Embedded Packet Capture

Feature History for Embedded Packet Capture

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature History for Embedded Packet Capture

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.12.1	Embedded Packet Capture	The Embedded Packet Capture feature is enhanced to support increased buffer size, continuous capture, and filtering of multiple MAC addresses in one Embedded Packet Capture (EPC) session.

Information About Embedded Packet Capture

The Embedded Packet Capture feature helps in tracing and troubleshooting packets. The Embedded Packet Capture on the controller is used for troubleshooting multiple issues, such as, authentication issues with RADIUS, AP join or disconnection, client forwarding, disconnection, and roaming, and other specific features such as multicast, mDNS, umbrella, mobility, and so on.This feature allows network administrators to capture data packets flowing through, to, and from a Cisco device. When troubleshooting an AP join or a client onboarding issue, if you are unable to stop capture as soon as an issue occurs, important information might be lost. In most cases, a buffer of 100 MB is not sufficient for data capture. Moreover, the existing Embedded Packet Capture feature supports only the filtering of one inner MAC address, which captures the traffic of a specific client. At times, it is difficult to pin-point which wireless client is facing an issue.

From Cisco IOS XE Dublin 17.12.1, the Embedded Packet Capture feature supports increased buffer size, continuous capture, and filtering of multiple MAC addresses in one Embedded Packet Capture session. There are no GUI steps to configure the Embedded Packet Capture enhancement.

Configuring Embedded Packet Capture (CLI)

With the Embedded Packet Capture feature enhancement, the buffer size is increased from 100 MB to 500 MB.

Note Buffer is of memory type. You can either maintain a memory buffer or copy the memory buffer that is present in a file to store more information.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**monitor capture** *epc-session-name* **interface GigabitEthernet** *interface-number* {**both** | **in** | **out**} **Example:** `Device# monitor capture epc-session1 interface GigabitEthernet 0/0/1 both`	Configures the Gigabit Ethernet interface for inbound, outbound, or both inbound and outbound packets. Gigabit is for Cisco 9800-CL controllers, for example, Gi1, Gi2, or Gi3. For physical controllers, you must specify the port channel, if configured. Examples for physical interfaces are Te or Tw. **Note** You can also run the **control-plane** command to capture the packet punt to the CPU.
Step 3	(Optional) **monitor capture** *epc-session-name* **limit duration** *limit-duration* **Example:** `Device# monitor capture epc-session1 limit duration 3600`	Configures monitor capture limit, in seconds.
Step 4	(Optional) **monitor capture** *epc-session-name* **buffer circular file** *no-of-files* **file-size** *per-file-size* **Example:** `Device# monitor capture epc-session1 buffer circular file 4 file-size 20`	Configures the file in circular buffer. (Buffer can be circular or linear). When **circular** is configured, the files work as a ring buffer. The value range of the number of files to be configured is from 2 to 5. The value range of the file size is from 1 MB to 500 MB.

	Command or Action	Purpose
		There are various keywords available for the **buffer** command, such as, **circular**, **file**, and **size**. Here, the **circular** command is optional. **Note** Circular buffer is needed for continuous capture. This step generates swap files in the controller. Swap files are not packet capture (PCAP) files, and therefore, cannot be analyzed. When the **export** command is run, the swap files are combined and exported as one PCAP file.
Step 5	**monitor capture** *epc-session-name* **match** {**any** | **ipv4** | **ipv6** | **mac** | **pklen-range**} **Example:** `Device# monitor capture epc-session1 match any`	Configures inline filters. **Note** You can configure filters and ACLs.
Step 6	(Optional) **monitor capture** *epc-session-name* **access-list** *access-list-name* **Example:** `Device# monitor capture epc-session1 access-list access-list1`	Configures a monitor capture specifying an access list as the filter for the packet capture.
Step 7	(Optional) **monitor capture** *epc-session-name* **continuous-capture http:***location/filename* **Example:** `Device# monitor capture epc-session1 continuous-capture https://www.cisco.com/epc1.pcap`	Configures continuous packet capture. Enables the automatic export of files to a specific location before the buffer is overwritten. **Note** • Circular buffer is needed for continuo capture. • Configure the filename with a .pcap extension. • An example of the filename and nomenclature used to generate the filename is as follows: CONTINUOUS_CAP_20230601130203.p CONTINUOUS_CAP_20230601130240.p • After the packets are exported automatically, the buffer is not cleared until it is overwritten by the new incom capture packets, or cleared, or deleted commands.

	Command or Action	Purpose
Step 8	(Optional) **[no] monitor capture** *epc-session-name* **inner mac** *MAC1* [*MAC2*… *MAC10*] **Example:** `Device# monitor capture epc-session1 inner mac 1.1.1 2.2.2 3.3.3 4.4.4`	Configures up to 10 MAC addresses as inner MAC filter. **Note** • You can not modify the inner MACs while the capture is in progress. • You can enter the MAC addresses in a single command or by using multiple command lines. Because of the character string limitation, you can enter only five MAC addresses in a single command line. You can enter the rest of the MAC addresses in the next command line. • If the number of configured inner MAC addresses is 10, a new MAC address cannot be configured until you delete an old configured inner MAC address.
Step 9	**monitor capture** *epc-session-name* **start** **Example:** `Device# no monitor capture epc-session1 start`	Starts capture of packet data.
Step 10	**monitor capture** *epc-session-name* **stop** **Example:** `Device# no monitor capture epc-session1 stop`	Stops capture of packet data.
Step 11	**monitor capture** *epc-session-name* **export** *filelocation/filename* **Example:** `Device# monitor capture epc-session1 export https://www.cisco.com/ecap-file.pcap`	Exports captured data for analysis when continuous capture is not configured.

Verifying Embedded Packet Capture

To view the configured file number and per file size, run the following command:

Note The following command is displayed irrespective of whether continuous capture is enabled or not. The configured inner MAC addresses are also displayed using this command.

```
Device# show monitor capture epc-session1
Status Information for Capture epc-session1
  Target Type:
 Interface: TwoGigabitEthernet0/0/0, Direction: BOTH
   Status : Inactive
  Filter Details:
    Capture all packets
  Inner Filter Details:
  Continuous capture: enabled
  Continuous capture path: ftp://mgcusr:mgcusr@10.124.19.169//home/mgcusr/xij/repo.pcap
  Buffer Details:
   Buffer Type: CIRCULAR
   No of files: 5
   File Size (in MB): 21
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 3600
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
```

To view the configured Embedded Packet Capture buffer files, run the following commands:

```
Device# show monitor capture epc-session1 buffer brief
 ----------------------------------------------------------------------------
 #   size   timestamp     source             destination      dscp    protocol
 ----------------------------------------------------------------------------
   0 1386    0.000000   192.168.10.117   ->  192.168.10.100   0  BE   UDP
   1 1378    0.000000   192.168.10.100   ->  192.168.10.117   0  BE   UDP
   2 1386    0.001007   192.168.10.117   ->  192.168.10.100   0  BE   UDP

Device# show monitor capture epc-session1 buffer dump
0
  0000:  6C8BD3FE AEC0F4BD 9E566E4B 8100000A   l........VnK....
  0010:  08004500 05500000 0000FF11 2073C0A8   ..E..P...... s..
  0020:  0A64C0A8 0A75147F 1480053C 00000010   .d...u.....<....
  0030:  03000000 00000288 0000C48E 8FC860CF   ..............`.
  0040:  DC8C3759 4B203468 95299EA5 00000000   ..7YK 4h.).......
  0050:  AAAA0300 00000800 4500050A 92154000   ........E.....@.
  0060:  40060BBC C0A80B67 C0A80B65 A7E0139D   @......g...e....
  0070:  32595FD8 0F2D6065 801001F6 EA440000   2Y_..-`e.....D..
  0080:  0101080A BFCB4934 A959414F 36373839   ......I4.YAO6789
  0090:  30313233 34353637 38393031 32333435   0123456789012345
  00A0:  36373839 30313233 34353637 38393031   6789012345678901
  00B0:  32333435 36373839 30313233 34353637   2345678901234567
  00C0:  38393031 32333435 36373839 30313233   8901234567890123
  00D0:  34353637 38393031 32333435 36373839   4567890123456789
  00E0:  30313233 34353637 38393031 32333435   0123456789012345
  00F0:  36373839 30313233 34353637 38393031   6789012345678901
  0100:  32333435 36373839 30313233 34353637   2345678901234567
.
.
.
```