



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.

- [EtherNet/IP, on page 1](#)
- [Profinet Multicast, on page 5](#)
- [S7 Broadcast, on page 6](#)
- [S7 Unicast, on page 7](#)
- [ICMPv6 Multicast, on page 8](#)
- [SNMP Unicast, on page 9](#)
- [WMI, on page 17](#)

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):

Flow

192.168.20.192
 IP: 192.168.20.192
 Port: 45896
 MAC: 52:54:dd:61:05:d7

1756-EN2T/D
 IP: 192.168.20.22
 Port: 44818
 MAC: 5c:88:16:ef:d1:2e

First activity: Feb 9, 2022 3:00:57 PM
 Last activity: Feb 9, 2022 3:00:57 PM

Tags: Active Discovery, Low Volume, EthernetIP

Basics

Properties Content Statistics Tags

Properties

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):

Flow

192.168.20.192
 IP: 192.168.20.192
 Port: 47928
 MAC: 52:54:dd:61:05:d7

1756-L81ES/B
 IP: 192.168.20.25
 Port: 44818
 MAC: 5c:88:16:ed:cc:8e

First activity: Feb 15, 2022 4:57:25 PM
 Last activity: Feb 15, 2022 4:57:25 PM

Tags: Low Volume, EthernetIP

8 Packets
 1.071 Volume

Basics

Properties Content Statistics Tags

Properties

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):

Properties	
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:

Controller Rack

1756-L71/B LOGIX5571 (...)

IP: 192.168.20.22

MAC: 5c:88:16:ef:d1:e4

First activity: Feb 15, 2022 5:53:45 PM

Last activity: Feb 15, 2022 5:53:45 PM

Sensor: -

Tags: Controller, Rockwell Automation

Activity tags: EthernetIP

Risk score: 70 See details

Modules:

- 1756-EN2T/D
- 1756-EN2TR/C (Port1-Link03)
- 1756-EN2T/D (Port1-Link02)
- 1756-RM2/A REDUNDANCY MODULE (Port1-Link01)
- 1756-L71/B LOGIX5571 (Port1-Link00)

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	

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:

Flow

52:54:dd:c1:f1:ed
IP: -
MAC: 52:54:dd:c1:f1:ed

SIEMENS
SIMATIC 300
IP: -
MAC: 08:00:06:92:c1:84

First activity
Feb 16, 2022 2:19:50 PM

Last activity
Feb 16, 2022 2:20:10 PM

Tags
Active Discovery,
S7Discovery

Basics

Properties Content Statistics Tags

Properties

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

The screenshot shows a network management interface with the following 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

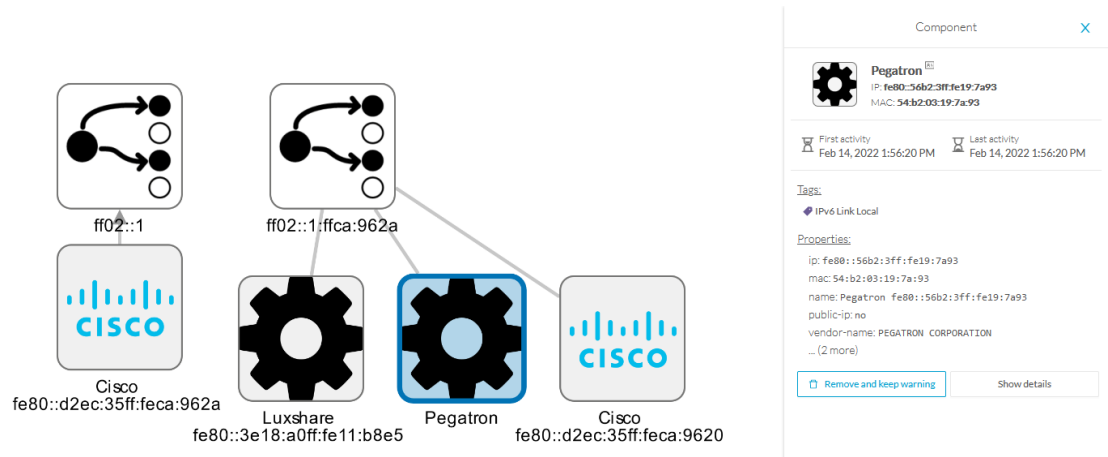
ICMPv6 Multicast

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:

Flow



192.168.22.192
IP: 192.168.22.192
Port: 58600
MAC: 52:54:00:61:05:d7






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


Basics

Properties Content Statistics Tags


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	

Flow



192.168.22.192
IP: 192.168.22.192
Port: 36281
MAC: 52:54:00:61:05:d7






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


Basics

Properties Content Statistics Tags


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:f4:4e: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 network nodes in a management interface. Each node has a 'Flow' header and a 'Properties' section.

Node 1: Managed Redundant Switch

- IP: 192.168.0.192
- Port: 36352
- MAC: 52:54:dd:c1:f1:ed
- Model: Managed Redundant Switch
- IP: 192.168.0.29
- Port: 161
- MAC: 00:90:e8:32:4ced
- First activity: Feb 17, 2022 11:12:14 AM
- Last activity: Feb 17, 2022 11:12:14 AM
- Tags: Net Management, Active Discovery, SNMP

Node 2: Moxa 192.168.0.28

- IP: 192.168.0.192
- Port: 48394
- MAC: 52:54:dd:c1:f1:ed
- Model: Moxa 192.168.0.28
- IP: 192.168.0.28
- Port: 161
- MAC: 00:90:e8:5c:f9:84
- First activity: Feb 17, 2022 11:12:14 AM
- Last activity: Feb 17, 2022 11:12:14 AM
- Tags: Net Management, Active Discovery, SNMP

Properties for Node 1:

- ethertype: IPv4
- protocol: UDP
- snmp-command: getBulkRequest
- 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

Properties for Node 2:

- ethertype: IPv4
- protocol: UDP
- snmp-command: getBulkRequest
- 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:

The screenshot displays a network flow for a SCALANCE X-300 switch. The flow details include the source IP (192.168.0.192), destination IP (192.168.0.35), port (161), and MAC address (00:0e:8c:9ad9:2c). The interface also shows activity timestamps and tags like 'Net Management' and 'Active Discovery, SNMP'. Below the flow details, the 'Properties' section lists various SNMP-related attributes:

Property	Description
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 1: BRS-646038BFF9AE

- IP: 192.168.0.192
- Port: 33687
- MAC: 52:54:00:11:f1:ed
- 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
- Packets: 100

Properties:

- ethertype: IPv4
- protocol: UDP
- snmp-command: getBulkRequest
- snmp-community: public
- snmp-hm-disc-fw-version-raw: HiOS-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-646038BFF9AE
- snmp-sys-objectid: 1.3.6.1.4.1.248.11.2.1.15
- snmp-sys-services: 2
- snmp-version: v2c

Flow 2: RS-58AB3C

- IP: 192.168.0.192
- Port: 40150
- MAC: 52:54:00:11:f1:ed
- 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
- Packets: 1

Properties:

- ethertype: IPv4
- protocol: UDP
- snmp-command: getBulkRequest
- snmp-community: public
- snmp-hmpriv-mgmt-fw-version: 07.1.05
- snmp-hmpriv-mgmt-model-ref: RS30-0802T1T15DAEHH
- 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:

Flow



192.168.0.192
IP: 192.168.0.192
Port: 39953
MAC: 52:54:00:11:11:ed



IE3300Mitsubishi.ccv
IP: 192.168.0.144
Port: 161
MAC: bc:4a:56:e0:99:eb

First activity
Feb 17, 2022 10:33:05 AM

Last activity
Feb 17, 2022 10:33:05 AM

Tags

- Net Management
- Active Discovery
- SNMP


Basics

Properties Content Statistics Tags


Properties

ethertype: IPv4	protocol: UDP
snmp-command: get-request	snmp-community: public
snmp-ent-physical-entry: IE-3300-8T2X Expandable Non-PoE Chassis	snmp-ent-physical-model-name: IE-3300-8T2X
snmp-ent-physical-serial-number: FCN2435P3L2	snmp-probe-software-rev: 17.3.1
snmp-sys-descr: Cisco IOS Software [Amsterdam], IE3x00 Switch Software (IE3x00-UNIVERSALK9-M), Version 17.3.1, RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2020 by Cisco Systems, Inc. Compiled Fri 07-Aug-20 19:15 by mcp	snmp-sys-name: IE3300Mitsubishi.ccv
snmp-sys-objectid: 1.3.6.1.4.1.9.1.3007	snmp-sys-services: 6
snmp-version: v2c	

Flow



192.168.0.192
IP: 192.168.0.192
Port: 37610
MAC: 52:54:00:11:11:ed



IE34ROCPLC.ccv
IP: 192.168.0.160
Port: 161
MAC: 6c:71:0d:14:d4:8b

First activity
Feb 17, 2022 10:33:25 AM

Last activity
Feb 17, 2022 10:33:25 AM

Tags

- Net Management
- Active Discovery
- SNMP

Basics

Properties Content Statistics Tags

Properties

ethertype: IPv4	protocol: UDP
snmp-command: get-request	snmp-community: public
snmp-ent-physical-entry: IE-3400-8T2S Expandable Advanced Non-PoE Chassis	snmp-ent-physical-model-name: IE-3400-8T2S
snmp-ent-physical-serial-number: FOC2401V07N	snmp-probe-software-rev: 17.4.1
snmp-sys-descr: Cisco IOS Software [Bengaluru], IE3x00 Switch Software (IE3x00-UNIVERSALK9-M), Version 17.4.1, RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2020 by Cisco Systems, Inc. Compiled Thu 26-Nov-20 21:57 by mcp	snmp-sys-name: IE34ROCPLC.ccv
snmp-sys-objectid: 1.3.6.1.4.1.9.1.2872	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:

The screenshot displays a network flow analysis interface. At the top, it shows a flow between two hosts: 192.168.0.192 (IP: 192.168.0.192, Port: 41716, MAC: 52-54-00-11-11-11) and AVEVASRV (IP: 192.168.0.51, Port: 161, MAC: 00-50-56-8F-4a-3c). The flow is identified as 'snmp-command: getBulkRequest'. The 'Properties' section lists the following details:

ethertype: IPv4	protocol: UDP
snmp-command: getBulkRequest	snmp-community: public
snmp-primary-domain-name: LAB-AUTOM-CCV	snmp-sys-descr: Hardware: Intel64 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

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