Configuring Device Sensor

About Device Sensor

Device Sensor uses protocols such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and DHCP to obtain endpoint information from network devices and make this information available to its clients. Device Sensor has internal clients, such as the embedded Device Classifier (local analyzer), Auto Smartports (ASP), MediaNet Service Interface Media Services Proxy, and EnergyWise. Device Sensor also has an external client, Identity Services Engine (ISE), which uses RADIUS accounting to receive and analyze endpoint data. When integrated with ISE, Device Sensor provides central policy management and device-profiling capabilities.

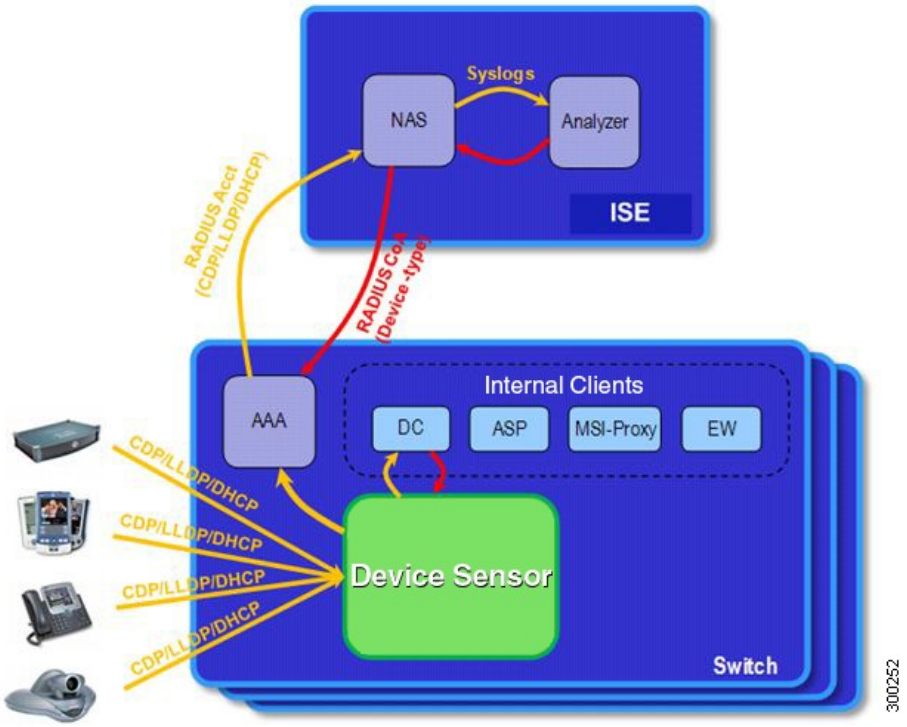
Note Cisco Identity Services Engine (ISE) based profiling is not supported on the LAN Base image.

Device profiling capability consists of two parts:

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

Device Sensor represents the embedded collector functionality. The following illustration shows a Device Sensor in the context of its internal clients and the ISE

Figure 1: Device Sensor Clients



Client notifications and accounting messages that contain profiling data and other session-related data are generated and sent to the internal clients and the ISE. By default, client notifications and accounting events are generated only when an incoming packet includes a Type-Length-Value (TLV) that has not previously been received within a given access session. You can enable client notifications and accounting events for TLV changes; that is, when a previously received TLV is received with a different value.

Device Sensor port security protects a switch from consuming memory and crashing during deliberate or unintentional denial-of-service (DoS)-type attacks. Device Sensor limits the maximum number of device monitoring sessions to 32 per port. While hosts are inactive, the age session limit is 12 hours.

MSP-IOS Sensor Device Classifier Interaction

Note To enable MSP, you must configure the profile flow command. Once done, when SIP, H323, or mDNS traffic are present, appropriate (SIP, H323, or mDNS) TLV notifications are sent to the IOS sensor.

MSP (Media Service Proxy) offers bandwidth reservation for audio or video flows and Metadata services to 3rd-party endpoints. To offer and install Media services, MSP must identify flow attributes and device details. MSP device identification requires automatic identification of various media end points in the network, thereby avoiding any change to the installed end point base. To offer MSP device discovery services, MSP leverages current IOS sensor capability for device classification. (Starting with Release IOS XE 3.3.0SG and IOS 15.1(1)SG, IOS sensor can be used to perform device identification. MSP uses the same functionality with the addition of SIP, H323, and Multicast DNS (mDNS) protocols.) Starting with Release IOS XE 3.4.0SG

and IOS 15.1(2)SG, MSP offers Media services to two kinds of media endpoints: IP Surveillance Cameras and Video-Conferencing Endpoints. Surveillance cameras are identified using mDNS protocol whereas Video-conference-Endpoints are identified using SIP and H.323 protocols.

mDNS compatible devices (Axis, Pelco cameras etc) send mDNS messages for DNS service discovery to a multicast IP address (224.0.0.251) on a standard mDNS port 5353. The mDNS client module listens to this UDP port, receives the mDNS message, and sends it in TLV format to the mDNS IOS sensor shim for further device classification. The module parses the mDNS query and Answer messages fields to create these TLVs.

A Session Initiation Protocol (SIP) registration message is used for SIP based device-discovery and is sent to Cisco Call manager by the SIP Client. A H.225 RAS client registration message is used for H323-based device discovery.

If no Cisco Unified Communicator Manager or GateKeeper exists in the topology, the Endpoint will not generate device Register messages. To handle device discovery in these scenarios, MSP expects the endpoint to make a SIP or H323 call so that MSP snoops the SIP invite or the H323 setup message to identify endpoint details and notify the IOS sensor.

After the IOS sensor receives these protocol details from MSP, the IOS sensor prepares Normalized TLVs, with the new protocols. These protocol details are sent to session manager for further classification.

Configuring Device Sensor

Device Sensor is enabled by default. Complete the following tasks when you want Device Sensor to include or exclude a list of TLVs (termed filter lists) for a particular protocol.

Note If you do not perform any Device Sensor configuration tasks, the following TLVs are included by default:

- CDP filter--secondport-status-type and powernet-event-type (types 28 and 29)
- LLDP filter--organizationally-specific (type 127)
- DHCP filter--message-type (type 53)

Enabling MSP

You must configure the MSP profile flow command to activate the MSP platform Packet parser. This is because the MSP device handler is tightly coupled with MSP flow parser. Not enabling this command means that MSP will not send SIP, H323 notifications to the IOS sensor.

To enable MSP, follow these steps, beginning in privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	profile flow **Example:** `Switch(config)# profile flow`	Enables MSP. Use the no form of the **profile flow** command to disable MSP.
Step 3	end **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Enabling Accounting Augmentation

For the Device Sensor protocol data to be added to accounting messages, you must first enable session accounting by using the following standard Authentication, Authorization, and Accounting (AAA) and RADIUS configuration commands:

```
Switch(config)# aaa new-model
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# radius-server host{hostname|ip-address}[auth-port port-number][acct-port
port-number] [timeout seconds][retransmit retries][key string]
Switch(config)# radius-server vsa send accounting
```

To add Device Sensor protocol data to accounting records, follow these steps, beginning in privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	device-sensor accounting **Example:** `Switch(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 3	end **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Creating a Cisco Discovery Protocol Filter

To create a CDP filter containing a list of TLVs that can be included or excluded in the Device Sensor output, follow these steps, beginning in privileged EXEC mode:

configure terminal

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor filter-list cdp list** *tlv-list-name*	

Creating an LLDP Filter

To create an LLDP filter containing a list of TLVs that can be included or excluded in the Device Sensor output, follow these steps, beginning in privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor filter-list lldp list tlv-list-name** **Example:** `Switch(config)# device-sensor filter-list lldp list lldp-list`	Creates a TLV list and enters LLDP sensor configuration mode, where you can configure individual TLVs.
Step 3	**tlv** { **name** *tlv-name* | **number** *tlv-number* } **Example:** `Switch(config-sensor-cdplist)# tlv number 10`	Adds individual LLDP 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 lldp list tlv-list-name command.
Step 4	**end** **Example:** `Switch(config-sensor-lldplist)# end`	Returns to privileged EXEC mode.

Creating a DHCP Filter

To create a DHCP filter containing a list of DHCP options that can be included or excluded in the Device Sensor output, follow these steps, beginning in privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor filter-list dhcp list option-list-name** **Example:** `device-sensor filter-list dhcp list option-list-name`	Creates an options list and enters DHCP sensor configuration mode, where you can specify individual DHCP options.
Step 3	**option** { **name** *option-name* | **number** *option-number* } **Example:** `Switch(config-sensor-dhcplist)# option number 50`	Adds individual DHCP options to the option list. You can delete the entire option list without removing options individually from the list by using the no device-sensor filter-list dhcp list option-list-name command.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Applying a Protocol Filter to the Device Sensor Output

Beginning in privileged EXEC mode, follow these steps to apply a CDP, LLDP, or DHCP filter to the sensor output. The output is session notifications to internal sensor clients and accounting requests to the RADIUS server.

Note Only one filter list can be included or excluded at a time.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor filter-spec** { **cdp** | **dhcp** | **ldp** } { **exclude** { **all** | **list** *list-name* } | **include list** *list-name* } **Example:** `Switch(config)# device-sensor filter-spec cdp include list list1`	Applies a specific protocol filter containing a list of protocol TLV fields or DHCP options to the Device Sensor output. • **cdp** –Applies a CDP TLV filter list to the device sensor output

	Command or Action	Purpose
		• **lldp** –Applies an LLDP TLV filter list to the device sensor output. • **dhcp** –Applies a DHCP option 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 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Tracking TLV Changes

By default, client notifications and accounting events are generated only when an incoming packet includes a TLV that has not previously been received within a given session.

To enable client notifications and accounting events for TLV changes, follow these steps, beginning in privileged EXCEC mode:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**device-sensor notify all-changes** **Example:** `Switch(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 3	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	

Verifying the Device Sensor Configuration

To verify the sensor cache entries for all devices, follow these steps, beginning in privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	**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. • mac-address is the MAC address of the endpoint
Step 2	**show device-sensor cache all** **Example:** `Switch(config)# device-sensor notify all-changes`	Displays sensor cache entries for all devices.

Troubleshooting Commands

The following commands can help troubleshoot Device Sensor.

- **debug device-sensor** { **errors** | **events** }
- **debug authentication all**

Restrictions for Device Sensor

- Only CDP, LLDP, and DHCP protocols are supported.
- The session limit for profiling ports is 32.
- The length of one 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.
- Device Sensor profiles devices that are only one hop away.

Configuration Examples for the Device Sensor Feature

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

```
Switch> enable
Switch# configure terminal
```

```
Switch(config)# device-sensor filter-list cdp list cdp-list
Switch(config-sensor-cdplist)# tlv name address-type
Switch(config-sensor-cdplist)# tlv name device-name
Switch(config-sensor-cdplist)# tlv number 34
Switch(config-sensor-cdplist)# end
```

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

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

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

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list dhcp list dhcp-list
Switch(config)# device-sensor filter-list dhcp list dhcp-list
Switch(config-sensor-dhcplist)# option name domain-name
Switch(config-sensor-dhcplist)# option name host-name
Switch(config-sensor-dhcplist)# option number 50
Switch(config-sensor-dhcplist)# end
```

The following example shows how to apply a CDP TLV filter list to the Device Sensor output:

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

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

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

Feature Information for Device Sensor

Table 1: Feature Information for Device Sensor

Feature Name	Releases	Feature Information
Device Sensor	Cisco IOS XE 3.6E	This feature was introduced.