Configuring Embedded Packet Capture

Embedded Packet Capture Overview

Embedded Packet Capture (EPC) is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from the device and to analyze them locally or save and export them for offline analysis. The captured data is stored in .pcap file format, which can be analyzed by using a standard packet analysis tool such as Wireshark. This feature facilitates troubleshooting by gathering information about the packet format. This feature also facilitates application analysis and security.

Embedded Packet Capture (EPC) provides an embedded systems management facility that helps in tracing and troubleshooting packets. The network administrator may define the capture buffer size and the maximum number of bytes of each packet to capture. The packet capture rate can be throttled using further administrative controls. For example, options allow for filtering the packets to be captured using an Access Control List and, optionally, further defined by specifying a maximum packet capture rate or by specifying a sampling interval.

Note Packet Capture is supported only on physical interfaces with the ingress direction. ACL filter needs to be configured before configuring EPC.

Configuring Embedded Packet Capture

Follow these steps to configure Embedded Packet Capture:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enable privileged EXEC mode.

	Command or Action	Purpose
Step 2	**monitor capture** *capture-name* **access-list** *access-list-name*	Configure a monitor capture specifying an access list as the core filter for the packet capture.
Step 3	**monitor capture** *capture-name* **limit duration** *seconds*	Configure monitor capture limits.
Step 4	**monitor capture** *capture-name* **interface** *interface-name* **in**	Configure monitor capture specifying an attachment point and the packet flow direction.
Step 5	**monitor capture** *capture-name* **buffer circular size** *bytes*	Configure a buffer to capture packet data. This size can be maximum 100 MB.
Step 6	**monitor capture** *capture-name* **start**	Start the capture of packet data at a traffic trace point into a buffer.
Step 7	**monitor capture** *capture-name* **export** *file-location/file-name*	Export captured data for analysis.
Step 8	**monitor capture** *capture-name* **stop**	Stop the capture of packet data at a traffic trace point.
Step 9	**monitor capture** *capture-name* **clear**	Clear the captured buffer data.
Step 10	**end**	Exit privileged EXEC mode.

Example

Monitoring and Maintaining Captured Data

Perform this task to monitor and maintain the packet data captured. Capture buffer details and capture point details are displayed.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enable privileged EXEC mode.
Step 2	**show monitor capture** *capture-buffer-name* **buffer dump**	(Optional) Display a hexadecimal dump of captured packet and its metadata.
Step 3	**show monitor capture** *capture-buffer-name* **parameter**	(Optional) Display a list of commands that were used to specify the capture.
Step 4	**debug epc capture-point**	(Optional) Enable packet capture point debugging.
Step 5	**debug epc provision**	(Optional) Enables packet capture provisioning debugging.
Step 6	**exit**	Exit privileged EXEC mode.

Example

Feature History

Feature Name	Release	Feature Information
Embedded Packet Capture	Cisco IOS XE 16.11.1	Initial support on Cisco Catalyst IE 3200, 3300, 3400, and Cisco Embedded Service 3300 Series Switches