



Annex: Active Discovery protocols

All protocols implemented in the Active Discovery feature use standard packets commonly used by vendors. The system will never send requests on the network without a clear configuration made by the user. It is possible to schedule requests at a pre-defined frequency.


Discovered devices' responses will depend on the protocol implemented by the manufacturer and the user configuration. Except for what is clearly stated in this documentation, no specific configuration is required on discovered devices. Devices may give an answer by default, but it can vary in the field depending on the configuration.

This annex gives examples of the packets used by Cisco Cyber Vision to discover devices and of typical answers the user can expect.

- [BACnet, on page 2](#)
- [DNP3, on page 3](#)
- [EtherNet/IP, on page 3](#)
- [Melsec, on page 8](#)
- [Modbus, on page 9](#)
- [OMRON, on page 10](#)
- [Profinet Multicast, on page 10](#)
- [S7 Broadcast, on page 11](#)
- [S7 Unicast, on page 12](#)
- [S7Plus, on page 13](#)
- [ICMPv6 Multicast, on page 14](#)
- [SNMP Unicast, on page 14](#)
- [WMI, on page 22](#)

BACnet

Device



192.168.30.194
BacNet ▲ None
IP: 192.168.30.194
MAC: 00:a0:03:f5:6d:56

[Edit](#) | [Manage group](#)

First activity
Jan 30, 2024 9:34:55 AM

Last activity
Jan 30, 2024 9:34:55 AM

Tags

- Controller
- Active Discovery BACnet

1
Activity

3
Events

7
Vulnerabilities

-
Credential

-
Variable

-
External Comm.

Basics
Risk score
Security
Activity
Automation

Properties
Components
Tags

Properties

Normalized Properties

fw-version: FW=01.21.67.272;WPC=1.8.22;SVS=300.8;SBC=13.23;

ip: 192.168.30.194

mac: 00:a0:03:f5:6d:56

model-name: PXM40.E

name: 192.168.30.194

project-version: AAS-20:AP=OpMon11_A.7.001;SU=SiUn;APT=OpMon11_A;APTV=7.001;

public-ip: no

vendor-name: Siemens Switzerland Ltd., I B T HVP

vlan-id: 30

Other Properties

bacnet-app-application-software-version: AAS-20:AP=OpMon11_A.7.001;SU=SiUn;APT=OpMon11_A;APTV=7.001;

bacnet-app-description: PXM40 11

bacnet-app-device-identifier: device-1

bacnet-app-device-name: PXM40

bacnet-app-firmware-revision: FW=01.21.67.272;WPC=1.8.22;SVS=300.8;SBC=13.23;

bacnet-app-location: B_01


bacnet-app-model-name: PXM40.E

name-ip: 192.168.30.194

vendor: Siemens Switzerland Ltd., I B T HVP

DNP3

Component



SEL-751
 IP: 192.168.47.40
 MAC: 00:30:a7:33:a6:1f
[Edit](#) | [Manage group](#)

First activity
Feb 1, 2024 5:31:22 PM

Last activity
Feb 5, 2024 12:19:59 PM

Tags

- ▶ Slave
- Activity tags**
- ▶ Active Discovery,
- ▶ Low Volume DNP3,
- ▶ EthernetIP

Other Properties

dnp3-device-hw-version:	751001G0X0X0
dnp3-device-id:	SEL-751
dnp3-device-location:	FEEDER RELAY
dnp3-device-manufacturer:	SEL
dnp3-device-product-name-model:	SEL751
dnp3-device-serial-number:	3230405008
dnp3-device-sw-version:	751-R302-V0-
enip-devicetype:	CipDeviceTypeGene
enip-name:	SEL-751-0
enip-serial:	a733a61f
enip-status:	SelfTesting/Unknwon
enip-vendor:	Schweitzer Engineeri
enip-version:	1.1
name-dnp3-device:	SEL-751
name-enip:	SEL-751-0
vendor:	SCHWEITZER ENGINEERING

EtherNet/IP

Ethernet/IP Active Discovery can be performed by Cisco Cyber Vision using Broadcast or Unicast mode. In any case, requests sent and component properties collected in return will be the same. The main differences will be:

- Broadcast will discover all devices in the local LAN.
- Unicast will only discover the devices and components which have an IPv4 address.
- Unicast will search for, once an EtherNet/IP node is discovered, the devices' content. If a device is a chassis with a backplane, it will be queried and all modules will send their properties.

The EtherNet/IP command used is the List Identity request (0x00063). This command will be sent to the IPv4 broadcast address or directly to an IPv4 address or to a module inside a backplane behind an IPv4 address. The result whether in Broadcast or Unicast will always be the same CIP Identity response (0x000c) with the following properties:

#	Name	Cyber Vision Properties	Example
---	------	-------------------------	---------

1	Vendor ID	enip-vendor	Rockwell Automation/Allen-Bradley
2	Device Type	enip-devicetype	ProgrammableLogicController
3	Product Code	enip-productcode	235
4	Revision	enip-version	33.012
5	Status	enip-status	AtLeastOneIOConnectionInRunMode, MinorRecoverableFault, ReservedBits12-15:0x3
6	Serial Number	enip-serial	01105356
7	Product Name	enip-name	1756-L81ES/B

EtherNet/IP Broadcast or Unicast

A Broadcast Ethernet/IP Active Discovery consists of a packet sent by the sensor which requests EtherNet/IP identities to all devices in the local LAN. For example, a sensor with an Active Discovery IPv4 address 192.168.20.192/24 will send this EtherNet/IP request to the Broadcast address, here 192.168.20.255. All devices in the IPv4 range 192.168.20.0 to 192.168.20.254 will answer with the packet described above (CIP Identity response (0x000c)).

A direct Unicast Ethernet/IP (i.e. no backplane) will consist of the same request but sent directly to the device. When a preset is configured to query EtherNet/IP devices, the system will take the list of components of this preset which have an IPv4 address. Then, the Active Discovery engine will try to reach each IPv4 with this EtherNet/IP identities request. All reachable EtherNet/IP nodes of this list will answer with the packet described above (CIP Identity response (0x000c)).

In both cases (Broadcast and Unicast), the answer will be sent by the discovered devices to the sensor's Active Discovery network interface. The answer will be a UDP packet for the Broadcast request and some TCP packets for the Unicast request.

Figure 1: Example of properties received from a Rockwell Automation EtherNet/IP communication adapter (1756-EN2T):

The screenshot displays a network flow entry for a Rockwell Automation EtherNet/IP communication adapter. The flow information includes the source IP 192.168.20.192, port 45896, and MAC 52:54:dd:61:05:d7. The destination is identified as 1756-EN2T/D with IP 192.168.20.22, port 44818, and MAC 5c88:16:efd1:2e. Activity timestamps show both first and last activity on Feb 9, 2022 at 3:00:57 PM. Tags include Active Discovery and Low Volume, with EthernetIP also noted. The Properties section lists the following details:

enip-command: ListIdentity	enip-devicetype: CommunicationsAdapter
enip-event: Equipment	enip-location: Endpoint
enip-name: 1756-EN2T/D	enip-productcode: 0xa6
enip-serial: 0114f91d	enip-status: AtLeastOneIOConnectionInRunMode
enip-status-ra-major: RUN	enip-status-ra-minor: ???
enip-vendor: Rockwell Automation/Allen-Bradley	enip-version: 11.001
ethertype: IPv4	protocol: UDP

Figure 2: Example of properties received from a Rockwell Automation EtherNet/IP safety controller (1756-L81ES):

The screenshot displays a network flow entry for a Rockwell Automation EtherNet/IP safety controller. The flow information includes the source IP 192.168.20.192, port 47928, and MAC 52:54:dd:61:05:d7. The destination is identified as 1756-L81ES/B with IP 192.168.20.25, port 44818, and MAC 5c88:16:redcc:8e. Activity timestamps show both first and last activity on Feb 15, 2022 at 4:57:25 PM. Tags include Low Volume and EthernetIP. Summary statistics show 8 Packets and 1.071 Volume. The Properties section lists the following details:

enip-command: ListIdentity	enip-devicetype: ProgrammableLogicController
enip-event: Equipment	enip-location: Endpoint
enip-name: 1756-L81ES/B	enip-productcode: 0xd3
enip-serial: 01105356	enip-status: AtLeastOneIOConnectionInRunMode, MinorRecoverableFault, ReservedBits12-15: 0x3
enip-status-ra-major: REM	enip-status-ra-minor: RUN
enip-vendor: Rockwell Automation/Allen-Bradley	enip-version: 33.012
ethertype: IPv4	protocol: TCP

Figure 3: Example of properties received from a Schneider Electric EtherNet/IP controller (TM221ME16R):

The screenshot shows a network management interface with the following details:

- Flow:** A gear icon representing a controller with IP 192.168.22.192, Port 33604, and MAC 52:54:dd:61:05:d7. It is connected to a Schneider Electric controller (TM221ME16R) with IP 192.168.22.63, Port 44818, and MAC 00:80:f4:0d:1d:04.
- Activity:** First activity on Feb 9, 2022 at 3:02:08 PM; Last activity on Feb 9, 2022 at 3:02:08 PM.
- Tags:** Active Discovery, Low Volume, EthernetIP.
- Properties Table:**

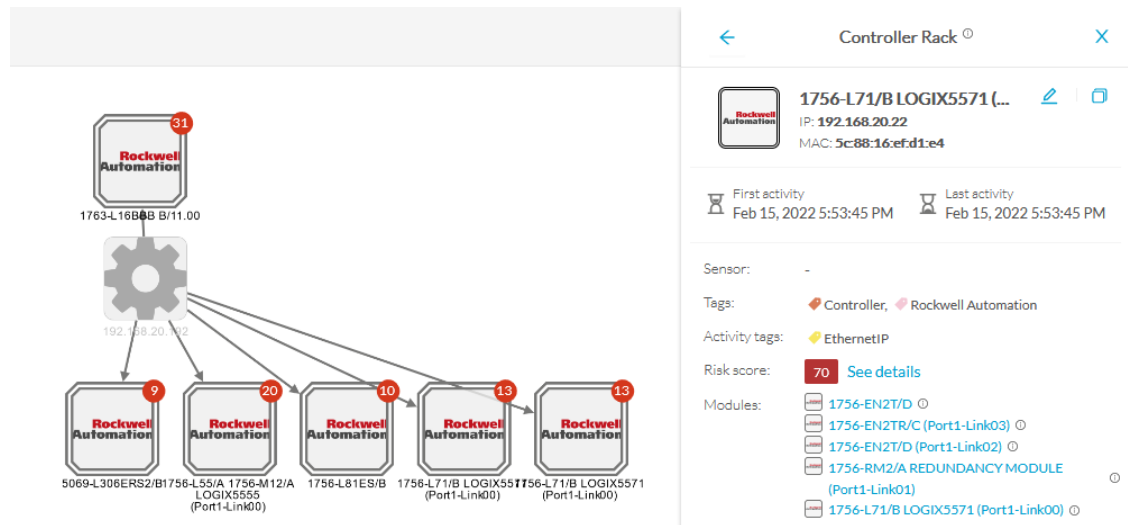
enip-command: ListIdentity	enip-devicetype: ProgrammableLogicController
enip-event: Equipment	enip-location: Endpoint
enip-name: TM221ME16R	enip-productcode: 0x1003
enip-serial: 08a48761	enip-status: Configured, AtLeastOneIOConnectionInRunMode
enip-status-ra-major: RUN	enip-status-ra-minor: ???
enip-vendor: Schneider Electric	enip-version: 1.6
ethertype: IPv4	protocol: UDP

Ethernet/IP backplane discovery

To browse backplanes, the Active Discovery policy with the Unicast EtherNet/IP protocol enabled needs to have the backplane discovery option set to enabled.

In such case, all EtherNet/IP nodes detected by Active Discovery Ethernet/IP Unicast will be queried again by the sensor. The sensor will try to know the backplane size and then send a request to the different modules (link addresses from 0 to the chassis size). All modules will then send their properties such as the product reference and the firmware version.

For example, an Ethernet/IP communication adapter with the IPv4 192.168.20.22 was first discovered. Then, all seven slots of the chassis backplane were queried. Four of them have answered back, which allowed Cisco Cyber Vision to build a Controller Rack:



A controller and a firmware version were discovered in the slot 0 of this backplane thanks to Active Discovery:

Properties

enip-cip-class: Connection Manager Object	enip-cip-request: true
enip-devicetype: ProgrammableLogicController	enip-event: Equipment
enip-location: Port1-Link00	enip-name: 1756-L71/B LOGIX5571
enip-productcode: 0x5c	enip-serial: 0115289b
enip-status: AtLeastOneIOConnectionInRunMode,ReservedBits12-15:0x3	enip-status-ra-major: REM
enip-status-ra-minor: RUN	enip-vendor: Rockwell Automation/Allen-Bradley
enip-version: 32.051	ethertype: IPv4
protocol: TCP	

Melsoft

Device



R08SF CPU

Mitsu ▲ None

IP: **192.168.24.29**

MAC: **10:4b:46:22:4a:c7**

[Edit](#) | [Manage group](#)

First activity
Jan 30, 2024 9:18:30 AM

Last activity
Jan 30, 2024 9:18:30 AM

Tags

Controller

Activity tags

Controller Info,

Active Discovery,

Mitsubishi Melsoft

- [Basics](#) [Risk score](#) [Security](#) [Activity](#)
- [Properties](#) [Components](#) [Tags](#)

Properties

Normalized Properties

fw-version: **16, 45, 03**

ip: **192.168.24.29**

mac: **10:4b:46:22:4a:c7**

model-name: **R60AD4, R08SF CPU, R65FM, R60DA4, RJ71EN71 RJ71GF11-T2**

name: **Unknown (Slot 5), RJ71GF11-T2 (Slot 2), Unknown (Slot 7), R08SF CPU, R65FM (Slot 1), R60DA4 (Slot 6), RJ71EN71(E+CCIEF (Slot 3))**

public-ip: **no**


serial-number: **4516721160010631, 00016C2611210481, 030616045C11F6010061, 16055C1180010061, 030767175021054517721760110661, 00026C1315C10031**

vendor-name: **Mitsubishi Electric Corporation**

vlan-id: **24**

Modbus

Device



BME H58 2040S
Schneider ▲ None
 IP: **192.168.22.76**
 MAC: **00:00:54:2f:fd:87**
[Edit](#) | [Manage group](#)

First activity
Jan 30, 2024 9:12:01 AM

Last activity
Jan 30, 2024 9:12:01 AM

Tags

- Controller
- Controller Info,
- Active Discovery Modbus

~ 1
Activity

-
Credential

[Basics](#)
[Risk score](#)
[Security](#)
[Activity](#)
[Automation](#)

[Properties](#)
[Components](#)
[Tags](#)

Properties

Normalized Properties

fw-version: **3.10.400**

hw-version: **16**

ip: **192.168.22.76**

mac: **00:00:54:2f:fd:87**

model-name: **BME H58 2040S**

model-ref: **BME H58 2040S**

name: **BME H58 2040S**

project-name: **Projet**

project-version: **0.0.43**

Other Properties

modbus-major-minor-revision: **v03.10**

modbus-product-code: **BME H58 2040S**

modbus-vendor-name: **Schneider Electric**

name-umas-cpu: **BME H58 2040S**

umas-engineering-station: **DESKTOP-E139G20**

umas-fw-version: **3.10.400**

umas-hardware-id: **2020d0e**

umas-hw-version: **16**

umas-libset-version: **V14.1**

OMRON

Device

192.168.45.85

Omron ▲ None

IP: **192.168.45.85**

MAC: **00:00:0a:d6:68:62**

[Edit](#) | [Manage group](#)

First activity
Jan 30, 2024 9:33:30 AM

Last activity
Jan 30, 2024 9:33:35 AM

Tags

Controller, OMRON

Activity tags

Controller Info,

Active Discovery **FINS**

Activity 1

Credential -

Basics Risk score Security Activity Automation

Properties Components Tags

Properties

Normalized Properties

fw-version: **1.41.02**

ip: **192.168.45.85**

mac: **00:00:0a:d6:68:62**

model-name: **NX1P2-9024DT1**

name: **192.168.45.85**

public-ip: **no**

serial-number: **7444**

vendor-name: **OMRON TATEISI ELECTRONICS CO.**

vlan-id: **45**

Other Properties

name-ip: **192.168.45.85**

omron-lot-id: **--- 29720**

omron-model: **NX1P2-9024DT1**

omron-serial: **7444**

omron-version: **1.41.02**

vendor: **OMRON TATEISI ELECTRONICS CO.**

Profinet Multicast

Cisco Cyber Vision Active Discovery can use a Profinet DCP service called Identify Request. This request will be sent by the sensor interfaces defined for Active Discovery. All Profinet devices will answer with a specific Profinet DCP identify response packet.

The request is sent by the sensor MAC address to a specific Ethernet Multicast address: 01:0e:cf:00:00:00. This Profinet DCP Multicast address will allow Cisco Cyber Vision to join all Profinet nodes on the local LAN. The answer of each node will be a specific Profinet DCP packet sent to the sensor MAC address.

The information collected are:

- The IP address + mask.
- The Manufacturer name.
- The name of the station.

Figure 4: For example, a Siemens S7-1500 controller:

Flow

52:54:dd:61:05:d7
IP: -
MAC: 52:54:dd:61:05:d7

SIEMENS

s7-1500rxrh-systemxb1.p...
IP: 192.168.21.50
MAC: ac:64:17:a6:37:54

First activity
Feb 16, 2022 1:19:01 PM

Last activity
Feb 16, 2022 1:19:22 PM

Tags
Active Discovery,
Profinet, Profinet DCP

Basics

Properties Content Statistics Tags

Properties

ethertype: PROFINET	profinetdcp-devicegw: 192.168.21.254
profinetdcp-deviceip: 192.168.21.50	profinetdcp-devicenetmask: 255.255.255.0
profinetdcp-manufacturername: S7-1500	profinetdcp-nameofstation: s7-1500rxrh-systemxb1.plcxb1.profinetxainterfacexb23431
profinetdcp-service-id: Identify	protocol:

S7 Broadcast

Cyber Vision Active Discovery can use a request on the protocol S7 discovery with a command: "identification". This request will be sent by the sensor interfaces defined for Active Discovery. All S7 devices will answer with a specific S7 Discovery identification response packet.

The request is sent by the sensor MAC address to the Ethernet broadcast address: ff:ff:ff:ff:ff:ff. The answer of each S7 protocol capable node will be a specific S7 discovery packet sent by the device MAC address to the sensor MAC address.

The information collected are:

- The model name.
- The name of the device.

Figure 5: For example, a Siemens S7-300 controller:

The screenshot displays a network flow for a Siemens SIMATIC 300 controller. The flow details are as follows:

Device	MAC	IP	Activity
Source	52:54:dd:c1:f1:ed	-	First activity: Feb 16, 2022 2:19:50 PM
Destination	52:54:dd:c1:f1:ed	-	Last activity: Feb 16, 2022 2:20:10 PM
Device	-	-	Tags: Active Discovery, S7Discovery

The 'Properties' section contains the following details:

ethertype: LLC	protocol:
s7discovery-command: identification	s7discovery-devicename: SIMATIC 300
s7discovery-model: S7-300 CP	s7discovery-type: response
snap-org-code: 0x080006	snap-org-name: Siemens
snap-protocol-id: 0x1fd	

S7 Unicast

The Active Discovery engine uses a specific S7 Unicast command to request properties from S7-compatible devices, such as:

- Hardware reference
- Firmware version

Basics Security Activity Automation


Properties Tags Sensors

Properties

Normalized Properties	Other Properties
fw-version: V 2.2.0	name-profinet: project-s7-1200
hw-version: 1	profinetdcp-devicerole: IO-Controller
ip: 192.168.21.41	profinetdcp-manufacturer-specific: S7-1200
mac: 00:1c:06:00:88:19	s7-fwver: V 2.2.0
model-ref: 6ES7 214-1AE30-0XB0	s7-hwref: 6ES7 214-1AE30-0XB0
name: project-s7-1200	s7-hwver: 1
public-ip: no	s7-moduleref: 6ES7 214-1AE30-0XB0
vendor-name: Siemens Numerical Control Ltd., Nanjing	s7-modulever: 1
	s7-rack: 0
	s7-slot: 0
	vendor: Siemens Numerical Control Ltd., Nanjing

S7Plus

Device



PLC_2

Siemens ▲ None

IP: 192.168.21.50

MAC: ac:64:17:a6:37:54

[Edit](#) | [Manage group](#)

First activity
Jan 30, 2024 8:59:41 AM

Last activity
Jan 30, 2024 10:45:22 AM

Tags

- Controller
- Activity tags
- Active Discovery,
- Profinet, Profinet DCP,
- S7 S7Plus

Other Properties

ComponentType: virtual
cotp-dst-tsap: SIMATIC-ROOT-ES, 101
name-s7-plc: PLC_2
profinetdcp-manufacturer-specific: S7-1500
profinetdcp-nameofstation: s7-1500rxrh-systemxb1.plcxb1.profinetxainte
s7-fwver: V 2.9.4
s7-hwver: 1
s7-modulename: PLC_2
s7-moduleref: 6ES7 515-2RM00-0AB0
s7-plcname: PLC_2
s7-rack: 0
s7-serialnumber: S C-M6DA37162020
s7-slot: 0, 1
s7plus-moduleref: 6ES7 515-2RM00-0AB0
vendor: Siemens AG

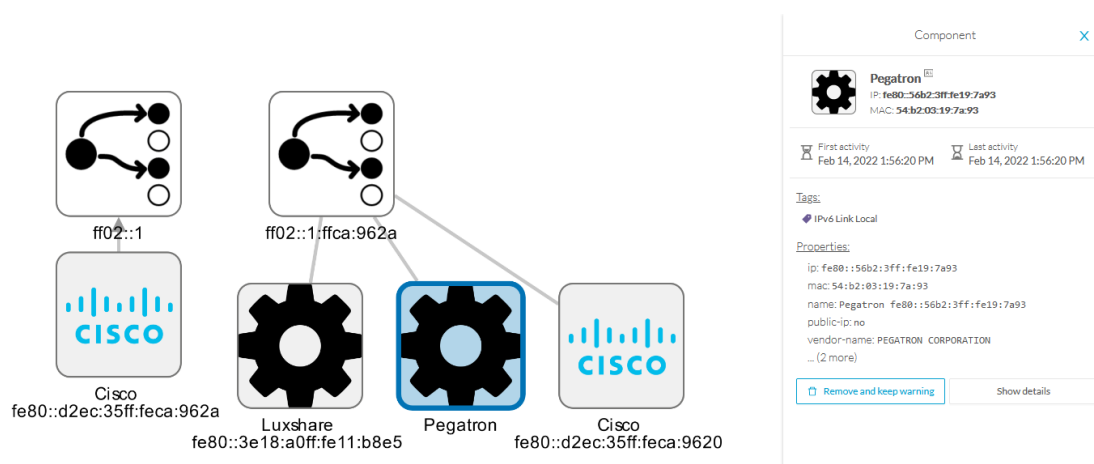
ICMPv6 Multicast

For the ICMPv6 Active Discovery protocol, the Cisco Cyber Vision sensor will use an ICMPv6 Echo request (ping) to the all-nodes link-local scope multicast address. The sensor will thus ping all IPv6 nodes on the local link. All reachable nodes will answer back with their link-local IPv6 address and their MAC address.

Cisco Cyber Vision sensors use a specific ICMPv6 packet, echo request (type 128) to the address `ff02::1` (All nodes on the local network segment) with a hop limit of 1.

The different nodes will answer with a ICMPv6 Neighbor solicitation (type 135) to the Solicited-Node Multicast address which has the form `ff02::1::ff` with the least-significant 24 bits of the sensor IPv6 Unicast address.

Figure 6: For example, a sensor with IPv6: `fe80::d2ec:35ff:feca:962a` is requesting `ff02::1`. Three different devices are answering back:



SNMP Unicast

Cisco Cyber Vision sensor can use the SNMP protocol to collect network devices information.

SNMP Active Discovery results highly depend on the configuration, type and version of the queried devices. Some devices might respond without any specific configuration, others might need complex configurations, and others not respond at all.

While doing SNMP Active Discovery, the sensor will try to read some generic and vendor-specific values. The generic values will be used by the sensor to build extra queries based on vendors and hardware models.

Generic values collected are:

Property	Description
snmp-sys-descr	Description
snmp-sys-name	Name

The Cisco Cyber Vision sensor Active Discovery supports:

- SNMP Version 2c (SNMPv2c) with a fallback in SNMP Version 1 (SNMPv1).

- SNMP Version 3 (SNMPv3).

SNMPv3 Active Discovery is able to provide authentication and encryption.

All SNMP versions will give the same results in the Cisco Cyber Vision application. They are important regarding data access. The subsequent section describes the SNMP results with different types of network devices.

AD SNMP with Schneider PLC

The Cisco Cyber Vision SNMP Active Discovery with Schneider Electric PLC requests generic values (snmp-sys-descr and snmp-sys-name).

Typical results with nodes where SNMP is enabled by default are:

The screenshot displays two examples of SNMP Active Discovery results for Schneider PLC devices. Each example includes a 'Flow' summary and a 'Properties' section.


Example 1: BMEP581020

- Flow Summary:** IP: 192.168.22.192, Port: 58600, MAC: 52:54:dd:61:05:d7. Device: BMEP581020, IP: 192.168.22.70, Port: 161, MAC: 00:80:14:29:27:2a. First activity: Feb 16, 2022 4:31:20 PM. Last activity: Feb 16, 2022 4:31:20 PM. Tags: Net Management, Active Discovery, SNMP.
- Properties:**
 - ethertype: IPv4
 - protocol: UDP
 - snmp-command: get-request
 - snmp-community: public
 - snmp-sys-descr: Modicon M580 - P58 1020 Processor - DIO
 - snmp-sys-name: BMEP581020
 - snmp-sys-objectid: 1.3.6.1.4.1.3833.1.7.255.46
 - snmp-sys-services: 74
 - snmp-version: v2c


Example 2: BMENOC0301

- Flow Summary:** IP: 192.168.22.192, Port: 36281, MAC: 52:54:dd:61:05:d7. Device: BMENOC0301, IP: 192.168.22.74, Port: 161, MAC: 00:00:54:30:10:89. First activity: Feb 16, 2022 4:31:30 PM. Last activity: Feb 16, 2022 4:31:31 PM. Tags: Net Management, Active Discovery, SNMP.
- Properties:**
 - ethertype: IPv4
 - protocol: UDP
 - snmp-command: get-request
 - snmp-community: public
 - snmp-sys-descr: Product: BMENOC0301 - Ethernet Communication Module, FwId 02.16
 - snmp-sys-name: BMENOC0301
 - snmp-sys-objectid: 1.3.6.1.4.1.3833.1.7.255.53
 - snmp-sys-services: 74
 - snmp-version: v2c

Flow



192.168.22.192
IP: 192.168.22.192
Port: 33685
MAC: 52:54:00:61:05:d7



TM262-15
IP: 192.168.22.73
Port: 161
MAC: 00:80:14:4e:86:f5

First activity
Feb 16, 2022 4:30:49 PM

Last activity
Feb 16, 2022 4:30:49 PM

Tags

- Net Management,
- Active Discovery, SNMP

Basics

Properties Content Statistics Tags

Properties


ethertype: IPv4	protocol: UDP
snmp-command: getBulkRequest	snmp-community: public
snmp-sys-descr: SCHNEIDER M262 Fast Ethernet TCP/IP	snmp-sys-name: TM262-15
snmp-sys-objectid: 1.3.6.1.4.1.3833.1.7.255.44	snmp-sys-services: 4
snmp-version: v2c	

AD SNMP with Siemens PLC


The Cisco Cyber Vision SNMP Active Discovery with Siemens PLC requests generic values (snmp-sys-descr and snmp-sys-name).

Typical results with nodes where SNMP is enabled by default are:

Flow



192.168.21.192
IP: 192.168.21.192
Port: 48006
MAC: 52:54:00:61:05:d7



project-s7-1200
IP: 192.168.21.41
Port: 161
MAC: 00:1c:06:00:88:19

First activity
Feb 16, 2022 4:18:30 PM

Last activity
Feb 16, 2022 4:18:30 PM

Tags

- Net Management,
- Active Discovery, SNMP


Basics

Properties Content Statistics Tags


Properties

ethertype: IPv4	protocol: UDP
snmp-command: get-request	snmp-community: public
snmp-sys-descr: Siemens, SIMATIC S7, CPU-1200, 6ES7 214-1AE30-0XB0, HW: 1, FW: V.2.2.0, SZVX7YYW002898	snmp-sys-objectid: 0.0
snmp-sys-services: 76	snmp-version: version-1

Flow



192.168.21.192
IP: 192.168.21.192
Port: 35904
MAC: 52:54:00:61:05:d7



cpu1512-sp
IP: 192.168.21.46
Port: 161
MAC: ac:64:17:81:21:3c

First activity
Feb 16, 2022 4:18:50 PM

Last activity
Feb 16, 2022 4:18:50 PM

Tags

- ◆ Net Management,
- ◆ Active Discovery, ◆ SNMP

Basics

Properties Content Statistics Tags

Properties


ethertype: IPv4	protocol: UDP
snmp-command: get-request	snmp-community: public
snmp-sys-descr: Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019	snmp-sys-objectid: 0.0
snmp-sys-services: 78	snmp-version: version-1

AD SNMP with Rockwell PLC


The Cisco Cyber Vision SNMP Active Discovery with Rockwell Automation PLC requests generic values (snmp-sys-descr and snmp-sys-name).

Typical results with nodes where SNMP is enabled by default are:

Flow



192.168.20.192
IP: 192.168.20.192
Port: 40265
MAC: 52:54:00:61:05:d7



1756-ENBT/A
IP: 192.168.20.20
Port: 161
MAC: 00:00:bc:5f:bc:ce

First activity
Feb 16, 2022 4:09:20 PM

Last activity
Feb 16, 2022 4:09:20 PM

Tags

- ◆ Net Management,
- ◆ Active Discovery, ◆ SNMP

Basics

Properties Content Statistics Tags

Properties

ethertype: IPv4	protocol: UDP
snmp-command: get-request	snmp-community: public
snmp-sys-descr: Rockwell Automation 1756-ENBT	snmp-sys-objectid: 1.3.6.1.4.1.95.1.12
snmp-sys-services: 79	snmp-version: v2c

AD SNMP with Moxa switches

The Cisco Cyber Vision SNMP Active Discovery with Moxa switches requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-moxapriv-model-name	Model

snmp-moxapriv-fw-version	Firmware version
--------------------------	------------------

Typical results with nodes where SNMP is enabled by default are:

The screenshot displays two nodes in a network management interface. Each node has a 'Flow' header and a 'Properties' section. The first node is a 'Managed Redundant Switch' with IP 192.168.0.192 and port 36552. The second node is a 'Moxa' switch with IP 192.168.0.28 and port 48394. Both nodes show 'snmp-moxapriv-fw-version' in their properties.

Node 1: Managed Redundant Switch

- IP: 192.168.0.192
- Port: 36552
- MAC: 52:54:dd:c1:f1:ed
- snmp-community: public
- snmp-moxapriv-fw-version-raw: V2.7
- snmp-moxapriv-model-name: EDS-405A-SS-SC
- snmp-sys-descr: MOXA EDS-405A-SS-SC
- snmp-sys-name: Managed Redundant Switch 09866
- snmp-sys-objectid: 1.3.6.1.4.1.8691.7.6
- snmp-sys-services: 2
- snmp-version: v2c

Node 2: Moxa 192.168.0.28

- IP: 192.168.0.28
- Port: 48394
- MAC: 00:90:e8:5c:f9:84
- snmp-community: public
- snmp-moxapriv-fw-version-raw: V5.1.12 build 17072518
- snmp-moxapriv-model-name: EDS-G508E
- snmp-sys-descr: EDS-G508E
- snmp-sys-objectid: 1.3.6.1.4.1.8691.7.69
- snmp-sys-services: 2
- snmp-version: v2c

AD SNMP with Siemens Switches

The Cisco Cyber Vision SNMP Active Discovery with Siemens switches requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-siemens-scalence-model-ref	Model
snmp-siemens-scalence-model-version	Firmware version

Typical results with nodes where SNMP is enabled by default are:

Flow

192.168.0.192
IP: 192.168.0.192
Port: 43342
MAC: 52:54:dd:c1:f1:ed

SIEMENS SCALANCE X-300
IP: 192.168.0.35
Port: 161
MAC: 00:0e:8c:9a:d9:2c

First activity
Feb 16, 2022 4:23:20 PM

Last activity
Feb 16, 2022 4:23:21 PM

Tags
Net Management,
Active Discovery, SNMP

Basics

Properties Content Statistics Tags

Properties

ethertype: IPv4 protocol: UDP

snmp-command: getBulkRequest snmp-community: public

snmp-siemens-scalence-model-ref: 6GK5 308-2FL00-2AA3 snmp-siemens-scalence-model-version: V2.2.0

snmp-sys-descr: SCALANCE X-300 snmp-sys-name: S10-4-S

snmp-sys-objectid: 1.3.6.1.4.1.4196.1.1.5.4 snmp-sys-services: 14

snmp-version: v2c

AD SNMP with Hirschmann hardware

The Cisco Cyber Vision SNMP Active Discovery with Hirschmann switches requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-hmpriv-mgmt-model-ref	Model
snmp-hmpriv-mgmt-fw-version	Firmware version
snmp-hm2-indus-model-ref	Model
snmp-hm2-indus-fw-version	Firmware version
snmp-hm-disc-fw-version	Model
snmp-hm-disc-model-ref	Firmware version

Typical results with nodes where SNMP is enabled by default are:

Flow

192.168.0.192
IP: 192.168.0.192
Port: 33687
MAC: 52:54:00:1c:1f:1e

BRS-646038BF9AE
IP: 192.168.0.32
Port: 161
MAC: 64:60:38:bf:f9:ae

First activity
Feb 17, 2022 11:12:15 AM

Last activity
Feb 17, 2022 11:12:15 AM

Tags
Net Management,
Active Discovery,
SNMP

100 Packets

Basics

Properties Content Statistics Tags

Properties

ethertype: IPv4 protocol: UDP

snmp-command: getBulkRequest snmp-community: public

snmp-hm-disc-fw-version-raw: H10S-25-08.5.00 2020-11-26 16:52 snmp-hm-disc-model-ref: BRS30-08040000-STCZ99HHSES

snmp-hm2-indus-fw-version: 08.5.00 snmp-hm2-indus-model-ref: BRS30-08040000-STCZ99HHSES

snmp-sys-descr: Hirschmann BOBCAT snmp-sys-name: BRS-646038BF9AE

snmp-sys-objectid: 1.3.6.1.4.1.248.11.2.1.15 snmp-sys-services: 2

snmp-version: v2c

Flow

192.168.0.192
IP: 192.168.0.192
Port: 40150
MAC: 52:54:00:1c:1f:1e

RS-58AB3C
IP: 192.168.0.31
Port: 161
MAC: ece5:55:58:ab:3c

First activity
Feb 17, 2022 11:12:15 AM

Last activity
Feb 17, 2022 11:12:15 AM

Tags
Net Management,
Active Discovery,
SNMP

1 Pack

Basics

Properties Content Statistics Tags

Properties

ethertype: IPv4 protocol: UDP

snmp-command: getBulkRequest snmp-community: public

snmp-hmpriv-mgmt-fw-version: 07.1.05 snmp-hmpriv-mgmt-model-ref: RS30-08021T1SDAEHH

snmp-sys-descr: Hirschmann Railswitch snmp-sys-name: RS-58AB3C

snmp-sys-objectid: 1.3.6.1.4.1.248.14.10.41 snmp-sys-services: 2

snmp-version: v2c

AD SNMP with Cisco hardware

The Cisco Cyber Vision SNMP Active Discovery with Cisco Hardware demands some specific configurations on the device side and requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-ent-physical-model-name	Model
snmp-ent-physical-entry	Description
snmp-ent-physical-serial-number	Serial number

snmp-probe-software-rev	Firmware version
-------------------------	------------------

Typical results with nodes where SNMP is enabled by default are:

The screenshot displays two nodes in a network management interface. Each node card shows a gear icon, IP address, port, MAC address, and a Cisco logo. The first node is labeled 'IE3300Mitsubishi.ccv' and the second is 'IE34ROCPLC.ccv'. Both nodes show activity timestamps for 'First activity' and 'Last activity' on Feb 17, 2022. The interface includes tabs for 'Basics', 'Properties', 'Content Statistics', and 'Tags'. The 'Properties' tab is selected, showing a list of attributes for each node.

Node 1: IE3300Mitsubishi.ccv

- IP: 192.168.0.192
- Port: 39933
- MAC: 52:54:00:12:1f:1e
- Protocol: UDP
- snmp-community: public
- snmp-probe-software-rev: 17.3.1
- snmp-sys-name: IE3300Mitsubishi.ccv
- snmp-sys-services: 6
- snmp-version: v2c

Node 2: IE34ROCPLC.ccv

- IP: 192.168.0.160
- Port: 37610
- MAC: 6c:71:0d:14:d4:8b
- Protocol: UDP
- snmp-community: public
- snmp-probe-software-rev: 17.4.1
- snmp-sys-name: IE34ROCPLC.ccv
- snmp-sys-services: 6
- snmp-version: v2c

AD SNMP with Microsoft Windows OS

The Cisco Cyber Vision SNMP Active Discovery with Microsoft Windows stations demands a specific operating system configuration and requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-primary-domain-name	Domain name of the machine

Typical results with nodes where SNMP is enabled by default are:

Flow

192.168.0.192
IP: 192.168.0.192
Port: 41716
MAC: 52:54:00:11:11:11

AVEVASRV
IP: 192.168.0.51
Port: 161
MAC: 00:50:56:8F:4a:3c

First activity: Feb 17, 2022 10:32:24 AM
Last activity: Feb 17, 2022 10:32:24 AM

Tags: Net Management, Active Discovery, SNMP

140 Packets

Basics

Properties Content Statistics Tags

Properties

ethertype: IPv4	protocol: UDP
snmp-command: getBulkRequest	snmp-community: public
snmp-primary-domain-name: LAB-AUTOM-CCV	snmp-sys-descr: Hardware: Intel164 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)
snmp-sys-name: AVEVASRV.lab-autom-ccv.local	snmp-sys-objectid: 1.3.6.1.4.1.311.1.1.3.1.2
snmp-sys-services: 76	snmp-version: v2c

WMI

WMI is used to collect the following Windows hosts' properties.

- wmi-caption: operating system's name and version
- wmi-kb-list: security updates installed in the host
- wmi-last-update: latest update date
- wmi-name: host name

Properties	
Normalized Properties	Other Properties
ip: 192.168.44.203	name-ip: 192.168.44.203
mac: 00:50:56:8f:12:51	vendor: VMware, Inc.
name: 192.168.44.203	wmi-caption: Microsoft Windows 10 Enterprise
os-name: Windows 10 Enterprise	wmi-kb-list: KB5012170 (Security Update)
public-ip: no	wmi-last-update: 3/8/2023
vendor-name: Microsoft Corporation	wmi-name: WMLAB1003LOC
	wmi-organization: escalation
	wmi-os-arch: 64-bit
	wmi-os-serial: 00329-00000-00003-AA417
	wmi-proc-architecture: x64
	wmi-proc-name: Intel(R) Xeon(R) Platinum 8260 CPU @ 2.40GHz
	wmi-service-pack-major-version: 0
	wmi-service-pack-minor-version: 0
	wmi-windows-build-number: 19044
	wmi-windows-sku: 4

