

Cisco Cyber Vision Active Discovery of Endpoints using DNP3 Protocol

White Paper

May 9, 2025

Contents

Introduction	3
Substation Automation Solution Architecture	3
Cisco Cyber Vision Active Discovery	4
Protocols supported by Active Discovery	6
Design Considerations for Active Discovery	6
DNP3 Protocol Active Discovery Example	6
DNP3 IED example information collected using Active Discovery	9
Conclusion	10

Introduction

Cisco Cyber Vision enables Operational Technology (OT) visibility in industrial deployments. Cyber Vision turns the network into an asset inventory sensor. Visibility of the OT traffic flows inside the Substation Electronic Security Perimeter (ESP) Zone is key to implementing security policies within the Substation.

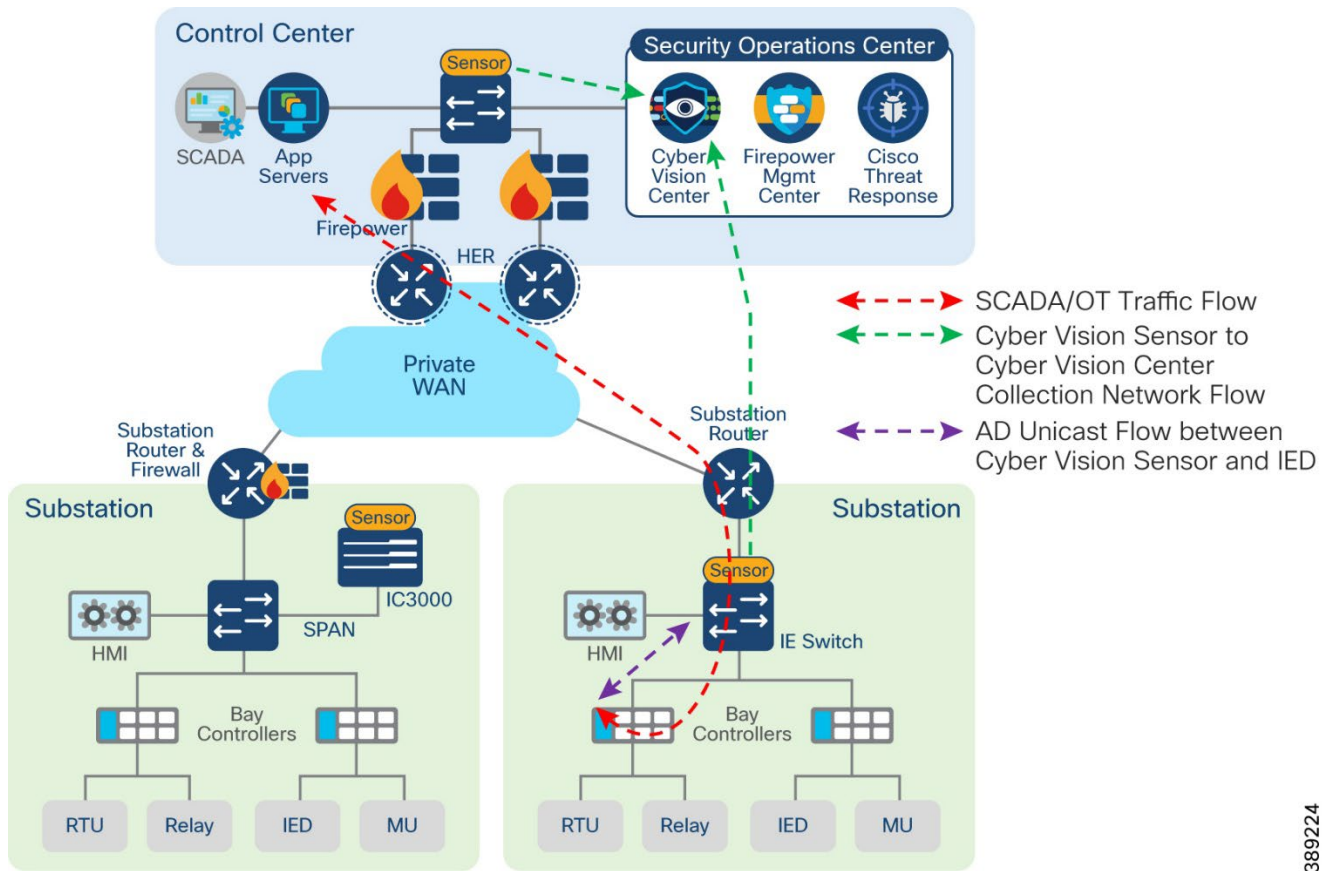
" You cannot protect what you cannot see."

This white paper discusses how Cyber Vision network sensors (for example, sensors embedded within the networking assets) actively discover information about Intelligent Electronic Devices (IEDs) positioned in the Bay level of a Substation.

Substation Automation Solution Architecture

The Cisco Substation Automation Architecture is segregated into control center, WAN, and substation blocks.

- The Cisco Cyber Vision Center application is hosted in the control center.
- The SCADA (DNP3 Front End Processor) is hosted in the control center.
- The DNP3 IED is connected to the station bus switch. Cisco IE Switches comprise the Station bus.
- The SEL 451R IED is used as an example in this white paper and is connected to the station bus.
- Cyber Vision Network Sensor is installed on Substation Station Bus Cisco IE Switch inside the ESP.
- OT Flow between the SCADA management system and the IED is depicted by the red dotted line in Figure 1.
- Communication between Cyber Vision Sensor and Cyber Vision Center is via a separate 'Collection' network as depicted by the green dotted line in Figure 1. This is a segregated connection via a VLAN to the Cyber Vision Center.
- Active Discovery (AD) flow between the Cyber Vision Sensor and the IED is depicted by the purple dotted line in Figure 1. Active Discovery is discussed in an upcoming section.



389224

Figure 1
Substation Architecture and OT Flows

For detailed information about the Cisco Substation Automation solution, refer to the latest validated design for Substation Automation: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/SA/3-1/SA-3-2-DG.pdf>

Cisco Cyber Vision Active Discovery

- Cyber Vision Network Sensor can get information about OT Endpoints via passive or active discovery methods.
- During normal operations many OT endpoints will not share many important asset details.
- Detailed asset information such as model number, serial number, and firmware is only exchanged over the network, for example, when an engineering station browses the device or downloads a new program.
- During normal operations this could take days to occur if the reliance were on a Passive Discovery (ERSPAN Approach).
- Active Discovery helps to get information immediately from the OT End points of interest.
- Active discovery does not require firewall access rules, as the Cyber Vision sensor sits close to the OT endpoint within the ESP network.

Figure 2 shows the Cyber Vision sensor embedded within the Cisco IE switch close to the OT endpoint. Both are within the same ESP and under any ESP firewall boundary which may be providing NAT to any north-south traffic.

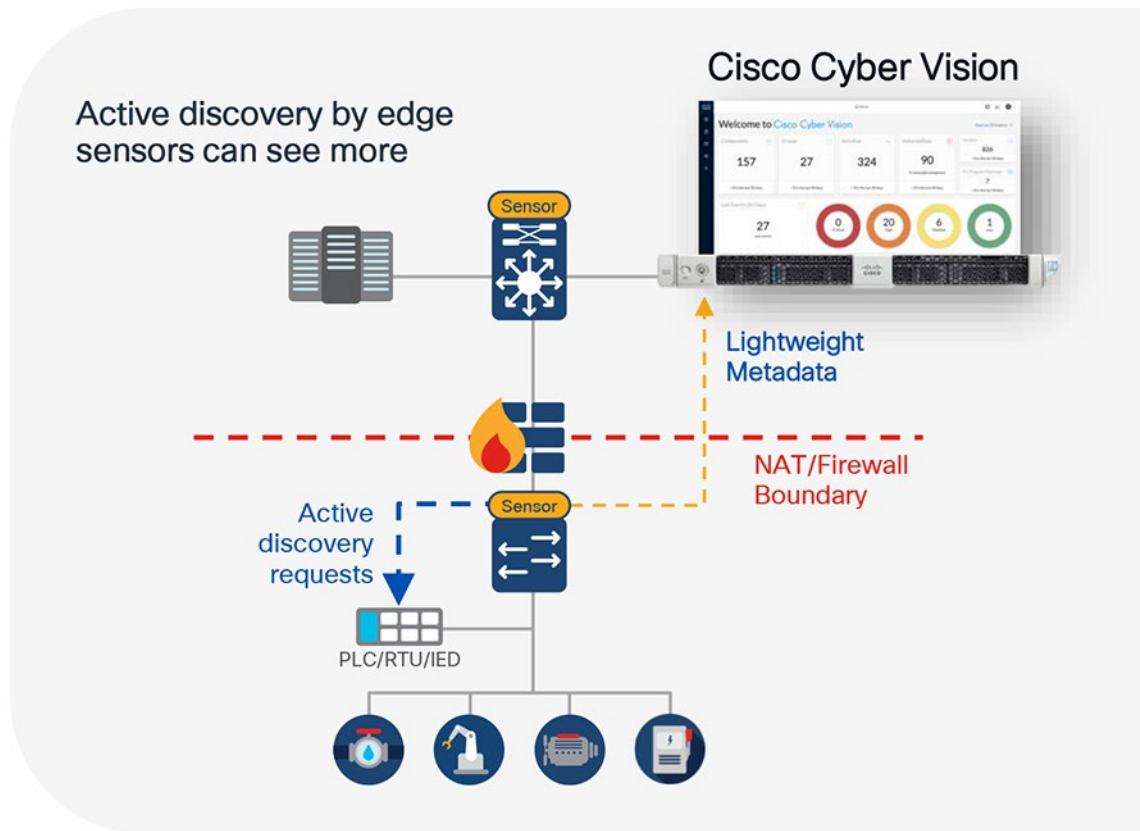


Figure 2
Cyber Vision Active Discovery

Active Discovery allows the sensor to send packets to the control network to discover previously-unseen devices and gather additional asset information for known devices.

There are two different types of Active Discovery operations:

- **Broadcast**
The Cyber Vision sensor broadcasts the configured control protocol packets targeting all the devices in the subnet. Devices that support the control protocol will give a response back (as if they were communicating with the Scada Master station) and appear in Cyber Vision.
- **Unicast**
The sensor sends unicast packets to known devices and analyzes the responses that are received.

Protocols supported by Active Discovery

- Broadcast: Profinet, ICMPv6, SiemensS7, EtherNet/IP, Beckhoff
- Unicast: **DNP3**, Modbus, SNMPv2, SNMPv3, OMRON, WMI, Melstion

For the latest information, refer to:

https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/Active-Discovery/Release-4-4-0/b_Cisco_Cyber_Vision_Active_Discovery_Configuration_Guide.html

Cisco Industrial Platforms with Embedded Network Sensors supporting Active Discovery:

- Cisco IE3x00, IE9300
- Cisco IR1101, IR18xx, IR8340
- Cisco IC3000
- Cisco Cat9300

Design Considerations for Active Discovery

- For Broadcast, Active Discovery the Cyber Vision Network Sensor should be in an OT subnet.
- For Unicast, Active Discovery the Cyber Vision Network Sensor can be in a different subnet. The Cyber Vision Network sensor must have a default gateway to be able to reach the OT Subnet where the target device is located.
- On the Cisco IE or IR, configure the APPGig Interface as a trunk interface that carries the Collection Network VLAN, Active Discovery VLAN, and ERSPAN VLANs to the Embedded Cyber Vision Sensor application.
- Choose the latest version of Cyber Vision software.

DNP3 Protocol Active Discovery Example

Steps to enable and use the active discovery method for DNP3:

- Step 1.** Workflow to enable DNP3 Active Discovery on the Cyber Vision Sensor.
- Step 2.** IOx Networking required to enable Cyber Vision Active Discovery.
- Step 3.** Configuration on the target DNP3 IED to respond back for Active Discovery probes.
- Step 4.** Triggering DNP3 Active Discovery to collect DNP3 Endpoint details.

How to enable DNP3 Active Discovery.

To configure Active Discovery on Network Sensor please refer to the configuration guide:

https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/Active-Discovery/Release-4-4-0/b_Cisco_Cyber_Vision_Active_Discovery_Configuration_Guide.html

Active Discovery can be triggered manually by the operator or can be configured to run at scheduled intervals.

IOx Networking with the Cisco Catalyst IE3400 Rugged switch with the embedded Network Sensor example.

In this example VLAN 112 is used for Active Discovery (this would be the OT traffic VLAN). Because DNP3 Active Discovery occurs via the unicast method, the Cyber Vision sensor and the OT endpoint can be in different subnets. See Figure 3.

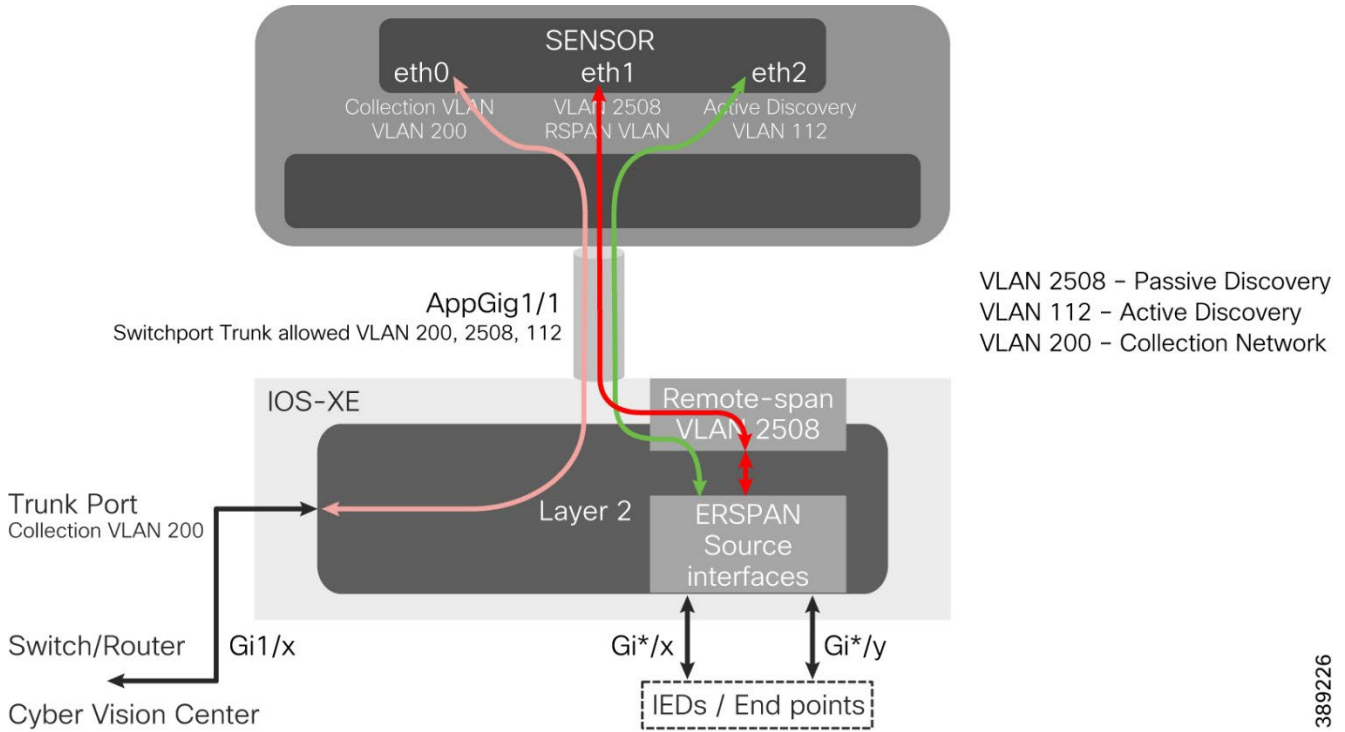


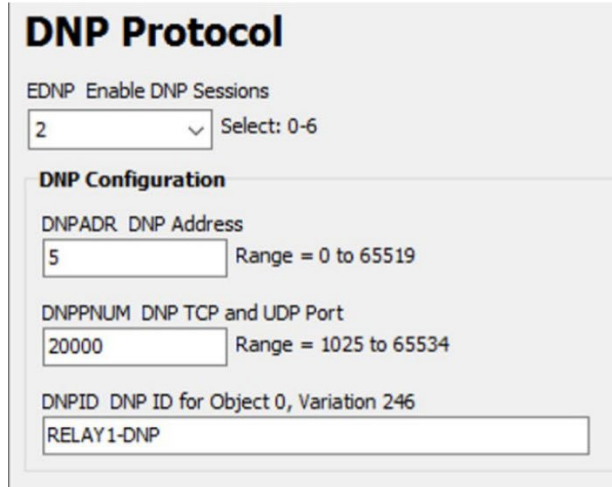
Figure 3
IOX Networking

389226

DNP3 IED SEL 451 configuration example to respond back to DNP3 Active Discovery.

Normally IEDs will only respond to the master SCADA stations, so allowing the IEDs to respond to the Active Discovery from the Cyber Vision sensor is also required. See Figure 4.

1) Device should be setup for 2 DNP3 masters.



DNP Protocol

EDNP Enable DNP Sessions
2 Select: 0-6

DNP Configuration

DNPADR DNP Address
5 Range = 0 to 65519

DNPPNUM DNP TCP and UDP Port
20000 Range = 1025 to 65534

DNPID DNP ID for Object 0, Variation 246
RELAY1-DNP

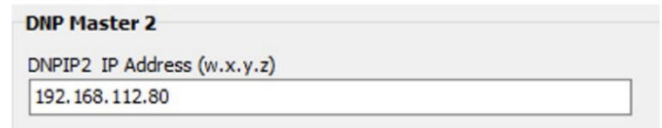
2) DNP Master 1 IP address.



DNP Master 1

DNPIP1 IP Address (w.x.y.z)
192.168.4.171

3) DNP Master 2 IP address in this example is that of the Active Discovery Sensor IP address.



DNP Master 2

DNPIP2 IP Address (w.x.y.z)
192.168.112.80

DNP3 Master SCADA is in OT Network

Active Discovery Cyber Vision Sensor is added as secondary Master which is different subnet

389227

Figure 4

DNP3 IED configuration for Active Discovery

DNP3 Active Discovery Logic on Cyber Vision Sensor.

Read operation is performed with DNP3 object AL_OBJ_DA_ALL (device attributes all, such as, 00 FE)

DNP3 IED example information collected using Active Discovery.

Components discovered via Active Discovery are tagged with the Active Discovery Label. In this example the complete information of the SEL 451R IED such as the serial number, firmware version, device serial number, and device type are collected. See Figure 5.

SEL- 451 DNP3 Flow

Component

Relay 1
IP: 192.168.112.53
MAC: 00:30:a7:21:c9:81
[Edit](#) [Manage group](#)
[Investigate in Cisco XDR](#)

First activity
Jan 22, 2025 10:15:47 AM

Last activity
Jan 22, 2025 10:27:47 AM

Tags
Controller, Master, Slave

Activity tags
Read Var, Time Management,
Active Discovery, Broadcast,
Low Volume, ARP, DNP3, NTP
(hide)

~20 Flows
4 Events
External Comm.

Basics Security Activity Automation

Properties Tags Sensors

Properties

Normalized Properties

- fw-version: R323-V2
- hw-version: 400MBR5
- ip: 192.168.112.53
- mac: 00:30:a7:21:c9:81
- model-ref: SEL-451-5 Relay
- name: Relay 1
- public-ip: no
- serial-number: 1200410196
- vendor-name: SCHWEITZER ENGINEERING
- vlan-id: 112

Other Properties

- dnp3-device-hw-version: 400MBR5
- dnp3-device-id: RELAY1-DNP
- dnp3-device-location: Station A
- dnp3-device-manufacturer: SEL
- dnp3-device-product-name-model: SEL-451-5 Relay
- dnp3-device-serial-number: 1200410196
- dnp3-device-sw-version: R323-V2
- name-dnp3-device: Relay 1
- name-ip: 192.168.112.53
- vendor: SCHWEITZER ENGINEERING

Components discovered via Active Discovery are tagged as Active Discovery Label

Figure 5
DNP3 IED Visibility using Active Discovery

Conclusion

Detected DNP3 IED SEL 451R which is the Protection and Control IED in bay level connected to Station Bus Switch and Cyber Vision Network Sensor IE3400. The method executed DNP3 Active Discovery using Cisco Cyber Vision to acquire complete information for DNP3 IEDs. In turn, this information can be used to create granular security policies to implement IEC 62443, NERC CIP Security Best Practices for Cybersecurity and to detect vulnerabilities of IEDs, if any, and baseline SCADA flows within substation ESP perimeter.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)