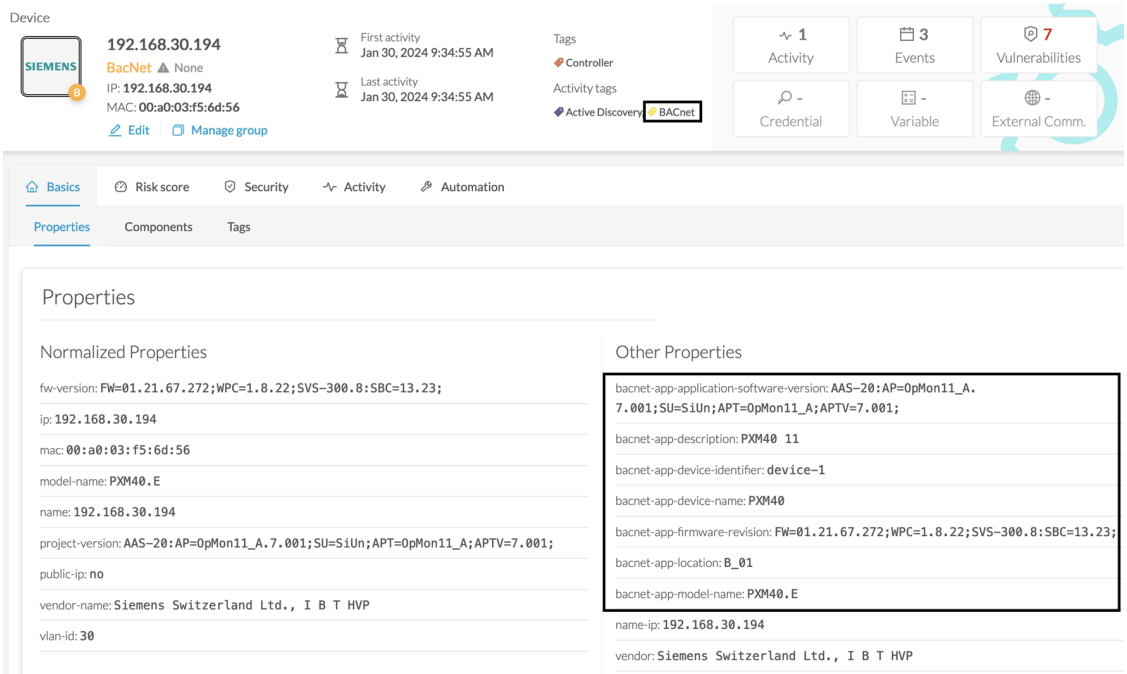
Annex: Active Discovery protocols

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.

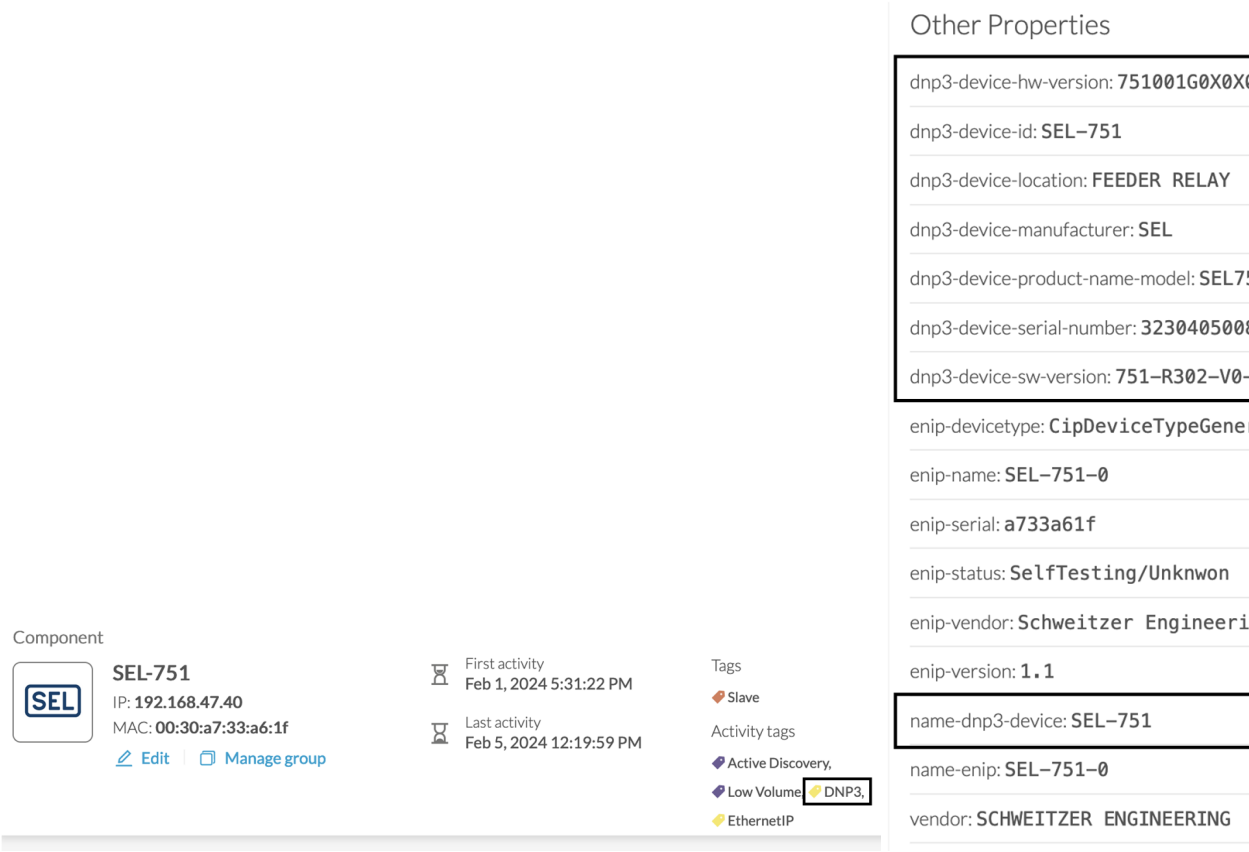
Discovered devices' responses will depend on the protocol implemented by the manufacturer and the user configuration. Except for what is clearly stated in this documentation, no specific configuration is required on discovered devices. Devices may give an answer by default, but it can vary in the field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


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
Activity tags
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



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 direclty 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):

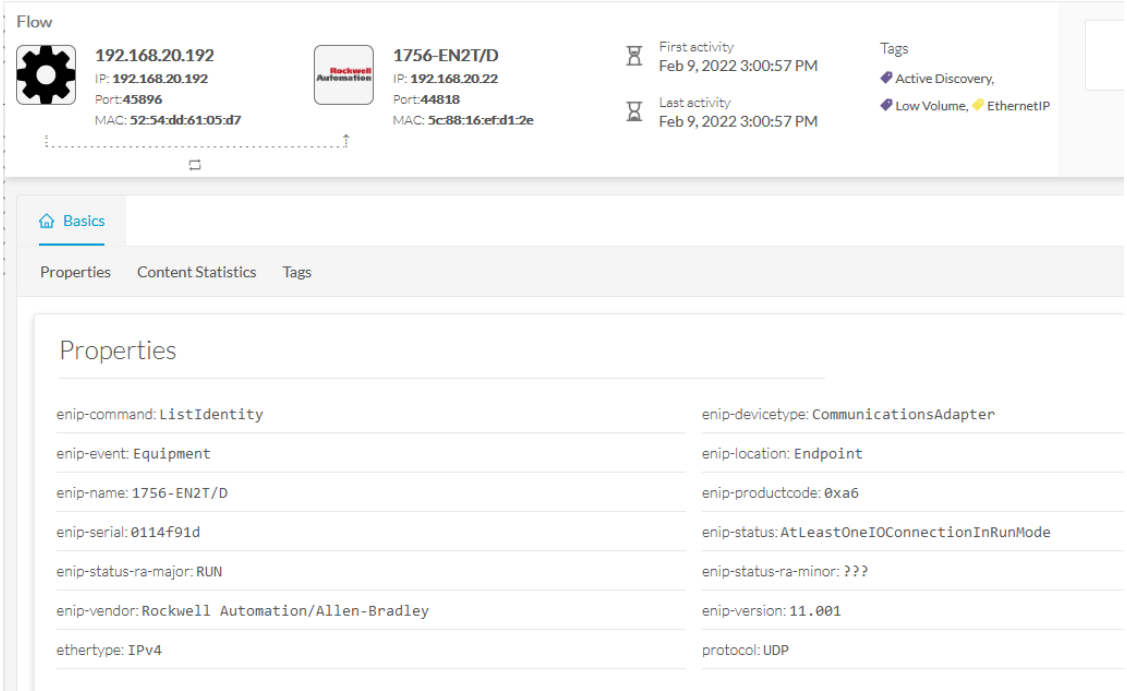


Figure 2: Example of properties received from a Rockwell Automation EtherNet/IP safety controller (1756-L81ES):

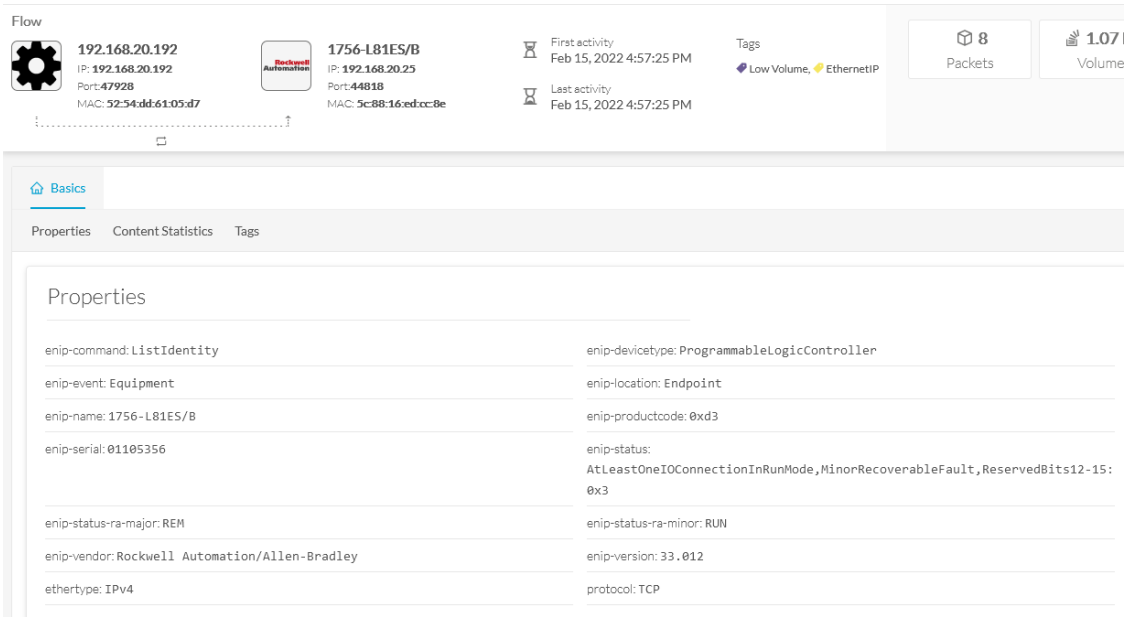
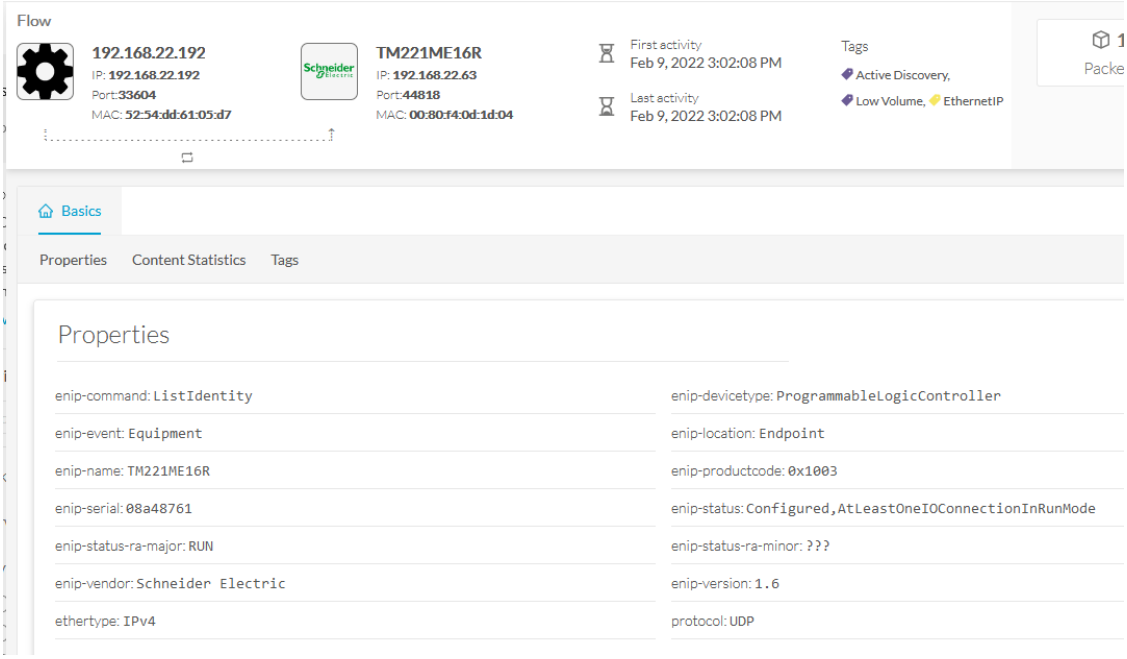


Figure 3: Example of properties received from a Schneider Eletric EtherNet/IP controller (TM221ME16R):

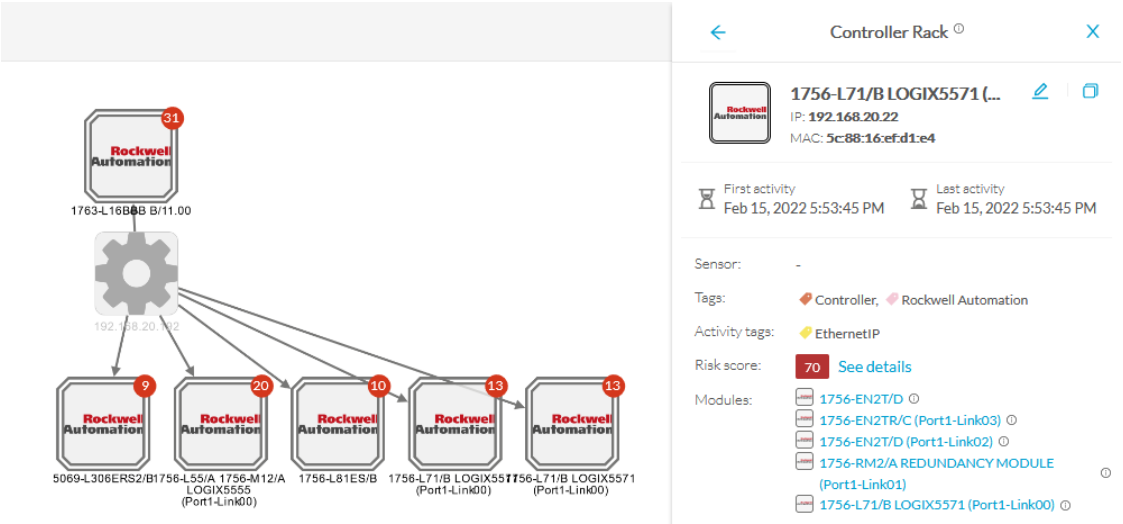


Ethernet/IP backplane discovery

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 form 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:

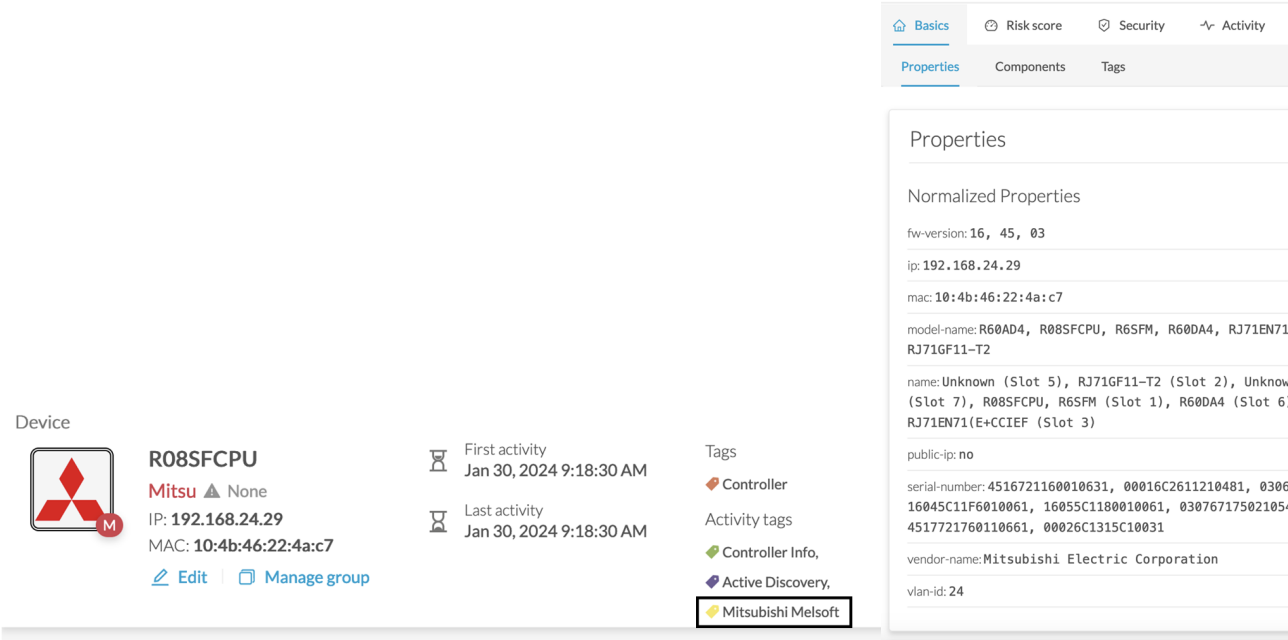


A controller and a firmware version were discovered in the slot 0 of this backplane thanks to Active Discovery:

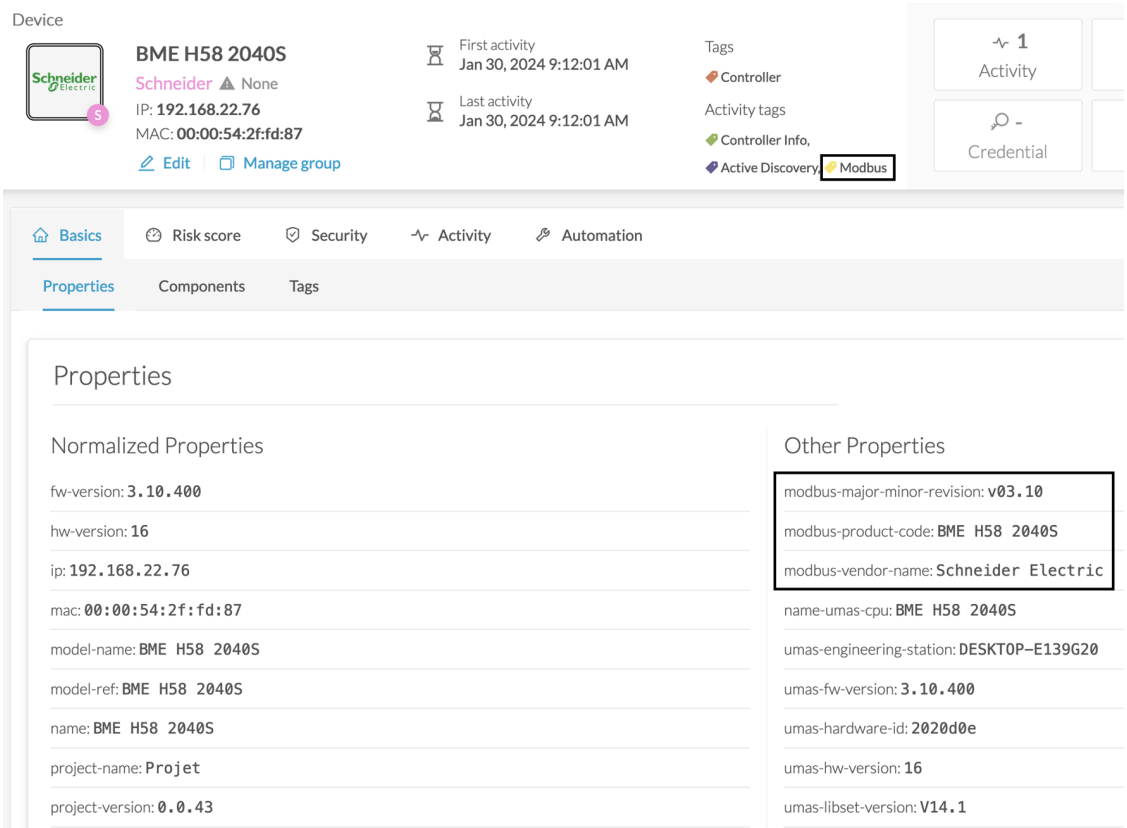
Properties

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`	

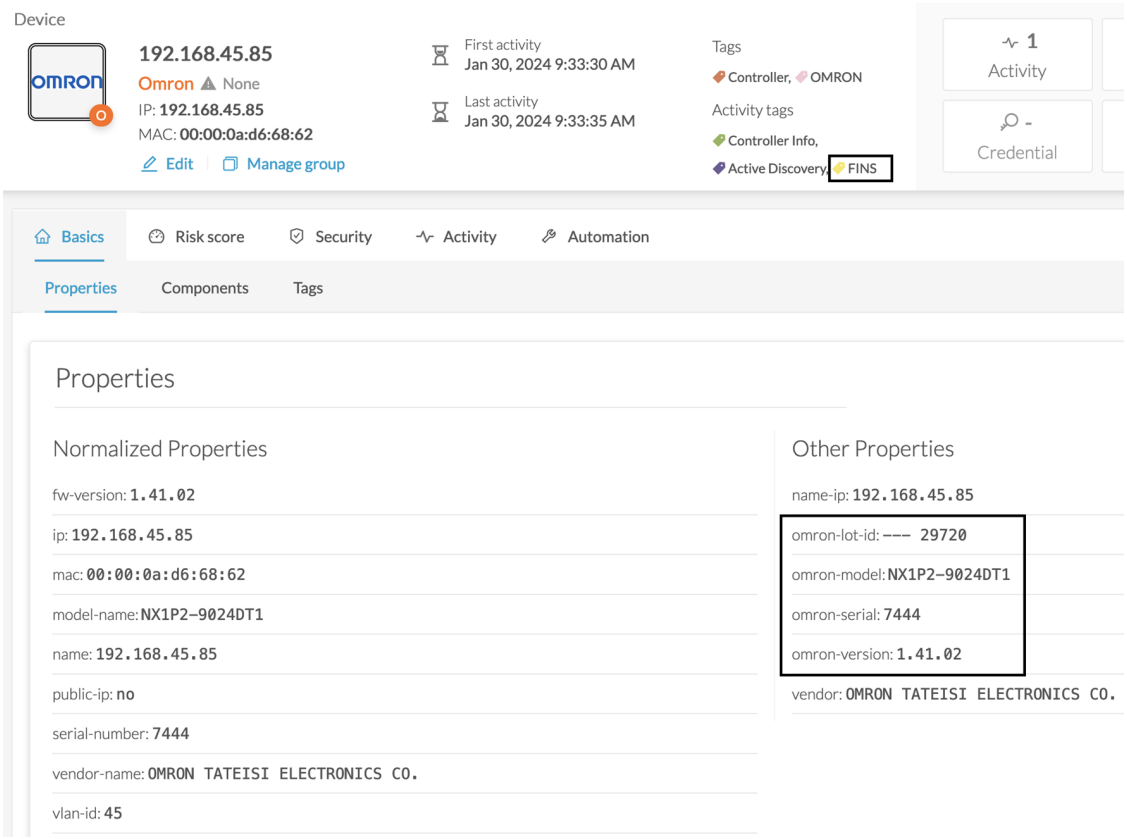
Melsoft


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, R08SFCPU, R6SFM, R60DA4, RJ71EN71
RJ71GF11-T2
name: Unknown (Slot 5), RJ71GF11-T2 (Slot 2), Unknow
(Slot 7), R08SFCPU, R6SFM (Slot 1), R60DA4 (Slot 6
RJ71EN71(E+CCIEF (Slot 3)
public-ip: no
serial-number: 4516721160010631, 00016C2611210481, 0306
16045C11F6010061, 16055C1180010061, 03076717502105
4517721760110661, 00026C1315C10031
vendor-name: Mitsubishi Electric Corporation
vlan-id: 24
Device
R08SFCPU
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

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
Activity tags
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



Profinet Multicast

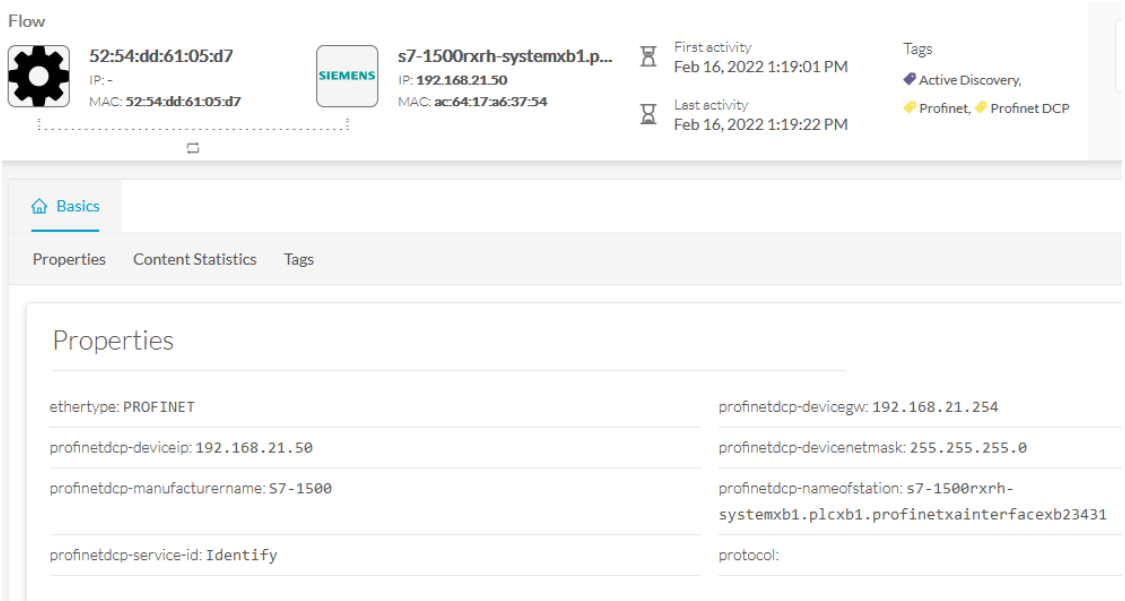
Cisco Cyber Vision Active Discovery can use a Profinet DCP service called Identify Request. This request will be sent by the sensor interfaces defined for Active Discovery. All Profinet devices will answer with a specific Profinet DCP identify response packet.

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:



S7 Broadcast

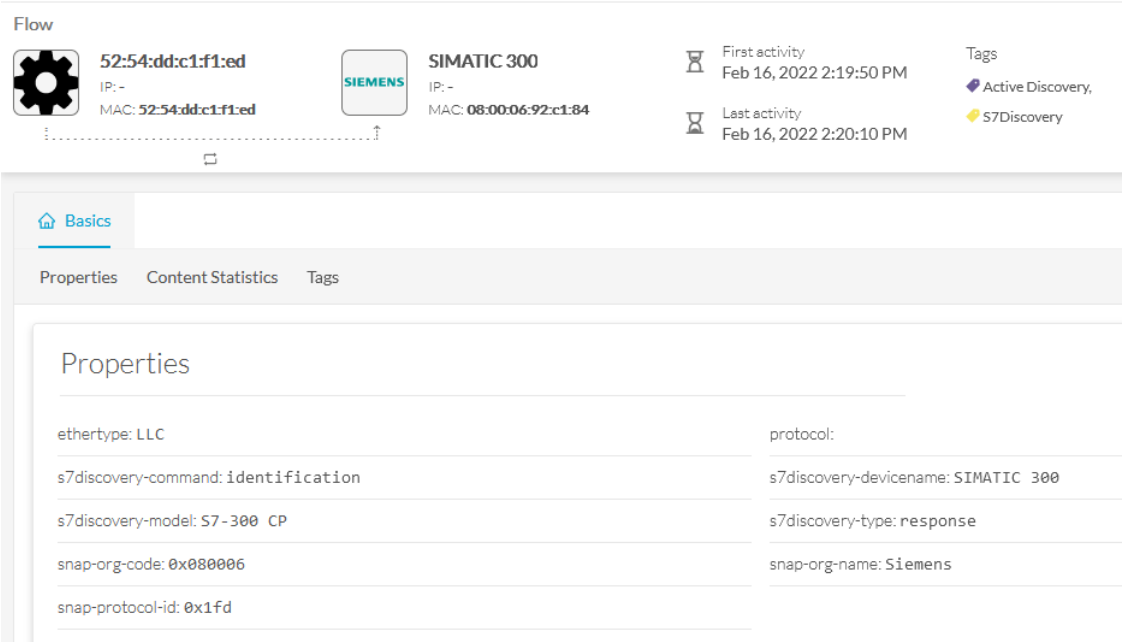
Cyber Vision Active Discovery can use a request on the protocol S7 discovery with a command: "identification". This request will be sent by the sensor interfaces defined for Active Discovery. All S7 devices will answer with a specific S7 Discovery identification response packet.

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.

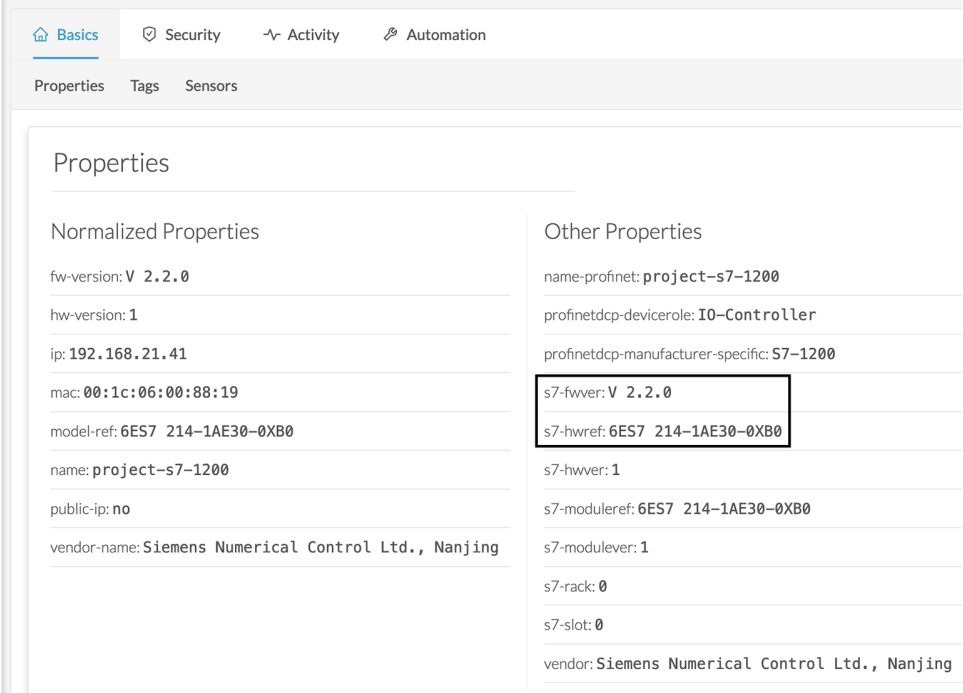
Figure 5: For example, a Siemens S7-300 controller:



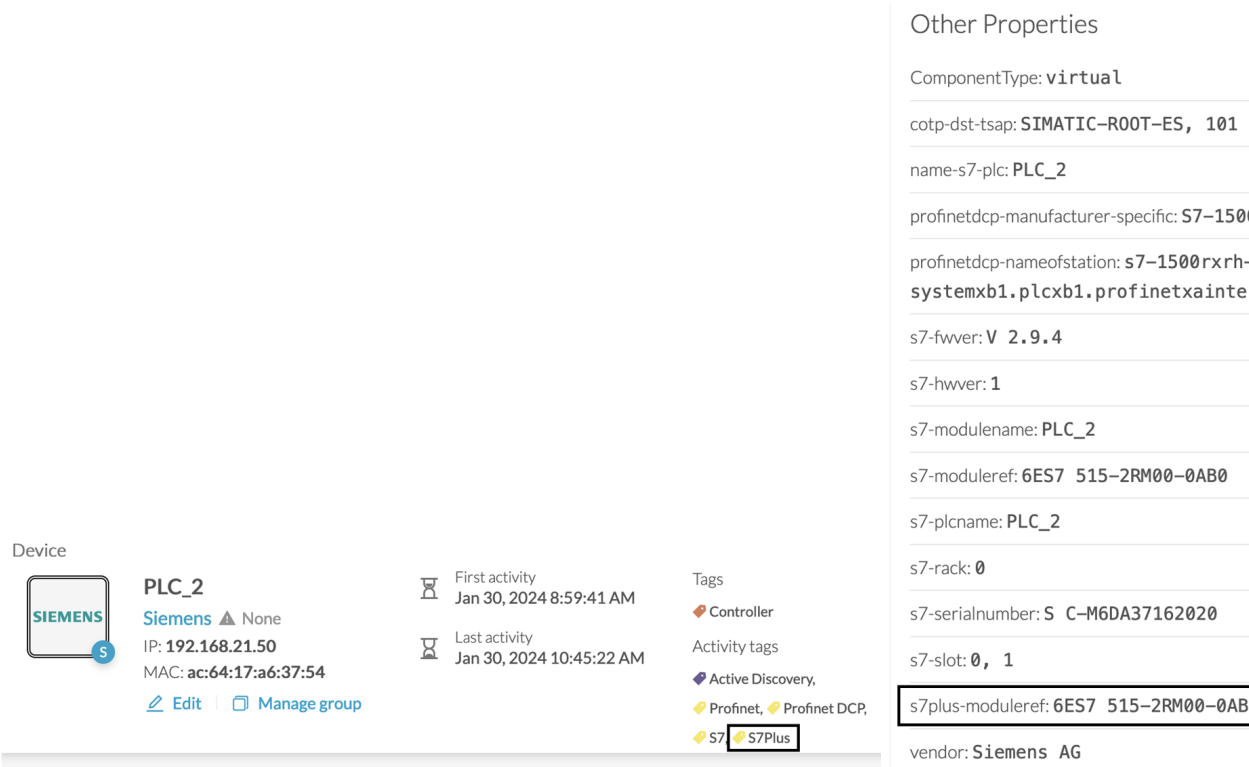
S7 Unicast

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

S7Plus


Device
SIEMENS
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: S7-150
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 515-2RM00-0AB
vendor: Siemens AG

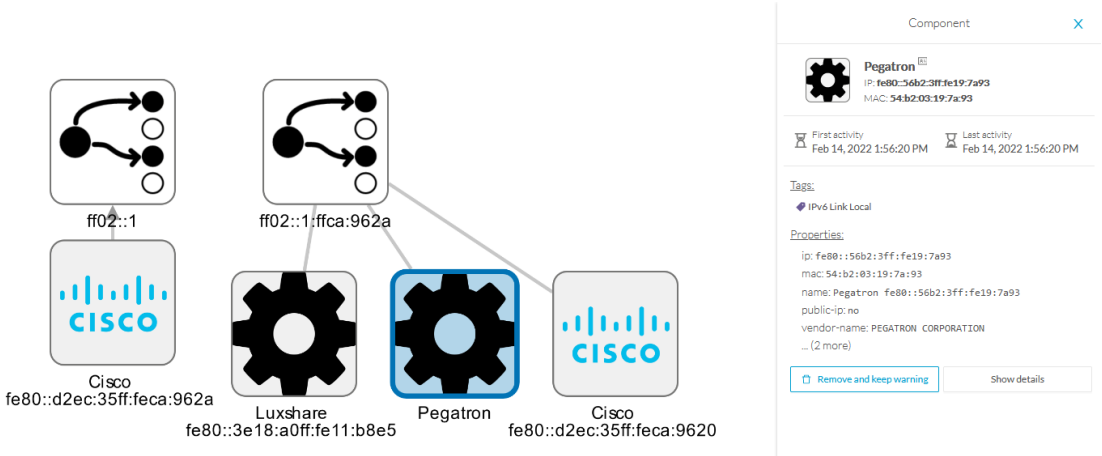
ICMPv6 Multicast

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 ff:02::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).

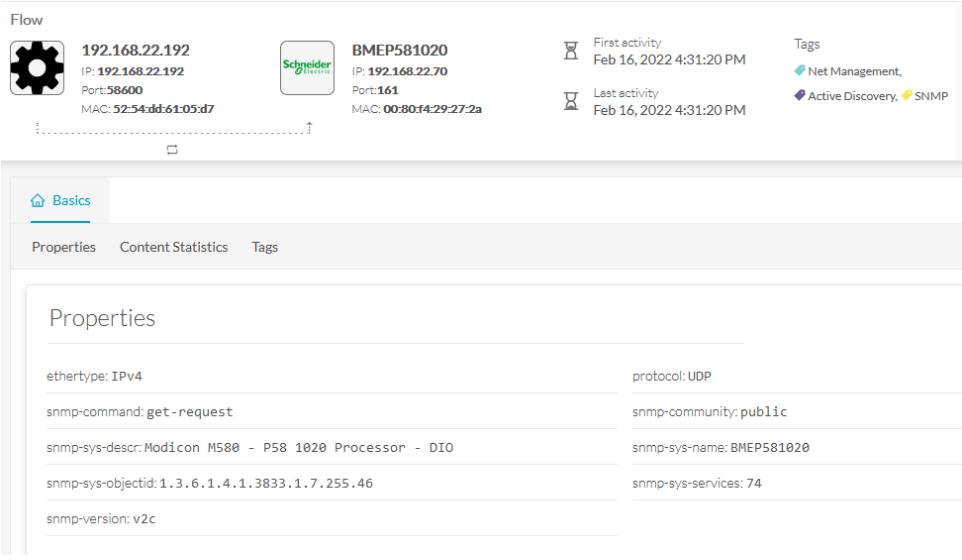
SNMPv3 Active Discovery is able to provide authentication and encryption.

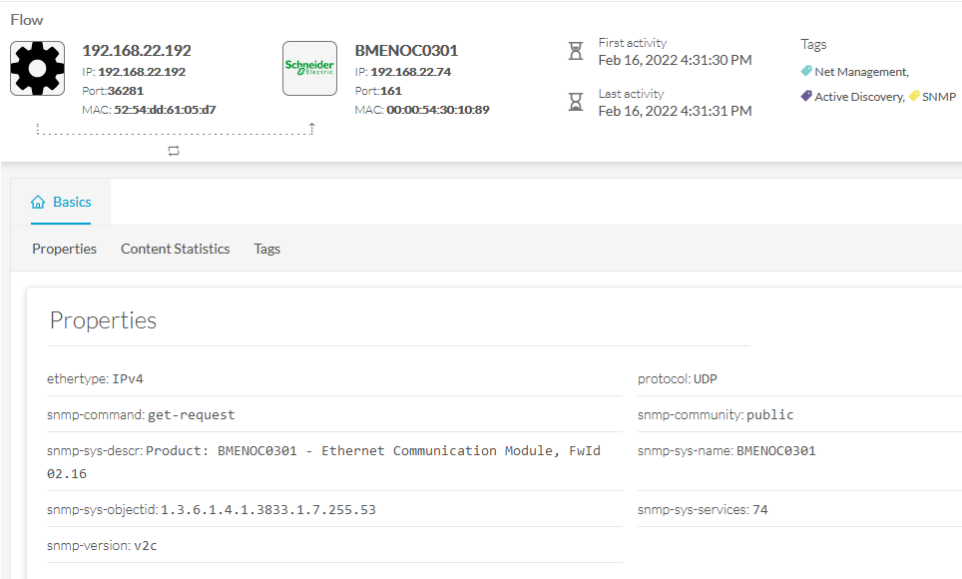
All SNMP versions will give the same results in the Cisco Cyber Vision application. They are important regarding data access. The subsequent section describes the SNMP results with different types of network devices.

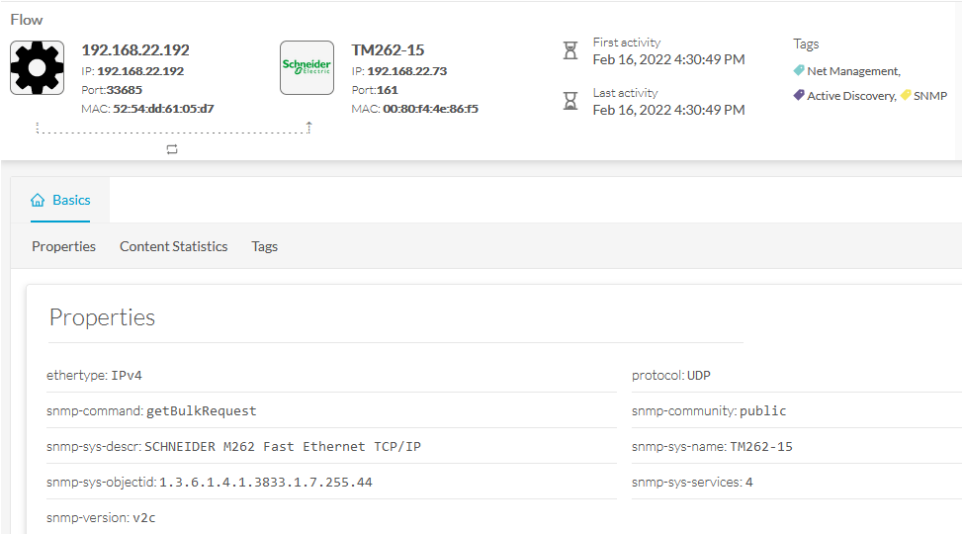
AD SNMP with Schneider PLC

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

Typcical results with nodes where SNMP is enabled by defaut are:



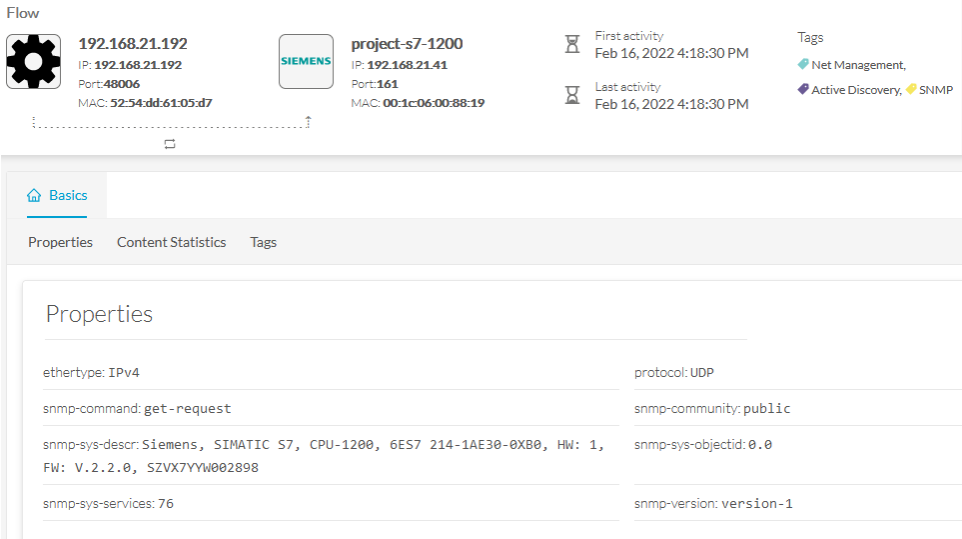


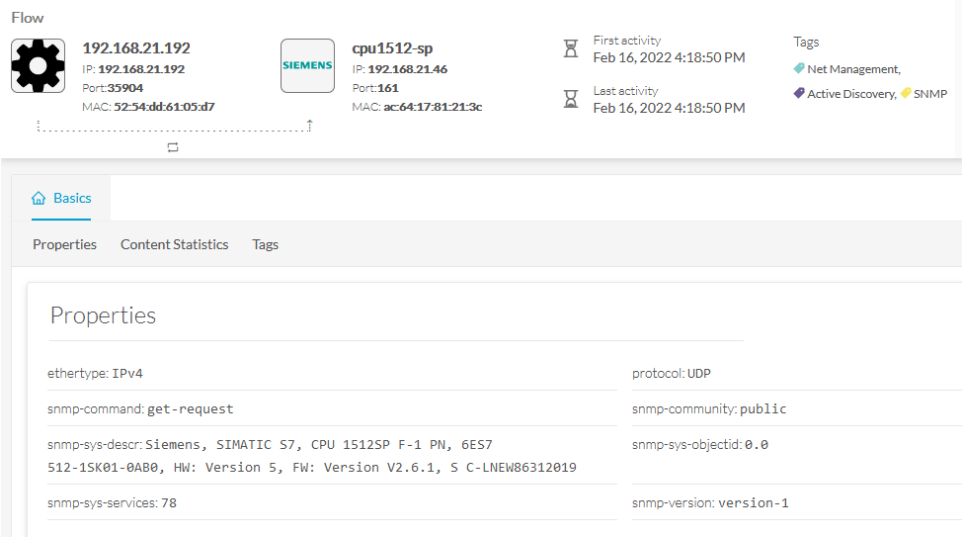


AD SNMP with Siemens PLC

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 defaut are:

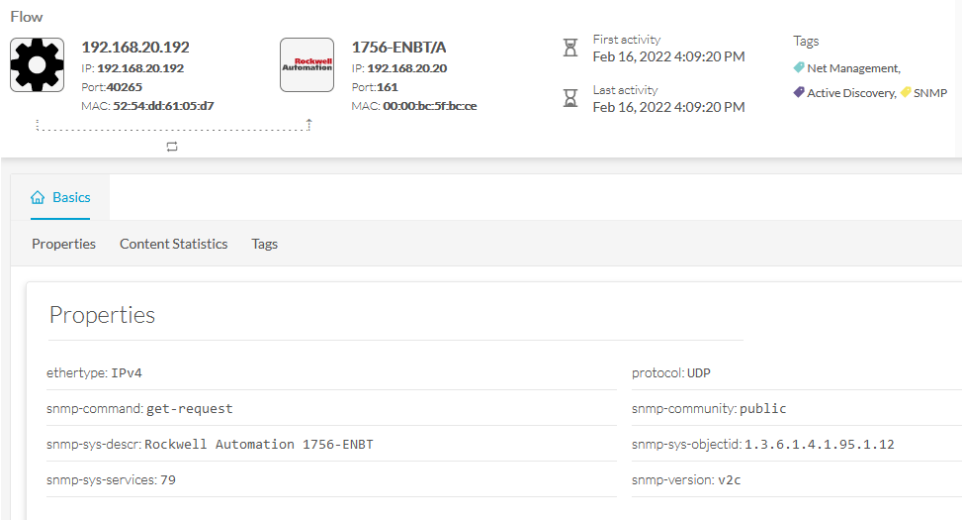




AD SNMP with Rockwell PLC

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 defaut are:



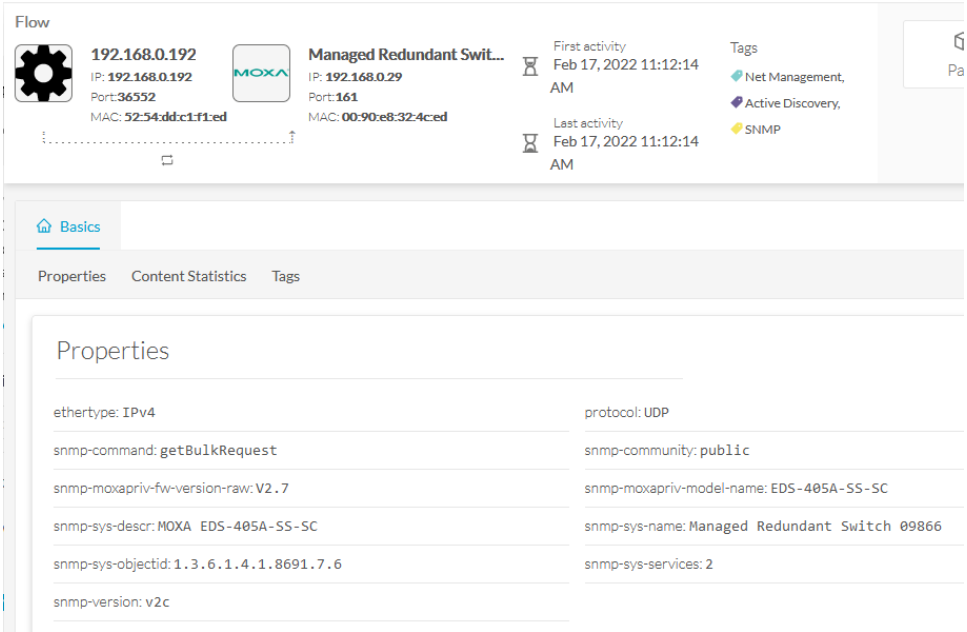
AD SNMP with Moxa switches

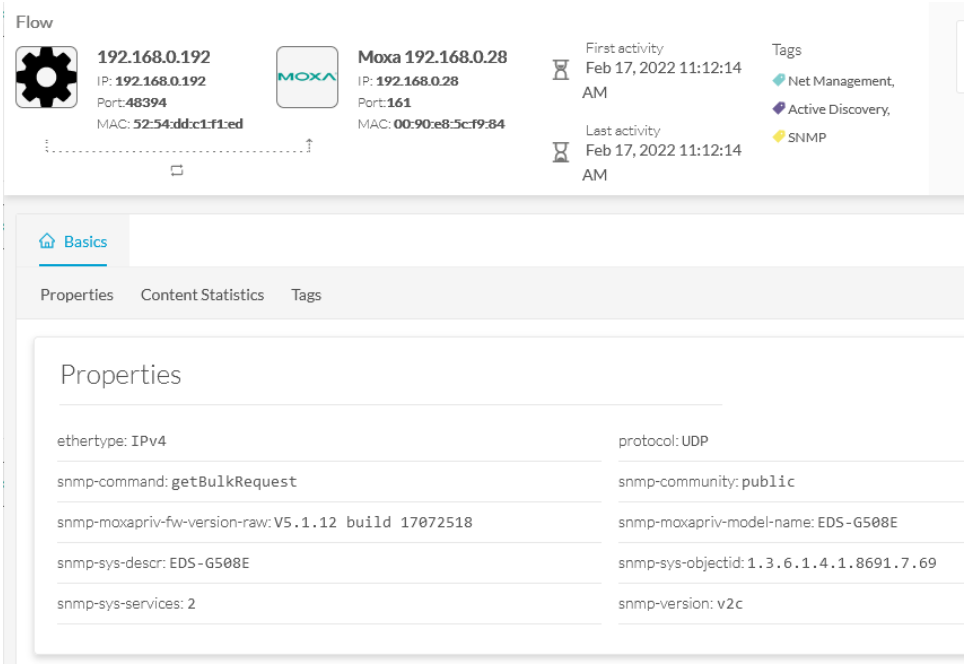
The Cisco Cyber Vision SNMP Active Discovery with Moxa switches requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-moxapriv-model-name	Model

snmp-moxapriv-fw-version	Firmware version

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



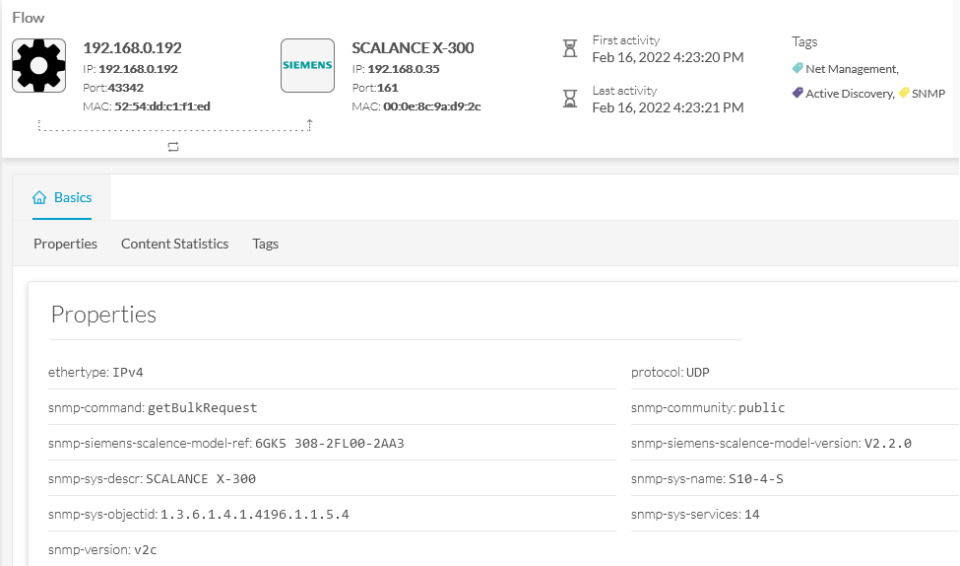


AD SNMP with Siemens Switches

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 defaut are:

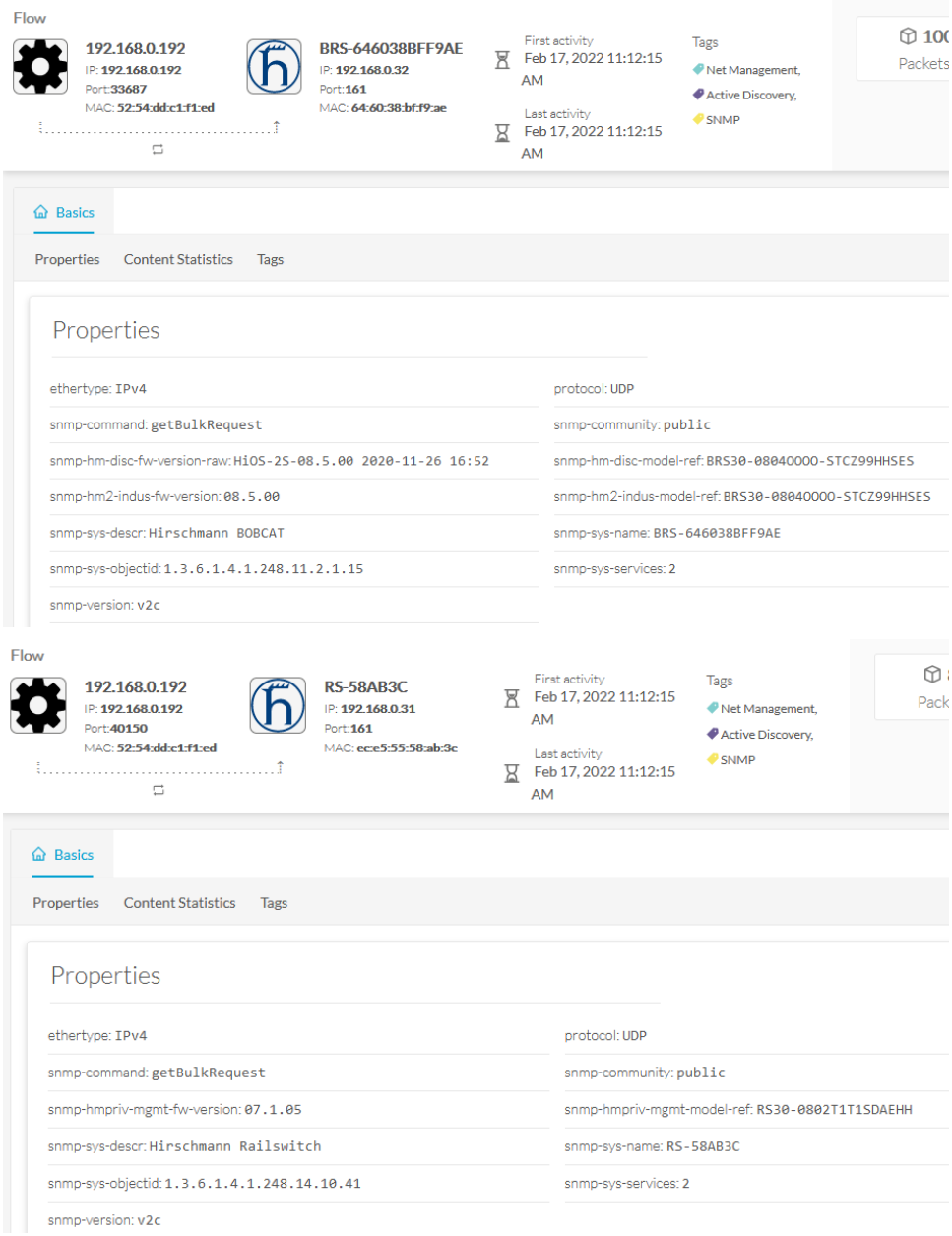


AD SNMP with Hirschmann hardware

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 defaut are:



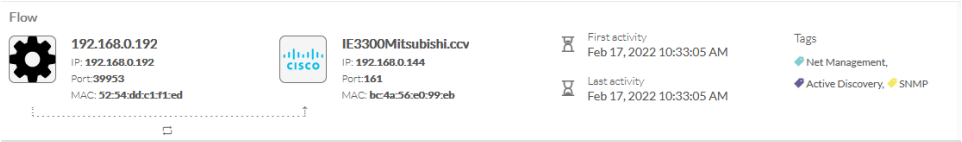
AD SNMP with Cisco hardware

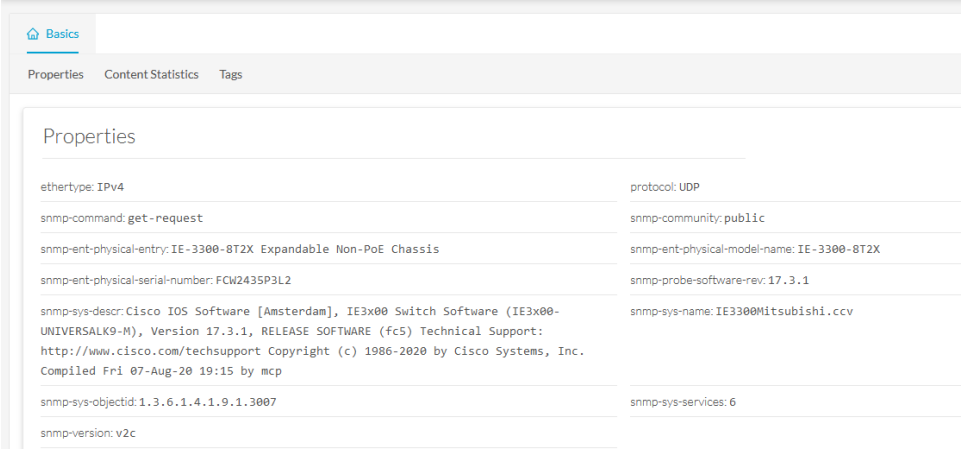
The Cisco Cyber Vision SNMP Active Discovery with Cisco Hardware demands some specific configurations on the device side and requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

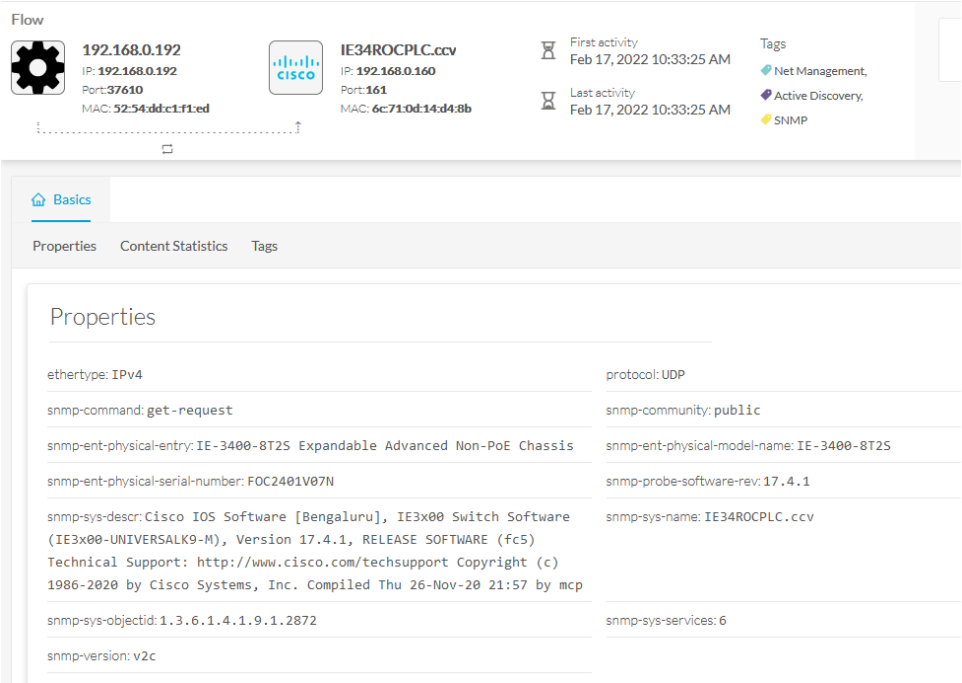
Property	Description
snmp-ent-physical-model-name	Model
snmp-ent-physical-entry	Description
snmp-ent-physical-serial-number	Serial number

snmp-probe-software-rev	Firmware version

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





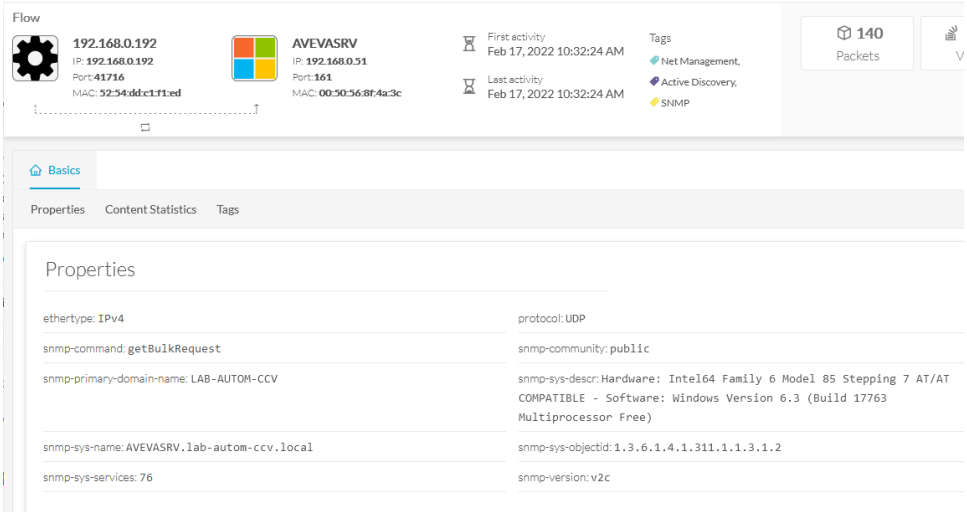


AD SNMP with Microsoft Windows OS

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 defaut are:



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

ip: `192.168.44.203`

mac: `00:50:56:8f:12:51`

name: `192.168.44.203`

os-name: `Windows 10 Enterprise`

public-ip: `no`

vendor-name: `Microsoft Corporation`

Other Properties

name-ip: `192.168.44.203`

vendor: `VMware, Inc.`

wmi-caption: `Microsoft Windows 10 Enterprise`

wmi-kb-list: `KB5012170 (Security Update)`

wmi-last-update: `3/8/2023`

wmi-name: `WMILAB1003LOC`

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`