Troubleshoot

This chapter describes how to configure Packet Capture over multiple WAP devices for troubleshooting. It includes the following topics:

Spectrum Intelligence

The Spectrum Intelligence page provide the status of spectrum analyzer capability and provides the link to view the spectrum data. The following page describes details about the Spectrum Analyzer.

Enable Spectrum Analysis Mode—The Spectrum Analysis Mode is either Dedicated Spectrum Analyzer or Hybrid Spectrum Analyzer or 3+1 Spectrum Analysis.

Step 1 Select **Troubleshoot** > **Spectrum Intelligence**

Step 2 Select the radio interface, then click **Set** button to start spectrum intelligence.

Step 3 Click **View Spectrum Data**, to see details on **Channel Quality** and **Non-WLAN Channel Utilization**.

View Spectrum Data—This launches the spectrum viewer when scan mode is set to Dedicated Spectrum Analyzer, or Hybrid Spectrum Analyzer, or 3+1 Spectrum Analyzer, radio status is On and the web page accessed only through ipv4 address.

Step 4 Click **Stop** to disable the Spectrum Analysis Mode status.

Packet Capture

The wireless packet capture feature enables capturing and storing the packets received and transmitted by the WAP device. The captured packets can then be analyzed by a network protocol analyzer for troubleshooting or performance optimization.

There are two methods of packet capture:

- **Local Capture Method** — Captured packets are stored in a file on the WAP device. The WAP device can transfer the file to a TFTP server. The file is formatted in pcap format and can be examined using Wireshark. You can choose **Save File on this Device** to select the local capture method.
- **Remote Capture Method** — Captured packets are redirected in real time to an external computer running Wireshark. You can choose **Stream to a Remote Host** to select the remote capture method.

  Captured packets could be redirected in real time to CloudShark, a web-based packet decoder and analyzer site. It is similar to Wireshark UI for packet analysis. You can choose **Stream to CloudShark** to select the remote capture method.

The WAP device can capture these types of packets:

- 802.11 packets received and transmitted on the radio interfaces. Packets captured on the radio interfaces include the 802.11 header.
- 802.3 packets received and transmitted on the Ethernet interface.
- 802.3 packets received and transmitted on the internal logical interfaces, such as VAPs and WDS interfaces.

Use the Packet Capture page to configure the parameters of the packet capture, start a local or remote packet capture, view the current packet capture status, and download a packet capture file.

Local Packet Capture

To initiate a local packet capture:

Step 1 Select **Troubleshoot** > **Packet Capture**.

Step 2 Ensure that **Save File on this Device** is selected for the Packet Capture Method.

Step 3 Configure these parameters:

- **Interface** — Enter a capture interface type for packet capture:
  - **Ethernet** — 802.3 traffic on the Ethernet port.
  - **Radio 1 (5 GHz) / Radio 2 (2.4 GHz)** — 802.11 traffic on the radio interface.
- **Duration** — Enter the time duration in seconds for the capture. The range is from 10 to 3600. The default is 60.
- **Max File Size** — Enter the maximum allowed size for the capture file in kilobytes (KB). The range is from 64 to 4096. The default is 1024.

Step 4 There are two modes for packet capture.

- **All Wireless Traffic** — Captures all wireless packets.
- **Traffic to/from this AP** — Captures the packets sent from the AP or received by the AP.

Step 5 Click **Enable Filters**. There are three checkboxes available (**Ignore Beacons, Filter on Client, Filter on SSID**).

- **Ignore Beacons** — Enables or disables the capturing of 802.11 beacons detected or transmitted by the radio.

- **Filter on Client** — Specifies the MAC address for WLAN client filter. Note that the Client filter is active only when a capture is performed on an 802.11 interface.
- **Filter on SSID** — Select a SSID name for packet capture.

Step 6 Click **Apply**. The changes are saved to the Startup Configuration.

Step 7 Click **Start Capture** and then click **Refresh** to obtain the **Packet Capture Status** which contains of the following data:

a) **Current Capture Status**
b) **Packet Capture Time**
c) **Packet Capture File Size**

In Packet File Capture mode, the WAP device stores the captured packets in the RAM file system. Upon activation, the packet capture proceeds until one of these events occurs:

- The capture time reaches the configured duration.
- The capture file reaches its maximum size.
- The administrator stops the capture.

Remote Packet Capture

The Remote Packet Capture feature enables you to specify a remote port as the destination port for packet captures. This feature works in conjunction with the Wireshark network analyzer tool for Windows. A packet capture server runs on the WAP device and sends the captured packets through a TCP connection to the Wireshark tool. Wireshark is an open source tool and is available for free; it can be downloaded from *https://www.wireshark.org/*.

A Microsoft Windows computer running the Wireshark tool allows you to display, log, and analyze the captured traffic. The remote packet capture facility is a standard feature of the Wireshark tool for Windows.

Note While the remote packet capture is not supported by the Linux, the Wireshark tool works under Linux and already created capture files can be viewed.

When the remote capture mode is in use, the WAP device does not store any captured data locally in its file system.

If a firewall is installed between the Wireshark computer and the WAP device, the Wireshark must be allowed to pass through the firewall policy of the computer. The firewall must also be configured to allow the Wireshark computer to initiate a TCP connection to the WAP device.

Stream to a Remote Host

To initiate a remote capture on a WAP device using **Stream to a Remote Host** option:

Step 1 Select **Troubleshoot** > **Packet Capture**.

Step 2 For the **Packet Capture Method**, click **Stream to a Remote Host** radio button.

Step 3 In the **Remote Capture Port** field, use the default port (2002), or if you are using a port other than the default, enter the desired port number used to connect Wireshark to the WAP device. The port range is from 1025 to 65530.

Step 4 There are two modes for packet capture.

- **All Wireless Traffic** — capture all wireless packets in the air.
- **Traffic to/from this AP** — capture the packet sent from the AP or the AP received.

Step 5 Next, check **Enable Filters**. Then choose from the following options:

- **Ignore Beacons** — Enables or disables the capturing of 802.11 beacons detected or transmitted by the radio.
- **Filter on Client** — Specifies the MAC address for WLAN Client filter. Note that the Client filter is active only when a capture is performed on an 802.11 interface.
- **Filter on SSID** — Select a SSID name for packet capture.

Step 6 If you want to save the settings for use at another time, click **Apply**. However, the selection of Remote as the Packet Capture Method is not saved.

Step 7 Click **Start Capture** to start the capture. To stop the capture, click **Stop Capture**.

Stream to CloudShark

To initiate a remote capture on a WAP device using **Stream to CloudShark** option, do the following:

Step 1 Select **Troubleshoot > Packet Capture**.

Step 2 For the **Packet Capture Method**, click **Stream to CloudShark** radio button.

Step 3 Configure the following parameters:

a) Interface — Enter a capture interface type for packet capture
b) Ethernet — 802.3 traffic on the Ethernet port
c) Radio 1 (2.4GHz) / Radio 2 (5GHz) — 802.11 traffic on the radio interface
d) Duration — Enter the time duration in seconds for capture. No duration limitation from CloudShark. The default is 60.
e) CloudShark URL - Enter the host name of CloudShark. The default URL: https://www.cloudshark.org
f) CloudShark API Key - Enter the valid API token you registered from CloudShark

Step 4 The communication with CloudShark is by HTTPS. If you want to use self-signed SSL certificate, select **Yes** option and click **Upload a certificate** to upload the certificate you signed.

Step 5 Enter the protocols you want to capture in Filter expression field. Only those packets after being filtered will be transferred to CloudShark

Step 6 There are two modes for packet capture:

a) **All Wireless Traffic** — Capture all wireless packets.
b) **Traffic To/From this AP** — Capture the packet sent from the AP or AP received.

Step 7 Click **Enable Filters**. The following three options are available:

a) **Ignore Beacons** — Enables or disables the capturing of 802.11 beacons detected or transmitted by the Radio
b) **Filter on Client** — Specifies the MAC address for WLAN Client Filter.

Note The Client Filter is active only when a capture is performed on an 802.11 interface.

c) **Filter on SSID** — Select a SSID name for packet capture.

Step 8 Click **Apply**. The changes are saved to the Startup Configuration.

Step 9 Click **Start Capture**. In the Packet Capture mode, the packets captured are transmitted to CloudShark site in real time. Upon activation, the packet capture proceeds until one of the following events occur:

a) The capture time reaches the configured duration.
b) The capture file reaches its maximum size.
c) The administrator stops the capture.

Wireshark

First, download Wireshark and install it on your computer. You can download Wireshark from https://www.wireshark.org/.

To initiate the Wireshark network analyzer tool for Microsoft Windows, follow these steps:

Step 1 On your computer, initiate the Wireshark tool.

Step 2 In the menu, click **Capture > Options**. A popup window appears.

Step 3 In the Interface field, select **Remote**. A popup window appears.

Step 4 In the Host field, enter the IP address of the WAP device.

Step 5 In the Port field, enter the port number of the WAP device. For example, enter 2002 if you used the default, or enter the port number if you used a port other than the default.

Step 6 Click **OK**.

Step 7 Select the interface from which you need to capture the packets. At the Wireshark popup window, next to the IP address, there is a drop-down menu to select the interfaces. The interface can be one of the following:

Linux bridge interface in the wap device

```
--rpcap://[192.168.1.220]:2002/brtrunk
```

Wired LAN interface

```
-- rpcap://[192.168.1.220]:2002/eth0
```

VAP0 traffic on radio 1

```
-- rpcap://[192.168.1.220]:2002/wlan0
```

802.11 traffic

```
-- rpcap://[192.168.1.220]:2002/radio1
```

At WAP361, VAP1 ~ VAP7 traffic

```
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7
```

At WAP150, VAP1 ~ VAP3 traffic

```
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3
```

You can trace up to four interfaces on the WAP device simultaneously. However, you must start a separate Wireshark session for each interface. To initiate additional remote capture sessions, repeat the Wireshark configuration steps. No configuration required on the WAP device.

Note The system uses four consecutive port numbers, starting with the configured port for the remote packet capture sessions. Verify that you have four consecutive port numbers available. We recommend that if you do not use the default port; use a port number greater than 1024.

When you are capturing traffic on the radio interface, you can disable beacon capture, but other 802.11 control frames are still sent to Wireshark. You can set up a display filter to show only:

- Data frames in the trace.
- Traffic on specific Basic Service Set IDs (BSSIDs).
- Traffic between two clients.

Some examples of useful display filters are:

- Exclude beacons and ACK/RTS/CTS frames:

  !(wlan.fc.type_subtype == 8 | | wlan.fc.type == 1)

- Data frames only:

  wlan.fc.type == 2

- Traffic on a specific BSSID:

  wlan.bssid == 00:02:bc:00:17:d0

- All traffic to and from a specific client:

  wlan.addr == 00:00:e8:4e:5f:8e

In remote capture mode, traffic is sent to the computer running Wireshark through one of the network interfaces. Depending on the location of the Wireshark tool, the traffic can be sent on an Ethernet interface or one of the radios. To avoid a traffic flood caused by tracing the packets, the WAP device automatically installs a capture filter to filter out all packets destined to the Wireshark application. For example, if the Wireshark IP port is configured to be 58000, then this capture filter is automatically installed on the WAP device:

not port range 58000-58004

Due to performance and security issues, the packet capture mode is not saved in NVRAM on the WAP device. If the WAP device resets, the capture mode is disabled and then you must enable it again to resume capturing traffic. Packet capture parameters (other than the mode) are saved in NVRAM.

Enabling the packet capture feature can create a security issue: Unauthorized clients may be able to connect to the WAP device and trace user data. The performance of the WAP device also is negatively impacted during packet capture, and this impact continues to a lesser extent even when there is no active Wireshark session. To minimize the performance impact on the WAP device during traffic capture, install capture filters to limit which traffic is sent to the Wireshark tool. When capturing 802.11 traffic, a large portion of the captured frames tend to be beacons (typically sent every 100 ms by all access points). Although Wireshark supports a display filter for beacon frames, it does not support a capture filter to prevent the WAP device from forwarding the captured beacon packets to the Wireshark tool. To reduce the performance impact of capturing the 802.11 beacons, disable the capture beacons mode.

Packet Capture File Download

You can download a capture file by TFTP to a configured TFTP server, or by HTTP/HTTPS to a computer. A capture is automatically stopped when the capture file download command is triggered.

Because the capture file is located in the RAM file system, it disappears if the WAP device is reset.

To download a packet capture file using TFTP:

Step 1 Click **Download to TFTP Server**.

Step 2 Specify a **Server IPv4 Address** in the field provided.

Step 3 Enter the **Destination File Name** to download if different from the default. By default, the captured packets are stored in the folder file /tmp/apcapture.pcap on the WAP device.

Step 4 Click **Download**.

Using HTTP

To download a packet capture file using HTTP:

Step 1 Click **Download to this Device**. A confirmation pop-up message will appear.

Step 2 Click **Yes**. A pop-up enables you to select a network location to save the file.

Support Information

This Support Information page displays the status of the CPU and RAM.

To record and display the CPU/RAM activity, follow these steps:

Step 1 Select **Troubleshoot** > **Support Information**.

Step 2 Click **CPU**— The device to record and display the CPU activity. To stop the recording, re-click **CPU**.

Step 3 Click **RAM**— The device to record and display the RAM activity. To stop the recording, re-click **RAM**.

The chart displays the **CPU/RAM** status as follows:

- A blue line shows the CPU activity.
- A red line show RAM activity.
- The first line chart update data every 1 seconds. It will show the CPU/RAM activity in 60 seconds.
- The second line chart update data every 5 seconds. It will show the CPU/RAM activity in 5 minutes.

Download CPU/RAM Data

Use the Support Information page to download CPU/RAM activity in your selected time. You can provide the text file to the technical support personnel to assist them in troubleshooting problems. To download the CPU/RAM data, do the following:

Step 1 Select **Troubleshoot > Support Information**.

Step 2 In the **Download Data** section, check **Enable** and **Apply** to enable the download.

Step 3 Select the time you wish to perform the download: **Today, Last 7 Days, Last 30 Days, All, Custom**.

Step 4 Complete the **To** and **From** fields with the yyyy-mm-dd and then set the time with the hh:mm:ss.

Step 5 Click **Download** to generate the file based on the current system settings. After a short pause, a window appears to enable you to save the file to your computer.