-limit** *rate*] command to define the criteria for filtering syslog messages based on severity, facility, or mnemonics.

Example:

```
Device(config)# logging discriminator my_desc severity includes 5 facility includes %IAD
mnemonics includes ASSET_DISCOVERY rate-limit 10
```

Note

- Adjust discriminator parameters according to your operational and security requirements.
- The **rate-limit** value set to 10, limits the number of messages per second to 10. This value prevents flooding of the syslog server.

Step 2 Use the **logging host** *ip-address* [**transport {tcp | udp}**] [**discriminator** *discriminator-name*] command to configure the remote syslog server IP address, specify the TCP transport port, and link the session to the defined discriminator.

Example:

```
Device(config)# logging host 192.168.1.77 transport tcp port 602 discriminator my_desc
```

Note
Ensure the syslog server is configured to accept TCP connections on the specified port.

The system generates a syslog entry in JSON format when a new asset is discovered.

Example syslog entry:

```
*Jan 16 03:50:52.535: %IAD-6-ASSET_DISCOVERY: New Asset {
"Interface": "Gi2/1",
"Status": "UP",
"IP-Address": "xx.xx.xx.xxx",
"MAC Addr": "D0:xx:xx:xx:xx:xx",
```

```
"Port Mode": "ACC",
"VLAN": 134,
"Serial No": "0x504D415",
"Device PID": "EtherNetIP Master S",
"Vendor": "UNKNOWN",
"Device Type": "UNKNOWN",
"SW ver": "UNKNOWN",
"Protocol": "CIP,IPDT",
"Last Reported Time": "03:49:20 UTC Fri Jan 16 1970"
}
```

Verify IAD status

Perform this task to verify the IAD inventory and current configuration status.

Procedure

Step 1 Use the **show iad inventory {interface | protocol}** command to display the IAD device inventory.

Example:

```
Device# show iad inventory
```

Supported protocols are cdp, cip, ipdt, lldp, and profinet.

Output:

```
Device# show iad inventory
Capability codes:
(R) Router, (B) Source Route Bridge, (T) Telephone, (H) Host
(C) DOCSIS Cable Device (W) WLAN Access Point (P) Repeater
(G) Trans Bridge, (F) Switch, (I) IGMP, (E) Phone, (S) Station
(D) Remote, (A) CVTA, (M) Two-port Mac Relay, (O) Other

Port Modes:
(ACC) Access , (TR) Trunk, (RO) Routed

Port    Mode  Vlan  Status  IP-Address       Mac Addr           Serial No    Device PID
    Vendor      Device Type    SW ver       Protocol      Reported Time
------- ----- ----- ------- ---------------  -----------------  -----------  ---------------
  ----------  -------------  ------------  ------------  --------------------
Gi1/1          0     DOWN
Gi1/2          0     DOWN
Gi1/3          0     DOWN
Gi1/4  ACC     1     UP      192.168.1.248   38:4B:24:6A:A6:48  Unknown     SCALANCE XC-200
  42          IO            Unknown      PN            19700121 20:49:59
Gi1/4  ACC     1     UP      192.168.1.17    E8:EB:34:04:31:49  Unknown     IE-3400-8P2S
  cisco       R,F,I         26.01.202602  CDP           19700121 20:49:37
Gi1/4  ACC     1     UP      Unknown         70:DA:48:B9:7E:47  Unknown     Cisco
  383         IO            Unknown      IPDT,PN       19700121 20:49:59
Gi1/4  ACC     1     UP      192.168.1.8     34:C0:F9:E5:72:EB  0x600F95A6  Stratix 5800
Ma  Unknown     Unknown       Unknown      CIP,IPDT      19700121 20:49:59
Gi1/4  ACC     1     UP      192.168.1.201   F4:BD:9E:BD:DB:30  Unknown     Unknown
  Unknown     Unknown       Unknown      IPDT          19700121 20:31:53
Gi1/4  ACC     1     UP      192.168.1.230   F0:78:16:A2:4B:42  Unknown     Unknown
  Unknown     Unknown       Unknown      IPDT          19700121 20:31:53
Gi1/5          0     DOWN
```

```
Gi1/6  ACC     1     UP      192.168.1.55    C8:60:8F:BF:9A:06  Unknown     IE-3100-3P1U2S
  cisco       R,F,I         26.01.202602  CDP,LLDP      19700121 20:49:58
Gi1/7  ACC     1     UP      192.168.1.90    34:C0:F9:E5:13:24  Unknown     1783-MMS10EA
  Allen-Bra   B,R           26.01.1prd11  CDP,LLDP      19700121 20:49:59
Gi1/7  ACC     1     UP      192.168.1.90    34:C0:F9:E5:13:2B  0x600F9314  Stratix 5800
Ma 1          Unknown     Unknown       CIP           19700121 20:49:59
Gi1/7  ACC     1     UP      192.168.1.101   24:0F:9B:5E:9D:8A  Unknown     Unknown
  Unknown     Unknown       Unknown       IPDT          19700121 20:45:37
Gi1/8  ACC     1     UP      11.4.3.1        54:51:DE:0C:84:0E  Unknown     C9200-24PXG
  cisco       R,F,I         17.6.4        CDP           19700121 20:49:43
Gi1/9  ACC     1     UP
Gi1/10 ACC     1     UP
Gi1/11         1     DOWN

Total entries displayed : 11
```

IAD is an aggregator protocol that collects information from supported discovery protocols and presents it in the output of the `show iad inventory` command. This command displays a table of discovered device entries with detailed attributes. For example, consider this entry:

```
Port    Mode  Vlan  Status  IP-Address       Mac Addr           Serial No    Device PID
    Vendor      Device Type    SW ver       Protocol      Reported Time
Gi1/4   ACC     1     UP    192.168.1.248   38:4B:24:6A:A6:48    Unknown     SCALANCE XC-200
    42          IO           Unknown      PN            19700121 20:49:59
```

The table presents device discovery fields and descriptions.

Field	Value	Description
Port	Gi1/4	The interface on which the device was discovered
Mode	ACC	Port mode
Vlan	1	VLAN ID associated with the port
Status	UP	The operational status of the port
IP-Address	xxx.xxx.x.xxx	IP address of the discovered device
Mac Addr	xx:xx:xx:xx:xx:xx	MAC address of the device
Serial No	Unknown	Product CIP Serial Number. Entries discovered through the CIP protocol will have a value included in this field.
Device PID	SCALANCE XC-200	Product ID or device name
Vendor	42	Vendor ID as reported by the discovery protocol
Device Type	IO	Type of the device
SW ver	Unknown	Software version of the device. Unknown value indicates that SW ver details are not provided by this protocol.
Protocol	PN	The discovery protocol used.
Reported Time	19700121 20:49:59	Timestamp when the device information was reported

Step 2 Use the **show iad status** command to display the current IAD configuration status.

Example:

```
Device# show iad status
```

Output:

```
Device# show iad status
IAD Information:
Status : Enabled
Export Status : Disabled
Send/Receive Notification to CDP : Enabled
Send/Receive Notification to CIP : Enabled
Send/Receive Notification to IPDT : Enabled
Send/Receive Notification to LLDP : Enabled
Send/Receive Notification to PROFINET : Enabled
Last discovery sent for CIP/Profinet : 16:39:20 UTC Fri Mar 21 2025
IAD Records Refresh Interval Rate : 21600 secs
IAD Records Export Interval Rate : 300 secs
```

Feature history

Table 1: IAD Feature history

Feature name	Release	Description
Industrial Asset Discovery (IAD) Completion	Cisco IOS XE 26.1.1	Initial release on IE3500 series switches.