Configuring Packet Capture

Information About Packet Capture

To resolve issues such as voice and security on wireless networks, you might need to dump packets from the AP for analysis while the AP continues to operate normally. The packets can be dumped on to an FTP server. This process of dumping packets for analysis is called Packet Capture. Use the controller to start or stop packet capture for clients. You can choose the type of packets that need to be captured using the controller CLI from the following types:

- Management Packets
- Control Packets
- Data Packets
  - Dot1X
  - ARP
  - IAPP
  - All IP
  - UDP with matching port number
  - DHCP
  - TCP with matching port number
  - Multicast frames
  - Broadcast frames

The packets are captured and dumped in the order of arrival or transmit of packets except for beacons and probe responses. The packet capture contains information such as channel, RSSI, data rate, SNR, and timestamp. Each packet is appended with additional information from the AP. You can choose to dump either just packet headers or full packets.

The following are some guidelines for packet capture:

- If FTP transfer time is slower than the packet rate, some of the packets do not appear in the capture file.
- If the buffer does not contain any packets, a known dummy packet is dumped to keep the connection alive.
- A file is created on the FTP server for each AP based on unique AP and controller name and timestamp. Ensure that the FTP server is reachable by the AP.
- If the FTP transfer fails or FTP connection is lost during packet capture, the AP stops capturing packets, notifies with an error message and SNMP trap, and a new FTP connection is established.

Restrictions for Packet Capture

- Packet capture can be enabled for only one client.
- This feature is not supported in intercontroller roaming scenarios. If you know the AP or the controller to which the client is going to roam, you can configure the packet capture for the client in the new controller or AP using the CLI.
- Not all packets in the air are captured, but only those that reach the radio driver.
- By default, a packet capture process is stopped after 10 minutes. You can, however, configure the packet capture to stop at any time between 1 to 60 minutes.

Configuring Packet Capture (CLI)

Step 1 Configure FTP parameters for packet capture by entering this command:

config ap packet-dump ftp serverip *ip-address* **path** *path* **username** *user_ID* **password** *password*

Step 2 Start or stop packet capture by entering this command:

config ap packet-dump {**start** *client-mac-address ap-name* | **stop**}

Step 3 Configure the buffer size for packet capture by entering this command:

config ap packet-dump buffer-size *size-in-kb*

Step 4 Configure the time for packet capture by entering this command:

config ap packet-dump capture-time *time-in-minutes*

The valid range is between 1 to 60 minutes.

Step 5 Configure the types of packets to be captured by entering this command:

config ap packet-dump classifier {**arp** | **broadcast** | **control** | **data** | **dot1x** | **iapp** | **ip** | **management** | **multicast** | {**tcp port** *port-number*} | {**udp port** *port-number*}} {**enable** | **disable**}

Step 6 Configure the packet length after truncation by entering this command:

config ap packet-dump truncate *length-in-bytes*

Step 7 Know the status of packet capture by entering this command:

show ap packet-dump status

Step 8 Configure debugging of packet capture by entering this command:

debug ap packet-dump {**enable** | **disable**}