HTTP Gleaning

The HTTP Gleaning feature allows the device sensor to extract the HTTP packet type, length, value (TLV) to derive information about the type of the end device.

Information About HTTP Gleaning

HTTP Gleaning Overview

The device sensor is used to gather endpoint data from network devices. The endpoint information helps to complete the profiling capability of devices. Profiling is the process of determining the endpoint type based on the information gleaned from various protocol packets from an endpoint during its connection to a network. The HTTP Gleaning feature allows the device sensor to extract the HTTP packet type, length, value (TLV) to get information about the type of the end device.

User-Agent is one such TLV that contains information such as end-device operating system details and the browser used for the operation. This information is gleaned by the device sensor. The device classifier can use this information to ascertain the device type.

HTTP User-Agent requires the following functionalities to support HTTP gleaning.

- HTTP packet handler

- HTTP packet header parser

- HTTP TLV gleaner (DSensor shim)

Device sensors use filters to include or exclude specific TLVs to be stored by the device sensor cache. The filter configuration is a two-step process.

1. Creating a protocol filter list.

2. Applying the protocol filter list to the filter specification.

The protocol filter list is a protocol-specific list that stores the list of TLVs that are configured as part of this list. You can configure any number of filter lists for a single protocol.

HTTP supports only one type of TLV. Hence, a filter list does not exist. HTTP gleaning is enabled by default. To stop the processing of HTTP TLVs by the device sensor, use the **device-sensor filter-spec http** command.

How to Configure HTTP Gleaning

Configuring the Device Sensor Filter Specification for the HTTP TLV

Before you begin

By default, the device sensor gleans the HTTP packets that are received from the client. However, the user can explicitly exclude the HTTP type, length, value (TLV) from gleaning.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **device-sensor filter-spec http exclude all**
4. **end**

DETAILED STEPS

	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-spec http exclude all** **Example:** `Device(config)# device-sensor filter-spec http exclude all`	Specifies that all TLVs should be excluded from the device sensor output.
Step 4	**end** **Example:** `Device(config)# end`	Exits gobal configuration mode and returns to privileged EXEC mode.

Verifying HTTP Gleaning

The following is sample output from the **show device-sensor cache** [**all** | **interface** | **mac**] command. The output shows that the HTTP TLVs are gleaned by the device sensor.

```
Device# show device-sensor cache all

Device: c8e0.eb17.0b6f on port Capwap0
--------------------------------------------------
Proto    Type:Name                      Len Value
HTTP     1:user-agent                   83 01 51 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 4D
                                            61 63 69 6E 74 6F 73 68 3B 20 49 6E 74 65 6C 20
                                            4D 61 63 20 4F 53 20 58 20 31 30 2E 38 3B 20 72
                                            76 3A 32 35 2E 30 29 20 47 65 63 6B 6F 2F 32 30
                                            31 30 30 31 30 31 20 46 69 72 65 66 6F 78 2F 32
                                            35 2E 00
DHCP     54:server-identifier           6 36 04 C0 A8 0A 01
DHCP     50:requested-address           6 32 04 C0 A8 0A 16
DHCP     0:                             8 00 06 44 AD D9 03 3B 00
DHCP     255:end                        2 FF 00
DHCP     12:host-name                   14 0C 0C 73 70 72 61 73 61 64 73 2D 6D 61 63
DHCP     61:client-identifier           9 3D 07 01 C8 E0 EB 17 0B 6F
DHCP     57:max-message-size            4 39 02 05 DC
DHCP     55:parameter-request-list      11 37 09 01 03 06 0F 77 5F FC 2C 2E
DHCP     53:message-type                3 35 01 03
```

The following table describes the significant fields shown in the display:

Table 1: show device-sensor cache all Field Descriptions

Field	Description
Proto	Name of the protocol.
Type:Name	Type and name of the type, length, value (TLV) .
Len	Length of the TLV
Value	Value of the TLV in hexadecimal format.

Additional References for HTTP Gleaning

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for HTTP Gleaning

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for HTTP Gleaning

Feature Name	Releases	Feature Information
HTTP Gleaning	Cisco IOS XE Fuji 16.8.1a	The HTTP Gleaning feature allows the device sensor to extract the HTTP packet type, length, value (TLV) to derive information about the type of the end device.