Device Sensor

The Device Sensor feature is used to gather raw endpoint data from network devices using protocols such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Dynamic Host Configuration Protocol (DHCP), DHCP version 6, and multicast DNS (mDNS). The endpoint data that is gathered is made available to registered clients in the context of an access session.

- Restrictions for Device Sensor, on page 1
- Information About Device Sensor, on page 1
- How to Configure Device Sensor, on page 3
- Configuration Examples for Device Sensor , on page 9
- Feature History for Device Sensor, on page 10

Restrictions for Device Sensor

- Only Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Dynamic Host Configuration Protocol (DHCP), Dynamic Host Configuration Protocol ersion 6 (DHCPv6), and multicast DNS (mDNS) protocols are supported.
- The session limit for profiling ports is 32.
- The length of one Type-Length-Value (TLV) must not be more than 1024 and the total length of TLVs (combined length of TLVs) of all protocols must not be more than 4096.
- The sensor profiles devices that are only one hop away.
- The Device Sensor feature is enabled by default, but cannot be disabled. Disabling device classifier using **no device classifier** command in global configuration mode does not disable device sensor. This is because device sensor is independent of IP device tracking and device classifier.

Information About Device Sensor

Device Sensor

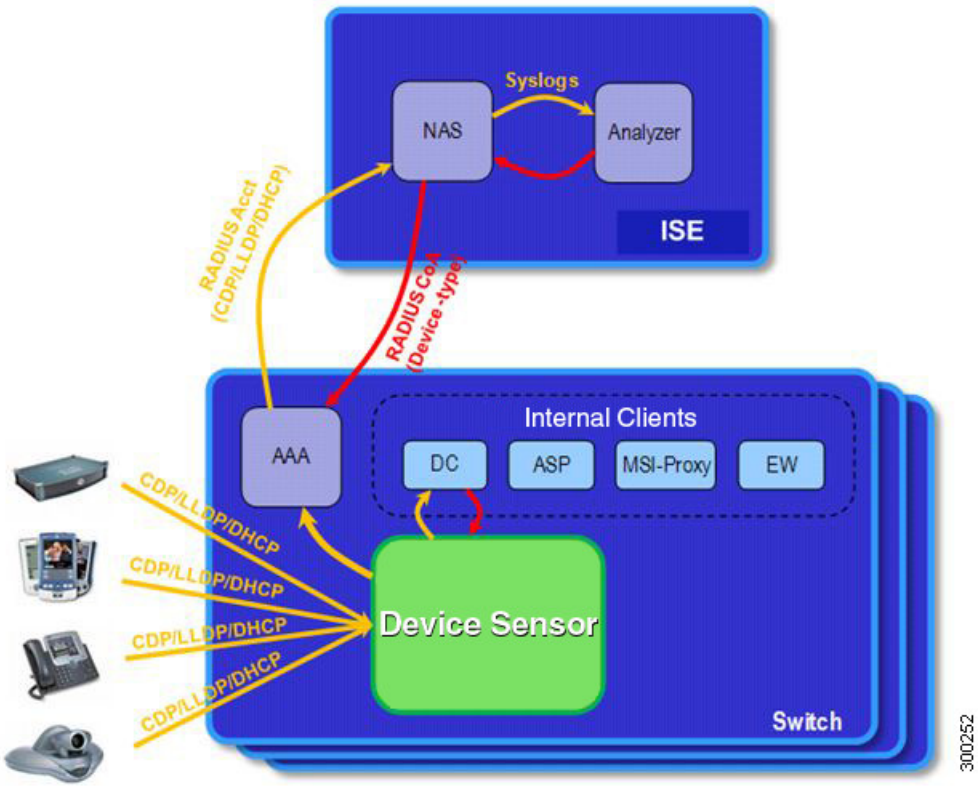
The device sensor is used to gather raw endpoint data from network devices. The endpoint information that is gathered helps in completing the profiling capability of devices. Profiling is the determination of the endpoint

type based on information gleaned from various protocol packets from an endpoint during its connection to a network.

The profiling capability consists of two parts:

- Collector—Gathers endpoint data from network devices.
- Analyzer—Processes the data and determines the type of device.

The device sensor represents the embedded collector functionality. The illustration below shows the Cisco sensor in the context of the profiling system and also features other possible clients of the sensor.



A device with sensor capability gathers endpoint information from network devices using protocols such as Cisco Discovery Protocol, LLDP, DHCPv6, mDNS and DHCP, subject to statically configured filters, and makes this information available to its registered clients in the context of an access session. An access session represents an endpoint's connection to the network device.

The device sensor has internal and external clients. The internal clients include components such as the embedded Device Classifier (local analyzer), ATM switch processor (ASP), MSI-Proxy, and EnergyWise (EW). The external client, that is the Identity Services Engine (ISE) analyzer, will use RADIUS accounting to receive additional endpoint data.

Client notifications and accounting messages containing profiling data along with the session events and other session-related data, such as the MAC address and the ingress port, are generated and sent to the internal and external clients (ISE). By default, for each supported peer protocol, client notifications and accounting events are only generated where an incoming packet includes a TLV that has not previously been received in the context of a given session. You can enable client notifications and accounting events for all TLV changes,

where either a new TLV has been received or a previously received TLV has been received with a different value using CLI commands.

The device sensor's port security protects the switch from consuming memory and crashing during deliberate or unintentional denial-of-service (DoS) type attacks. The sensor limits the maximum device monitoring sessions to 32 per port (access ports and trunk ports). In case of lack of activity from hosts, the idle session time is 12 hours.

How to Configure Device Sensor

The device sensor is enabled by default.

The following tasks are applicable only if you want to configure the sensor based on your specific requirements.

Note If you do not perform these configuration tasks, then the following TLVs are included by default:

- Cisco Discovery Protocol filter—secondport-status-type and powernet-event-type (type 28 and 29).
- LLDP filter—organizationally-specific (type 127).
- DHCP filter—message-type (type 53).

Enabling Accounting Augmentation

Perform this task to add device sensor protocol data to accounting records.

Before you begin

- The device must be in IBNS 1.0 mode before performing this task.
- For the sensor protocol data to be added to the accounting messages, you must enable session accounting by using the standard authentication, authorization, and accounting (AAA), and RADIUS configuration commands.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**device-sensor accounting** **Example:** `Device(config)# device-sensor accounting`	Enables the addition of sensor protocol data to accounting records and also enables the generation of additional accounting events when new sensor data is detected.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Protocol Attributes in Access and Accounting Requests

Perform this task to create an attribute filter-list and to bind an attribute filter-list with authentication and accounting requests.

Before you begin

The device must be in IBNS 2.0 mode before performing this task.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device(config)# configure terminal`	Enters global configuration mode.
Step 3	**access-session attributes filter-list list** *list-name* **Example:** `Device(config)# access-session attributes filter-list list mylist`	Adds access-session protocol data to accounting and authentication records and enters common filter list configuration mode. The **filter-list** keyword configures a sensor protocol filter list to accounting and authentication records.
Step 4	{**cdp** | **dhcp** | **dhcpv6** | **http** | **lldp** | **vlan-id**} **Example:** `Device(config-com-filter-list)# dhcp`	Includes the specified protocol for the attribute.
Step 5	**exit** **Example:** `Device(config-com-filter-list)# exit`	Exits common filter list configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**access-session** {**accounting** | **authentication**} **attributes filter-spec include list** *list-name* **Example:** `Device(config)# access-session authentication attributes filter-spec include list mylist`	Configures a sensor protocol filter specification, and binds an attribute filter list with accounting and authentication records.
Step 7	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Creating a Protocol Filter

Perform this task to create a CDP, LLDP, DHCP, mDNS, or DHCPv6 filter containing TLVs that can be included or excluded in the device sensor output.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**device-sensor** {**filter-list***cdp* | *dhcp* | *dhcpv6* | *mdns* | *lldp*} {**list***tlv-list-name*} **Example:** `Device(config)# device-sensor filter-list cdp list cdp-list`	Applies a sensor protocol filter list and enters configuration mode, where you can configure individual TLVs. • **cdp** - Applies a Cisco Discovery Protocol TLV filter list. • **lldp** - Applies an Link Layer Discovery protocol TLV filter list. • **dhcp** - Applies a Dynamic Host Configuration Protocol TLV filter list. • **dhcpv6** - Applies a Dynamic Host Configuration Protocol version 6 TLV filter list. • **mdns** - Applies a Multicast DNS Protocol TLV filter list.

	Command or Action	Purpose
		• **list***list-name* - Specifies the protocol TLV filter list name.
Step 4	**option** {**name** *option-name* | **number** *option-number*} **Example:** `Device(config-sensor-cdplist)# tlv number 10`	This step applies only to DHCP protocol. Adds individual DHCP options to the option list. You can delete the option list without individually removing options from the list by using the **no device-sensor filter-list dhcp list** *option-list-name* command. • You can delete the TLV list without individually removing TLVs from the list by using the **no device-sensor filter-list cdp list** *tlv-list-name* command.
Step 5	**tlv** {**name** *tlv-name* | **number** *tlv-number*} **Example:** `Device(config-sensor-cdplist)# tlv number 10`	Adds individual Cisco Discovery Protocol TLVs to the TLV list. • You can delete the TLV list without individually removing TLVs from the list by using the **no device-sensor filter-list cdp list** *tlv-list-name* command.
Step 6	**end** **Example:** `Device(config-sensor-cdplist)# end`	Returns to privileged EXEC mode.

Applying a Protocol Filter to the Sensor Output

Perform this task to apply a Cisco Discovery Protocol, LLDP, or DHCP filter to the sensor output. Session notifications are sent to internal sensor clients and accounting requests.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**device-sensor filter-spec** {**cdp** | **dhcp** | **lldp**} {**exclude** {**all** | **list** *list-name*} | **include list** *list-name*} **Example:** `Device(config)# device-sensor filter-spec cdp include list list1`	Applies a specific protocol filter containing a list of TLV fields to the device sensor output. • **cdp**—Applies a Cisco Discovery Protocol TLV filter list to the device sensor output. • **lldp**—Applies an LLDP TLV filter list to the device sensor output. • **dhcp**—Applies a DHCP TLV filter list to the device sensor output. • **dhcpv6**—Applies a DHCPv6 TLV filter list to the device sensor output. • **mdns**—Applies an mDNS TLV filter list to the device sensor output. • **exclude**—Specifies the TLVs that must be excluded from the device sensor output. • **include**—Specifies the TLVs that must be included from the device sensor output. • **all**—Disables all notifications for the associated protocol. • **list** *list-name*—Specifies the protocol TLV filter list name.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Tracking TLV Changes

Perform this task to enable client notifications and accounting events for all TLV changes. By default, for each supported peer protocol, client notifications and accounting events will only be generated where an incoming packet includes a TLV that has not previously been received in the context of a given session.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**device-sensor notify all-changes** **Example:** `Device(config)# device-sensor notify all-changes`	Enables client notifications and accounting events for all TLV changes, that is, where either a new TLV is received or a previously received TLV is received with a new value in the context of a given session. **Note** Use the **default device-sensor notify** or the **device-sensor notify new-tlvs** command to return to the default TLV.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying the Device Sensor Configuration

Perform this task to verify the sensor cache entries for all devices.

Procedure

Step 1 **enable**

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show device-sensor details**

Displays protocol configuration details for all devices.

Example:

```
Device# show device-sensor details
```

Step 3 **show device-sensor cache mac** *mac-address*

Displays sensor cache entries (the list of protocol TLVs or options received from a device) for a specific device.

Example:

```
Device# show device-sensor cache mac 0024.14dc.df4d
```

Step 4 **show device-sensor cache all**

Displays sensor cache entries for all devices.

Example:

```
Device# show device-sensor cache all

Device: 001c.0f74.8480 on port GigabitEthernet2/1
```

Configuration Examples for Device Sensor

Examples: Configuring the Device Sensor

The following example shows how to create a Cisco Discovery Protocol filter containing a list of TLVs:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list cdp list cdp-list
Device(config-sensor-cdplist)# tlv name address-type
Device(config-sensor-cdplist)# tlv name device-name
Device(config-sensor-cdplist)# tlv number 34
Device(config-sensor-cdplist)# end
```

The following example shows how to create an LLDP filter containing a list of TLVs:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list lldp list lldp-list
Device(config-sensor-lldplist)# tlv name chassis-id
Device(config-sensor-lldplist)# tlv name management-address
Device(config-sensor-lldplist)# tlv number 28
Device(config-sensor-lldplist)# end
```

The following example shows how to create a DHCP filter containing a list of options:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list dhcp list dhcp-list
Device(config-sensor-lldplist)# option name address-type
Device(config-sensor-lldplist)# option name device-name
Device(config-sensor-lldplist)# option number 34
Device(config-sensor-lldplist)# end
```

The following example shows how to apply a Cisco Discovery Protocol TLV filter list to the device sensor output:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-spec cdp include cdp-list1
Device(config
Device(config-sensor-lldplist)# end)# end
```

The following example shows how to enable client notifications and accounting events for all TLV changes:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor notify all-changes
Device(config)# end
```

Feature History for Device Sensor

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature Information for Device Sensor

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.8.1a	Device Sensor	The Device Sensor feature is used to gather raw endpoint data from network devices using protocols such as Cisco Discovery Protocol, Link Layer Discovery Protocol (LLDP), and DHCP. The endpoint data that is gathered is made available to registered clients in the context of an access session.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.