HPE Aruba Networking Central Troubleshooting Guide

Hewlett Packard Enterprise

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America

Contents

Chapter 1
About this Guide

HPE Aruba Networking Central is a cloud-based network management platform that manages your wireless, WAN, and wired networks with Instant AOS APs, Gateways, and Switches.

This guide provides the necessary background information and available resources to troubleshoot features and services offered in HPE Aruba Networking Central.

This document does not cover every possible trouble event that might occur on HPE Aruba Networking Central but, instead focuses on those events that are frequently seen by the Technical Assistance Center (TAC) or frequently asked questions from newsgroups.

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, HPE Aruba Networking will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 1: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://networkingsupport.hpe.com/home
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200

International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

Chapter 2
Troubleshooting Workflows

This section provides details on the typical issues that you might face with the devices managed by HPE Aruba Networking Central network and the steps to help troubleshoot these issues.

For more information on the troubleshooting workflows, see the following topics:

- Client Connectivity
- Device Issues
- AI Insights
- Network Check

Client Connectivity

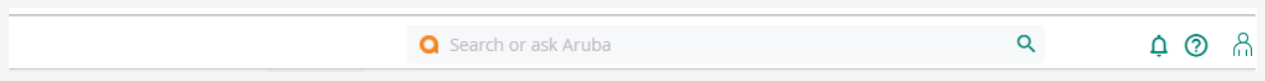
The following section provides details on the typical issues that you might face while connecting to the clients in the HPE Aruba Networking Central network and the steps to help troubleshoot these issues.

Troubleshooting Made Easy Using the Search Bar

When there are many clients and devices in a network, it is difficult for a user to navigate and identify a particular client or a device to diagnose an issue. The search bar in the **HPE Aruba Networking Central** app enables users to search for clients, devices, and infrastructure connected to the network. The search engine uses Natural Language Processing (NLP) to analyze queries and return relevant search results.

The following figure illustrates the search bar option in HPE Aruba Networking Central.

Figure 1 *Search Bar*



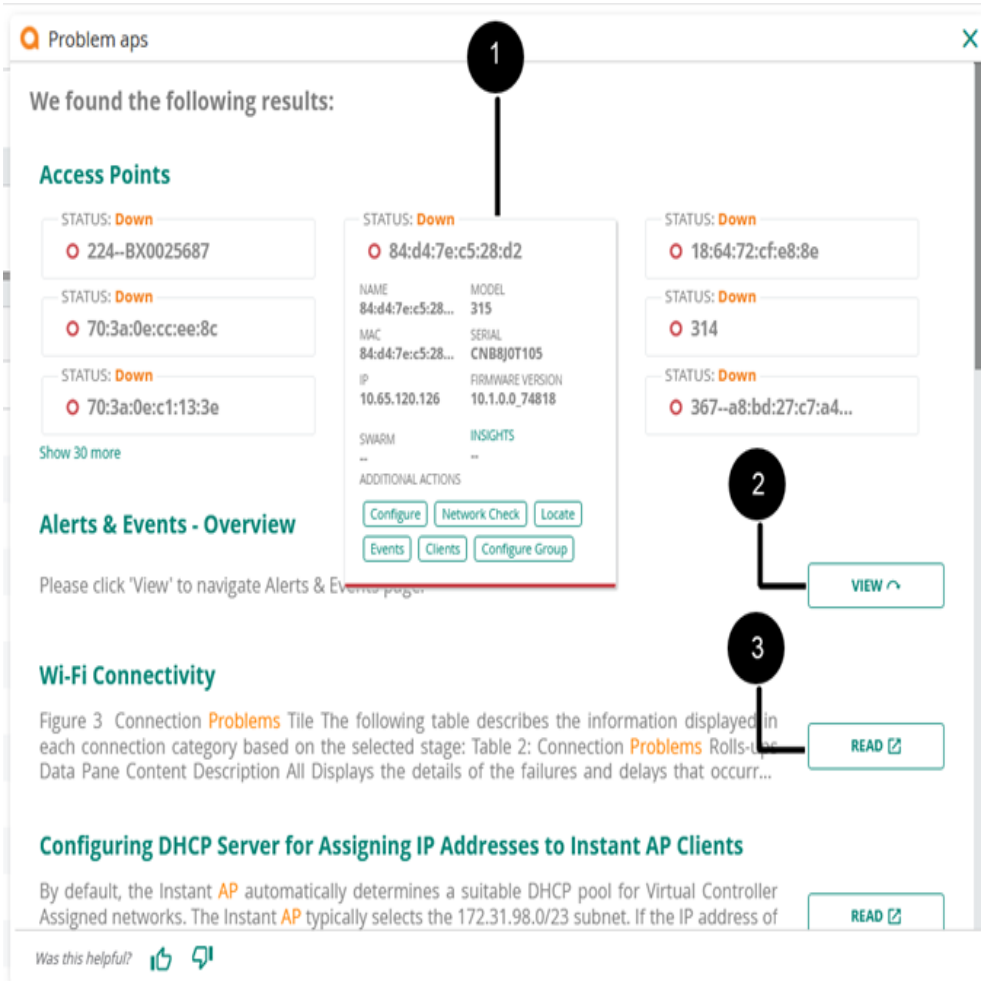
To start a search in the HPE Aruba Networking Central UI, click the search bar or press **/** (forward slash) on your computer keyboard.

When you click the search bar, you can see the search suggestions in the **Recent** and **Suggested Search** list.

- **Recent**—Shows the searches performed recently in the search bar. These suggestions help you quickly look at the previous searches.
- **Suggested Search**—Shows search suggestions corresponding to the workflow that you follow in the **HPE Aruba Networking Central** app. The suggested search help you perform onboarding, monitoring, configuring, and troubleshooting tasks.

The following figure illustrates the sample search results in HPE Aruba Networking Central.

Figure 2 *Sample Search Result*



AI Search

This is selectively available HPE Aruba Networking Central feature. Contact your Account Manager to enable it in your HPE Aruba Networking Central account.

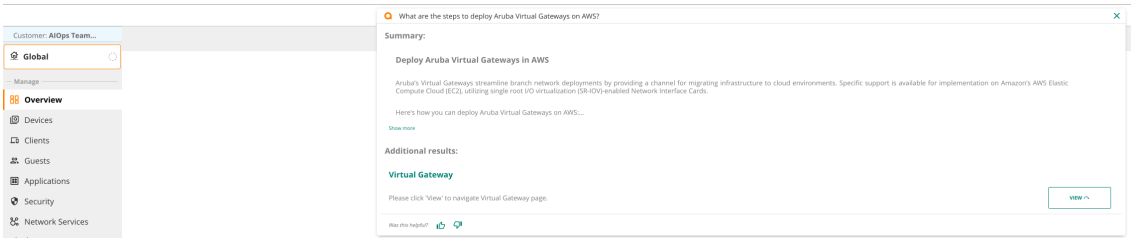
By integrating the latest advancements in AI/ML and leveraging sophisticated Large Language Models (LLMs), the **Search** bar transcends the capabilities of conventional search functions. It is engineered to not only comprehend the explicit keywords but to interpret the underlying intent of user inquiries. This intelligent design allows the system to offer predictive suggestions, anticipate needs, and provide a search experience that feels intuitive and human-like.

In addition to these summaries, the **Search** bar creates pathways by providing direct links to both the HPE Aruba Networking Central user interface and the TechDocs WebHelp. This integrated approach ensures that users have immediate access to detailed information, offering depth and context at their fingertips.

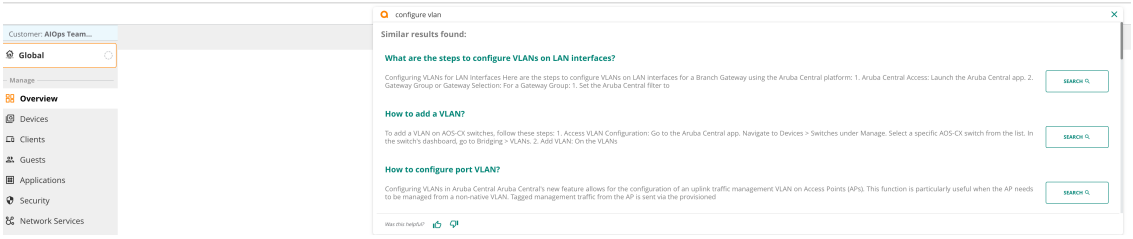
While searching for a relevant information for any query that you might have, you can type the query in the **Search** bar and a summary for the specific query will be displayed along with the links to the HPE Aruba Networking Central user interface and documentation Webhelp for further detailed information.

The **Search** bar has the following three capabilities for easy search:

- It provides documentation summary of the query that you have typed in the **Search** bar along with links to HPE Aruba Networking Central user interface and documentation TechDocs WebHelp.



- It assists in forming queries/ questions (auto-complete) that you might have based on the keywords that you have entered in the **Search** bar.



You can also provide your feedback, by clicking thumbs up or thumbs down displayed at the bottom of the search results.

From the search results, you can navigate to:

- **Search Cards**—displays monitoring summary and links to configuration, monitoring, and troubleshooting pages in the **HPE Aruba Networking Central** app.
- **View**—relevant links to the corresponding pages in the **HPE Aruba Networking Central** app.
- **Read**—relevant links to the help pages in the HPE Aruba Networking Central Help Center.

For more information on the list of recommended search terms for different categories, see Using the Search Bar.

Datapath of a WLAN Client

HPE Aruba Networking Central automatically populates the datapath of a WLAN client.

To view the datapath of a WLAN client, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The **Clients** page is displayed in **List** view.

NOTE

By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
   - **All**—Displays a list of all the clients connected to the network.
   - **AP**—Displays a list of clients connected to the Instant AP.

- **Switch**—Displays a list of clients connected to the switch.
- **Gateway**—Displays a list of clients connected to the gateway.

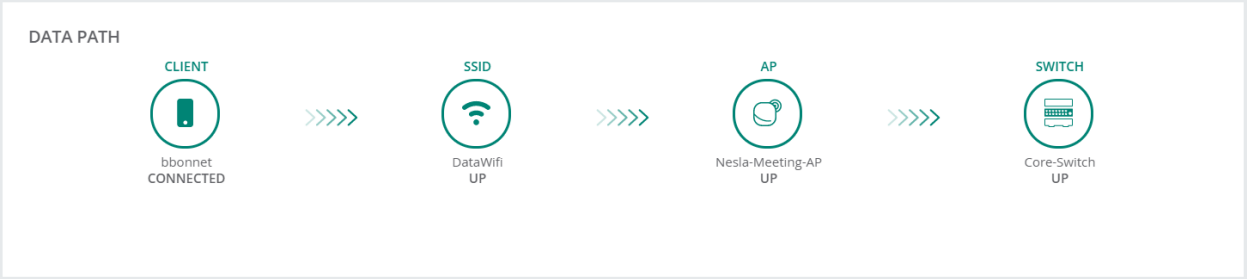
4. To filter the clients based on the state of connectivity, click the connectivity type from the **Client Summary** bar:
   - **Connecting**—Displays a list of client connections that are in progress.
   - **Connected**—Displays a list of clients that are successfully connected to the network.
   - **Failed**—Displays a list of all failed client connections.
   - **Offline**—Displays a list of all offline clients.
   - **Blocked—Displays** a list of all blocked clients.
5. In the **Clients Summary** bar, click **Wireless**, **Wired**, or **Remote** to filter the clients based on connectivity type.
6. In the **Clients** table, click a client listed under **Client Name**.

   The **Summary** tab is displayed.
7. In the **Client Details** page, the **Data Path** pane displays the datapath of the client in the network.

   The **Datapath** can be one of the following:
   - **Client** > **SSID** > **AP**
   - **Client** > **SSID** > **AP** > **Switch**
   - **Client** > **SSID** > **AP** > **Switch** > **Gateway**
   - **Client** > **SSID** > **AP** > **Gateway**

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

Figure 3 *Client—Datapath*



Client Health Issues

Client health is the efficiency at which an AP transmits downstream traffic to a particular client. This value is determined as the ratio of ideal airtime required for transmitting a packet from an AP to a client to the actual time taken for the packet transmission in percentage. Ideal air time assumes the highest data rate without any retransmission.

A client health metric of 100% means the actual airtime that the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means that the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means that the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.

Viewing the Client Health

To view the client health, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The **Clients** page is displayed in **List** view.

By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
   - **All**—Displays a list of all the clients connected to the network.
   - **AP**—Displays a list of clients connected to the Instant AP.
   - **Switch**—Displays a list of clients connected to the switch.
   - **Gateway**—Displays a list of clients connected to the gateway.

The wired client will show up in the **All Clients** page only if the client is connected to an HPE Aruba Networking 2540 Series, HPE Aruba Networking 2920 Series, HPE Aruba Networking 2930F Series, HPE Aruba Networking 2930M Series, HPE Aruba Networking 3810 Series, or HPE Aruba Networking 5400R Series switch.

4. To filter clients based on the network to which the clients are connected, click the network type from the **Clients Summary** bar:
   - **All**—Displays a list of all the clients connected to the network.
   - **Wireless**—Displays a list of clients connected to the wireless network.
   - **Wired**—Displays a list of clients connected to the wired network.
   - **Remote**—Displays a list of clients connected through a VPN. The remote clients are denoted by the icon.
5. To filter the clients based on the state of connectivity, click the connectivity type from the **Clients Summary** bar:
   - **Connecting**—Displays a list of client connections that are in progress.
   - **Connected**—Displays a list of clients that are successfully connected to the network.
   - **Failed**—Displays a list of all failed client connections.
   - **Offline**—Displays a list of all offline clients.
   - **Blocked**—Displays a list of all blocked clients.
6. In the **Clients** table, click the **Health** column to view the health of the client. The value of the client health can be one of the following:
   - **Poor**—0-30
   - **Fair**—31-70
   - **Good**—71-100

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

Offline Clients

Offline clients are the clients that were seen in a selected time duration, but are currently disconnected from the HPE Aruba Networking Central network. HPE Aruba Networking Central provides details of offline clients connected to the wireless and wired network. The **Clients** page provides a summary view of all the clients connected to the network.

To view the offline clients, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The **Clients** page is displayed in **List** view.

By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
   - **All**—Displays a list of all the clients connected to the network.
   - **AP**—Displays a list of clients connected to the Instant AP.
   - **Switch**—Displays a list of clients connected to the switch.
   - **Gateway**—Displays a list of clients connected to the gateway.

The wired client will show up in the **All Clients** page only if the client is connected to an HPE Aruba Networking 2540 Series, HPE Aruba Networking 2920 Series, HPE Aruba Networking 2930F Series, HPE Aruba Networking 2930M Series, HPE Aruba Networking 3810 Series, or HPE Aruba Networking 5400R Series switch.

4. To filter clients based on the network to which the clients are connected, click the network type from the **Clients Summary** bar:
   - **All**—Displays a list of all the clients connected to the network.
   - **Wireless**—Displays a list of clients connected to the wireless network.
   - **Wired**—Displays a list of clients connected to the wired network.
   - **Remote**—Displays a list of clients connected through a VPN. The remote clients are denoted by the  icon.
5. In the **Clients Summary** bar, click **Offline** to view the offline clients.

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

The **Clients** table lists the details of each client. By default, **All** clients is selected and the table displays the following columns: **Client Name**, **Status**, **IP Address**, **VLAN**, **Connected To**, **SSID/Port**, **AP Role**, **Gateway Role**, and **Health**. The default columns displayed are different and contextual based on AP, switch, and gateway.

Click the ellipsis  icon to perform additional operations:

- **Select All**—Selects all columns.
- **Reset Columns**—Resets the table view to the default columns.

HPE Aruba Networking Central allows you to download the global list of events to your local browser.

Click  to download the list of events as a **.csv** file.

If a filter icon appears next to the column header, click and enter the filter criteria or select a filter criteria. For example, to search a client, click the predefined filter criteria: **ConnectingConnected**, **Offline**, **Failed**, or **Blocked** from the **Client Summary** bar and in the **Client Name** column enter the name of the client. HPE Aruba Networking Central provides a near-instant refresh of the client status if the client is connecting or connected to an access point.

Table 2: *All Client Details*

Column Names	Applicability	Description
Client Name	▪ All ▪ AP ▪ Switch ▪ Gateway	Username, hostname, or MAC address of the client. Click the client name to view the **Summary** page.
Status	▪ All ▪ AP ▪ Switch ▪ Gateway	Client connection status. Use the filter option to view the following: ▪ Connecting—Applicable only for wireless clients. ▪ Connected—Applicable for all client types. ▪ Offline—Applicable for all client types. ▪ Failed—Applicable only for wireless clients. ▪ Blocked—Applicable only for wireless clients. Hover the cursor over the status column to view a pop-up summary based on the connection status. The status summary is populated based on the status type. Each status type and the summary is described below: ▪ **Connecting**: ◦ **Client name**—Name of the client. ◦ **Last Seen Time**—Date and time the

Table 2: *All Client Details*

Column Names	Applicability	Description
		client was last connected. ▪ **Connected**: ◦ **Client name**—Name of the client. ◦ **Authentication**—Type of authentication. Displays the authentication label only for authenticated clients. ◦ **IP address**—Client IP address. ◦ **Connected Since**—Date and time at which the client was connected. ◦ **Failure Stage**—Stage of the connection where the client failed to connect. It is not applicable for the wired clients, so displayed as NA. ◦ **Health Score**—Device health. ◦ **Connected Device Port**—The device port that the wired client is connected to. ▪ **Failed**: ◦ **Client name**—Name of the client. ◦ **Last Seen Time**—Date and time the client was last connected. ◦ **Failure Stage**—Stage of the connection where the client failed to

Table 2: *All Client Details*

Column Names	Applicability	Description
		connect. ◦ **Failure Reason**—Reason for the connection failure. ▪ **Offline**: ◦ **Client name**—Name of the client. ◦ **Authentication**—Type of authentication. Displays the authentication label only for authenticated clients. ◦ **IP address**—Client IP address ◦ **Connected Since**—Date and time at which the client was connected. ◦ **Last Seen Time**—Date and time the client was last connected. ◦ **Failure Stage**—Stage of the connection where the client failed to connect. ◦ **Connected Device Port**—The device port that the wired client is connected to. ▪ **Blocked**: ◦ **Client name**—Name of the client. ◦ **Last Seen Time**—Date and time the client was last connected.
IP Address	▪ All ▪ AP	IP address of the client.

Table 2: *All Client Details*

Column Names	Applicability	Description
	▪ Switch ▪ Gateway	
VLAN	▪ All ▪ AP ▪ Switch ▪ Gateway	VLAN of the device to which the client is connected.
Connected To	All	AP name, Switch name, or Gateway name. This is the first layer 2 hop for the client. If the device does not have a name, the MAC address is displayed.
AP Role	▪ All ▪ AP	Role assigned by the AP.
Gateway Role	▪ All ▪ Gateway	Role assigned by the HPE Aruba Networking Gateway.
Health	▪ All ▪ AP	Client health. The value can be one of the following: ▪ **Poor**—0-30 ▪ **Fair**—31-70 ▪ **Good**—71-100
SSID/Port	▪ All ▪ AP ▪ Switch ▪ Gateway	Displays the SSID for wireless clients and the port number for wired clients. The column title displays **SSID** and **Port** interchangeably based on the device filters. For APs, the column title displays **SSID**. For switch and gateway, the column title displays **Port**.
Insights	▪ All ▪ AP	The total number of AI insights generated for the client.
Switch Role	▪ All ▪ Switch	Role assigned by the HPE Aruba Networking switch.
Failure Stage	▪ All ▪ AP	Failure status of the client that failed to connect. The failure reasons could be:

Table 2: *All Client Details*

Column Names	Applicability	Description
		▪ Association failure ▪ MAC authentication failure ▪ 802.1X authentication failure ▪ Key exchange failure ▪ DHCP failure ▪ Captive Portal failure
Group Name	▪ All ▪ AP ▪ Switch ▪ Gateway	Displays the name of the group that the device is connected to. The **Connected To** column displays the device name that the client is connected to.
Site Name	▪ All ▪ AP ▪ Switch ▪ Gateway	Displays the name of the site that the device is connected to. The **Connected To** column displays the device name that the client is connected to.
MAC Address	▪ All ▪ AP ▪ Switch ▪ Gateway	MAC address of the client.
Hostname	▪ All ▪ AP ▪ Gateway	Host name of the client.
User Name	▪ All ▪ AP ▪ Switch ▪ Gateway	Username of the client.
Key Management	▪ All ▪ AP	Security mode used by the client.
Authentication	▪ All ▪ AP ▪ Switch ▪ Gateway	Authentication type used by the client to connect with the device.

Table 2: *All Client Details*

Column Names	Applicability	Description
Global Unicast IPv6 Address	▪ All ▪ AP ▪ Gateway	When the IPv6 address is present for a client, you can view its Global Unicast IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed.
Link Local IPv6 Address	▪ All ▪ AP ▪ Gateway	When the IPv6 address is present for a client, you can view its Link Local IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed.
Capabilities	▪ All ▪ AP	Client 802.11 capabilities.
Usage	▪ All ▪ AP ▪ Switch ▪ Gateway	Total data usage for the selected time period.
Last Seen Time	▪ All ▪ AP ▪ Switch ▪ Gateway	Date and time when the client was last seen.
Connected Since	▪ All ▪ AP ▪ Switch ▪ Gateway	Date and time since when the client was connected.
AP Name	▪ All ▪ AP	Name of the AP.
AP Mac Address	▪ All ▪ AP	MAC address of the AP.
Channel/Band	▪ All ▪ AP	Last connected channel and band.
Switch Name	▪ All ▪ Switch	Name of the switch.
Port	▪ All ▪ Switch ▪ Gateway	Port number of the switch.

Table 2: *All Client Details*

Column Names	Applicability	Description
Gateway Name	▪ All ▪ Gateway	Name of the HPE Aruba Networking Gateway.
Tunneled	▪ All ▪ AP ▪ Switch ▪ Gateway	Tunnel mode is applicable for the HPE Aruba Networking Gateway managed WLAN, UBT, or PBT client.
Segmentation	▪ All ▪ AP ▪ Switch ▪ Gateway	Type of segmentation. The type of segmentation can be: ▪ None ▪ UBT ▪ PBT ▪ Underlay ▪ Overlay **NOTE:** To view the details about dynamic segmentation, a gateway must be licensed in HPE Aruba Networking Central and connected to the switch.
Client Category	▪ All ▪ AP ▪ Gateway	Displays the category of the profiled device. For example, Access Points, Computer, Smart Device, VoIP phone.
Client Family	▪ All ▪ AP ▪ Gateway	Displays the type of operating system or vendor. For example, if the client category is Computer, the client family can be Windows, Linux, or Apple Mac.
Client OS	▪ All ▪ AP ▪ Gateway	Displays the operating system that the device runs on. For example, if the client category is Computer and the client family is Windows, the client OS can be Windows or Windows 8/10.

Issues in the Application Layer

In an HPE Aruba Networking Central-managed network, Network Check aims to identify, diagnose, and debug issues on your network. The **Network Check** tab under **Analyze** > **Tools** page captures the

troubleshooting utilities that are used to test a network entity and collect results based on your selection. You must have admin privileges or read-write privileges to perform network checks.

The following tests are available to diagnose issues pertaining to WLAN network connections:

- **HTTP Test**—The HTTP test is a performance test to identify the time taken to load a web page. It sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, the issue could be isolated to the client device.
- **HTTPS Test**—The HTTPS test is a performance test to identify the time taken to load a web page. It sends packets to the HTTPS URL and tries to establish a connection and exchange data. If the HTTPS website returns a response, the issue could be isolated to the client device.
- **TCP Test**—The TCP test verifies network connectivity to remote hosts with the remote host-port combination approach. It sends packets to the host, for example, an FTP server, and tries to establish a connection and exchange data. If the FTP server returns a response, the issue could be isolated to the client device.

HTTP Test

To perform an HTTP test, complete the following steps:

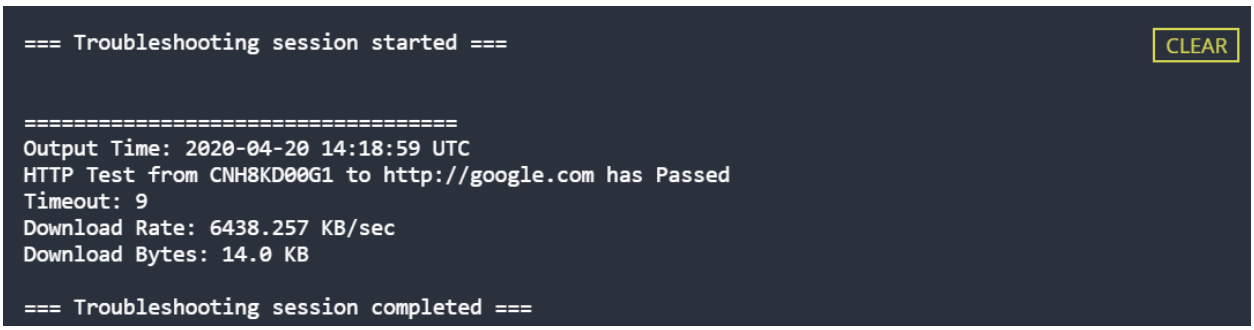
1. In the **HPE Aruba Networking Central** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Tools**.

   The Network Check tab is displayed.
4. From the **Device Type** drop-down list, select **Access Point**.
5. From the **Test** drop-down list, select **HTTP Test**.
6. The value in the **Sources** drop-down list is auto-populated based on the wireless client selected.
7. In the **URL** field, enter the HTTP URL for which you want to perform the HTTP test. For example, http://*hostname* or http://*ipaddress*.
8. Optionally, expand **Show Additional Test Settings** to enter the timeout value in seconds in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.

Show Additional Test Settings is disabled when no **Test** type is selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 4 *HTTP Test—Device Output*



NOTE

The HTTP test is supported only from AOS 8.3.0.0 or later versions. The test support only IPv4 address or domain name in the URL field.

HTTPS Test

To perform an HTTPS test, complete the following steps:

1. In the **HPE Aruba Networking Central** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Tools**.

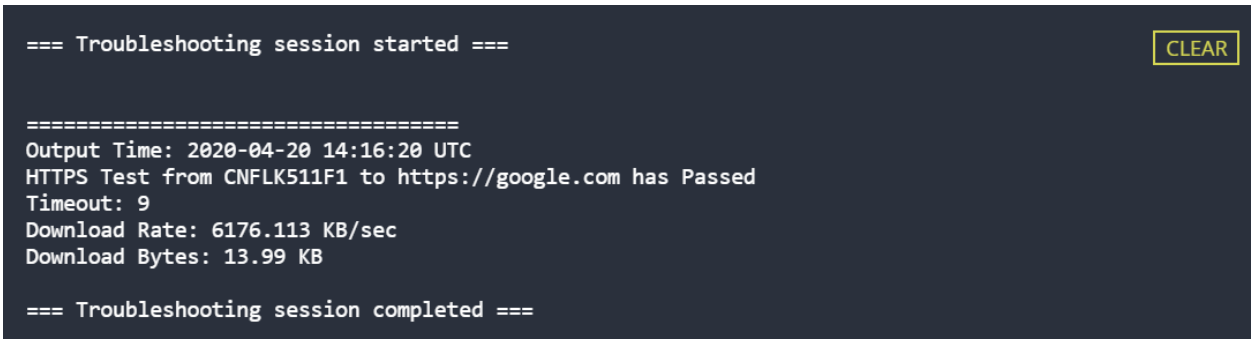
   The Network Check tab is displayed.
4. From the **Device Type** drop-down list, select **Access Point**.
5. From the **Test** drop-down list, select **HTTPS Test**.
6. The value in the **Sources** drop-down list is auto-populated based on the wireless client selected.
7. In the **URL** field, enter the HTTPS URL for which you want to perform the HTTPS test. For example, https://*hostname* or http://*ipaddress*.
8. Optionally, expand **Show Additional Test Settings** to enter the timeout value in seconds in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.

NOTE

Show Additional Test Settings is disabled when no **Test** type is selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 5 *HTTPS Test—Device Output*



NOTE

The HTTPS test is supported only from AOS 8.4.0.0 or later versions. The test support only IPv4 address or domain name in the URL field.

TCP Test

To perform a TCP test, complete the following steps:

1. In the **HPE Aruba Networking Central** app, search for a specific wireless client in the **Search Bar**.

2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Tools**.

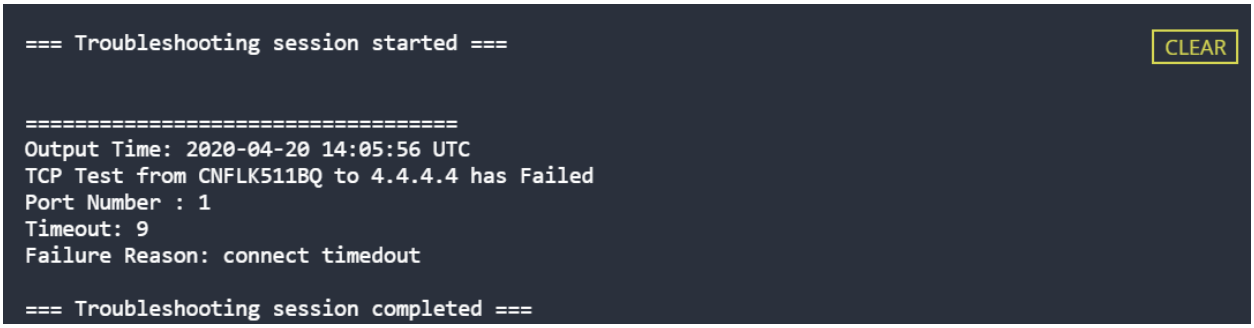
   The Network Check tab is displayed.
4. From the **Device Type** drop-down list, select **Access Point**.
5. From the **Test** drop-down list, select **TCP Test**.
6. The value in the **Sources** drop-down list is auto populated based on the wireless client selected.
7. In the **Host** field, enter the IPv4 address. Hostname is not supported.
8. In the **Port** field, enter the port number. The port number should be in the range 1 to 65535.
9. Optionally, expand **Show Additional Test Settings** to enter the timeout value in seconds in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.

NOTE

Show Additional Test Settings is disabled when no **Test** type is selected.

10. Click **Run**. The output is displayed in the **Device Output** section.

Figure 6 *TCP Test—Device Output*



NOTE

The TCP test is supported only from AOS 8.3.0.0 or later versions.

Viewing the Device Output

After you execute troubleshooting commands on the device, HPE Aruba Networking Central displays the output in the **Device Output** section of the **Tools** page.

The output pane displays a list of devices on which the troubleshooting commands were executed, the test type, initial timestamp, source, and target. It also shows the status of the tests as, in progress, complete, and the buffer time. If there are multiple devices, select the device for which you want to view the output.

NOTE

Output history of a device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.

- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click **Export** to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *HPE Aruba Networking Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for AOS-S switch CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Roaming Issues in a Wireless Client

Roaming is the process of a wireless client moving from one source AP to another AP within the same Extended Service Set (ESS) without losing connection. When a wireless client roams between two APs, the association to the new AP terminates the previous AP association and the destination AP creates an event.

In HPE Aruba Networking Central, the **Roaming Experience** pane provides the details of the roaming events and latency parameters of a client.

Viewing the Roaming Experience Pane

To view the **Roaming Experience** pane, complete the following steps:

1. In the **HPE Aruba Networking Central** app, search for a specific wireless client in the **Search Bar**.
2. Click any one of the wireless clients listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. In the **Client Details** page, the **Roaming Experience** pane displays the details of the roaming events and latency parameters of a client.

The **Roaming Experience** pane displays two views, the grid view and the trend view.

Grid View

The grid view is the default view and provides the following information:
Table 3: *Grid View*

Parameter	Description
Date/Time	Displays the date and time of occurrence of the client roaming/association events.
SSID	The SSID to which the client is connected.
Latency(ms)	Roaming latency in milliseconds between source and destination AP. **NOTE:** Roaming latencies above 50 ms are considered as high latency roaming events.
To BSSID	The BSSID of the destination AP.
Source AP	AP to which the client was connected.

Parameter	Description
Destination AP	AP to which the client is connected.
Roaming Type	The type of roaming. Click the ⌄ icon to filter the data based on the following roaming types: ▪ 11r ▪ okc ▪ 802.11
Band	Radio band on which the client is connected.
RSSI (dBm)	Received Signal Strength Indicator (RSSI) on the client. It is the estimated measure of the power level received by client from the AP.

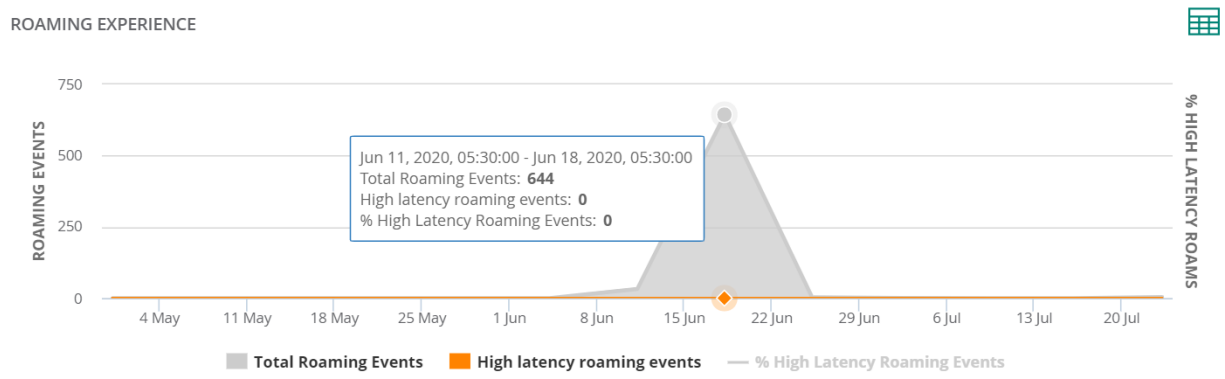
NOTE

- By default, the **Roaming Experience** table displays data for the last 3 hours. To view the table for a different time range, use the **Time Range Filter**.
- A search filter is provided only for the **Data/Time** and **Roaming Type** columns.

Trend View

The trend view displays a chart that shows the percentage of high latency roaming events, total roaming events, and the number of high latency roaming events at a particular instance based on the value selected in the **Time Range Filter**.

Figure 7 *Roaming Experience—Trend View*



Client Connection to the Network

When a client tries to connect to the AP or the network, and is unable to do so, you can navigate to the **Clients** page and check the reasons for failure.

The **Clients** page provides a list view of all the clients connected to the network. You can filter clients based on the network the clients are connected to. This page displays key client information and also allows you to view a specific client detail page.

To view the list of **Failed** clients, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The **Clients** page is displayed in **List** view.

By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
   - **All**—Displays a list of all the clients connected to the network.
   - **AP**—Displays a list of clients connected to the Instant AP.
   - **Switch**—Displays a list of clients connected to the switch.
   - **Gateway**—Displays a list of clients connected to the gateway.

The wired clients will show up in the **All Clients** page only if the client is connected to an HPE Aruba Networking 2540 Series, HPE Aruba Networking 2920 Series, HPE Aruba Networking 2930F Series, HPE Aruba Networking 2930M Series, HPE Aruba Networking 3810 Series, or HPE Aruba Networking 5400R Series switch.

4. To filter clients based on the network to which the clients are connected, click the network type from the **Client Summary** bar:
   - **All**—Displays a list of all the clients connected to the network.
   - **Wireless**—Displays a list of clients connected to the wireless network.
   - **Wired**—Displays a list of clients connected to the wired network.
   - **Remote**—Displays a list of clients connected through a VPN. The remote clients are denoted by the icon.
5. In the **Client Summary** bar, click **Failed** to view a list of all failed client connections.
6. In the **Clients** table, the **Failure Stage** column provides the following information:

Table 4: *Client Details*

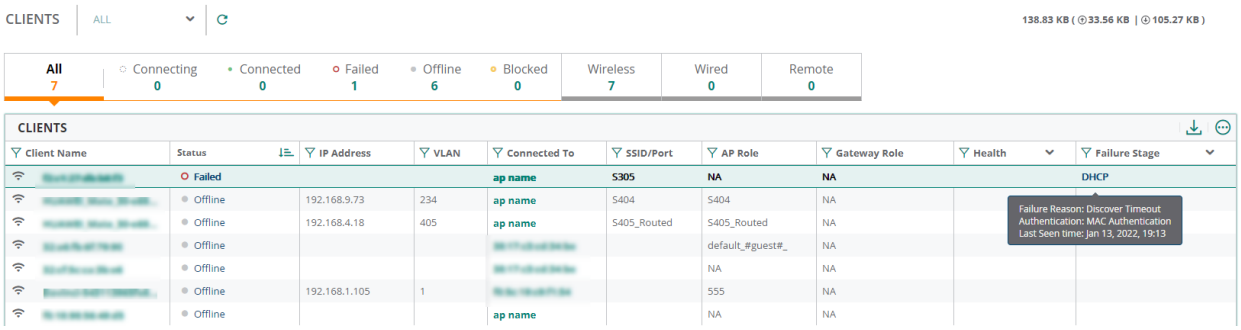
Failure Stage	▪ All ▪ AP	Failure status of the client that failed to connect. The failure reasons could be: ▪ Association error ▪ MAC authentication error ▪ 802.1X authentication error ▪ Key exchange error ▪ DHCP error ▪ Captive Portal error

Hover over the specific failure stage to display detailed information regarding the type of error. For example, if the failure stage column displays failure stage as **DHCP**, and you hover your mouse over **DHCP**, it displays the following:

- **Failure Reason**
- **Last Seen time**

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

Figure 8 *Client Details*



You must also check if multiple failures have occurred and if the client is denylisted. When a client is denylisted, it is not allowed to associate with an AP in the network. If a client is connected to the network when it is denylisted, a deauthentication message is sent to force client disconnection. You can denylist a client manually or dynamically.

Denylisting Clients Manually

Manual denylisting adds the MAC address of a client to the denylist. These clients are added into a permanent denylist and are not allowed to connect to the network unless they are removed from the denylist.

To add a client to the denylist manually, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the access points are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
   The Security details page is displayed.
5. Click the **Denylisting** accordion.
6. Under **Manual Denylisting**, click **+** and enter the MAC address of the client to be denylisted.
7. Click **OK**.
8. Click **Save Settings**.

To delete a client from the manual denylist, select the MAC Address of the client under the **Manual Denylisting**, and then click the delete icon.

NOTE

You can configure a maximum number of authentication failures by the clients, after which a client must be denylisted. For the denylisting to take effect, you must enable the denylisting option when you create or edit the WLAN SSID profile. Go to **WLANs** > **Security** > **Advanced Settings** and enable the **Denylisting** option.

Denylisting Clients Dynamically

Clients can be denylisted dynamically when they exceed the authentication failure threshold or when a denylisting rule is triggered as part of the authentication process.

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically denylisted by an Instant AP.

In session firewall based denylisting, an ACL rule automates denylisting. When the ACL rule is triggered, it sends out denylist information, and the client is denylisted.

To configure the denylisting duration, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the access points are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
   The Security details page is displayed.
5. Click the **Denylisting** accordion.
6. Under **Dynamic Denylisting**, enter the following information:
   a. For **Auth Failure Denylist Time**, enter the duration after which the clients that exceed the authentication failure threshold must be denylisted.
   b. For **Policy Enforcement Failure Rule Denylisted Time**, enter the duration after which the clients can be denylisted due to an ACL rule trigger.
7. Click **Save Settings**.

NOTE

You can configure a maximum number of authentication failures by the clients, after which a client must be denylisted. To enable session-firewall-based denylisting, select the **Denylist** check box in the **Access Rule** page during the WLAN SSID profile creation.

After the failure reasons are detected, select the client and navigate to the **Clients Detail** page. Click **Tools** under **Analyze** in the left navigation pane, and perform network check and advance troubleshooting check under **Network Check** and **Commands** respectively.

Client Live Troubleshooting

HPE Aruba Networking Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis. Live troubleshooting is supported only if the Instant APs are running 8.4.0.0 firmware version or a later version.

To troubleshoot a client at the site level, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Sites**.
2. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.
3. Enter the MAC address of the client and click **Start Troubleshooting**.

To troubleshoot a wireless client, complete the following steps:

1. In the **HPE Aruba Networking Central** app, search for the specific wireless client in the **Search Bar** for which you want to perform live troubleshooting.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.

The troubleshooting session runs for 15 minutes and the status is displayed every minute. If you want to stop, live troubleshooting, click **Stop Troubleshooting** to go back to the historical view.

After the live troubleshooting session ends, the details of the events are displayed in the live events table.

Live Events Details

The following details are captured and displayed in the **Live Events** table:

- **Occurred On**—Displays the timestamp of the event. Use the filter option to filter the events by date and time.
- **Device Name**—Displays the name of the device that the client is connected to. Set the filter to select a specific device under **Sites**.
- **AP Name**—Displays the name of the AP that the client is connected to. Use the filter option to select a specific AP.
- **Category**—Displays the category of the event. Use the filter option to filter the events by category.
- **Description**—Displays a description of the event. Use the filter option to filter the events based on description.

Packet Capture

HPE Aruba Networking Central allows you to interact and launch a targeted packet capture on a client connected to a specific access point or a switch. After you start packet capture from the UI, HPE Aruba Networking Central notifies the access point and the switch. The default packet capture duration is 15 minutes. After you start packet capture, use the toggle button to stop packet capture, or go back to the **Client Overview** page.

For packet capture, for a wired client connected to an HPE Aruba Networking 5400R Switch Series (V3 mode), ensure that “no-allow v2 modules” is set for the switch. Packet capture for stack switches works only if the client is connected to the commander of the stack.

Starting Packet Capture

You can start packet capture from the wireless or wired clients page. Packet capture can be done at a site level (wireless client only) or for a selected client.

To start packet capture at a site level, perform the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Sites** that contains at least one device. The dashboard context for the selected site is displayed.
2. Under **Analyze**, click **Live Events**.The **Live Events** page is displayed.
3. Enter the MAC address of the client.

NOTE

At a site level, HPE Aruba Networking Central does not support packet capture for a wired client connected to a switch.

4. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
5. Click **Start Troubleshooting**.

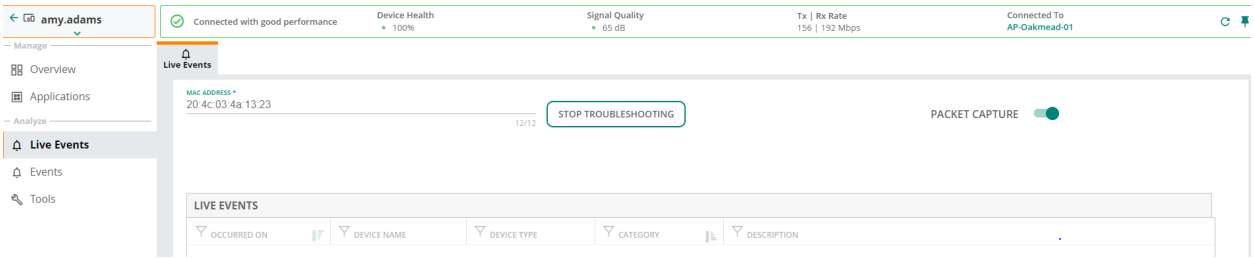
To start packet capture for a wireless or wired client, perform the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The Clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the name of the wireless or wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** or **Wired** to filter the clients connected to the wireless or wired clients respectively.
5. Enter the client name in the **Client Name** column, and click the client name.
6. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed. The client live troubleshooting starts automatically for the selected client.
7. Click **Stop Troubleshooting** to stop live troubleshooting.
8. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
9. Click **Start Troubleshooting** to live troubleshoot the selected client. Live packet capture starts for the selected client.

   The live troubleshooting session runs for a duration of 15 minutes. After the live troubleshooting session ends, a **Download PCAP** text appears above the live events table. Click **Download PCAP** to download the generated PCAP file on your local system.

Figure 9 *Live Events*



Notifying Network and Client Anomalies to the Administrator

The **Wi-Fi Connectivity** page in HPE Aruba Networking Central enables you to check connection details of all the clients connected to an AP in the network. The data can be used to notify administrators of the possible anomalies in the network.

To view the **Wi-Fi Connectivity** page, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Groups** or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Overview**, click **Wi-Fi Connectivity**.

   The **Wi-Fi Connectivity** page is displayed.

NOTE

To view the connectivity data for all the Instant APs in the **Wi-Fi Connectivity** dashboard, ensure the NTP server is configured for all the devices and time is synced correctly corresponding to the respective time zone. If the time stamp is not correct, the telemetry data received from the Instant APs will be dropped. Also, set the firewall to allow traffic on port 123 to sync the time with the NTP server.

By default, the graphs on the **Wi-Fi Connectivity** page is plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Time Range Filter** icon. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, and 1 month.

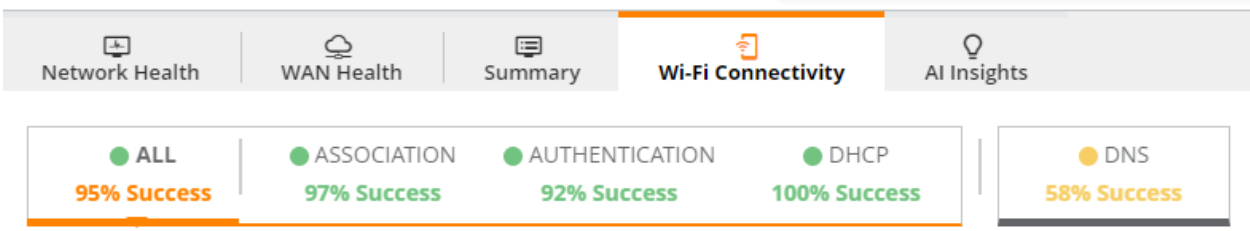
This section includes the following topics:

- Connectivity Summary Bar
- Connection Experience
- AI Insights
- Connection Problems
- Connection Events

Connectivity Summary Bar

The connectivity summary bar displays the details of all clients in percentage. It displays the percentage success rate of each stage for the users to know the network performance.

Figure 10 *Connectivity Summary Bar*



The following table describes the information displayed in each section:

Table 5: *Connectivity Summary Bar*

Field	Description
All	Displays the aggregated success percentage of **Association**, **Authentication**, and **DHCP** for all clients connected to the network.
Association	Displays the percentage of successful attempts made by a client to connect to the network.
Authentication	Displays the percentage of successful attempts of client authentication.

Table 5: *Connectivity Summary Bar*

Field	Description
DHCP	Displays the percentage of successful attempts of DHCP requests and responses when onboarding a client.
DNS	Displays the percentage of successful attempts in the detected DNS resolutions, when a client is connected to the network.

Connection Experience

The **Connection Experience** tile displays the overall success percentage, total number of attempts, number of successful attempts, total delays, and the total failures for each stage based on the selected time range filter. To view the connection experience for individual stage, select the stage type from the **Connectivity Summary** bar, the **Connection Experience** displays the chart for the selected stage. Select **All** to view the success percentage for all the stages. You can hover over the time series graph to view the success percentage for a specific time. The individual stage displays the **Attempts**, **Failures**, **Success**, and **Delays** on the time series graph.

Figure 11 *Connection Experience Tile—Global or Group Context*

Only in the site context, the **Connection Experience** tile provides the **Baseline Comparison** option. You can compare the connection with either **Company Baseline** or **Class Baseline**.

The following comparisons are available:

- **Company Baseline**—Compares the connection between the selected site and other sites associated to the same user. It is selected by default.

- **Class Baseline**—Compares the selected site and sites having similar configuration. The baseline is denoted by orange dotted line on the time series graph and the blue line is the Wi-Fi connection of the selected site.

Figure 12 *Connection Experience Tile—Site Context*

AI Insights

The **AI Insights** tile provides a list of AI Insights generated for a selected time range. To view the details, click on a selected **AI Insight**. The page gets redirected to the AI Insights under the **AI Insights** page. Click each of the listed AI Insight for a detailed analysis based on the impact on the network.

NOTE

AI Insights is not implemented at a Group level and the page displays **No AI Insights observed**.

Connection Problems

The **Connection Problems** tile displays the details of **Failures** and **Delays** graphically for each of the categories from the drop-down list. Each graph displays the top five MAC addresses or SSID based on the selected category. Each category in the **Connection Problems** drop-down lists changes based on the selected stage in the **Connectivity Summary** bar. Selecting the required category from the drop-down displays the failures and delays in a pie chart with percentage, and a bar graph with the number of failures and delays. Hover the cursor over each graph to view the number of failures or delays for each stage.

Figure 13 *Connection Problems Tile*

The following table describes the information displayed in each connection category based on the selected stage:

Table 6: *Connection Problems Rolls-Ups*

Data Pane Content	Description
All	Displays the details of the failures and delays that occurred during a client connection. The chart displays the failure details of Association, Authentication, and DHCP for each client. The Connection Problems drop-down list includes the following categories: ▪ **By Stage** ▪ **By Clients** ▪ **By Access Points** ▪ **By Band** ▪ **By SSID**
Association	Charts the details of the failures and delays that occurred during a client association. The **Connection Problems** drop-down list includes the following categories: ▪ **By Clients** ▪ **By Access Points** ▪ **By Band** ▪ **By SSID** ▪ **By Reason**
Authentication	Charts the details of the failures and delays that occurred during a client authentication. The **Connection Problems** drop-down list includes the following categories: ▪ **By Type** ▪ **By Clients**

Data Pane Content	Description
	▪ **By Access Points** ▪ **By Band** ▪ **By SSID** ▪ **By Server**
DHCP	Charts the details of the failures and delays that occurred during the attempts of DHCP requests and responses by a client. The **Connection Problems** drop-down list includes the following categories: ▪ **By Clients** ▪ **By Access Points** ▪ **By Reason**
DNS	Charts the details of the failures and delays that occurred during the attempts in detected DNS resolutions when a client is connected to the network. The **Connection Problems** drop-down list includes the following categories: ▪ **By Access Points** ▪ **By Reason** ▪ **By Server**

Connection Events

The **Connection Events** table details out the list of delays and failures for each client based on the client MAC addresses. Click the **List** icon to view the connection events table. Click the **Connection Events** drop-down list to filter the events **By Clients** or **By Access Points**. The **Connection Events** table displays the following information:

Table 7: *Connection Events*

Data Pane Content	Description
MAC Address	Displays the MAC address of the client.
Name	Displays the name of the access point.
Delays	Displays the delays that occurred during the event.
Failures	Displays the failure details that occurred during the event.

Client Devices do not Discover Printers across the Subnet

For client devices to discover printers across the subnet, you have to turn on the AirGroup service available in HPE Aruba Networking Central.

AirGroup is a zero configuration networking protocol that enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home.

Bonjour can be installed on computers running Microsoft Windows and is supported by the new network-capable printers. Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these devices. The AirGroup solution supports both wired and wireless devices. Wired

devices that support Bonjour services are part of AirGroup when connected to a VLAN that is terminated on the Virtual Controller.

In addition to the mDNS protocol, Instant APs also support Universal Plug and Play (UPnP) and Digital Living Network Alliance (DLNA) enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network.

DLNA also provides the ability to share data between the Windows or Android-based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

To enable AirGroup services, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to a group that contains at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
3. Click the **Config** icon.
   The tabs to configure access points is displayed.
4. Click **Show Advanced**, and then click the **Services** tab.
   The Services details page is displayed.
5. Click the **AirGroup** accordion.
6. Select the **AirGroup** check box.

- The **mDNS (Bonjour)** and **SSDP (DLNA/UPNP)** check-boxes are selected by default. Select at least **mDNS (Bonjour)** or **SSDP (DLNA/UPNP)** to proceed further.
- Optionally, select the **Guest Bonjour Multicast** check box to allow guest users to use the Bonjour services that are enabled in a guest VLAN. When **Guest Bonjour Multicast** is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup does not discover or enforce policies in the guest VLAN.

7. Expand **AirGroup Settings**, and then select the **AirPrint** check box to enable wireless printing between AirPrint capable devices and AirPrint compatible printers.
   - Optionally, when enabling an AirGroup service, define disallowed roles. The disallowed roles are not allowed to use the specific AirGroup service. To disallow roles:
     1. Click **Edit** against **Disallowed Roles**.
     2. Move the roles from the **Available** pool to the **Selected** pool.
     3. Click **Ok**.
   - Optionally, when enabling an AirGroup service, define disallowed VLANs. The disallowed VLANs are not allowed to use the specific AirGroup service. To disallow VLANs:
     1. Click **Edit** against **Disallowed VLANs**.
     2. Type the VLANs in **Enter comma-separated list of VLAN IDs**. Separate multiple VLANs with a comma.
     3. Click **Ok**.
   - Optionally, configure and enable a new AirGroup service. If defined, disallowed roles or VLANs are not allowed to use the new AirGroup service. To configure and enable a new AirGroup service:
     1. Click **Add New Service**.
     2. Type the service name in **Service Name**. Use alphanumeric characters.

3. Type a service ID in **Service ID**. Use **+** to add additional service IDs.

   Sample service ID: **urn:schemas-upnp-org:service:RenderingControl:1** or **_sleep-proxy._udp**.
4. Click **Ok**.
5. Select the check box against the new AirGroup service.

8. Optionally, under **ClearPass Settings** sub-accordion, configure the following parameters listed:

Table 8: *ClearPass Settings*

Mode	Description
ClearPass Policy Manager Server 1	Specify the ClearPass Policy Manager server to use. Select one from the drop-down or define a new ClearPass Policy Manager server.
Enforce ClearPass Registration	Specify is ClearPass registration should be enforced.

9. Click **Save Settings**.

Poor Voice Call Quality Issues

The growing use of Wi-Fi and the proliferation of mobile tablet and smartphone clients cause control and visibility challenges for communication and collaboration applications. To overcome these challenges, HPE Aruba Networking offers the Unified Communication and Collaboration (UCC) application service to manage your enterprise communication ecosystem.

The UCC application on HPE Aruba Networking Central devices provides a seamless user experience for voice calls, video calls, and application sharing when using communication and collaboration tools. The UCC application actively monitors voice, video, and application sharing sessions, provides traffic visibility, and allows you to prioritize the required sessions. The UCC application also leverages the functions of the service engine on the cloud platform and provides rich visual metrics for analytical purposes.

To access the UCC application, obtain a valid subscription. To obtain a subscription for the UCC application, contact the HPE Aruba Networking Central Sales team.

To analyze the VOIP call quality of a specific client, complete the following steps:

1. In the WebUI app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Manage**, click **Applications** > **UCC**.

   The **UCC** page is displayed in the **List** view.

Alternatively, you can also perform the following steps to navigate to the **UCC** tab to check the VOIP call quality of a specific client:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Clients**.
   The Clients page is displayed in the **List** view.
3. In the **Clients Summary** bar, click **Wireless** to filter the clients connected to the wireless network.
4. In the **Clients** table, click a client listed under **Client Name**.
   The Summary tab is displayed.
5. Under **Manage**, click **Applications** > **UCC**.
   The UCC page is displayed in the **List** view.
6. Click the **Summary** icon to view the UCC dashboard.

Summary View

The **Summary** view in the **Applications > UCC** page provides the following information:

Time Filter

The time filter allows you to set a time range to display the corresponding data on the graph. You can set the filter to any of the following time ranges:

- **3 Hours**—The graph displays the details for the past three hours.
- **1 Day**—The graph displays the details for the current day.
- **1 Week**—The graph displays the details for the current week.
- **1 Month**—The graph displays the details for the current month.

Summary Bar

The banner in the header pane shows the following call quality details:

- **Calls**—Displays the total number of calls that have ended.
- **Good**—Displays the total number of good calls that have ended. A good call has an UCC RTPA score of more than 70.
- **Fair**—Displays the total number of fair calls that have ended. A fair call has an UCC RTPA score in the range of 30 to 70.
- **Poor**—Displays the total number of poor calls that have ended. A poor call has an UCC RTPA score of less than 30.
- **Unknown**—Displays the total number of calls whose status is unknown. A call is classified as unknown if the ALG does not support RTPA or the UCC score is not available.

Click any option to view the corresponding graph. For example, if you click **Good**. The **Calls** graph displays only the calls that are categorized as good for the selected time range.

NOTE

- For the ALG like Skype SDN, the end-to-end Mean Opinion Score (MOS) is used. A good call has a MOS of more than 3.5, a fair call has a MOS in the range of 2.0 to 3.5, a poor call has a MOS of less than 2.0, and an unknown call does not have a MOS.
- Wi-Fi Calling calls are not tracked. Wi-Fi Calling calls are not assigned an UCC RTPA score and are categorized as unknown.

By comparing the call quality and client health score, you can find out if the wireless network was the reason for the poor quality of VOIP calls. A poor value of the client health indicates that the issue is at

the wireless network side. In that case, go to the **Overview** > **AI Insights** page in the wireless **Client Details** page and check if the client is dwelling on the 2.4 GHz band. If the client is dwelling on the 2.4 GHz band, configure the VOIP Wireless LAN to the 5 GHz band.

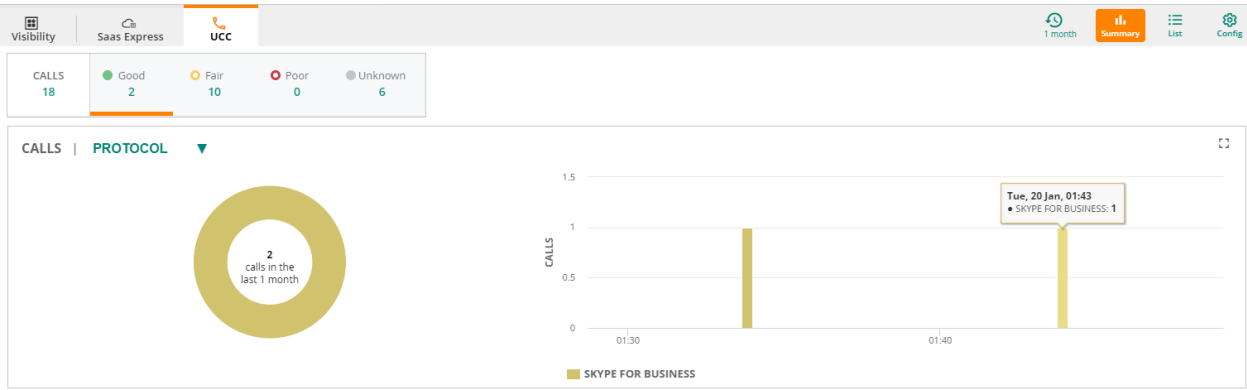
If there are no client insights in the **AI Insights** page, you must check for the following AI Insights in the site context:

- **Access Points were impacted by high 5 GHz usage**
- **Access Points impacted by high 2.4 GHz usage**
- **Access Points had an excessive number of channel changes**

Calls

The **Calls** graph displays a donut graph and bar graph of all, good, fair, poor, or unknown calls. You can filter the graph by **SSID**, **Protocol**, **OS**, **Session Type**, or **Quality**. By default, the graph is displayed for **Protocol**. Hover over any segment on the graph to view additional information. Click any segment on the graph to open the list view. Click the **Enlarge** icon to view the enlarged graph.

Figure 14 *Summary View*



Client Insights: Traffic Pattern Visibility

The **Application** page displays the **Visibility** tab.

The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications and websites. You can use this data to analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard. This data helps users to troubleshoot any traffic issues for any specific client. The tab consists of a list view and a graph view. The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**

Viewing Visibility Dashboard

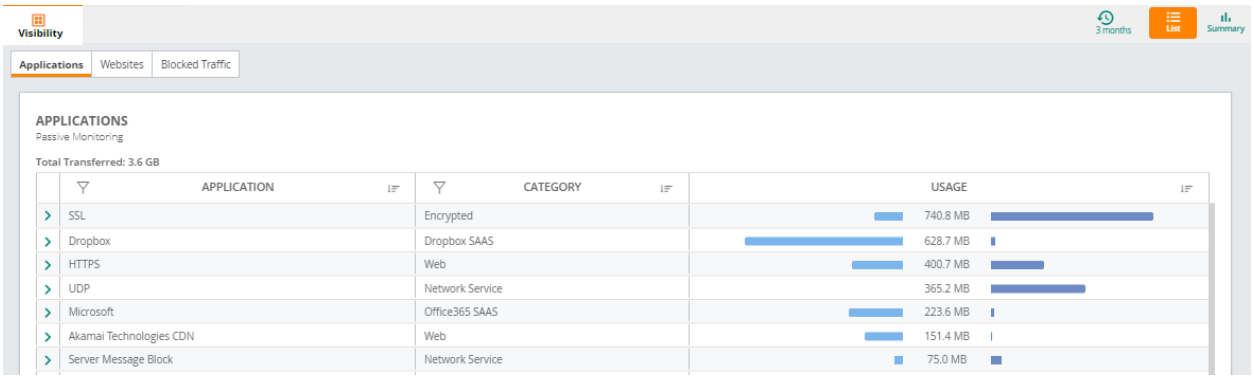
To view the **Visibility** dashboard, complete the following steps:

1. In the WebUI, set the filter to one of the options under **Groups** or **Sites**.
   For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Applications**.
   The visibility dashboard is displayed.

The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**
- **Blocked Traffic**

Figure 15 ***Visibility*** *dashboard at the global level*



Graph View in the Visibility Dashboard

Click the **Summary** icon in the **Visibility** dashboard to view both the applications and websites graphical information:

- **Applications**
  - **Applications**—The stacked bar graph and the pie chart in this tab displays details of the client traffic flowing to or from the top five classified applications listed on the **Applications** table. The legend below the graph displays the list of applications to which the traffic flow is detected. Select or deselect the application check box to show or hide the traffic flow data from the pie chart and stacked bar. By hovering the mouse on a pie chart and stacked bar, you can view the size of data flowing to and from the application same as displayed in legend.
  - **Categories**—The stacked bar graph in this tab displays details of the client traffic flowing to or from the top five classified application categories listed on the **Applications** table. The legend below the graph displays the list of applications categories to which the traffic flow is detected. Select or deselect the application category check box to show or hide the traffic flow data from the pie chart and stacked bar. By hovering the mouse on a pie chart and stacked bar, you can view the size of data flowing to and from the application same as displayed in legend.
- **Websites**
  - **Reputations**—The stacked bar graph and the pie chart in this tab displays details of client traffic flow for the top three reputations listed on the **Websites** table. The legend displays the list of websites based on its reputation, to which the traffic flow is detected. Select or deselect the reputation check box to show or hide the data from the pie chart and stacked bar. By hovering the mouse on a pie chart and stacked bar, you can view the size of data flowing to and from each of the websites that are categorized based on reputation.
  - **Web Categories**—The stacked bar graph and the pie chart in this tab displays details of client traffic flow for the top five web categories listed on the **Websites** table. Select or deselect the web category check box to show or hide the data from the pie chart and stacked bar. You can view the size of data flowing to and from each of the web categories by hovering the mouse on both the

stacked bar graph and pie chart. The legend below the graph displays the list of websites based on its reputation, to which the traffic flow is detected.

Figure 16 ***Visibility*** *dashboard in summary view*

- The Applications (Apps) and Web Categories charts are also displayed in the **Applications** pages for the Group, Site, APs, and Gateways levels.
- Application Visibility data is updated every 0th minute of every hour. The data population on the **Applications > Visibility** dashboard may be delayed by an hour when compared to the Application Visibility data displayed in the **Applications** pages for the Group, Site, APs, and Gateways levels.
- To view client traffic details, ensure that the DPI access rules are enabled on the Instant AP device.

NOTE

Device Issues

The following section provides details on the typical issues that you might face with devices provisioned and managed in the HPE Aruba Networking Central network and the steps to help troubleshoot these issues.

APs are not seen in the HPE Aruba Networking Central Network

HPE Aruba Networking Central validates device connectivity by the network Web socket connection that the device maintains with HPE Aruba Networking Central. If there is no communication of state information from the device for more than 5 minutes, HPE Aruba Networking Central marks the device as offline and the device is not configurable. You must also add device subscription licenses to enable the AP to appear in the HPE Aruba Networking Central network.

If the AP moves to a new network and the new connected Virtual Controller is not licensed, the AP is not shown in the network. For an AP to show up in HPE Aruba Networking Central, you must make sure that the MAC address and the serial number of the AP is added in the device inventory and also the AP is licensed in the inventory. Even after adding the device inventory, if the AP is not showing up in HPE

Aruba Networking Central you must verify if the following ports and URLs are allowed by the firewall at the customer's site:

- TCP Port 443
- TCP Port 80
- UDP Port 123
- activate.arubanetworks.com
- device.arubanetworks.com
- rcs-m.central.arubanetworks.com (console)
- pool.ntp.org (time server)

If all the ports and URLs are allowed by the firewall and you are still unable to see the AP in HPE Aruba Networking Central, raise a ticket with the Technical Support.

Devices are Offline in the HPE Aruba Networking Central Network

If there is a network outage or the device looses a web socket connection to HPE Aruba Networking Central at the customer site, the device goes offline and is unable to communicate with HPE Aruba Networking Central. Apart from network issues, there are a few physical issues that could also cause the device to go offline.

- The LEDs on the AP are turned OFF.
- System LED lights are blinking in green or red—Depending on the warning and error messages the color of the LED lights change from green to red.
- Bad Ethernet port—If the Ethernet port on the AP has gone bad or the cable itself has some issue.
- Cable falling off—The AP is so heated up and has caused some physical damage. The AP shuts down automatically and reboots again because of the thermal issue.
- PoE issue—An AP is powered up either through an adapter or through the Ethernet port. There are two scenarios where an AP might not come up:
  - The Ethernet port does not provide sufficient power to the AP.
  - The Uplink port or PoE port is disabled or not configured correctly.

The **Switch Details** page will display PoE alerts and the status of the port that is connected to the AP.

To solve these physical issues of a device, you must issue a direct Return Merchandise Authorization (RMA).

Under Standard Warranty or Limited Lifetime Warranty (LLW) hardware RMAs are handled through best effort. Out of warranty and/or expired contract hardware requires Service Renewal prior to an RMA. TAC only handles defective RMAs under proper entitlement.

Cabling Issues in Switch

The **Cable Test** enables testing of the electrical connections in the switch cable. It checks whether the cabling is conformed to the cabling plans and is of expected quality. It is useful for production and maintenance.

To use the **Cable Test** feature, make sure that your switch is running the following software versions:

- AOS-CX switches: 10.11.1000 and later versions
- AOS-S switches: 16.05.000 and later versions

Cable Test

To perform a **Cable Test** on a switch, complete the following steps:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch listed under **Device Name** for which you want to perform the cable test.

        The dashboard context for the switch is displayed.
2. Under **Analyze** > **Tools**, click **Device Check**.
3. By default, the **Device Type** displays switch and the **Sources** drop-down list displays the selected switch..
4. From the **Test** drop-down list, select **Cable Test**.
5. From the **Port** drop-down list, enter a port number.
6. Click **Run**. The output is displayed in the **Cable Test Results** section.

- By default, the **Device Type** is set to **Switch** if a switch is configured in the data path, else a warning is displayed.
- The action will cause a loss of link on all tested ports and will take several seconds per port to complete.
- Enter port numbers and/or port ranges separated by commas. For stacking switch, enter member id/port number.

Figure 17 *Cable Test-Device Output*

Reboot an IoT Sensor

Users can reboot an IoT sensor to troubleshoot and conduct event log analysis, renegotiate LLDP power supplied, apply new role configuration, or for enhanced serviceability.

The **PoE Bounce** test reboots an IoT sensor port interface and forces a client to re-initiate a DHCP request.

PoE Bounce is supported only from AOS Switch version 16.04.000 or later.

PoE Bounce

To perform a **PoE Bounce** test on a switch, complete the following steps:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

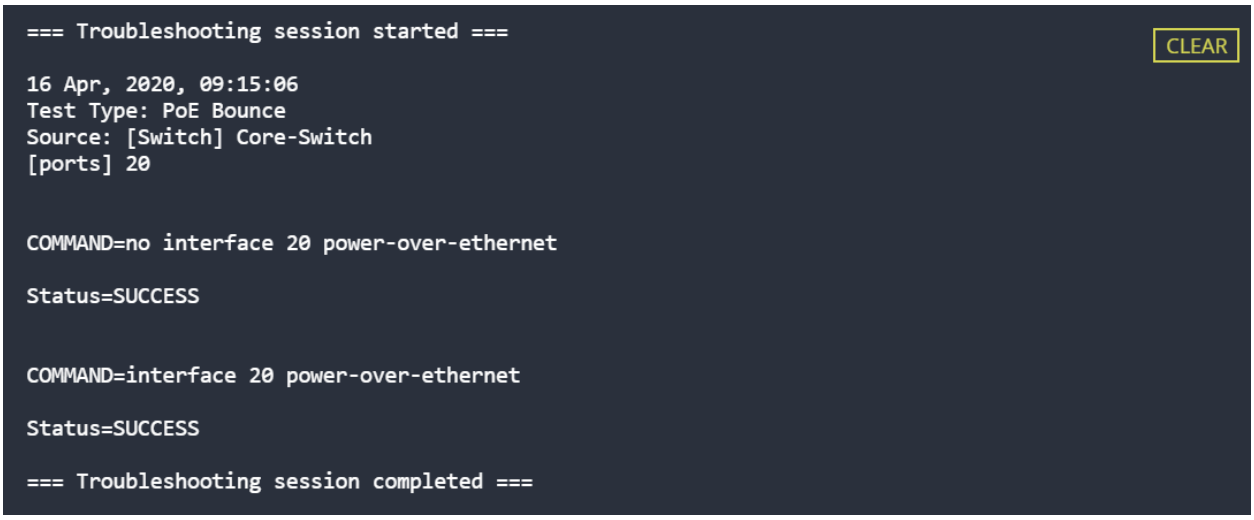
     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch listed under **Device Name** for which you want to perform the PoE bounce test.

        The dashboard context for the switch is displayed.
2. Under **Analyze** > **Tools**, click **Device Check**.
3. From the **Sources** drop-down list, select a source.
4. From the **Test** drop-down list, select **PoE Bounce**.
5. From the **Port** drop-down list, enter a port number.
6. Click **Run**. The output is displayed in the **Device Output** section.

- By default, the **Device Type** is set to **Switch** if a switch is configured in the data path, else a warning is displayed.
- Multiple device selections is not allowed at this level.
- Devices which are already running commands shall not execute newly added commands.

Figure 18 *PoE Bounce Test-Device Output*



Device Troubleshooting with Remote Console

HPE Aruba Networking Central allows you to open a remote console for a CLI session through SSH for a gateway, switch, and access point to troubleshoot device issues. Users with admin roles can access the device directly from the console to debug any device issues.

You can view the already recorded sessions or can create a new session to start troubleshooting your device.

NOTE

When you create a new session HPE Aruba Networking Central records and saves it for future analysis.

Viewing Recorded Console Sessions

HPE Aruba Networking Central records an ongoing troubleshooting session and saves it for future analysis. You can view and download the session recordings and replay it anytime to diagnose any devise issues in the network.

To view the recorded sessions, complete the following steps:

1. In the WebUI, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

        The dashboard context for the device is displayed.
2. Under **Analyze** > **Tools**, click the **Console** tab.

   The **Remote Console Session** page is displayed and by default, the **New Session** tab is selected.
3. Click the **Saved Sessions** tab.

4. From the **Device Type** drop-down list, select the device type.
5. Select the device and click **View Recorded Session**.

   The **Remote Console** terminal appears and starts playing the most recent recorded session.

You can perform the following tasks from the **Remote Console** section:

- Click to open the **Device** pane to see the list of devices that have active sessions.
- Click the device drop-down list at the right corner to select the session that you want to play. You can also delete a session by clicking the delete icon available next to each session name.
- Click the maximize icon to maximize the remote console pane.
- Click the download icon to download a recorded session and replay for offline analysis.

Historical Events & Event Categorization

The **Alerts and Events** dashboard displays a list of alerts and events generated for events pertaining to device pre-provisioning and configuration. You can view events generated by AOS-S and AOS-CX switches, gateways, and access points. HPE Aruba Networking Central also allows you to troubleshoot issues related to a wireless client connected to an access point or a wired client connected to a switch or gateway. You can troubleshoot a specific device from the **Events** page by clicking the **Device Hostname** or the **Device MAC** and navigating to the device details page. Similarly, you can also troubleshoot a client issue on the client details page, by clicking the **Client MAC** from the **Events** page. On the device/client details page, you can select **Tools** option to start troubleshooting the issue.

To display events that occurred in the past, use the Time Range Filter ( ) option. You can select one of the following: **3 Hours**, **1 Week**, **1 Day**, or **1 Month**. To be more specific the **Events** table also provides a sort option where you can filter events specific to date and time.

To filter events by type you can use the **Advanced Filtering** option. You can also search events using the AI search capability that the **Description** column provides. For example, if you want to search and troubleshoot events related to "Captive Portal" failure, you can either filter it out using the advanced filtering option or, you can type "Captive Portal" in the description column header of the **Events** table and all the events related to captive portal failures are displayed.

The **Alerts & Events** page is not visible to users who do not have edit and view permission to the **Alerts & Events** page.

Events in List View

To view a summary of events, complete the following procedure:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.

c. Click a device listed under **Device Name**.

The dashboard context for the device is displayed.

2. Under **Analyze**, click **Alerts & Events**.

   By default, the **Alerts & Events** page displays the alert and events in the **List** view.

   The **Alerts & Events** dashboard offers a list view, summary view, and a configuration view.

Configuration view is only available at the **Global** context.

3. In the **Alerts & Events** summary bar, click **Events**.

   By default, the **List** view is selected and a consolidated list of events is displayed in the events table.

4. To view the graphs displaying alerts and events, click the **Summary** icon.

Events in Summary View

The graphs in the **Summary** view displays the summary of all events that occurred over a period of time. The events are displayed by type under which the maximum events are generated. Hover your mouse over the bar graphs to see the total count of events generated under each category.

The event graphs are displayed for the time range selected. Select the time range from the Time Range Filter ( ) to filter alerts and events and display historical events that occurred in the past which can be used to troubleshoot an issue for which the event was generated.

Advanced Event Filtering

HPE Aruba Networking Central allows you to filter the events based on the event types. To filter events based on types, complete the following steps:

1. In the **Events** page, click **Click here for advanced filtering** to filter the events based on event types.
2. Select the event type and click **Filter**.

   You can select multiple event types from the advanced filtering option.
3. The events table displays the list of events generated in each event type.

   The filter summary bar displays the total number of events in the selected category and the type (s) of events.
4. Optionally, to clear advanced filtering option, from the events summary bar, click **Clear All**.

   The advanced filtering gets cleared.

The following table describes the information displayed in each column of the **Events** table:

Table 9: *Events Pane*

Data Pane Content	Description
Occurred On	Displays the timestamp of the event. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the events.

Data Pane Content	Description
Device Type	Displays the type of the device, Access Point, Gateway, Switch, and Client. Use the filter option to filter events by device types.
Device Hostname	Displays the host name of the device where the event is generated. Use the filter option to filter events by hostname.
Device MAC	Displays the MAC address of the device. Use the filter option to filter events by device MAC.
Client MAC	Displays the MAC address of the client. Use the filter option to filter events by client MAC.
BSSID	Displays the BSSID of the device. Use the filter option to filter events by BSSID.
Event Type	Displays the type of the event.
Label	Displays the label name of the event. Use the filter option to filter events by label.
Site	Displays the site name of the event. Use the filter option to filter events by site.
Group	Displays the group name of the event. Use the filter option to filter events by group.
Description	Displays the description of the event. Use the column filter to perform a free search and filter an event based on the description. You can type a search phrase including client MAC, reason code, or BSSID and filter the events.
Collected Data	Displays the collected data for a specific event to perform any troubleshooting diagnosis. Use the filter to select the data type **CLI Logs**, **Dynamic PCAP**, or **Crash Logs**

To customize the **Alerts & Events** table, click the ellipses icon to select the required columns, or click **Reset to default** to set the table to the default columns.

HPE Aruba Networking Central allows you to download the global list of events to your local browser.

Click to download the list of events as a **.csv** file.

Onboarding & Post Connectivity Metrics Event

The **Alerts and Events** dashboard displays a list of alerts and events generated for events pertaining to device pre-provisioning and configuration. You can view events generated by AOS-S and AOS-CX switches, gateways, and access points. HPE Aruba Networking Central also allows you to troubleshoot issues related to a wireless client connected to an access point or a wired client connected to a switch or gateway.

To display events that occurred in the past, use the Time Range Filter ( ) option. You can select one of the following: **3 Hours**, **1 Week**, **1 Day**, or **1 Month**. To be more specific the **Events** table also provides a sort option where you can filter events specific to date and time.

NOTE

The **Alerts & Events** page is not visible to users who do not have edit and view permission to the **Alerts & Events** page.

There are various types of supported events available in HPE Aruba Networking Central, and one of the events is about onboarding clients that generate in three scenarios:

- Client successfully onboarded the device
- Client failed to onboard to the device
- Client time out to onboard the device

NOTE

Client onboarding failure and client onboarding timeout is listed in a single event, as onboarding failure with `reason_str` as a differentiator between the two.

To filter events by type you can use the **Advanced Filtering** option. You can also search events using the AI search capability that the **Description** column provides. If you want to search and troubleshoot events related to "Onboarding Client Failure", you can either filter it out using the advanced filtering option or, you can type "Onboarding Client Failure" in the description column header of the **Events** table and all the events related to onboarding failure are displayed.

NOTE

Onboarding events are only subscribed for APs running on firmware version 8.11 and above.

Following are the onboarding events that get generated depending on the success or failure phases:

Table 10: *Onboarding Client Events*

Event	Description
Client Onboarding Success	Onboarding success for client [*Client MAC* and time taken for Onboarding success is *Onboarding Success Time* ms.
Client Onboarding Failure - Deauthentication/Disassociation	Onboarding failed for client [*Client MAC* in Deauthentication/Disassociation phase to BSSID *BSSID* on channel [*Channel*] of AP hostname [*Device Hostname*].
Client Onboarding Failure - Authentication/Association	Onboarding failed for client [*Client MAC* in Authentication/Association phase to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client Onboarding Failure - MAC Authentication	Onboarding failed for client [*Client MAC*] in MAC Authentication phase to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client Onboarding Failure - Dot1x Authentication	Onboarding failed for client [*Client MAC*] in Dot1x Authentication phase to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client Onboarding Failure - Key Exchange	Onboarding failed for client [*Client MAC*] in Key Exchange phase to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client Onboarding Failure - L3 Failure	Onboarding failed for client [*Client MAC*] in L3 phase to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client Onboarding Failure - L3 Timeout	Onboarding failed for client [*Client MAC*] in L3 phase timeout to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].

Event	Description
Client Onboarding Failure - Captive Portal Authentication	Onboarding failed for client [*Client MAC*] in Captive Portal Authentication phase to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].

You can view the details of the events in the metadata provided in the UI and use the details to troubleshoot any onboarding event failure. The reason of the failure is also mentioned in the metadata, or you can also hover over the event description and view the reason.

Viewing the Events table

To view a summary of events, complete the following procedure:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

        The dashboard context for the device is displayed.
2. Under **Analyze**, click **Alerts & Events**.

   By default, the **Alerts & Events** page displays the alert and events in the **List** view.

   The **Alerts & Events** dashboard offers a list view, summary view, and a configuration view.

Configuration view is only available at the **Global** context.

3. In the **Alerts & Events** summary bar, click **Events**.

   By default, the **List** view is selected and a consolidated list of events is displayed in the events table.
4. To view the graphs displaying alerts and events, click the **Summary** icon.

Advanced Event Filtering

To filter events based on types, complete the following steps:

1. In the **Events** page, click **Click here for advanced filtering** to filter the events based on event types.
2. Select the event type and click **Filter**.

   You can select multiple event types from the advanced filtering option.
3. The events table displays the list of events generated in each event type.

   The filter summary bar displays the total number of events in the selected category and the type (s) of events.

4. Optionally, to clear advanced filtering option, from the events summary bar, click **Clear All**.
   The advanced filtering gets cleared.

To customize the **Alerts & Events** table, click the ellipses icon to select the required columns, or click **Reset to default** to set the table to the default columns.

HPE Aruba Networking Central allows you to download the global list of events to your local browser.

Click to download the list of events as a **.csv** file.

WAN and LAN Widgets in the Microbranch Solutions

The WAN and the LAN widgets in Microbranch solutions enables you to view and monitor WAN and LAN interfaces, the tunnels configured, and the path steering data for all the IDPS policies configured. Any issues that occur in these areas can be diagnosed and you can troubleshoot the issue with the help of the data obtained under these widgets.

Viewing the WAN > Summary tab

The **Summary** tab under **Manage** > **WAN** page in the gateway dashboard displays the port status, WAN interfaces, and Go Live options.

To navigate to the **WAN > Summary** tab in the gateway dashboard, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.
   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **WAN** > **Summary**.
   To exit the gateway dashboard, click the back arrow on the filter.
   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

WAN Interfaces

- Lists the WAN interfaces and provides the total number of WAN interfaces. Displays the summary of WAN uplinks. The following details are displayed for the port:

NOTE

Click the settings icon to reset or set the default columns that are displayed.

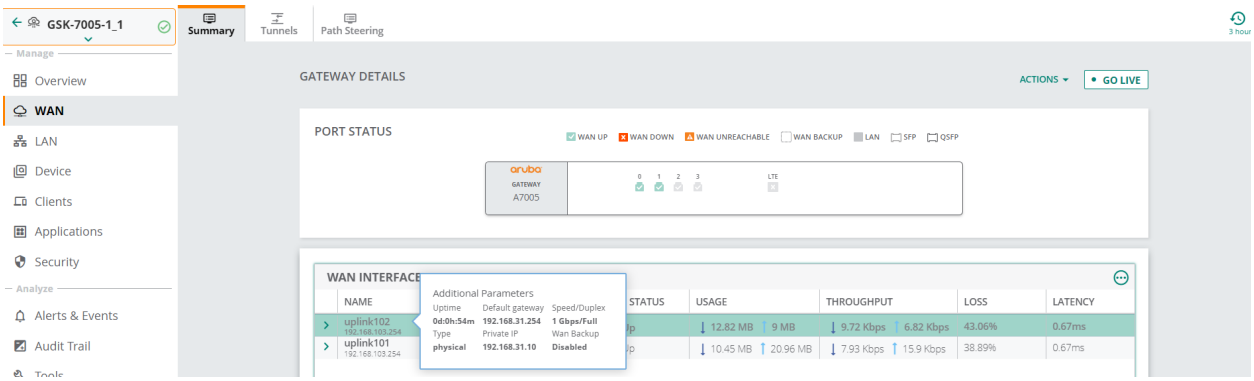
  - **Total WAN Interfaces**—Total number of WAN interfaces available.
  - **Name**—Name of the WAN interface.
  - **Port—Port** number along with the associated VLAN ID.
  - **WAN Status**—WAN reachability status.
  - **VPN Status**—VPNC reachability status.
  - **Usage**—WAN interface usage (Sent and Received).

- **Throughput**—WAN interface transmit and receive performance in Kbps.
- **Loss**—Loss percentage.
- **Latency**—The latency in milliseconds.

In the **WAN Interfaces** table, click a port number to display the **Packets** and **Errors** details.

- The following graphs are displayed under the **Packets** tab:
  - **Unicast**—The number of unicast packets per second.
  - **Multicast**—The number of multicast packets per second.
  - **Broadcast**—The number of broadcast packets per second.
- The following graphs are displayed under the **Errors** tab:
  - **CRC Errors**—The number of cyclic redundancy errors logged.
  - **Error Frames**—The number of error frames logged.
  - **Collisions**—The number of collisions encountered.
- **Additional Parameters**—In the **WAN Interfaces** table, hover on the WAN interface name to view the additional parameter for the WAN interface.

  Figure 19 *Additional Parameters*



  The following additional parameters are displayed for the WAN interface:
  - **Uptime**—Uptime of the uplink (DD-HH-MM).
  - **Default Gateway**—Default gateway.
  - **Speed/Duplex**—Port speed.
  - **Type**—Service provider uplink type (Physical / Virtual).
  - **Private IP**—Private IP address.
  - **WAN Backup**—Backup of WAN interface (Enabled or Disabled).

Expand the **WAN Interface** name to see the following details.

- **WAN Availability**—Provides an overall graphical representation of the selected interface's WAN availability based on reachability. The graph shows the selected WAN port's ability to reach its default gateway and health check IP.
- **VPN Availability**—Provides an overall graphical representation of the selected interface's VPN availability based on reachability.
- **Usage**—Provides a snapshot of the WAN usage and is available for **All Traffic**, **Internet**, and **VPN** specific information. You can see the incoming and outgoing traffic for the gateways with time plotted on the x-axis. Hover over the chart to see the incoming and outgoing traffic for a particular

time frame.

- **Top Applications**—Displays application level WAN usage per-uplink for top ten applications. Click the **Go to Applications** link to view details in the **Applications** tab.
  The WAN visibility is available only for 3 hours time range.

Click the following icons to see the chart in logarithmic scale or linear scale.

- Logarithmic Scale—Click this icon to view chart in logarithmic scale.
- Linear Scale—Click this icon to view chart in linear scale.

Click Received or Sent at the bottom of the chart to view or hide the usage chart for received or sent data.

- **Throughput**—Provides a graphical representation of the selected WAN interface's throughput. The graph displays the WAN interface's transmit and receive performance in bps.

  Click the following icons to see the chart in logarithmic scale or linear scale.

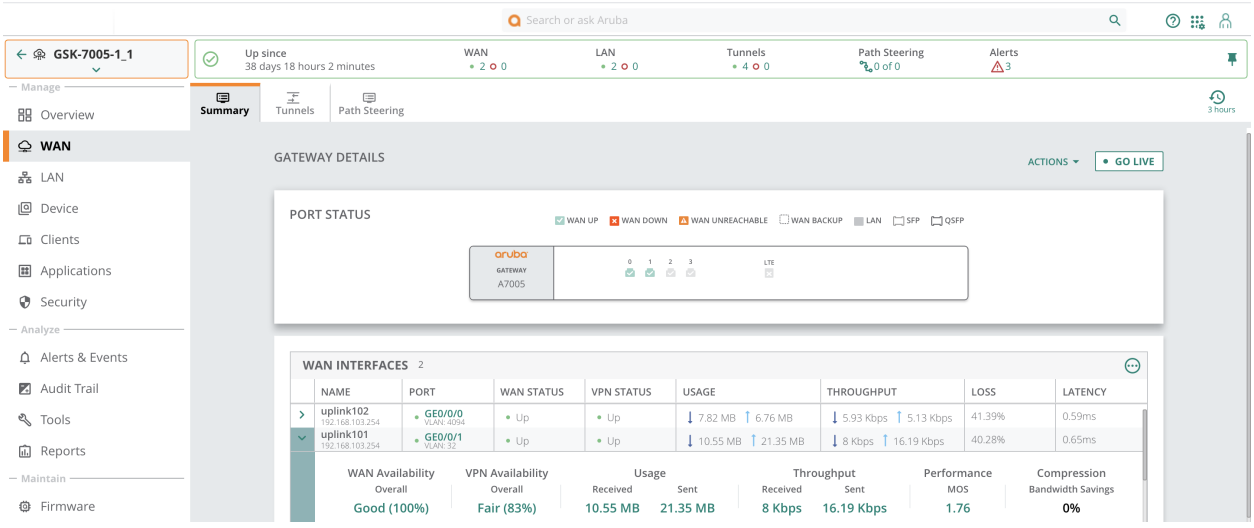
  - Logarithmic Scale—Click this icon to view chart in logarithmic scale.
  - Linear Scale—Click this icon to view chart in linear scale.

  Click Received or Sent at the bottom of the chart to view or hide the usage chart for received or sent data.

- **Performance**—The Performance section displays the MOS score of the interface and the following graphs based on the probe that is selected. For a health check probe, only Latency and Packet Loss graphs are displayed.
  - **Latency**—The latency in milliseconds.
  - **Packet Loss**—Displays the packet loss in percentage.
  - **Jitter**—Displays the jitter in milliseconds.
  - **MOS Score**—Displays the MOS score.
- **WAN Compression**—Provides bandwidth savings of WAN compression uplink, along with optimized and non optimized packets and the average bandwidth saved in percentage.

Live Monitoring for Device State is enabled for **Status Header Tile**, **Port Status** and **WAN Interfaces**.

Figure 20 *WAN_Live Monitoring*



Viewing the LAN > Summary Tab

The **Summary** tab under **Manage** > **LAN** page in the gateway dashboard displays the port status, LAN interfaces summary, and VLAN interfaces summary.

To navigate to the **LAN > Summary** tab in the gateway dashboard, complete the following steps:

1. In the **HPE Aruba Networking Central** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **LAN** > **Summary**.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

LAN Interfaces Summary

The table displays the summary of LAN interfaces and total number of LAN interfaces. The following details are displayed for the port:

- **Port**—Port number. Click on the Port to open the **Port Details** pop-up page.
- **Admin State**—Administrative state of the LAN interface. Values are **Enabled** or **Disabled**.
- **Operational State**—Operational state of the LAN interface. Values are **Up** or **Down**.
- **Port Speed**—Port speed.
- **VLANs**—Range of VLANs.
- **MTU**—MTU value.

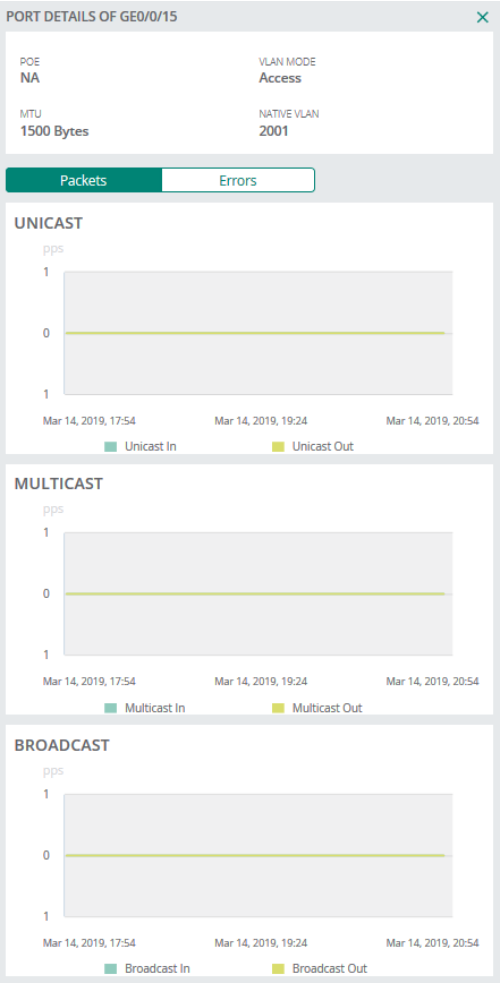
Port Details Pop-Up page

Click on a port in the **Port Status** or **LAN Interfaces Summary** page to display the **Port Details** pop-up page. The page has two tabs, **Packets** and **Errors**.

- The following graphs are displayed under the **Port Details > Packets** tab:
  - **Unicast**—The number of unicast packets per second.
  - **Multicast**—The number of multicast packets per second.
  - **Broadcast**—The number of broadcast packets per second.

  Hover over any point of time on the x-axis to get data about packets for that instant of time.

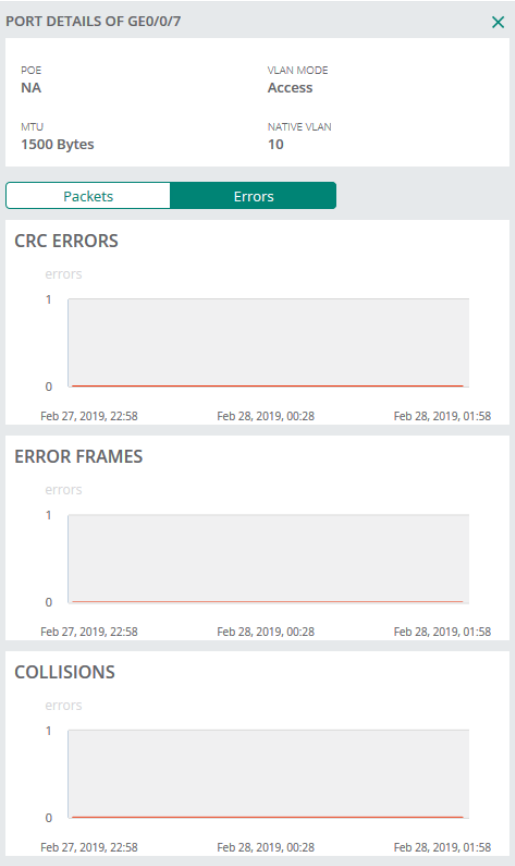
Figure 21 *Port Details—Packets*



- The following graphs are displayed under the **Port Details** > **Errors** tab:
  - **CRC Errors**—The number of cyclic redundancy errors logged.
  - **Error Frames**—The number of error frames logged.
  - **Collisions**—The number of collisions encountered.

Hover over any point of time on the x-axis to get data about packets for that instant of time.

Figure 22 *Port Details—Errors*



AI Insights

The following section describes the anomalies observed in the HPE Aruba Networking Central network that might affect the quality of the overall network performance and the steps to help troubleshoot these issues.

AI Insights Anomalies

The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level for the selected time range. Each insight provides specific details on the occurrences of these events for easy debugging.

In this release the insights are classified under three categories:

- Connectivity—Issues related to the wireless connectivity in the network.
- Wireless Quality—Issues related to the RF Info or RF Health in the network.
- Availability—Issues related to the health of your network infrastructure and the devices in the network such as, APs, switches, and gateways.

  To launch the **AI Insights** dashboard, complete the following steps:

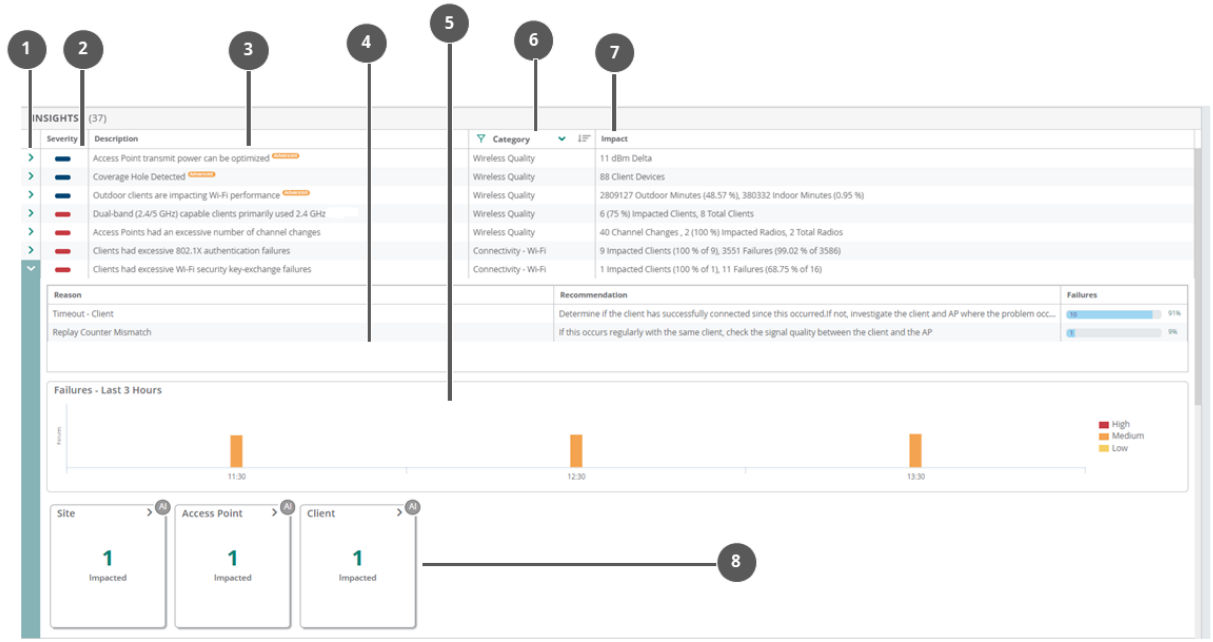
  1. In the **HPE Aruba Networking Central** app, set the filter to **Global**.The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Overview** > **AI Insights**.

   The Insights table is displayed. AI Insights listed in the dashboard are sorted from high priority to low priority.

3. Click › against each insight to view the further details.

Figure 23 *Insight Details*



Callout Number	Description
1	Click this arrow to expand any specific insight to view further details.
2	Displays the insight severity, using the following colors: ■ Red—High priority ■ Orange—Medium priority ■ Yellow—Low priority **NOTE:** The insights marked in blue color ( ) in the severity column are the configuration recommendation insights.
3	Short description of the insight.
4	Insight Summary displays the reason why the insight was generated along with the recommendation. It also shows the number and percentage of failures that occurred against each failure reason. The reasons are classified into: ■ Static—These reasons rely on HPE Aruba Networking's domain expertise. ■ Dynamic—These reasons are generated based on error codes that is received from infrastructure devices.
5	Time Series graph is a graphical representation of the failure percentage or failure events that occurred for the selected time range. The entries in each time series bar can be customized to highlight a specific entry by clicking on it. Only one specific entry can be highlighted at a time.

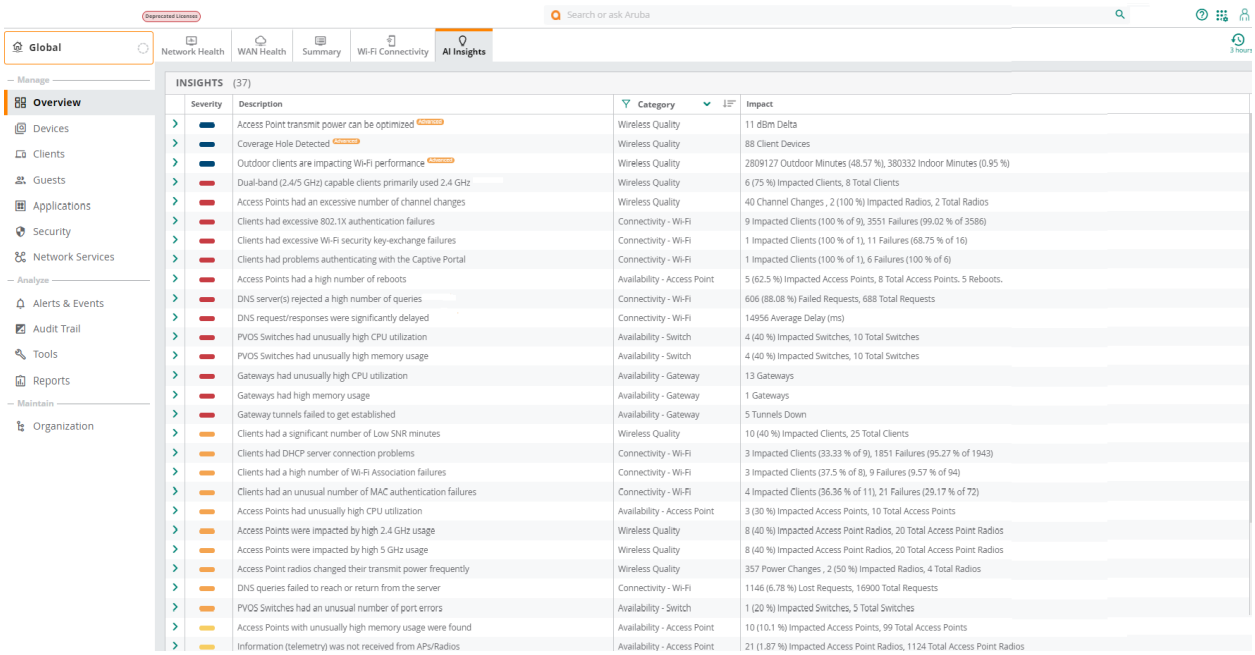
Callout Number	Description
6	Category of the insight.
7	Short description of the impact.
8	Cards display additional information specific to each insight. Cards might vary for each insight based on the context the insight is accessed from.

All AI Insights generated are listed in the **Global > AI Insights** dashboard. Alternatively, AI Insights for a specific site, device, or client can be viewed by selecting the respective context.

NOTE

AI Insights are displayed for a selected time period based on the time selected in the **Time Range Filter**. You can select one of the following: **3 Hours**, **1 Week**, **1 Day**, or **1 Month**.

Figure 24 *AI Insights Dashboard*



For more information, see AI Insights in Global Dashboard.

Network Check

The following section provides details on the typical network issues that you might face with the devices managed by the HPE Aruba Networking Central network and the steps to help troubleshoot these issues.

Network Performance

To identify the network speed, you must perform a network check on the APs in the network. A network check aims to identify, diagnose, and debug issues detected in an HPE Aruba Networking Central-managed network. The **Network Check** tab on the **Tools** page captures the troubleshooting utilities that are used to test a network entity and collect results based on your selection.

The following tests are available for APs to troubleshoot issues pertaining to WLAN network connections:

- Ping Test
- NSLookup
- Traceroute
- TCP Test
- HTTP Test
- HTTPS Test
- Speed Test (iPerf)

Ping Test

Sends ICMP echo packets to the hostname or IP addresses of the selected devices to check for latency issues.

To perform a ping test on APs, complete the following steps:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the ping test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Sources** drop-down list, select the sources.

   You can select multiple APs.
5. From the **Test** drop-down list, select **Ping Test**.
6. From the **Destination Type** drop-down list, select one of the following:
   - **Hostname/IP Address**—Enter the hostname or IP address.
   - **Client**—Select a client.

7. Select the SSID from the **SSID** drop-down list.

- For devices running firmware version below AOS-10.3, the **SSID** option is not visible.
- For devices running firmware version between AOS-10.3 and AOS-10.4, **SSID** is visible only if Underlay SSID is configured on that device. Even if Overlay is configured on the device, pinging over Overlay is not supported.
- For devices running firmware version AOS-10. 4 and above both Overlay and Underlay SSIDs will be displayed in the drop-down list.
- If you select client from the **Destination Type** drop-down list, the SSID is automatically selected based on the client.

8. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:

Show Additional Test Setting is not displayed when a **Test** type is not selected.

   a. In the **Packet Size** field, enter the packet size in order to capture and store the data packet to analyze network issues at a later stage. The range is from 10 to 65507 bytes.
   b. In the **Count** field, enter the count. The value should be between 1 to 2147483647.
   c. Select **Port** from the **Source Interface** drop-down list and select the port number.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 25 *Ping Test—Device Output*

As mentioned in the steps, you can ping a client, gateway, or a WAN IP address to identify the wireless speed. When you ping the client, it sends the packets at a specified speed. If the network is slow, the time taken for the transfer will be high and some packets may get lost in the process. This behavior indicates that there is an issue between the AP and the client. Hence, when you notice that the network is slow, execute a ping test in **Tools** and check if the ping test is optimal. Similarly, you can choose your destination to be a gateway or a WAN/IP address. The tests show the same network speed from an AP to a gateway or from an AP to an outside WAN.

NSLookup

NSLookup is a program to query internet domain name servers. To perform a NSLookup test on APs, complete the following steps:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the traceroute test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **NSLOOKUP**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the hostname or IP address.
7. To use additional parameters, click **Show Additional Test Settings** and in the **DNS Server** field enter the hostname or IP address.

Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The output is displayed in the **Device Output** section.

The **show lhm status** command displays the number of times all configured NSLookup policies have been run. For more information, see Troubleshooting AP Connectivity Issues.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on APs, complete the following steps:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

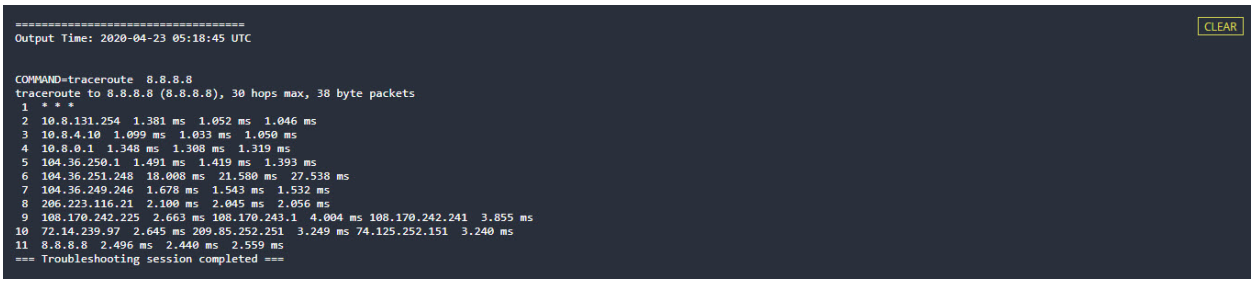
     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the traceroute test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.

3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the hostname or IP address.
7. Click **Run**. The output is displayed in the **Device Output** section.

Figure 26 *Traceroute Test—Device Output*



TCP Test

Sends packets to the host such as an FTP server, and tries to establish a connection and exchanges data. If the FTP server returns a response, the issue could be isolated to the client device.

To perform a TCP test on APs, complete the following steps:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

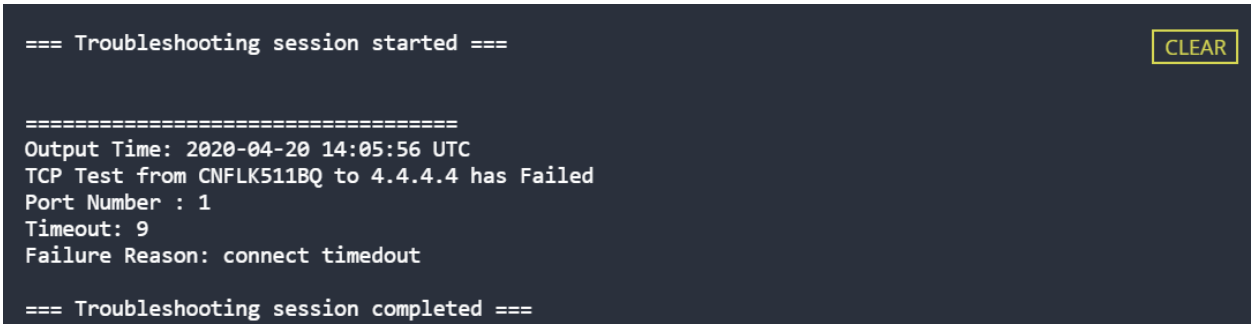
        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the TCP test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **TCP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter a valid IPv4 address in the **Host** field. Hostname is not supported.
7. Enter the port number in the **Port** field. The port number should be between 1 to 65535.
8. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, to enter the timeout value in seconds.
   The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.

Show Additional Test Settings is not displayed when a **Test** type is not selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 27 *TCP Test—Device Output*



NOTE

The TCP test is supported only from AOS-8.3.0.0 or later versions.

HTTP Test

Sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, the issue could be isolated to the client device.

To perform an HTTP test on APs, complete the following steps:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the HTTP test.

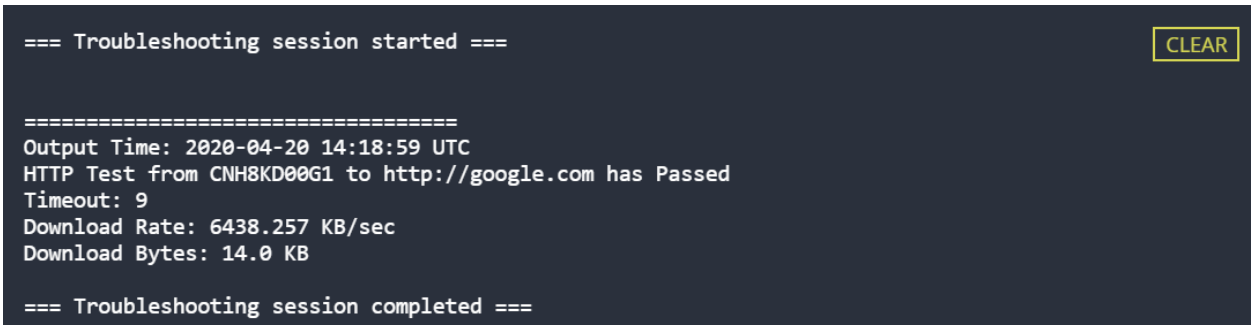
        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTP URL for which you want to perform the HTTP test, in the **URL** field, For example, http://*hostname* or http://*ipaddress*.
7. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds.
   The value should be between 1 to 10 seconds. The default timeout value is 1 second.

NOTE

Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The test output is displayed in the **Device Output** section.

Figure 28 *HTTP Test—Device Output*



NOTE

The HTTP test is supported only from AOS-8.3.0.0 or later versions. The test support only IPv4 address or domain name in the URL field.

HTTPS Test

Sends packets to the HTTPS URL and tries to establish a connection and exchange data. If the HTTPS website returns a response, the issue could be isolated to the client device. HTTPS is a performance test to identify the time taken to load a web page.

To perform an HTTPS URL test on APs, complete the following steps:

1. In the **HPE Aruba Networking Central** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the HTTPS test.

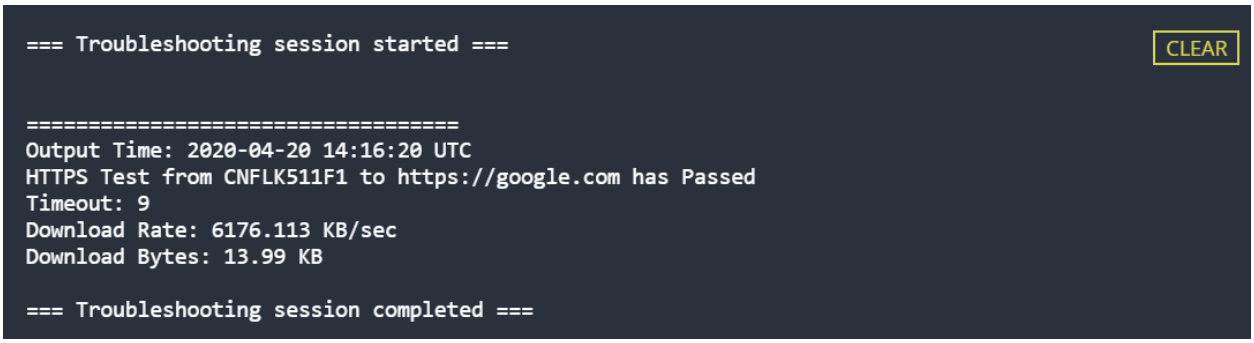
        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTPS Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTPS URL for which you want to perform the HTTPS test in the **URL** field, For example, https://*URL* or https://*IPv4*.
7. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds.
   The value should be between 1 to 10 seconds. The default timeout value is 1 second.

NOTE

Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The test output is displayed in the **Device Output** section.

Figure 29 *HTTPS Test—Device Output*



NOTE

If there is an application server running at the customer site and the application server has HTTPS, and HTTP service enabled you can run these tests from the AP to the server. After you run the test, the test status, download rate, and the download bytes indicate the network speed.

Speed Test (iPerf)

Performs a speed test to measure network speed and bandwidth. The speed test diagnostic tool is available only for Instant APs. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

To execute a speed test on APs, complete the following steps:

1. In the WebUI app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the speed test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Speed Test (iPerf)**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. In the **Host** field, enter a valid hostname.
7. From the **Protocol** drop-down list, select the protocol. The available options are **TCP** or **UDP**.
8. To use additional parameters, click **Show Additional Test Settings** and in the **Options** field, enter the option. For example, bandwidth.

NOTE

Show Additional Test Settings is not when a **Test** type is not selected.

9. Click **Run**. The test output is displayed in the **Device Output** section.

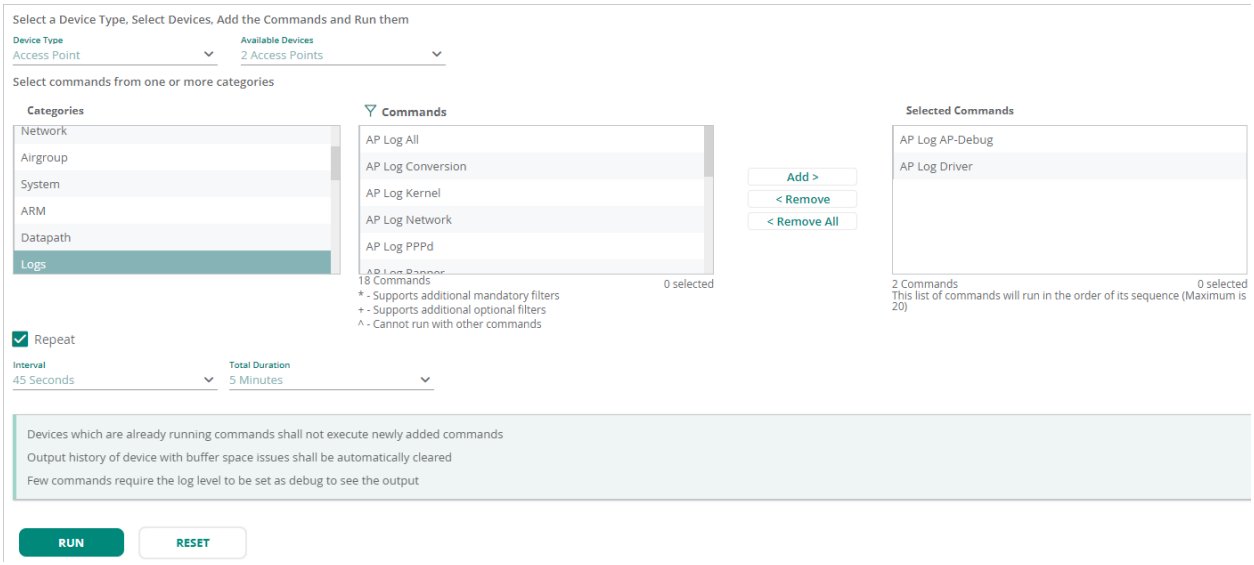
Figure 30 *Speed Test—Device Output*

NOTE

While troubleshooting APs, a maximum of 20 APs are listed in the drop-down list. If there are more than 20 APs, use the **Search** option to search for an AP on which you would like to perform diagnostic checks.

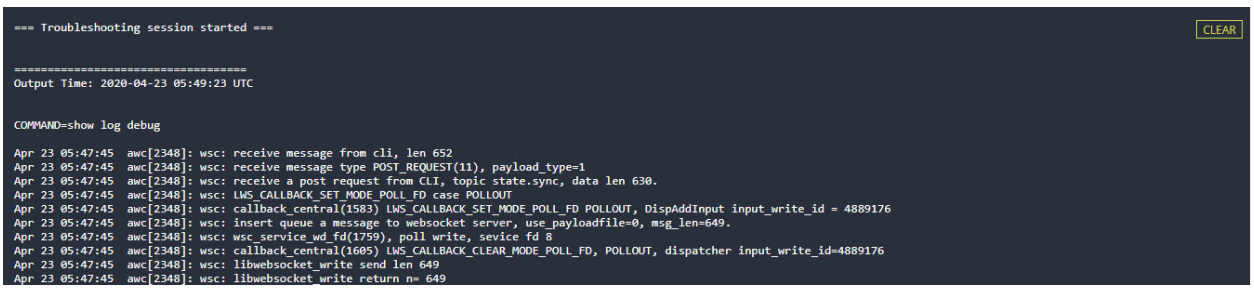
In addition to the **Network Check** tests, you can also leverage the **Commands** tab to troubleshoot your network performance using the available CLI commands. The **Commands** tab on the **Tools** page lists commands specific to a particular device to test the device entity and collect results based on your selection.

Figure 31 *Advanced Device Troubleshooting*



When a troubleshooting operation is initiated, HPE Aruba Networking Central establishes a session with the devices selected for the troubleshooting operation and displays the output in the **Device Output**.

Figure 32 *Command Test—Device Output*



Viewing the Device Output

After you execute troubleshooting commands on the device, HPE Aruba Networking Central displays the output in the **Device Output** section of the **Tools** page.

The output section displays information, such as the list of devices on which the troubleshooting commands were executed, initial timestamp, **Test Type**, **Source**, and **Target**. It also shows the status of the tests as, in progress, complete, and buffer time. If there are multiple devices, select the device for which you want to view the output.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click **Export** to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.