CHAPTER 15

Monitoring Clients and Users

About Wired and Wireless Clients

A client is a device that is connected to an access point or a switch. Cisco Prime Infrastructure supports both wired and wireless clients. After you add controllers and switches to Prime Infrastructure, the client discovery process starts. Wireless clients are discovered from managed controllers or autonomous access points. The controllers are polled during regular client status poll. The wireless client count includes autonomous clients as well. In the case of switches, Prime Infrastructure polls for clients immediately after the device is added and updates the device information in the database. For wired clients, the client status polling to discover client associations occurs every two hours (by default). A complete polling happens twice every day to poll complete information of all wired clients connected to all switches.

Prime Infrastructure uses background tasks to perform the data polling operations. There are three tasks associated with clients:

1. Autonomous AP Client Status
2. Lightweight Client Status
3. Wired Client Status

You can refresh the data collection tasks (such as polling interval) from the Administration > Settings > Background Tasks page.

Client status (applicable only for wired clients) is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the SNMP connection to the wired switch is lost.

For the clients of autonomous access point managed by Prime Infrastructure and for the clients authenticated using Local Extensible Authentication Protocol (LEAP), the username is not registered and is displayed as unknown.

Prime Infrastructure supports both identity and non-identity wired clients. The support for wired clients is based on the identity service. The identity service provides secure network access to users and devices and it also enables the network administrators to provision services and resources to the users based on their job functions.

Prime Infrastructure do not poll end hosts connected through VLAN 1000-1024.

Prime Infrastructure does not support VRF. Therefore, if a client is connected to a VRF-configured device, you cannot view client information.
Client Dashlets on the General Dashboard

When you log into Prime Infrastructure, the General dashboard displays a few client-related dashlets.

- **Client Count By Association/Authentication**—Displays the total number of clients by Association and authentication in Prime Infrastructure over the selected period of time.
  - Associated client—All clients connected regardless of whether it is authenticated or not.
  - Authenticated client—All clients connected and passed authentication, authorization and other policies, and ready to use the network.
- **Client Count By Wireless/Wired**—Displays the total number of wired and wireless clients in Prime Infrastructure over the selected period of time.

Client Dashboard

The Client dashboard (Dashboard > Overview > Client) page displays the client-related dashlets. These dashlets enable you to monitor the clients on the network. The data for graphs is also polled/updated periodically and stored in Prime Infrastructure database. On the other hand, most of the information in the Client Details page are polled directly from the controller/switch.

Monitoring Clients and Users

Choose Monitor > Monitoring Tools > Clients and Users to view all the wired and wireless clients in your network. In addition, you can view the client association history and statistical information. These tools are useful when users complain of network performance as they move throughout a building with their laptop computers. The information might help you assess what areas experience inconsistent coverage and which areas have the potential to drop coverage.

Access the Client Detail page by clicking on a MAC Address to help you identify, diagnose, and resolve client issues.

Related Topics

- Managing Data Collection and Retention
- Tracking Clients
- Interactive Graphs
- Client Dashboard
- Filtering Clients and Users
- Viewing Clients and Users
Filtering Clients and Users

The Monitor > Monitoring Tools > Clients and Users page lists all associated clients by default. There are preset filters that allow you to view a subset of clients.

The WGB, Wired Guest, and Office Extended Access Point 600 (OEAP 600) are tracked as wireless clients. Prime Infrastructure only remembers sorting column which is indexed including MAC Address, IP Address, Username, AP MAC Address and SSID. Sorting on non-indexed column causes serious performance issue when loading the client list page. You can still sort the table by any column. But after you leave this page, Prime Infrastructure will not remember the last used sorting column if it is not indexed.

In addition, you can use the filter icon ( ) to filter the records that match the filter rules. If you want to specify a filter rule, choose All from the Show drop-down list before you click .

When you select a preset filter and click the filter icon, the filter criteria is dimmed. You can only see the filter criteria but cannot change it. When the All option is selected to view all the entries, clicking the filter icon shows the quick filter options, where you can filter the data using the filterable fields. You can also enter text in the free form text box for table filtering.

You can use the advanced search feature to narrow the client list based on specific categories and filters.

Related Topics
- Filtering on IP Addresses

Filtering on IP Addresses

When you perform advanced client filtering on IPv6 addresses, each octet that you specify must be a complete octet. If you specify a partial octet, the filtering might not show correct results.

The following example shows how the advanced client filtering works on IPv6 addresses. This example assumes that you have the following IP addresses in the system:

10.10.40.1
10.10.40.2
10.10.40.3
10.10.240.1
Fec0::40:20
Fe80::240:20

If you search for all IP addresses containing 40, you get the following result:

10.10.40.1
10.10.40.2
10.10.40.3
Fec0::40:20

The IP addresses that contain 240 are not filtered because the filtering feature expects you to enter a complete octet.

Related Topic
- Search Methods
Viewing Clients and Users

To view complete details in the Monitor > Monitoring Tools > Clients and Users page and to perform operations such as Radio Measurement, users in User Defined groups should have the required permission before they access the Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location pages.

The following attributes are populated only when the ISE is added to Prime Infrastructure:

- ISE
- Endpoint Type
- Posture
- Authorization Profile Name

Prime Infrastructure queries the ISE for client authentication records for the last 24 hours to populate this data. If the client is connected to the network 24 hours before it is discovered in Prime Infrastructure, you might not see the ISE-related data in the table. You might see the data in client details page. To work around this, reconnect the client to the network. The ISE information is shown in the table after the next client background task run.

To view clients and users, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users to view both wired and wireless clients information. The Clients and Users page appears.

The Clients and Users table displays a few columns by default. If you want display the additional columns that are available, click ⚙, and then click Columns. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

**Step 2** Choose a client or user. The following information appears depending on the selected client/user.

- Client Attributes
- Client Statistics
- Client Statistics
- Client Association History
- Client Event Information
- Client Location Information
- Wired Location History
- Client CCXv5 Information

Related Topics

- Modifying the Clients and Users Page
- Filtering Clients and Users

Exporting Clients and Users

You can quickly export your clients and users list into a CSV file (spreadsheet format with comma-separated values).
When to Use the Client Troubleshooting Tool

Prime Infrastructure provides a troubleshooting tool to help you diagnose and solve issues experienced with both wired and wireless clients. This tool relies on SNMP to discover clients and collect client data. If Cisco Identity Services Engine (ISE) is integrated with Prime Infrastructure, the tool also collects ISE-based client statistics and other data shown in Prime Infrastructure’s client dashlets and reports.

Launch the client troubleshooting tool whenever you need to:

- Monitor the status of a client connection.
- Verify the current and past locations of users and their devices.
- Troubleshoot client connectivity problems.
- Troubleshoot current client issues.
- View client issue history.
- Obtain the location history for location-assisted clients.

The client troubleshooting feature is available for identity wired clients (those that are identified by ISE) and not for non-identity wired clients.

Related Topics

- Launching the Client Troubleshooting Tool
- Searching for Clients
- Analyzing Client Connection Logs
- Viewing Client Event History and Event Logs

Launching the Client Troubleshooting Tool

You can launch the Client Troubleshooting tool for any client from the Clients and Users page.

Step 1

Choose Monitor > Monitoring Tools > Clients and Users. The Clients and Users page lists all the clients the system knows (including those not currently associated).
Chapter 15  Monitoring Clients and Users

Launching the Client Troubleshooting Tool

Step 2  Click the MAC Address for the client having connection problems that you want to troubleshoot.
You may find it handy to narrow the client list first, by using the Search feature. See “Troubleshooting Clients Using the Search Feature” in Related Topics.

Step 3  Click Troubleshoot and Debug.

Related Topics

- About the Client Troubleshooting Page
- How the Client Troubleshooting Tool Gives Advice
- Searching for Clients

About the Client Troubleshooting Page

The Client Troubleshooting page provides:

- Details on the current or last session for a selected wired or wireless client.
- The client’s current/last connection status, shown as a series of graphic icons.
- If connection problems are detected:
  - The nature of the connection problem (also indicated by graphic icons)
  - Advice on how to troubleshoot that problem.

Figure 15-1 shows the complete Client Troubleshooting page for a wireless client that has connected successfully. The upper Properties section of the page provides the same session details for a successfully connected client that you would see on the Clients and Users page.

Also note that, as this is a successful connection, the lower Troubleshoot section shows green check marks as the status for each stage of the wireless connection process, and provides no advice on troubleshooting the connection.

Figure 15-1  Client Troubleshooting page for Successful Wireless Client
Figure 15-2 shows the Troubleshoot section of the Client Troubleshooting page for a different wireless client (for simplicity, we have collapsed the Properties section by clicking on the section’s right arrow icon). This client had trouble connecting. As you can see, there is an alert on the 802.1X Authentication portion of the connection process and a list of steps to try to determine exactly why this was a problem.

This number and type of connection status icons, and advice in the Troubleshoot section, will vary according to the kind of client, the stage of the connection process that had problems, and the likely sources of the problem. For more information, see “How the Client Troubleshooting Tool Gives Advice” in Related Topics.

**Figure 15-2**  **Client Troubleshooting page for Unsuccessful Wireless Client**

1. Properties
2. Troubleshoot
3. Recommendation

**Related Topics**
- Launching the Client Troubleshooting Tool
How the Client Troubleshooting Tool Gives Advice

Prime Infrastructure determines the number of connection areas and the type of troubleshooting advice to present on the Client Troubleshooting page based on the stages the client passes through when establishing connection and connectivity protocols involved at each stage. Table 15-1 summarizes these stages and protocols involved at each stage.

<table>
<thead>
<tr>
<th>Connection Stage</th>
<th>Link Connectivity</th>
<th>802.1X Authentication</th>
<th>MAC Authentication</th>
<th>Web Authentication</th>
<th>IP Connectivity</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MAC Authentication</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Web Authentication</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 15-2 Details the troubleshooting advice presented for each kind of problem detected during the stages of connection building.

<table>
<thead>
<tr>
<th>Client State</th>
<th>Problem</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Connectivity</td>
<td>Cannot find the client in the network</td>
<td>• Check whether the client cable is plugged into the network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client is using the proper cable to connect to the network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the port to which the client is connected is not disabled administratively.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the port to which the client is connected is not error disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the speed and duplex are set to Auto on the port to which the client is connected.</td>
</tr>
<tr>
<td>Authentication in progress</td>
<td>If the client has been in this state for a long time, check the following:</td>
<td>• If the client has been in this state for a long time, check the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Check whether the supplicant on the client is configured properly as required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Modify the timers related to the authentication method and try again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Use the fall back authentication feature if you are not sure which authentication method works with the client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Try disconnecting and reconnecting.</td>
</tr>
<tr>
<td>Client State</td>
<td>Problem</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>802.1X Authentication</td>
<td>802.1X Authentication Failure</td>
<td>• Check whether the RADIUS server(s) is reachable from the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client choice of EAP is supported by the RADIUS server(s).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the username/password/certificate of the client is valid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the certificates used by the RADIUS server are accepted by the client.</td>
</tr>
<tr>
<td>MAC Authentication</td>
<td>MAC Authentication Failure</td>
<td>• Check whether the RADIUS server(s) is reachable from the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the MAC address of the client is in the list of known clients on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the MAC address of the client is not in the list of excluded clients.</td>
</tr>
<tr>
<td>Web Authentication</td>
<td>Client could not be authenticated through web/guest interface</td>
<td>• Check whether the guest credentials are valid and have not expired.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client can be redirected to the login page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the RADIUS server is reachable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that pop-ups are not blocked.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the DNS resolution on the client is working.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the client is not using any proxy settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client can access https://&lt;virtual-ip&gt;/login.html</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the browser of the client accepts the self-signed certificate offered by the controller.</td>
</tr>
<tr>
<td>IP Connectivity</td>
<td>Client could not complete DHCP interaction</td>
<td>• Check whether the DHCP server is reachable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the DHCP server is configured to serve the WLAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the DHCP scope is exhausted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether multiple DHCP servers are configured with overlapping scopes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the local DHCP server is present. If the DHCP bridging mode is enabled (move it to second), the client is configured to get the address from the DHCP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check if the client has the static IP configured and ensure that the client generates IP traffic.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Authorization Failure</td>
<td>• Ensure that the VLAN defined for authorization is available on the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the default port ACL is configured for ACL authorization.</td>
</tr>
<tr>
<td>Successful Connection</td>
<td>None</td>
<td>None. This indicates that all previous stages were completed successfully.</td>
</tr>
</tbody>
</table>

Related Topics
- Launching the Client Troubleshooting Tool
Searching for Clients

- Searching for Clients
- Analyzing Client Connection Logs

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Type the full or partial client MAC address in the Advanced Search text box, and click Search. The Search Results page appears.

Step 3 Click View List to view the clients that match the search criteria in the Clients page. The Monitor > Monitoring Tools > Clients and Users page appears.

You can click the Reset link to set the table to the default display so that the search criteria is no longer applied.

Step 4 Select a client, and then click the Troubleshoot. The Troubleshooting Client page appears. If you are troubleshooting a Cisco-compatible Extension v5 client (wireless), your Troubleshooting Client page will have additional tabs.

If you receive a message that the client does not seem to be connected to any access point, you must reconnect the client and click Refresh.

Related Topics
- Launching the Client Troubleshooting Tool
- Analyzing Client Connection Logs

Analyzing Client Connection Logs

Step 1 Launch the Client Troubleshooting Tool for the client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.

Step 2 Click the Log Analysis tab to view log messages logged against the client.

Step 3 Click Start to begin capturing log messages about the client from the controller.

Step 4 Click Stop to stop log message capture.

Step 5 Click Clear to clear all log messages. Log messages are captured for ten minutes and then automatically stopped. Click Start to continue.

Step 6 Click one of the links under Select Log Messages to display log messages (the number between parentheses indicates the number of messages).

Related Topics
- Launching the Client Troubleshooting Tool
- Searching for Clients
- Viewing Client Event History and Event Logs
Viewing Client Event History and Event Logs

Step 1: Launch the Client Troubleshooting Tool. See “Launching the Client Troubleshooting Tool” in Related Topics.
Step 2: Click the Events tab to display the event history of a client.
Step 3: Click the Event Log tab to view the event log.
Step 4: Click Start to begin capturing log messages from the client.
Step 5: Click Stop when a sufficient number of messages have been collected.

The Client Troubleshooting Event log and Messaging features are available to CCX Version 6 clients only if the Management Service version is 2 and later.

Related Topics
- Launching the Client Troubleshooting Tool
- Searching for Clients

Checking Client ISE Authentication History and Identity Services

Step 1: Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.
Step 2: Click the Identity Services Engine tab to view information about ISE authentication.
Step 3: Enter the date and time ranges to retrieve historical authentication and authorization information, and then click Submit. The results of the query are displayed in the Authentication Records portion of the page.
Step 4: Click the Identity Services Engine tab to view information about the identity services parameters. You must configure the Identity Services Engine (ISE) before you access this tab.

If the ISE is not configured, it provides a link to add an ISE to Prime Infrastructure. The ISE provides authentication records to Prime Infrastructure via REST API. The network administrator can choose a time period for retrieving authentication records from the ISE.

Related Topics
- Launching the Client Troubleshooting Tool
- Searching for Clients
- Checking Client Clean Air Environment
Checking Client Clean Air Environment

Step 1  Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.

Step 2  Click the CleanAir tab to view information about the air quality parameters and active interferer for the CleanAir-enabled access point.

Step 3  Click CleanAir Details to know more about the air quality index.

Related Topics

- Launching the Client Troubleshooting Tool
- Searching for Clients

Running Diagnostic Tests on Problem Clients

Step 1  Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.

Step 2  (Optional) Click the Test Analysis tab if Cisco-compatible Extension Version 5 or Version 6 clients are available.

Step 3  Check the check box for the applicable diagnostic test, enter any appropriate input information, and click Start. The Test Analysis tab allows you to run a variety of diagnostic tests on the client.

Related Topics

- Launching the Client Troubleshooting Tool
- Searching for Clients
- When to Run Diagnostic Tests on Problem Clients

When to Run Diagnostic Tests on Problem Clients

Before you begin, ensure that you have reviewed the test qualifications and restrictions. See Related Topics.

The following diagnostic tests are available on the Test Analysis tab:

- DHCP—Executes a complete DHCP Discover/Offer/Request/ACK exchange to determine that the DHCP is operating properly between the controller and client.
- IP Connectivity—Causes the client to execute a ping test of the default gateway obtained in the DHCP test to verify that IP connectivity exists on the local subnet.
- DNS Ping—Causes the client to execute a ping test of the DNS server obtained in the DHCP test to verify that IP connectivity exists to the DNS server.
Chapter 15      Monitoring Clients and Users

Pinging Problem Clients with Text Messages

- DNS Resolution—Causes the DNS client to attempt to resolve a network name known to be resolvable to verify that name resolution is functioning correctly.
- 802.11 Association—Directs an association to be completed with a specific access point to verify that the client is able to associate properly with a designated WLAN.
- 802.1X Authentication—Directs an association and 802.1X authentication to be completed with a specific access point to verify that the client is able to properly complete an 802.1x authentication.
- Profile Redirect—At any time, the diagnostic system might direct the client to activate one of the configured WLAN profiles and to continue operation under that profile.

To run the profile diagnostic test, the client must be on the diagnostic channel. This test uses the profile number as the input. To indicate a wildcard redirect, enter 0. With this redirect, the client is asked to disassociate from the diagnostic channel and associate with any profile. You can also enter a valid profile ID. Because the client is on the diagnostic channel when the test is run, only one profile is returned in the profile list. You should use this profile ID in the profile redirect test (when wildcard redirecting is not desired).

Related Topics
- Launching the Client Troubleshooting Tool
- Searching for Clients
- Running Diagnostic Tests on Problem Clients

Pinging Problem Clients with Text Messages

Step 1
Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.

Step 2
(Optional) For Cisco-compatible Extension Version 5 or Version 6 clients, a Messaging tab will appear which can be used to send an instant text message to the user of this client. From the Message Category drop-down list, choose a message, and click Send.

Related Topics
- Launching the Client Troubleshooting Tool
- Running Diagnostic Tests on Problem Clients

Viewing Real Time Troubleshooting (RTTS) Details

Step 1
Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.

Step 2
Click the RTTS tab to view the Real Time Troubleshooting (RTTS) details.

Step 3
Select modules to debug and debug level.

Step 4
Click Run. The RTTS manager executes a set of commands in the controllers connected to the client based on the selected debug modules and debug level and displays the RTTS details.
Step 5  Click the Filter tab to filter the RTTS details based on debug time, controller name, controller IP, severity, and debug message.

Step 6  Click the Export tab to export the debug details as a csv file.

You can also debug other controllers based on the selected debug modules and debug levels by using the Choose different controllers option.

The RTTS Manager supports five concurrent RTTS debug sessions and each debug session is limited to five devices.

Related Topics

- Launching the Client Troubleshooting Tool
- Debug Commands for RTTS

### Debug Commands for RTTS

Table 15-3 contains the list of debug commands for Legacy controllers and Converged Access Controllers 5760/3850/3650 Wireless LAN Controllers (WLCs).

<table>
<thead>
<tr>
<th>Controller</th>
<th>Modules to Debug</th>
<th>Debug Level</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy</td>
<td>All</td>
<td>Debug Level</td>
<td>debug capwap info enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug dot1x all enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug mobility directory enable</td>
</tr>
<tr>
<td>Dot1.x</td>
<td>Detail</td>
<td></td>
<td>debug dot1x all enable</td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td></td>
<td>debug dot1x events enable</td>
</tr>
<tr>
<td></td>
<td>High Level</td>
<td></td>
<td>debug dot1x states enable</td>
</tr>
<tr>
<td>Legacy Mobility</td>
<td>Detail</td>
<td></td>
<td>debug mobility packet enable</td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td></td>
<td>debug mobility keepalive enable</td>
</tr>
<tr>
<td></td>
<td>High Level</td>
<td></td>
<td>debug mobility config enable</td>
</tr>
<tr>
<td>Wireless Client Join</td>
<td>Detail</td>
<td></td>
<td>debug client &lt;macAddress&gt;</td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td></td>
<td>debug client &lt;macAddress&gt;</td>
</tr>
<tr>
<td></td>
<td>High Level</td>
<td></td>
<td>debug client &lt;macAddress&gt;</td>
</tr>
</tbody>
</table>
Table 15-3 List of Debug Commands for Legacy Controllers and NGWC Controllers

<table>
<thead>
<tr>
<th>Controller</th>
<th>Modules to Debug</th>
<th>Debug Level</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGWC</td>
<td>All</td>
<td>Debug</td>
<td>debug capwap ap error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug dot1x events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug capwap ios detail</td>
</tr>
<tr>
<td>Dot1.x</td>
<td>Detail</td>
<td>Debug</td>
<td>debug wcm-dot1x detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug wcm-dot1x all</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug dot1x all</td>
</tr>
<tr>
<td>Error</td>
<td></td>
<td>Debug</td>
<td>debug wcm-dot1x errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug dot1x errors</td>
</tr>
<tr>
<td>High Level</td>
<td></td>
<td>Debug</td>
<td>debug wcm-dot1x trace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug wcm-dot1x event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug wcm-dot1x error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug client mac-address &lt;macAddress&gt;</td>
</tr>
<tr>
<td>Mobility</td>
<td>Detail</td>
<td>Debug</td>
<td>debug mobility all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Error</td>
<td>debug mobility error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Level</td>
<td>debug mobility handoff</td>
</tr>
<tr>
<td>Wireless</td>
<td>Detail</td>
<td>Debug</td>
<td>debug wcdb error</td>
</tr>
<tr>
<td>Client</td>
<td></td>
<td></td>
<td>debug wcdb event</td>
</tr>
<tr>
<td>Join</td>
<td></td>
<td></td>
<td>debug wcdb db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug ip dhcp snooping events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug ip dhcp server events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug client mac &lt;macAddress&gt;</td>
</tr>
<tr>
<td>Error</td>
<td></td>
<td></td>
<td>debug client mac &lt;macAddress&gt;</td>
</tr>
<tr>
<td>High Level</td>
<td></td>
<td></td>
<td>debug client mac &lt;macAddress&gt;</td>
</tr>
</tbody>
</table>

Related Topic
- Launching the Client Troubleshooting Tool

Tracking Clients

This feature enables you to track clients and be notified when they connect to a network.

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.
This table supports a maximum of 2000 rows. To add or import new rows, you must first remove some older entries.
Step 3 Click Add to track a single client, and then enter the following parameters:
Tracking Multiple Clients

This feature enables you to track multiple clients and be notified when they connect to a network.

Step 1
Choose Monitor > Monitoring Tools > Clients and Users.

Step 2
Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.

Step 3
Click Add to track a single client, and then enter the following parameters:

- Client MAC address
- Expiration—Choose Never or enter a date.

Step 4
If you have a long list of clients, click Import to track multiple clients. This allows you to import a client list from a CSV file. Enter the MAC address and username.

A sample CSV file can be downloaded that provides data format:

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format
00:40:96:b6:02:cc,10/07/2010
00:02:8a:a2:2e:60,Never
```

A maximum of 2000 clients can be tracked. If you have reached the limit, you will have to remove some clients from the list before you can add more.

Related Topics
- Launching the Client Troubleshooting Tool
- Specifying Notification Settings

Specifying Notification Settings

Step 1
Choose Monitor > Monitoring Tools > Clients and Users.

Step 2
Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.

Step 3
Select the tracked client(s) for which you want to specify notification settings.

Step 4
Select a notification settings option from the following:
• Purged Expired Entries—You can set the duration to keep tracked clients in Prime Infrastructure database. Clients can be purged as follows:
  – after 1 week
  – after 2 weeks
  – after 1 month
  – after 2 months
  – after 6 months
  – kept indefinitely
• Notification Frequency—You can specify when Prime Infrastructure sends a notification of a tracked client:
  – on first detection
  – on every detection
• Notification Method—You can specify that the tracked client event generates an alarm or sends an email message.

  **Step 5** Enter the email address.
  **Step 6** Click **Save**.

---

**Related Topics**

- Tracking Clients
- Identifying Unknown Users

---

**When to Assign a Username**

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administer can assign a username to a device.

If a client device is authenticated to the network through web auth, Prime Infrastructure might not have username information for the client (applicable only for wired clients).

Clients are marked as unknown when the NMSP connection to the wired switch is lost. A client status (applicable only for wired client) is noted as connected, disconnected, or unknown:

• Connected clients—Clients that are active and connected to a wired switch.
• Disconnected clients—Clients that are disconnected from the wired switch.
• Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost.

**Related Topics**

- Identifying Unknown Users
Identifying Unknown Users

Step 1  Choose Monitor > Monitoring Tools > Clients and Users.
Step 2  Click Identify Unknown Users.
Step 3  Click Add to add a user.
Step 4  Enter the MAC address and username and click Add.
        Once a username and MAC address have been added, Prime Infrastructure uses this data for client lookup by matching the MAC address.
Step 5  Repeat Step 3 to Step 4 to enter a MAC Address and its corresponding username for each client.
Step 6  Click Save.
        The username is updated only when the next association of the client occurs.
        This table supports a maximum of 10,000 rows. To add or import new rows, you must first remove some older entries.

Related Topics
- When to Assign a Username
- Tracking Clients
- Modifying the Clients and Users Page

Modifying the Clients and Users Page

You can add, remove, or reorder columns in the Clients table.

Step 1  Choose Monitor > Monitoring Tools > Clients and Users.
Step 2  Click the settings icon, then click Columns.
Step 3  Select the columns to show
Step 4  Click Reset to restore the default view.
Step 5  Click Close to confirm the changes.

Related Topics
- Tracking Clients
- Enabling Automatic Client Troubleshooting

Enabling Automatic Client Troubleshooting

In the Settings > Client page, you can enable automatic client troubleshooting on a diagnostic channel. This feature is available only for Cisco-compatible Extension clients Version 5.
To enable automatic client troubleshooting, follow these steps:

Step 1 Choose Administration > Settings > System Settings.
Step 2 From the left sidebar menu, choose Client.
Step 3 Check the Automatically troubleshoot client on diagnostic channel check box.
When the check box is selected, Prime Infrastructure processes the diagnostic association trap. When it is not selected, Prime Infrastructure raises the trap, but automated troubleshooting is not initiated.
Step 4 Click Save.

Related Topics
- Modifying the Clients and Users Page
- Obtaining Radio Measurements for a Client

When to Obtain Radio Measurements for a Client

In the client page, you can obtain radio measurements only if the client is Cisco-compatible Extensions v2 (or higher) and in the associated state (with a valid IP address). If the client is busy when asked to do the measurement, it determines whether to honor the measurement or not. If it declines to make the measurement, it shows no data from the client.

This feature is available to CCX Version 6 clients only if the Foundation service version is 1 or later.

Related Topic
- Obtaining Radio Measurements for a Client

Obtaining Radio Measurements for a Client

To receive radio measurements, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Click the circle next to a client.
You can also perform a search for a specific client using Prime Infrastructure Search feature. See “Searching for Clients” in Related Topics.
Step 3 From the Test drop-down list, choose Radio Measurement.
The Radio Measurement option only appears if the client is Cisco-compatible Extensions v2 (or higher) and is in the associated state (with a valid IP address).
Step 4 Check the check box to indicate if you want to specify beacon measurement, frame measurement, channel load, or noise histogram.
Click Initiate. The different measurements produce differing results. See “Radio Measurement Results for a Client” in Related Topics.
The measurements take about 5 milliseconds to perform. A message from Prime Infrastructure indicates the progress. If the client chooses not to perform the measurement, that is communicated.

**Related Topics**

- Searching for Clients
- When to Obtain Radio Measurements for a Client
- Radio Measurement Results for a Client

**Radio Measurement Results for a Client**

Depending on the measurement type requested, the following information might appear:

- **Beacon Response**
  - Channel—The channel number for this measurement
  - BSSID—6-byte BSSID of the station that sent the beacon or probe response
  - PHY—Physical Medium Type (FH, DSS, OFDM, high rate DSS or ERP)
  - Received Signal Power—The strength of the beacon or probe response frame in dBm
  - Parent TSF—The lower 4 bytes of serving access point TSF value
  - Target TSF—The 8-byte TSF value contained in the beacon or probe response
  - Beacon Interval—The 2-byte beacon interval in the received beacon or probe response
  - Capability information—As found in the beacon or probe response

- **Frame Measurement**
  - Channel—Channel number for this measurement
  - BSSID—BSSID contained in the MAC header of the data frames received
  - Number of frames—Number of frames received from the transmit address
  - Received Signal Power—The signal strength of 802.11 frames in dBm

- **Channel Load**
  - Channel—The channel number for this measurement
  - CCA busy fraction—The fractional duration over which CCA indicated the channel was busy during the measurement duration defined as ceiling (255 times the duration the CCA indicated channel was busy divided by measurement duration)

- **Noise Histogram**
  - Channel—The channel number for this measurement
  - RPI density in each of the eight power ranges

**Related Topics**

- When to Obtain Radio Measurements for a Client
- Obtaining Radio Measurements for a Client
Viewing Client V5 Statistics

To access the Statistics request page, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.
**Step 2** Select a client.
**Step 3** From the Test drop-down list, choose V5 Statistics.
   This menu is shown only for CCX v5 and later clients.
**Step 4** Click Go.
**Step 5** Select the desired type of stats (Dot11 Measurement or Security Measurement).
**Step 6** Click Initiate to initiate the measurements.
   The duration of measurement is five seconds.
**Step 7** Depending on the V5 Statistics request type, the following counters are displayed in the results page:
   - Dot11 Measurement
     - Transmitted Fragment Count
     - Multicast Transmitted Frame Count
     - Failed Count
     - Retry Count
     - Multiple Retry Count
     - Frame Duplicate Count
     - Rts Success Count
     - Rts Failure Count
     - Ack Failure Count
     - Received Fragment Count
     - Multicast Received Frame Count
     - FCS Error Count—This counter increments when an FCS error is detected in a received MPDU.
     - Transmitted Frame Count
   - Security
     - Pairwise Cipher
     - Tkip ICV Errors
     - Tkip Local Mic Failures
     - Tkip Replays
     - Ccmp Replays
     - Ccmp Decryp Errors
     - Mgmt Stats Tkip ICV Errors
     - Mgmt Stats Tkip Local Mic Failures
     - Mgmt Stats Tkip Replays
     - Mgmt Stats Ccmp Replays
Viewing Client Operational Parameters

To view specific client operational parameters, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Select a client.

**Step 3** From the Test drop-down list, choose Operational Parameters.

The following information is displayed:

Operational Parameters:

- Device Name—User-defined name for device.
- Client Type—Client type can be any of the following:
  - laptop(0)
  - pc(1)
  - pda(2)
  - dot11mobilephone(3)
  - dualmodephone(4)
  - wgb(5)
  - scanner(6)
  - tabletpc(7)
  - printer(8)
  - projector(9)
  - videoconfsystem(10)
  - camera(11)
  - gamingsystem(12)
  - dot11deskphone(13)
  - cashregister(14)
  - radiotag(15)
- rfidsensor(16)
- server(17)

- SSID—SSID being used by the client.
- IP Address Mode—The IP address mode such as static configuration or DHCP.
- IPv4 Address—IPv4 address assigned to the client.
- IPv4 Subnet Address—IPv4 subnet address assigned to the client.
- IPv6 Address—IPv6 address assigned to the client.
- IPv6 Subnet Address—IPv6 address assigned to the client.
- Default Gateway—The default gateway chosen for the client.
- Operating System—Identifies the operating system that is using the wireless network adapter.
- Operating System Version—Identifies the version of the operating system that is using the wireless network adapter.
- WNA Firmware Version—Version of the firmware currently installed on the client.
- Driver Version—
- Enterprise Phone Number—Enterprise phone number for the client.
- Cell Phone Number—Cell phone number for the client.
- Power Save Mode—Displays any of the following power save modes: awake, normal, or maxPower.
- System Name—
- Localization—

Radio Information:
- Radio Type—The following radio types are available:
  - unused(0)
  - fhss(1)
  - dsss(2)
  - irbaseband(3)
  - ofdm(4)
  - hrdss(5)
  - erp(6)
- Radio Channel—Radio channel in use.

DNS/WNS Information:
- DNS Servers—IP address for DNS server.
- WNS Servers—IP address for WNS server.

Security Information:
- Credential Type—Indicates how the credentials are configured for the client.
- Authentication Method—Method of authentication used by the client.
- EAP Method—Method of Extensible Authentication Protocol (EAP) used by the client.
- Encryption Method—Encryption method used by the client.
• Key Management Method—Key management method used by the client.

Related Topics
• Viewing Client Operational Parameters
• Viewing Client Profiles

Viewing Client Profiles

To view specific client profile information, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Monitor &gt; Monitoring Tools &gt; Clients and Users.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a client.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the More drop-down list, choose Profiles.</td>
</tr>
</tbody>
</table>

The following information is displayed:
• Profile Name—List of profile names as hyperlinks. Click a hyperlink to display the profile details.
• SSID—SSID of the WLAN to which the client is associated.

Related Topics
• Disabling Current Clients

Disabling Current Clients

To disable a current client, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Monitor &gt; Monitoring Tools &gt; Clients and Users.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a client.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Disable. The Disable Client page appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter a description in the Description text box.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>

Once a client is disabled, it cannot join any network/ssid on controller(s). To enable the client again, choose Configuration > Network > Network Devices > Wireless Controller > Device Name > Security > Manually Disabled Clients, and remove the client entry.

Related Topics
• Viewing Client Profiles
• Removing Current Clients
Removing Current Clients

To remove a current client, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Select a client.

**Step 3** Choose Remove.

**Step 4** Click Remove to confirm the deletion.

Related Topic
- Enabling Mirror Mode

Enabling Mirror Mode

When a client is enabled, mirror mode enables you to duplicate (to another port) all the traffic originating from or terminating at a single client device or access point.

Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port because any connections to this port become unresponsive.

To enable mirror mode, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Select a client.

**Step 3** From the More drop-down list, choose Enable Mirror Mode.

**Step 4** Click Go.

Related Topics
- Mapping Recent Client Locations

Mapping Recent Client Locations

Note Cisco MSE is not required to be managed in Cisco Prime Infrastructure for Recent Map to work.

To display a high-resolution map of the client recent location, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Choose a client from the Client Username column.

**Step 3** From the More drop-down list, choose Recent Map (High Resolution).
Step 4  Click Go.

Related Topic
•  Mapping Current Client Locations

Mapping Current Client Locations

Note  Cisco MSE is not required to be managed in Cisco Prime Infrastructure for Present Map to work.

To display a high-resolution map of the client current location, follow these steps:

Step 1  Choose Monitor > Monitoring Tools > Clients and Users.
Step 2  Select a client.
Step 3  From the More drop-down list, choose Present Map (High Resolution).
Step 4  Click Go.

Related Topic
•  Running Client Sessions Reports

Running Client Sessions Reports

To view the most recent client session report results for a client, follow these steps:

Step 1  Choose Monitor > Monitoring Tools > Clients and Users.
Step 2  Select a client.
Step 3  From the More drop-down list, choose Client Sessions Report.
Step 4  Click Go. The Client Session report details display.

Related Topic
•  Viewing Client Roam Reason Reports

Viewing Client Roam Reason Reports

To view the most recent roam report for this client, follow these steps:

Step 1  Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Select a client.
Step 3 From the More drop-down list, choose Roam Reason.
Step 4 Click Go.

This page displays the most recent roam report for the client. Each roam report has the following information:

- New AP MAC address
- Old (previous) AP MAC address
- Previous AP SSID
- Previous AP channel
- Transition time—Time that it took the client to associate to a new access point.
- Roam reason—Reason for the client roam.

**Related Topic**
- Viewing Detecting Access Point Details

## Viewing Detecting Access Point Details

To display details of access points that can hear the client including the signal strength/SNR, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Select a client.
Step 3 From the More drop-down list, choose Detecting APs.
Step 4 Click Go.

**Related Topic**
- Viewing Client Location History

## Viewing Client Location History

To display the history of the client location based on RF fingerprinting, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Select a client.
Step 3 From the More drop-down list, choose Location History.
Step 4 Click Go.
Viewing Voice Metrics for a Client

To view traffic stream metrics for this client, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Clients and Users**.

**Step 2** Select a client.

**Step 3** From the **More** drop-down list, choose **Voice Metrics**.

**Step 4** Click **Go**.

The following information appears:

- **Time**—Time that the statistics were gathered from the access point(s).
- **QoS**
- **AP Ethernet MAC**
- **Radio**
- **% PLR (Downlink)**—Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
- **% PLR (Uplink)**—Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
- **Avg Queuing Delay (ms) (Uplink)**—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
- **% Packets > 40 ms Queuing Delay (Downlink)**—Percentage of queuing delay packets greater than 40 ms.
- **% Packets 20ms—40ms Queuing Delay (Downlink)**—Percentage of queuing delay packets greater than 20 ms.
- **Roaming Delay**—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.

Related Topic

- Viewing Voice Metrics for a Client