Troubleshooting

This appendix contains the following sections:

- Information About Troubleshooting, page 18-1
- Interpreting LEDs, page 18-2
- System Messages, page 18-3
- Viewing System Resources, page 18-6
- Using the CLI to Troubleshoot Problems, page 18-8
- Configuring System and Message Logging, page 18-9
- Viewing Access Point Event Logs, page 18-16
- Uploading Logs and Crash Files, page 18-17
- Uploading Core Dumps from the Controller, page 18-20
- Uploading Packet Capture Files, page 18-23
- Monitoring Memory Leaks, page 18-26
- Troubleshooting CCXv5 Client Devices, page 18-27
- Using the Debug Facility, page 18-42
- Configuring Wireless Sniffing, page 18-47
- Troubleshooting Access Points Using Telnet or SSH, page 18-49
- Debugging the Access Point Monitor Service, page 18-52
- Troubleshooting OfficeExtend Access Points, page 18-53
- Troubleshooting Mesh Access Points, page 18-55

Information About Troubleshooting

This appendix lists system messages that can appear on the Cisco UWN solution interfaces, describes the LED patterns on controllers and lightweight access points, and provides CLI commands that can be used to troubleshoot problems on the controller. It contains these sections:
Interpreting LEDs

Information About Interpreting LEDs

This section describes how to interpret controller LEDs and lightweight access point LEDs.

This section contains the following topics:

- Interpreting Controller LEDs, page 18-2
- Interpreting Lightweight Access Point LEDs, page 18-2
- Interpreting OfficeExtend LEDs, page 18-53

Interpreting Controller LEDs


Interpreting Lightweight Access Point LEDs

See the quick start guide or hardware installation guide for your specific access point for a description of the LED patterns. See the list of access points and the respective documentation at http://www.cisco.com/en/US/products/hw/wireless/index.html.
# System Messages

## Information About System Messages

Table 18-1 lists some common system messages and their descriptions. For a complete list of system messages, see the *Cisco Wireless LAN Controller System Message Guide*.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apf_utils.c 680: Received a CIF field without the protected bit set from mobile xx:xx:xx:xx:xx</td>
<td>A client is sending an association request on a security-enabled WLAN with the protected bit set to 0 (in the Capability field of the association request). As designed, the controller rejects the association request, and the client sees an association failure.</td>
</tr>
<tr>
<td>dtl_arp.c 480: Got an idle-timeout message from an unknown client xx:xx:xx:xx:xx</td>
<td>The controller’s network processing unit (NPU) sends a timeout message to the central processing unit (CPU) indicating that a particular client has timed out or aged out. This situation typically occurs when the CPU has removed a wireless client from its internal database but has not notified the NPU. Because the client remains in the NPU database, it ages out on the network processor and notifies the CPU. The CPU finds the client that is not present in its database and then sends this message.</td>
</tr>
<tr>
<td>STATION_DISASSOCIATE</td>
<td>The client may have intentionally terminated usage or may have experienced a service disruption.</td>
</tr>
<tr>
<td>STATION_DEAUTHENTICATE</td>
<td>The client may have intentionally terminated usage or this message could indicate an authentication issue.</td>
</tr>
<tr>
<td>STATION_AUTHENTICATION_FAIL</td>
<td>Check disable, key mismatch, or other configuration issues.</td>
</tr>
<tr>
<td>STATION_ASSOCIATE_FAIL</td>
<td>Check the load on the Cisco radio or signal quality issues.</td>
</tr>
<tr>
<td>LRAD_ASSOCIATED</td>
<td>The associated lightweight access point is now managed by this controller.</td>
</tr>
<tr>
<td>LRAD_DISASSOCIATED</td>
<td>The lightweight access point may have associated to a different controller or may have become completely unreachable.</td>
</tr>
<tr>
<td>LRAD_UP</td>
<td>The lightweight access point is operational; no action is required.</td>
</tr>
<tr>
<td>LRAD_DOWN</td>
<td>The lightweight access point may have a problem or is administratively disabled.</td>
</tr>
<tr>
<td>LRADIF_UP</td>
<td>The Cisco radio is UP.</td>
</tr>
</tbody>
</table>
### Table 18-1 System Messages and Descriptions (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LRADIF_DOWN</td>
<td>The Cisco radio may have a problem or is administratively disabled.</td>
</tr>
<tr>
<td>LRADIF_LOAD_PROFILE_FAILED</td>
<td>The client density may have exceeded the system capacity.</td>
</tr>
<tr>
<td>LRADIF_NOISE_PROFILE_FAILED</td>
<td>The non-802.11 noise has exceeded the configured threshold.</td>
</tr>
<tr>
<td>LRADIF_INTERFERENCEPROFILE_FAILED</td>
<td>802.11 interference has exceeded the threshold limits on the channel; check channel assignments.</td>
</tr>
<tr>
<td>LRADIF_COVERAGEPROFILE_FAILED</td>
<td>A possible coverage hole has been detected. Check the lightweight access point history to see if it is a common problem and add lightweight access points if necessary.</td>
</tr>
<tr>
<td>LRADIF_LOADPROFILE_PASSED</td>
<td>The load is now within threshold limits.</td>
</tr>
<tr>
<td>LRADIF_NOISEPROFILE_PASSED</td>
<td>The detected noise is now less than threshold limits.</td>
</tr>
<tr>
<td>LRADIF_INTERFERENCEPROFILE_PASSED</td>
<td>The detected interference is now less than threshold limit.</td>
</tr>
<tr>
<td>LRADIF_COVERAGEPROFILE_PASSED</td>
<td>The number of clients receiving a poor signal are within threshold limit.</td>
</tr>
<tr>
<td>LRADIF_CURRENT_TXPOWER_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>LRADIF_CURRENT_CHANNEL_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>LRADIF_RTS_THRESHOLD_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>LRADIF_ED_THRESHOLD_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>LRADIF_FRAGMENTATION_THRESHOLD_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>RRM_DOT11_A_GROUPING_DONE</td>
<td>Informational message.</td>
</tr>
<tr>
<td>RRM_DOT11_B_GROUPING_DONE</td>
<td>Informational message.</td>
</tr>
<tr>
<td>ROGUE_AP_DETECTED</td>
<td>May be a security issue. Use maps and trends to investigate.</td>
</tr>
<tr>
<td>ROGUE_AP_REMOVED</td>
<td>A detected rogue access point has timed out. The unit might have shut down or moved out of the coverage area.</td>
</tr>
<tr>
<td>AP_MAX_ROGUE_COUNT_EXCEEDED</td>
<td>The current number of active rogue access points has exceeded system threshold limit.</td>
</tr>
<tr>
<td>LINK_UP</td>
<td>Positive confirmation message.</td>
</tr>
<tr>
<td>LINK_DOWN</td>
<td>A port may have a problem or is administratively disabled.</td>
</tr>
<tr>
<td>LINK_FAILURE</td>
<td>A port may have a problem or is administratively disabled.</td>
</tr>
<tr>
<td>AUTHENTICATION_FAILURE</td>
<td>An attempted security breech has occurred. Investigate.</td>
</tr>
</tbody>
</table>
### Table 18-1  System Messages and Descriptions (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP_NEWROOT</td>
<td>Informational message.</td>
</tr>
<tr>
<td>STP_TOPOLOGY_CHANGE</td>
<td>Informational message.</td>
</tr>
<tr>
<td>IPSEC_ESP_AUTH_FAILURE</td>
<td>Check WLAN IPsec configuration.</td>
</tr>
<tr>
<td>IPSEC_ESP_REPLAY_FAILURE</td>
<td>Check for an attempt to spoof an IP address.</td>
</tr>
<tr>
<td>IPSEC_ESP_POLICY_FAILURE</td>
<td>Check for an IPsec configuration mismatch between the WLAN and client.</td>
</tr>
<tr>
<td>IPSEC_INV.Navigate</td>
<td>Informational message.</td>
</tr>
<tr>
<td>IPSEC_OTHER_POLICY_FAILURE</td>
<td>Check for an IPsec configuration mismatch between the WLAN and client.</td>
</tr>
<tr>
<td>IPSEC_IKE_NEG_FAILURE</td>
<td>Check for an IPsec IKE configuration mismatch between the WLAN and client.</td>
</tr>
<tr>
<td>IPSEC_SUITE_NEG_FAILURE</td>
<td>Check for an IPsec IKE configuration mismatch between the WLAN and client.</td>
</tr>
<tr>
<td>IPSEC_INVALID_COOKIE</td>
<td>Informational message.</td>
</tr>
<tr>
<td>RADIOS_EXCEEDED</td>
<td>The maximum number of supported Cisco radios has been exceeded. Check for a controller failure in the same Layer 2 network or add another controller.</td>
</tr>
<tr>
<td>SENSED_TEMPERATURE_HIGH</td>
<td>Check fan, air conditioning, and/or other cooling arrangements.</td>
</tr>
<tr>
<td>SENSED_TEMPERATURE_LOW</td>
<td>Check the room temperature and/or other reasons for low temperature.</td>
</tr>
<tr>
<td>TEMPERATURE_SENSOR_FAILURE</td>
<td>Replace the temperature sensor as soon as possible.</td>
</tr>
<tr>
<td>TEMPERATURE_SENSOR_CLEAR</td>
<td>The temperature sensor is operational.</td>
</tr>
<tr>
<td>POE_CONTROLLER_FAILURE</td>
<td>Check ports; a possible serious failure has been detected.</td>
</tr>
<tr>
<td>MAX_ROGUE_COUNT_EXCEEDED</td>
<td>The current number of active rogue access points has exceeded system threshold limit.</td>
</tr>
<tr>
<td>SWITCH_UP</td>
<td>The controller is responding to SNMP polls.</td>
</tr>
<tr>
<td>SWITCH_DOWN</td>
<td>The controller is not responding to SNMP polls; check controller and SNMP settings.</td>
</tr>
<tr>
<td>RADIUS_SERVERS_FAILED</td>
<td>Check the network connectivity between RADIUS and the controller.</td>
</tr>
<tr>
<td>CONFIG_SAVED</td>
<td>The running configuration has been saved to flash; it will be active after a reboot.</td>
</tr>
<tr>
<td>MULTIPLE_USERS</td>
<td>Another user with the same username has logged in.</td>
</tr>
<tr>
<td>FAN_FAILURE</td>
<td>Monitor the controller temperature to avoid overheating.</td>
</tr>
<tr>
<td>POWER_SUPPLY_CHANGE</td>
<td>Check for a power-supply malfunction.</td>
</tr>
</tbody>
</table>
Information About Viewing System Resources

You can determine the amount of system resources being used by the controller such as the current controller CPU usage, system buffers, and web server buffers.

Guidelines and Limitations

The Cisco 5500 Series Controllers have multiple CPUs, so you can view individual CPU usage. For each CPU, you can see the percentage of the CPU in use and the percentage of the CPU time spent at the interrupt level (for example, 0%/3%).

Viewing System Resources (GUI)


---

### Table 18-1 System Messages and Descriptions (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COLD_START</td>
<td>The controller may have been rebooted.</td>
</tr>
<tr>
<td>WARM_START</td>
<td>The controller may have been rebooted.</td>
</tr>
</tbody>
</table>
Viewing System Resources (CLI)

On the controller CLI, enter these commands:

- **show cpu**

  Information similar to the following appears:

  Current CPU(s) load: 0%
  Individual CPU load: 0%/0%, 0%/1%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%

  Where the first number is the CPU percentage that the controller spent on the user application and the second number is the CPU percentage that the controller spent on the OS services.

- **show tech-support**

  Information similar to the following appears:

  System Information
  Manufacturer's Name.............................. Cisco Systems Inc.
  Product Name..................................... Cisco Controller
  Product Version............................... 6.0.165.0
  ...
  -----------------Show cpu-------------------
  Current CPU(s) Load.............................. 0%
  Individual CPU Load............................. 0%/3%, 0%/1%, 0%/1%, 0%/1%, 0%/0%, 0%/1%

  -----------------Show system buffers------------
  System Buffers
  Max Free Buffers............................... 4608
  Free Buffers................................... 4596
  Buffers In Use................................. 12

  Web Server Resources
  Descriptors Allocated.......................... 259
**Using the CLI to Troubleshoot Problems**

If you experience any problems with your controller, you can use the commands in this section to gather information and debug issues.

1. **show process cpu**—Shows how various tasks in the system are using the CPU at that instant in time. This command is helpful in understanding if any single task is monopolizing the CPU and preventing other tasks from being performed.

   Information similar to the following appears:

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>CPU Use</th>
<th>Reaper</th>
</tr>
</thead>
<tbody>
<tr>
<td>reaperWatcher</td>
<td>(3/124)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>osapiReaper</td>
<td>(10/121)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>TempStatus</td>
<td>(255/1)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>emWeb</td>
<td>(255/1)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>cliWebTask</td>
<td>(255/1)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>UtilTask</td>
<td>(255/1)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
</tbody>
</table>

   In the example above, the following fields provide information:

   - The Name field shows the tasks that the CPU is to perform.
   - The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task divided by a range of system priorities.
   - The CPU Use field shows the CPU usage of a particular task.
   - The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a “T”). If the task is being watched by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.

   **Note**

   If you want to see the total CPU usage as a percentage, enter the *show cpu* command.

2. **show process memory**—Shows the allocation and deallocation of memory from various processes in the system at that instant in time.

   Information similar to the following appears:

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>BytesInUse</th>
<th>BlocksInUse</th>
<th>Reaper</th>
</tr>
</thead>
<tbody>
<tr>
<td>reaperWatcher</td>
<td>(3/124)</td>
<td>0</td>
<td>0</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>osapiReaper</td>
<td>(10/121)</td>
<td>0</td>
<td>0</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>TempStatus</td>
<td>(255/1)</td>
<td>308</td>
<td>1</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>emWeb</td>
<td>(255/1)</td>
<td>294440</td>
<td>4910</td>
<td>(0/0)% T 300</td>
</tr>
<tr>
<td>cliWebTask</td>
<td>(255/1)</td>
<td>738</td>
<td>2</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>UtilTask</td>
<td>(255/1)</td>
<td>308</td>
<td>1</td>
<td>(0/0)% T 300</td>
</tr>
</tbody>
</table>

   In the example above, the following fields provide information:
- The Name field shows the tasks that the CPU is to perform.
- The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task divided by a range of system priorities.
- The BytesInUse field shows the actual number of bytes used by dynamic memory allocation for a particular task.
- The BlocksInUse field shows the chunks of memory that are assigned to perform a particular task.
- The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a “T”). If the task is being watched by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.

3. `show tech-support`—Shows information related to the state of the system, including the current configuration, last crash file, CPU utilization, and memory utilization.

4. `show run-config`—Shows the complete configuration of the controller. To exclude access point configuration settings, use the `show run-config no-ap` command.

Note If you want to see the passwords in clear text, enter the `config passwd-cleartext enable` command. To execute this command, you must enter an admin password. This command is valid only for this particular session. It is not saved following a reboot.

5. `show run-config commands`—Shows the list of configured commands on the controller. This command shows only values configured by the user. It does not show system-configured default values.

### Configuring System and Message Logging

This section contains the following topics:

- Information About System and Message Logging, page 18-9
- Configuring System and Message Logging (GUI), page 18-10
- Viewing Message Logs (GUI), page 18-12
- Configuring System and Message Logging (CLI), page 18-12

### Information About System and Message Logging

System logging allows controllers to log their system events to up to three remote syslog servers. The controller sends a copy of each syslog message as it is logged to each syslog server configured on the controller. Being able to send the syslog messages to multiple servers ensures that the messages are not lost due to the temporary unavailability of one syslog server. Message logging allows system messages to be logged to the controller buffer or console.
### Configuring System and Message Logging (GUI)

**Step 1** Choose **Management > Logs > Config**. The Syslog Configuration page appears.

![Syslog Configuration Page](image)

**Figure 18-2  Syslog Configuration Page**

**Step 2** In the Syslog Server IP Address text box, enter the IP address of the server to which to send the syslog messages and click **Add**. You can add up to three syslog servers to the controller. The list of syslog servers that have already been added to the controller appears below this text box.

**Note** If you want to remove a syslog server from the controller, click **Remove** to the right of the desired server.

**Step 3** To set the severity level for filtering syslog messages to the syslog servers, choose one of the following options from the Syslog Level drop-down list:

- **Emergencies** = Severity level 0 — System is unusable
- **Alerts** = Severity level 1 (default value) — Immediate action required
- **Critical** = Severity level 2 — Critical condition
- **Errors** = Severity level 3 — Error condition
- **Warnings** = Severity level 4 — Warning condition
- **Notifications** = Severity level 5 — Normal but significant condition
- **Informational** = Severity level 6 — Informational message
- **Debugging** = Severity level 7 — Message that appears during debugging

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog servers. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog servers.

**Step 4** You can set the facility for outgoing syslog messages to the syslog servers. The facility level is used to specify what type of program is logging the message. Choose one of the following options from the Syslog Facility drop-down list:
- **Kernel** = Facility level 0—Kernel messages
- **User Process** = Facility level 1—User-level messages
- **Mail** = Facility level 2—Mail System messages
- **System Daemons** = Facility level 3—System Daemons messages
- **Authorization** = Facility level 4—Security and Authorization messages
- **Syslog** = Facility level 5 (default value)—Syslog Daemon messages
- **Line Printer** = Facility level 6—Line Printer subsystem
- **USENET** = Facility level 7—User-initiated processes or application messages
- **Unix-to-Unix Copy** = Facility level 8—UNIX-to-UNIX Copy system messages
- **Cron** = Facility level 9—Cron Daemon messages
- **FTP Daemon** = Facility level 11—FTP Daemon messages
- **System Use 1** = Facility level 12—Reserved for system messages
- **System Use 2** = Facility level 13—Reserved for system messages
- **System Use 3** = Facility level 14—Reserved for system messages
- **System Use 4** = Facility level 15—Reserved for system messages
- **Local Use 0** = Facility level 16—Reserved for local use
- **Local Use 1** = Facility level 17—Reserved for local use
- **Local Use 2** = Facility level 18—Reserved for local use
- **Local Use 3** = Facility level 19—Reserved for local use
- **Local Use 4** = Facility level 20—Reserved for local use
- **Local Use 5** = Facility level 21—Reserved for local use
- **Local Use 6** = Facility level 22—Reserved for local use
- **Local Use 7** = Facility level 23—Reserved for local use

**Step 5** Click **Apply** to commit your changes.

**Step 6** To set the severity level for logging messages to the controller buffer and console, choose one of the following options from both the Buffered Log Level and Console Log Level drop-down lists:

- **Emergencies** = Severity level 0
- **Alerts** = Severity level 1
- **Critical** = Severity level 2
- **Errors** = Severity level 3 (default value)
- **Warnings** = Severity level 4
- **Notifications** = Severity level 5
- **Informational** = Severity level 6
- **Debugging** = Severity level 7
- **Disable**— This option is available only for the Console Log level. Select this option to disable console logging.

If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.
Step 7  Select the **File Info** check box if you want the message logs to include information about the source file. The default value is enabled.

Step 8  Select the **Trace Info** check box if you want the message logs to include traceback information. The default value is disabled.

Step 9  Click **Apply** to commit your changes.

Step 10  Click **Save Configuration** to save your changes.

---

### Viewing Message Logs (GUI)

To view message logs using the controller GUI, choose **Management > Logs > Message Logs**. The Message Logs page appears.

**Figure 18-3  Message Logs Page**

![Message Logs Page](image)

**Note**

To clear the current message logs from the controller, click **Clear**.

---

### Configuring System and Message Logging (CLI)

To configure system and message logging using the controller CLI, follow these steps:

**Step 1**  To enable system logging and set the IP address of the syslog server to which to send the syslog messages, enter this command:

```
config logging syslog host server_IP_address
```

You can add up to three syslog servers to the controller.
To remove a syslog server from the controller, enter this command:
```
cfg logging syslog host server_IP_address delete
```

**Step 2** To set the severity level for filtering syslog messages to the syslog server, enter this command:
```
cfg logging syslog level severity_level
```
where `severity_level` is one of the following:
- `emergencies` = Severity level 0
- `alerts` = Severity level 1
- `critical` = Severity level 2
- `errors` = Severity level 3
- `warnings` = Severity level 4
- `notifications` = Severity level 5
- `informational` = Severity level 6
- `debugging` = Severity level 7

**Note** As an alternative, you can enter a number from 0 through 7 for the `severity_level` parameter.

**Note** If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog server. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog server.

**Step 3** To set the severity level for filtering syslog messages for a particular access point or for all access points, enter this command:
```
cfg ap logging syslog level severity_level {Cisco_AP | all}
```
where `severity_level` is one of the following:
- `emergencies` = Severity level 0
- `alerts` = Severity level 1
- `critical` = Severity level 2
- `errors` = Severity level 3
- `warnings` = Severity level 4
- `notifications` = Severity level 5
- `informational` = Severity level 6
- `debugging` = Severity level 7

**Note** If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the access point. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the access point.

**Step 4** To set the facility for outgoing syslog messages to the syslog server, enter this command:
**config logging syslog facility** *facility_code*

where *facility_code* is one of the following:

- **authorization** = Authorization system. Facility level = 4.
- **auth-private** = Authorization system (private). Facility level = 10.
- **cron** = Cron/at facility. Facility level = 9.
- **daemon** = System daemons. Facility level = 3.
- **ftp** = FTP daemon. Facility level = 11.
- **kern** = Kernel. Facility level = 0.
- **local0** = Local use. Facility level = 16.
- **local1** = Local use. Facility level = 17.
- **local2** = Local use. Facility level = 18.
- **local3** = Local use. Facility level = 19.
- **local4** = Local use. Facility level = 20.
- **local5** = Local use. Facility level = 21.
- **local6** = Local use. Facility level = 22.
- **local7** = Local use. Facility level = 23.
- **lpr** = Line printer system. Facility level = 6.
- **mail** = Mail system. Facility level = 2.
- **news** = USENET news. Facility level = 7.
- **sys12** = System use. Facility level = 12.
- **sys13** = System use. Facility level = 13.
- **sys14** = System use. Facility level = 14.
- **sys15** = System use. Facility level = 15.
- **syslog** = The syslog itself. Facility level = 5.
- **user** = User process. Facility level = 1.
- **uucp** = Unix-to-Unix copy system. Facility level = 8.

**Step 5** To set the severity level for logging messages to the controller buffer and console, enter these commands:

- **config logging buffered** *severity_level*
- **config logging console** *severity_level*

where *severity_level* is one of the following:

- **emergencies** = Severity level 0
- **alerts** = Severity level 1
- **critical** = Severity level 2
- **errors** = Severity level 3
- **warnings** = Severity level 4
- **notifications** = Severity level 5
- **informational** = Severity level 6
- **debugging** = Severity level 7
Note  As an alternative, you can enter a number from 0 through 7 for the severity_level parameter.

Note  If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.

Step 6  To save debug messages to the controller buffer, the controller console, or a syslog server, enter these commands:

- config logging debug buffered {enable | disable}
- config logging debug console {enable | disable}
- config logging debug syslog {enable | disable}

By default, the console command is enabled, and the buffered and syslog commands are disabled.

Step 7  To cause the controller to include information about the source file in the message logs or to prevent the controller from displaying this information, enter this command:

config logging fileinfo {enable | disable}

The default value is enabled.

Step 8  To cause the controller to include process information in the message logs or to prevent the controller from displaying this information, enter this command:

config logging procinfo {enable | disable}

The default value is disabled.

Step 9  To cause the controller to include traceback information in the message logs or to prevent the controller from displaying this information, enter this command:

config logging traceinfo {enable | disable}

The default value is disabled.

Step 10  To enable or disable timestamps in log messages and debug messages, enter these commands:

- config service timestamps log {datetime | disable}
- config service timestamps debug {datetime | disable}

where

- datetime = Messages are timestamped with the standard date and time. This is the default value.
- disable = Messages are not timestamped.

Step 11  To save your changes, enter this command:

save config

Viewing System and Message Logs (CLI)

To see the logging parameters and buffer contents, enter this command:

show logging
Information similar to the following appears:

Logging to buffer:
- Logging of system messages to buffer:
  - Logging filter level.......................... errors
  - Number of system messages logged.......... 8716
  - Number of system messages dropped........ 2906
- Logging of debug messages to buffer......... Disabled
  - Number of debug messages logged........... 0
  - Number of debug messages dropped.......... 0

Logging to console:
- Logging of system messages to console:
  - Logging filter level.......................... errors
  - Number of system messages logged.......... 0
  - Number of system messages dropped........ 11622
- Logging of debug messages to console......... Enabled
  - Number of debug messages logged........... 0
  - Number of debug messages dropped.......... 0

Logging to syslog:
- Syslog facility................................ local0
- Logging of system messages to syslog:
  - Logging filter level.......................... errors
  - Number of system messages logged.......... 8716
  - Number of debug messages dropped.......... 0
  - Number of remote syslog hosts............. 0
    - Host 0....................................... Not Configured
    - Host 1....................................... Not Configured
    - Host 2....................................... Not Configured
- Logging of traceback............................ Disabled
- Logging of process information............... Disabled
- Logging of source file informational........ Enabled
- Timestamping of messages........................
  - Timestamping of system messages............ Enabled
  - Timestamp format............................ Date and Time
  - Timestamping of debug messages............... Enabled
  - Timestamp format............................ Date and Time

Logging buffer (8722 logged, 2910 dropped)

*Mar 26 09:23:13.574: %MM-3-INVALID_PKT_RECV: mm_listen.c:5508 Received an invalid packet from 1.100.163.144. Source member:0.0.0.0. source member unknown.

Previous message occurred 2 times.

*Mar 26 09:22:44.925: %MM-3-INVALID_PKT_RECV: mm_listen.c:5508 Received an invalid packet from 1.100.163.144. Source member:0.0.0.0. source member unknown.

...

Viewing Access Point Event Logs

This section contains the following topics:

- Information About Access Point Event Logs, page 18-17
- Viewing Access Point Event Logs (CLI), page 18-17
Information About Access Point Event Logs

Access points log all system messages (with a severity level greater than or equal to notifications) to the access point event log. The event log can contain up to 1024 lines of messages, with up to 128 characters per line. When the event log becomes filled, the oldest message is removed to accommodate a new event message. The event log is saved in a file on the access point flash, which ensures that it is saved through a reboot cycle. To minimize the number of writes to the access point flash, the contents of the event log are written to the event log file during normal reload and crash scenarios only.

Viewing Access Point Event Logs (CLI)

Use these CLI commands to view or clear the access point event log from the controller:

- To see the contents of the event log file for an access point that is joined to the controller, enter this command:

  show ap eventlog Cisco_AP

  Information similar to the following appears:

  AP event log download has been initiated
  Waiting for download to complete

  AP event log download completed.
  ======================== AP Event log Contents =====================
  *Sep 22 11:44:00.573: %CAPWAP-5-CHANGED: CAPWAP changed state to IMAGE
  *Sep 22 11:44:01.514: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down
  *Sep 22 11:44:01.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to down
  *Mar 1 00:00:39.078: %CAPWAP-3-ERRORLOG: Did not get log server settings from DHCP.
  *Mar 1 00:00:42.142: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
  *Mar 1 00:00:42.151: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
  *Mar 1 00:00:42.158: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
  *Mar 1 00:00:48.121: %CAPWAP-3-CLIENTERRORLOG: Set Transport Address: no more AP manager IP addresses remain
  *Mar 1 00:01:48.122: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN
  *Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down
  *Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to administratively down

- To delete the existing event log and create an empty event log file for a specific access point or for all access points joined to the controller, enter this command:

  clear ap-eventlog {specific Cisco_AP | all}

Uploading Logs and Crash Files

This section contains the following topics:
Prerequisites to Upload Logs and Crash Files

- Follow the instructions in this section to upload logs and crash files from the controller. However, before you begin, ensure you have a TFTP or FTP server available for the file upload. Follow these guidelines when setting up a TFTP or FTP server:
  - If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Uploading Logs and Crash Files (GUI)

**Step 1** Choose Command > Upload File. The Upload File from Controller page appears.

**Figure 18-4 Upload File from Controller Page**

**Step 2** From the File Type drop-down list, choose one of the following:
- Event Log
- Message Log
- Trap Log
- Crash File

**Step 3** From the Transfer Mode drop-down list, choose TFTP or FTP.

**Step 4** In the IP Address text box, enter the IP address of the TFTP or FTP server.
Step 5  In the File Path text box, enter the directory path of the log or crash file.

Step 6  In the File Name text box, enter the name of the log or crash file.

Step 7  If you chose FTP as the Transfer Mode, follow these steps:
   a. In the Server Login Username text box, enter the FTP server login name.
   b. In the Server Login Password text box, enter the FTP server login password.
   c. In the Server Port Number text box, enter the port number of the FTP server. The default value for the server port is 21.

Step 8  Click Upload to upload the log or crash file from the controller. A message appears indicating the status of the upload.

---

### Uploading Logs and Crash Files (CLI)

Step 1  To transfer the file from the controller to a TFTP or FTP server, enter this command:

```
transfer upload mode {tftp | ftp}
```

Step 2  To specify the type of file to be uploaded, enter this command:

```
transfer upload datatype datatype
```

where `datatype` is one of the following options:

- **crashfile**—Uploads the system’s crash file.
- **errorlog**—Uploads the system’s error log.
- **panic-crash-file**—Uploads the kernel panic information if a kernel panic occurs.
- **systemtrace**—Uploads the system’s trace file.
- **traplog**—Uploads the system’s trap log.
- **watchdog-crash-file**—Uploads the console dump resulting from a software-watchdog-initiated reboot of the controller following a crash. The software watchdog module periodically checks the integrity of the internal software and makes sure that the system does not stay in an inconsistent or nonoperational state for a long period of time.

Step 3  To specify the path to the file, enter these commands:

- **transfer upload serverip server_ip_address**
- **transfer upload path server_path_to_file**
- **transfer upload filename filename**

Step 4  If you are using an FTP server, also enter these commands:

- **transfer upload username username**
- **transfer upload password password**
- **transfer upload port port**

  **Note**  The default value for the `port` parameter is 21.

Step 5  To see the updated settings, enter this command:
Uploading Core Dumps from the Controller

This section contains the following topics:

- Information About Uploading Core Dumps from the Controller, page 18-20
- Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI), page 18-20
- Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (CLI), page 18-21

Information About Uploading Core Dumps from the Controller

To help troubleshoot controller crashes, you can configure the controller to automatically upload its core dump file to an FTP server after experiencing a crash. You cannot upload the core dump file directly to an FTP or TFTP server but you can upload a crash file to an FTP or TFTP server. The controllers save the core dump file to flash memory following a crash.

Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI)

Step 1
Choose Management > Tech Support > Core Dump to open the Core Dump page.

Figure 18-5 Core Dump Page

---

Step 6
When prompted to confirm the current settings and start the software upload, answer y.
Step 2  To enable the controller to generate a core dump file following a crash, select the **Core Dump Transfer** check box.

Step 3  To specify the type of server to which the core dump file is uploaded, choose **FTP** from the Transfer Mode drop-down list.

Step 4  In the IP Address text box, enter the IP address of the FTP server.

**Note**  The controller must be able to reach the FTP server.

Step 5  In the File Name text box, enter the name that the controller uses to label the core dump file.

Step 6  In the User Name text box, enter the username for FTP login.

Step 7  In the Password text box, enter the password for FTP login.

Step 8  Click **Apply** to commit your changes.

Step 9  Click **Save Configuration** to save your changes.

---

**Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (CLI)**

Step 1  To enable or disable the controller to generate a core dump file following a crash, enter this command:

```
config coredump { enable | disable }
```

Step 2  To specify the FTP server to which the core dump file is uploaded, enter this command:

```
config coredump ftp server_ip_address filename
```

where

- `server_ip_address` is the IP address of the FTP server to which the controller sends its core dump file.

  **Note**  The controller must be able to reach the FTP server.

- `filename` is the name that the controller uses to label the core dump file.

Step 3  To specify the username and password for FTP login, enter this command:

```
config coredump username ftp_username password ftp_password
```

Step 4  To save your changes, enter this command:

```
save config
```

Step 5  To see a summary of the controller's core dump file, enter this command:

```
show coredump summary
```

Information similar to the following appears:

```
Core Dump is enabled
FTP Server IP.................................... 10.10.10.17
FTP Filename..................................... file1
FTP Username..................................... ftpuser
```
Uploading Core Dumps from Controller to a TFTP or FTP Server (CLI)

**Note**
This procedure is not applicable for Cisco 2106 and 4400 controllers.

**Step 1**
To see information about the core dump file in flash memory, enter this command:

```
show coredump summary
```

Information similar to the following appears:

- Core Dump is disabled
- Core Dump file is saved on flash

```
Sw Version.................................... 6.0.83.0
File Size..................................... 9081788
File Name Suffix........................... filename.gz
```

**Step 2**
To transfer the file from the controller to a TFTP or FTP server, enter these commands:

- `transfer upload mode {tftp | ftp}`
- `transfer upload datatype coredump`
- `transfer upload serverip server_ip_address`
- `transfer upload path server_path_to_file`
- `transfer upload filename filename`

**Note**
After the file is uploaded, it ends with a .gz suffix. If desired, you can upload the same core dump file multiple times with different names to different servers.

**Step 3**
If you are using an FTP server, also enter these commands:

- `transfer upload username username`
- `transfer upload password password`
- `transfer upload port port`

**Note**
The default value for the `port` parameter is 21.

**Step 4**
To view the updated settings, enter this command:

```
transfer upload start
```

**Step 5**
When prompted to confirm the current settings and start the software upload, answer **y**.
Uploading Packet Capture Files

This section contains the following topics:

- Information About Uploading Packet Capture Files, page 18-23
- Guidelines and Limitations, page 18-24
- Uploading Packet Capture Files (GUI), page 18-24
- Uploading Packet Capture Files (CLI), page 18-25

Information About Uploading Packet Capture Files

When a Cisco 5500 Series Controller's data plane crashes, it stores the last 50 packets that the controller received in flash memory. This information can be useful in troubleshooting the crash.

When a crash occurs, the controller generates a new packet capture file (*.pcap) file, and a message similar to the following appears in the controller crash file:

Last 5 packets processed at each core are stored in "last_received_pkts.pcap" captured file.
- Frame 36,38,43,47,49, processed at core #0.
- Frame 14,27,30,42,45, processed at core #1.
- Frame 15,18,20,32,48, processed at core #2.
- Frame 11,29,34,37,46, processed at core #3.
- Frame 7,8,12,31,35, processed at core #4.
- Frame 21,25,39,41,50, processed at core #5.
- Frame 16,17,19,22,33, processed at core #6.
- Frame 6,10,13,23,26, processed at core #7.
- Frame 9,24,28,40,44, processed at core #8.
- Frame 1,2,3,4,5, processed at core #9.

You can use the controller GUI or CLI to upload the packet capture file from the controller. You can then use Wireshark or another standard packet capture tool to view and analyze the contents of the file. 

Figure 18-6 shows a sample output of a packet capture file in Wireshark.
Guidelines and Limitations

- Only Cisco 5500 Series Controllers generate packet capture files. This feature is not available on other controller platforms.
- Ensure that you have a TFTP or FTP server available for the file upload. Follow these guidelines when setting up a TFTP or FTP server:
  - If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Uploading Packet Capture Files (GUI)

**Step 1** Choose **Commands > Upload File** to open the Upload File from Controller page.
Step 2  From the File Type drop-down list, choose **Packet Capture**.

Step 3  From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

Step 4  In the IP Address text box, enter the IP address of the TFTP or FTP server.

Step 5  In the File Path text box, enter the directory path of the packet capture file.

Step 6  In the File Name text box, enter the name of the packet capture file. These files have a .pcap extension.

Step 7  If you are using an FTP server, follow these steps:
   a. In the Server Login Username text box, enter the username to log into the FTP server.
   b. In the Server Login Password text box, enter the password to log into the FTP server.
   c. In the Server Port Number text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 8  Click **Upload** to upload the packet capture file from the controller. A message appears indicating the status of the upload.

Step 9  Use Wireshark or another standard packet capture tool to open the packet capture file and see the last 50 packets that were received by the controller.

---

**Uploading Packet Capture Files (CLI)**

Step 1  Log on to the controller CLI.

Step 2  Enter the `transfer upload mode {tftp | ftp}` command.

Step 3  Enter the `transfer upload datatype packet-capture` command.

Step 4  Enter the `transfer upload serverip server-ip-address` command.

Step 5  Enter the `transfer upload path server-path-to-file` command.

Step 6  Enter the `transfer upload filename last_received_pkts.pcap` command.

Step 7  If you are using an FTP server, enter these commands:
   - `transfer upload username username`
   - `transfer upload password password`
   - `transfer upload port port`
Monitoring Memory Leaks

This section provides instructions for troubleshooting hard-to-solve or hard-to-reproduce memory problems.

Caution
The commands in this section can be disruptive to your system and should be run only when you are advised to do so by the Cisco Technical Assistance Center (TAC).

Monitoring Memory Leaks (CLI)

Step 1
To enable or disable monitoring for memory errors and leaks, enter this command:

```
config memory monitor errors {enable | disable}
```

The default value is disabled.

Note
Your changes are not saved across reboots. After the controller reboots, it uses the default setting for this feature.

Step 2
If you suspect that a memory leak has occurred, enter this command to configure the controller to perform an auto-leak analysis between two memory thresholds (in kilobytes):

```
config memory monitor leaks low_thresh high_thresh
```

If the free memory is lower than the `low_thresh` threshold, the system crashes, generating a crash file. The default value for this parameter is 10000 kilobytes, and you cannot set it below this value.
Set the high_thresh threshold to the current free memory level or higher so that the system enters auto-leak-analysis mode. After the free memory reaches a level lower than the specified high_thresh threshold, the process of tracking and freeing memory allocation begins. As a result, the debug memory events enable command shows all allocations and frees, and the show memory monitor detail command starts to detect any suspected memory leaks. The default value for this parameter is 30000 kilobytes.

**Step 3**
To see a summary of any discovered memory issues, enter this command:

```
show memory monitor
```

Information similar to the following appears:

Memory Leak Monitor Status:
low_threshold(10000), high_threshold(30000), current status(disabled)

Memory Error Monitor Status:
Crash-on-error flag currently set to (disabled)
No memory error detected.

**Step 4**
To see the details of any memory leaks or corruption, enter this command:

```
show memory monitor detail
```

Information similar to the following appears:

Memory error detected. Details:
- Corruption detected at pmalloc entry address: (0x179a7ec0)
- Corrupt entry:headerMagic(0xdeadf00d), trailer(0xabcde), entriesize(128),bytes(100),thread(Unknown task name, task id = (332096592)), file(pmalloc.c),line(1736),time(1027)

Previous 1K memory dump from error location.
```
(179a7ac0): 00000000 00000000 00000000 ceeff00d readf00d 00000080 00000000 00000000
(179a7ae0): 17958b20 00000000 1175608c 00000078 00000000 readceef 179a7af0 00000001
(179a7b00): 0000003f 0000006f 00000001 00000004 00000001 00000009 00000009 0000002d
(179a7b20): 00000001 00000002 00000001 00000001 00000009 00000000 00000000 5d7b9aba
(179a7b40): cbddf004 192f465e 7791acc8 e5032242 5365788c a1b7cee6 00000000 00000000
(179a7b60): 00000000 00000000 00000000 00000000 00000000 ceeff00d readf00d 00000080
(179a7b80): 00000000 00000000 17958dc0 00000000 1175608c 00000000 readceef 179a7ba0 00000001
(179a7ba0): 179a7ba4 00000001 00000003 00000006 00000001 00000004 00000001 00003763
(179a7bc0): 00000002 00000002 00000001 00000001 00000002 00000000 00000000 0000001e
(179a7be0): 000001a 00000089 00000000 00000000 00000008 00000000 00000000 17222194
(179a7c00): 1722246c 1722246c 00000000 00000000 00000000 00000000 00000000 ceeff00d
(179a7c20): readf00d 00000080 00000000 00000000 00000000 179a7b78 00000000 1175608c 000000078
```

**Step 5**
If a memory leak occurs, enter this command to enable debugging of errors or events during memory allocation:

```
debug memory {errors | events} {enable | disable}
```

---

**Troubleshooting CCXv5 Client Devices**

This section contains the following topics:

- Information About Troubleshooting CCXv5 Client Devices, page 18-28
Information About Troubleshooting CCXv5 Client Devices

The controller supports three features designed to help troubleshoot communication problems with CCXv5 clients: diagnostic channel, client reporting, and roaming and real-time diagnostics. See the “Configuring Cisco Client Extensions” section on page 8-57 for more information on CCX.

Guidelines and Limitations

These features are supported only on CCXv5 clients. They are not supported for use with non-CCX clients or with clients running an earlier version of CCX.

Configuring Diagnostic Channel

The diagnostic channel feature enables you to troubleshoot problems regarding client communication with a WLAN. The client and access points can be put through a defined set of tests in an attempt to identify the cause of communication difficulties the client is experiencing and then allow corrective measures to be taken to make the client operational on the network. You can use the controller GUI or CLI to enable the diagnostic channel, and you can use the controller CLI or WCS to run the diagnostic tests.

Note

We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface.

Configuring the Diagnostic Channel (GUI)

Step 1
Choose WLANs to open the WLANs page.

Step 2
Create a new WLAN or click the ID number of an existing WLAN.

Note
We recommend that you create a new WLAN on which to run the diagnostic tests.

Step 3
When the WLANs > Edit page appears, choose the Advanced tab to open the WLANs > Edit (Advanced) page.
Step 4 If you want to enable diagnostic channel troubleshooting on this WLAN, select the Diagnostic Channel check box. Otherwise, leave this check box unselected, which is the default value.

Note You can use the CLI to initiate diagnostic tests on the client. See the “Configuring the Diagnostic Channel (CLI)” section on page 18-29 for details.

Step 5 Click Apply to commit your changes.

Step 6 Click Save Configuration to save your changes.

Configuring the Diagnostic Channel (CLI)

Step 1 To enable diagnostic channel troubleshooting on a particular WLAN, enter this command:

```
config wlan diag-channel {enable | disable} wlan_id
```

Step 2 To verify that your change has been made, enter this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier......................... 1
Profile Name............................ employee1
Network Name (SSID).................... employee
Status................................. Disabled
MAC Filtering......................... Disabled
Broadcast SSID......................... Enabled
AAA Policy Override.................. Disabled
Number of Active Clients............. 0
Exclusionlist Timeout............... 60 seconds
Session Timeout...................... Infinity
Interface.............................. virtual
WLAN ACL.............................. unconfigured
DHCP Server.......................... Default
DHCP Address Assignment Required... Disabled
Quality of Service.................... Silver (best effort)
```
Step 3  To send a request to the client to perform the DHCP test, enter this command:

```
config client ccx dhcp-test client_mac_address
```

Note This test does not require the client to use the diagnostic channel.

Step 4  To send a request to the client to perform the default gateway ping test, enter this command:

```
config client ccx default-gw-ping client_mac_address
```

Note This test does not require the client to use the diagnostic channel.

Step 5  To send a request to the client to perform the DNS server IP address ping test, enter this command:

```
config client ccx dns-ping client_mac_address
```

Note This test does not require the client to use the diagnostic channel.

Step 6  To send a request to the client to perform the DNS name resolution test to the specified hostname, enter this command:

```
config client ccx dns-resolve client_mac_address host_name
```

Note This test does not require the client to use the diagnostic channel.

Step 7  To send a request to the client to perform the association test, enter this command:

```
config client ccx test-association client_mac_address ssid bssid \{802.11a | 802.11b | 802.11g\} channel
```

Step 8  To send a request to the client to perform the 802.1X test, enter this command:

```
config client ccx test-dot1x client_mac_address profile_id bssid \{802.11a | 802.11b | 802.11g\} channel
```

Step 9  To send a request to the client to perform the profile redirect test, enter this command:

```
config client ccx test-profile client_mac_address profile_id
```

The `profile_id` should be from one of the client profiles for which client reporting is enabled.

Note Users are redirected back to the parent WLAN, not to any other profile. The only profile shown is the user’s parent profile. However, parent WLAN profiles can have one child diagnostic WLAN.

Step 10 Use these commands if necessary to abort or clear a test:

- To send a request to the client to abort the current test, enter this command:

```
config client ccx test-abort client_mac_address
```

Only one test can be pending at a time, so this command aborts the current pending test.
Chapter 18  Troubleshooting

Troubleshooting CCXv5 Client Devices

To clear the test results on the controller, enter this command:

```
config client ccx clear-results client_mac_address
```

**Step 11**
To send a message to the client, enter this command:

```
config client ccx send-message client_mac_address message_id
```

where `message_id` is one of the following:

- 1 = The SSID is invalid.
- 2 = The network settings are invalid.
- 3 = There is a WLAN credibility mismatch.
- 4 = The user credentials are incorrect.
- 5 = Please call support.
- 6 = The problem is resolved.
- 7 = The problem has not been resolved.
- 8 = Please try again later.
- 9 = Please correct the indicated problem.
- 10 = Troubleshooting is refused by the network.
- 11 = Retrieving client reports.
- 12 = Retrieving client logs.
- 13 = Retrieval complete.
- 14 = Beginning association test.
- 15 = Beginning DHCP test.
- 16 = Beginning network connectivity test.
- 17 = Beginning DNS ping test.
- 18 = Beginning name resolution test.
- 19 = Beginning 802.1X authentication test.
- 20 = Redirecting client to a specific profile.
- 21 = Test complete.
- 22 = Test passed.
- 23 = Test failed.
- 24 = Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
- 25 = Log retrieval refused by the client.
- 26 = Client report retrieval refused by the client.
- 27 = Test request refused by the client.
- 28 = Invalid network (IP) setting.
- 29 = There is a known outage or problem with the network.
- 30 = Scheduled maintenance period.
- 31 = The WLAN security method is not correct.
- 32 = The WLAN encryption method is not correct.
- 33 = The WLAN authentication method is not correct.
Step 12 To see the status of the last test, enter this command:

```
show client ccx last-test-status client_mac_address
```

Information similar to the following appears for the default gateway ping test:

```
Test Type........................................ Gateway Ping Test
Test Status...................................... Pending/Success/Timeout
Dialog Token...................................... 15
Timeout.......................................... 15000 ms
Request Time..................................... 1329 seconds since system boot
```

Step 13 To see the status of the last test response, enter this command:

```
show client ccx last-response-status client_mac_address
```

Information similar to the following appears for the 802.1X authentication test:

```
Test Status...................................... Success
Response Dialog Token.................................... 87
Response Status.................................. Successful
Response Test Type............................... 802.1x Authentication Test
Response Time.................................... 3476 seconds since system boot
```

Step 14 To see the results from the last successful diagnostics test, enter this command:

```
show client ccx results client_mac_address
```

Information similar to the following appears for the 802.1X authentication test:

```
dot1x Complete................................... Success
EAP Method....................................... *1,Host OS Login Credentials
dot1x Status.................................. 255
```

Step 15 To see the relevant data frames captured by the client during the previous test, enter this command:

```
show client ccx frame-data client_mac_address
```

Information similar to the following appears:

```
LOG Frames:
Frame Number:.................................... 1
Last Frame Number:................................ 1120
Direction:....................................... 1
Timestamp:....................................... 0d 00h 50m 39s 863954us
Frame Length:.................................... 197
Frame Data:
```
00000000: 80 00 00 00 ff ff ff ff ff ff 00 12 44 bd bd b0 ............D...
```
```
00000010: 00 12 44 bd bd b0 f0 af 43 70 00 f2 82 01 00 00 ..D.....Cp......
```
```
00000020: 64 00 11 08 00 01 00 01 08 8c 12 98 24 b0 48 60  d...........$.H`
```
```
00000030: 6c 05 04 01 02 00 00 85 1e 00 00 89 00 0f 00 ff 1..........
```
```
00000040: 03 19 00 41 50 32 3d 33 3d 31 30 00 00 00 00 00 00 00 00 00 00 00 AP23-10........
```
```
00000050: 00 00 00 00 00 00 26 96 06 00 40 96 00 ff ff dd ....&....
```
```
00000060: 18 00 50 f2 01 01 00 00 50 f2 05 01 01 00 00 50 f2 ..P...P...P.
```
```
00000070: 05 01 00 00 40 96 00 28 00 dd 06 00 40 96 01 01 ....@...(....
```
```
00000080: 00 dd 05 00 40 96 03 04 dd 16 00 40 96 04 00 02 ....@......@
```
```
00000090: 07 a4 00 00 23 a4 00 00 42 43 00 00 62 32 00 00 ....#...BC..b2..
```
```
000000a0: dd 05 00 40 96 0b 01 dd 18 00 50 f2 02 01 01 82 ....@......P...
```
```
000000b0: 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f .....'...BC`.b2/
```
```
LOG Frames:
Frame Number:.................................... 2
```
Configuring Client Reporting

The client reporting protocol is used by the client and the access point to exchange client information. Client reports are collected automatically when the client associates. You can use the controller GUI or CLI to send a client report request to any CCXv5 client any time after the client associates. There are four types of client reports:

- **Client profile**—Provides information about the configuration of the client.
- **Operating parameters**—Provides the details of the client’s current operational modes.
- **Manufacturers’ information**—Provides data about the wireless LAN client adapter in use.
- **Client capabilities**—Provides information about the client’s capabilities.

**Configuring Client Reporting (GUI)**

**Step 1** Choose **Monitor > Clients** to open the Clients page.
Step 2  Click the MAC address of the desired client. The Clients > Detail page appears.

![Clients > Detail Page](Figure 18-9)

<table>
<thead>
<tr>
<th>Client Properties</th>
<th>AP Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>AP Address</td>
</tr>
<tr>
<td></td>
<td>00:0b:05:69:e5:31</td>
</tr>
<tr>
<td>IP Address</td>
<td>AP Name</td>
</tr>
<tr>
<td>10.1.0.201</td>
<td>ap-62:00:90</td>
</tr>
<tr>
<td>Client Type</td>
<td>AP Type</td>
</tr>
<tr>
<td>Regular</td>
<td>802.11a</td>
</tr>
<tr>
<td>User Name</td>
<td>WLAN Profile</td>
</tr>
<tr>
<td></td>
<td>ssid1</td>
</tr>
<tr>
<td>Port Number</td>
<td>Status</td>
</tr>
<tr>
<td>1</td>
<td>Associated</td>
</tr>
<tr>
<td>Interface</td>
<td>Association ID</td>
</tr>
<tr>
<td>management</td>
<td>1</td>
</tr>
<tr>
<td>WLAN ID</td>
<td>802.11 Authentication</td>
</tr>
<tr>
<td>0</td>
<td>Open System</td>
</tr>
<tr>
<td>CCX Version</td>
<td>Reassociation Code</td>
</tr>
<tr>
<td>CCXv5</td>
<td>0</td>
</tr>
<tr>
<td>ESSID Version</td>
<td>Static Code</td>
</tr>
<tr>
<td>Not Supported</td>
<td>0</td>
</tr>
<tr>
<td>Mobility Role</td>
<td>CF Pollable</td>
</tr>
<tr>
<td>Local</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Mobility Peer IP Address</td>
<td>CF Poll Request</td>
</tr>
<tr>
<td>N/A</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Policy Manager State</td>
<td>Short Preamble</td>
</tr>
<tr>
<td>REN</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Mirror Mode</td>
<td>PDCD</td>
</tr>
<tr>
<td>Disable</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Management Frame Protection</td>
<td>Channel Agility</td>
</tr>
<tr>
<td>No</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Security Information</td>
<td>Timeout</td>
</tr>
<tr>
<td>Security Policy completing</td>
<td>0</td>
</tr>
<tr>
<td>Yes</td>
<td>WEP State</td>
</tr>
<tr>
<td>Policy Type</td>
<td>WEP Disable</td>
</tr>
<tr>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Encryption Cipher</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
</tr>
<tr>
<td>EAP Type</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Quality of Service Properties</td>
<td></td>
</tr>
<tr>
<td>802.11 State</td>
<td>Enabled</td>
</tr>
<tr>
<td>U-RFSD Support</td>
<td>Disabled</td>
</tr>
<tr>
<td>QoS Level</td>
<td>Silver</td>
</tr>
<tr>
<td>DSCP Code Point (QOS)</td>
<td>Disabled</td>
</tr>
<tr>
<td>802.1P Tag</td>
<td>Disabled</td>
</tr>
<tr>
<td>Average Data Rate</td>
<td>Disabled</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>Disabled</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>Disabled</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>Disabled</td>
</tr>
<tr>
<td>Client Statistics</td>
<td></td>
</tr>
<tr>
<td>Bytes Received</td>
<td>641114</td>
</tr>
<tr>
<td>Bytes Sent</td>
<td>1269984</td>
</tr>
<tr>
<td>Packets Received</td>
<td>9910</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>9316</td>
</tr>
<tr>
<td>Policy Errors</td>
<td>0</td>
</tr>
<tr>
<td>RSSI</td>
<td>-51</td>
</tr>
<tr>
<td>SNR</td>
<td>53</td>
</tr>
<tr>
<td>Sample Time</td>
<td>Thu Aug 30 11:14:54 2007</td>
</tr>
<tr>
<td>Excessive Retransmit</td>
<td>0</td>
</tr>
<tr>
<td>Retransmit</td>
<td>0</td>
</tr>
<tr>
<td>Success Count</td>
<td>0</td>
</tr>
<tr>
<td>Fail Count</td>
<td>0</td>
</tr>
<tr>
<td>Tx Retransmit</td>
<td>0</td>
</tr>
</tbody>
</table>

Step 3  Click Send CCXv5 Req to send a report request to the client.
**Chapter 18      Troubleshooting**

**Troubleshooting CCXv5 Client Devices**

**Note**
You must create a Trusted Profile using ACAU for Cisco CB21AG or equivalent software from your CCXv5 vendor.

**Step 4**
Click **Display** to view the parameters from the client. The Client Reporting page appears.

![Client Reporting Page](image)

**Figure 18-10**
Client Reporting Page

This page lists the client profiles and indicates if they are currently in use. It also provides information on the client’s operating parameters, manufacturer, and capabilities.
Step 5  Click the link for the desired client profile. The Profile Details page appears.

**Figure 18-11  Profile Details Page**

This page shows the client profile details, including the SSID, power save mode, radio channel, data rates, and 802.11 security settings.

### Configuring Client Reporting (CLI)

**Step 1**  To send a request to the client to send its profiles, enter this command:

```
config client ccx get-profiles client_mac_address
```

**Step 2**  To send a request to the client to send its current operating parameters, enter this command:

```
config client ccx get-operating-parameters client_mac_address
```

**Step 3**  To send a request to the client to send the manufacturer’s information, enter this command:

```
config client ccx get-manufacturer-info client_mac_address
```

**Step 4**  To send a request to the client to send its capability information, enter this command:

```
config client ccx get-client-capability client_mac_address
```

**Step 5**  To clear the client reporting information, enter this command:

```
config client ccx clear-reports client_mac_address
```

**Step 6**  To see the client profiles, enter this command:
show client ccx profiles client_mac_address

Information similar to the following appears:

Number of Profiles............................... 1
Current Profile................................. 1

Profile ID....................................... 1
Profile Name..................................... wifiEAP
SSID............................................. wifiEAP
Security Parameters[EAP Method,Credential]..... EAP-TLS,Host OS Login Credentials
Auth Method...................................... EAP
Key Management.................................. WPA2+CCKM
Encryption....................................... AES-CCMP
Power Save Mode.................................. Constantly Awake

Radio Configuration:
Radio Type....................................... DSSS
  Preamble Type.................................. Long preamble
  CCA Method..................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries................................... 6
  Fragment Threshold........................... 2342
  Radio Channels............................... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode.................................. Automatic
  Rate List (MB).................................. 1.0 2.0

Radio Type....................................... HRDSSS(802.11b)
  Preamble Type.................................. Long preamble
  CCA Method..................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries................................... 6
  Fragment Threshold........................... 2342
  Radio Channels............................... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode.................................. Automatic
  Rate List (MB).................................. 5.5 11.0

Radio Type....................................... ERP(802.11g)
  Preamble Type.................................. Long preamble
  CCA Method..................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries................................... 6
  Fragment Threshold........................... 2342
  Radio Channels............................... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode.................................. Automatic
  Rate List (MB).................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Radio Type....................................... OFDM(802.11a)
  Preamble Type.................................. Long preamble
  CCA Method..................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries................................... 6
  Fragment Threshold........................... 2342
  Radio Channels............................... 36 40 44 48 52 56 60 64 149 153 157 161 165
  Tx Power Mode.................................. Automatic
  Rate List (MB).................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Step 7

To see the client operating parameters, enter this command:

show client ccx operating-parameters client_mac_address

Information similar to the following appears:

Client Mac....................................... 00:40:96:b2:8d:5e
Radio Type....................................... OFDM(802.11a)
Chapter 18  Troubleshooting

Troubleshooting CCXv5 Client Devices

Radio Type....................................... OFDM(802.11a)
Radio Channels.................................. 36 40 44 48 52 56 60 64 100 104 108 112
116 120 124 128 132 136 140 149 153 157 161 165
Tx Power Mode.................................. Automatic
Rate List(MB).................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Power Save Mode.............................. Normal Power Save
SSID............................................. wifi
Security Parameters[EAP Method,Credential]....... None
Auth Method...................................... None
Key Management................................... None
Encryption....................................... None
Device Name..................................... Wireless Network Connection 15
Device Type..................................... 0
OS Id............................................ Windows XP
OS Version...................................... 5.1.2600 Service Pack 2
IP Type.......................................... DHCP address
IPv4 Address..................................... Available
IP Address....................................... 70.0.4.66
Subnet Mask..................................... 255.0.0.0
Default Gateway.................................. 70.1.0.1
IPv6 Address..................................... Not Available
IPv6 Address..................................... 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0
IPv6 Subnet Mask............................... 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0
DNS Servers..................................... 103.0.48.0
WINS Servers.....................................
System Name...................................... URAVAL3777
Firmware Version................................. 4.0.0.187
Driver Version................................... 4.0.0.187

Step 8
To see the client manufacturer information, enter this command:

show client ccx manufacturer-info client_mac_address

Information similar to the following appears:

Manufacturer OUI................................. 00:40:96
Manufacturer ID.................................. Cisco
Manufacturer Model.............................. Cisco Aironet 802.11a/b/g Wireless Adapter
Manufacturer Serial.............................. FOC1046N3SX
Mac Address..................................... 00:40:96:82:8d:5e
Radio Type..................................... DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)
Antenna Type..................................... Omni-directional diversity
Antenna Gain..................................... 2 dBi

Rx Sensitivity:
Radio Type..................................... DSSS
Rx Sensitivity.................................. Rate:1.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity.................................. Rate:2.0 Mbps, MinRssi:-95, MaxRssi:-30
Radio Type..................................... HRDSSS(802.11b)
Rx Sensitivity.................................. Rate:3.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity.................................. Rate:5.5 Mbps, MinRssi:-95, MaxRssi:-30
Radio Type..................................... ERP(802.11g)
Rx Sensitivity.................................. Rate:6.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity.................................. Rate:9.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity.................................. Rate:12.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity.................................. Rate:18.0 Mbps, MinRssi:-95, MaxRssi:-30

Step 9
To see the client’s capability information, enter this command:
show client ccx client-capability client_mac_address

Note
This command displays the client’s available capabilities, not current settings for the capabilities.

Information similar to the following appears:

Service Capability......................... Voice, Streaming (uni-directional) Video, Interactive (bi-directional) Video
Radio Type........................................ DSSS OFDM(802.11a) HRDSSS(802.11b) ERP(802.11g)
Radio Type........................................ DSSS
Radio Channels............................... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode.................................. Automatic
Rate List (MB)................................. 1.0 2.0
Radio Type........................................ HRDSSS(802.11b)
Radio Channels............................... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode.................................. Automatic
Rate List (MB)................................. 5.5 11.0
Radio Type........................................ ERP(802.11g)
Radio Channels............................... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode.................................. Automatic
Rate List (MB)................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Radio Type........................................ OFDM(802.11a)
Radio Channels............................... 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
Tx Power Mode.................................. Automatic
Rate List (MB)................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Configuring Roaming and Real-Time Diagnostics

You can use roaming and real-time logs and statistics to solve system problems. The event log enables you to identify and track the behavior of a client device. It is especially useful when attempting to diagnose difficulties that a user may be having on a WLAN. The event log provides a log of events and reports them to the access point. There are three categories of event logs:

- Roaming log—This log provides a historical view of the roaming events for a given client. The client maintains a minimum of five previous roaming events including failed attempts and successful roams.
- Robust Security Network Association (RSNA) log—This log provides a historical view of the authentication events for a given client. The client maintains a minimum of five previous authentication attempts including failed attempts and successful ones.
- Syslog—This log provides internal system information from the client. For example, it may indicate problems with 802.11 operation, system operation, and so on.

The statistics report provides 802.1X and security information for the client. You can use the controller CLI to send the event log and statistics request to any CCXv5 client any time after the client associates.
Configuring Roaming and Real-Time Diagnostics (CLI)

**Step 1** To send a log request, enter this command:

```bash
cfg client ccx log-request log_type client_mac_address
```

where **log_type** is roam, rsna, or syslog.

**Step 2** To view a log response, enter this command:

```bash
show client ccx log-response log_type client_mac_address
```

where **log_type** is roam, rsna, or syslog.

Information similar to the following appears for a log response with a **log_type** of roam:

```
Tue Jun 26 18:28:48 2007 Roaming Response LogID=133: Status=Successful
   Event Timestamp=0d 00h 00m 13s 322396us
   Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,
   Transition Time=3125(ms)
   Transition Reason: Normal roam, poor link
   Transition Result: Success
```

```
Tue Jun 26 18:28:48 2007 Roaming Response LogID=133: Status=Successful
   Event Timestamp=0d 00h 00m 16s 599006us
   Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,
   Transition Time=3235(ms)
   Transition Reason: Normal roam, poor link
   Transition Result: Success
```

```
Tue Jun 26 18:28:48 2007 Roaming Response LogID=133: Status=Successful
   Event Timestamp=0d 00h 00m 08s 815477us
   Source BSSID=00:0b:85:81:06:d2, Target BSSID=00:0b:85:81:06:d2,
   Transition Time=3281(ms)
   Transition Reason: First association to WLAN
   Transition Result: Success
```

Information similar to the following appears for a log response with a **log_type** of rsna:

```
Tue Jun 26 18:24:09 2007 RSNA Response LogID=132: Status=Successful
   Event Timestamp=0d 00h 00m 00s 246578us
   Target BSSID=00:14:1b:58:86:cd
   RSNA Version=1
   Group Cipher Suite=00-0f-ac-02
   Pairwise Cipher Suite Count = 1
      Pairwise Cipher Suite 0 = 00-0f-ac-04
   AKM Suite Count = 1
      AKM Suite 0 = 00-0f-ac-01
   RSN Capability = 0x0
   RSNA Result: Success
```

```
Tue Jun 26 18:24:09 2007 RSNA Response LogID=132: Status=Successful
   Event Timestamp=0d 00h 00m 00s 246625us
   Target BSSID=00:14:1b:58:86:cd
   RSNA Version=1
   Group Cipher Suite=00-0f-ac-02
   Pairwise Cipher Suite Count = 1
      Pairwise Cipher Suite 0 = 00-0f-ac-04
   AKM Suite Count = 1
```
Step 3
To send a request for statistics, enter this command:

```
config client ccx stats-request measurement_duration stats_name client_mac_address
```

where `stats_name` is dot11 or security.

Step 4
To view the statistics response, enter this command:

```
show client ccx stats-report client_mac_address
```

Information similar to the following appears:

```
Measurement duration = 1

dot11TransmittedFragmentCount = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount = 3
dot11RetryCount = 4
dot11MultipleRetryCount = 5
dot11FrameDuplicateCount = 6
```
Using the Debug Facility

This section contains the following topics:

- Information About Using the Debug Facility, page 18-42
- Configuring the Debug Facility (CLI), page 18-43

Information About Using the Debug Facility

The debug facility enables you to display all packets going to and from the controller CPU. You can enable it for received packets, transmitted packets, or both. By default, all packets received by the debug facility are displayed. However, you can define access control lists (ACLs) to filter packets before they are displayed. Packets not passing the ACLs are discarded without being displayed.

Each ACL includes an action (permit, deny, or disable) and one or more fields that can be used to match the packet. The debug facility provides ACLs that operate at the following levels and on the following values:

- **Driver ACL**
  - NPU encapsulation type
  - Port
- **Ethernet header ACL**
  - Destination address
  - Source address
  - Ethernet type
  - VLAN ID
- **IP header ACL**
  - Source address
  - Destination address
  - Protocol
  - Source port (if applicable)
  - Destination port (if applicable)
- **EoIP payload Ethernet header ACL**
  - Destination address
  - Source address

---

dot11RTSSuccessCount = 7
dot11RTSFailureCount = 8
dot11ACKFailureCount = 9
dot11ReceivedFragmentCount = 10
dot11MulticastReceivedFrameCount = 11
dot11FCSErrorCount = 12
dot11TransmittedFrameCount = 13
Using the Debug Facility

- Ethernet type
- VLAN ID

- **EOIP payload IP header ACL**
  - Source address
  - Destination address
  - Protocol
  - Source port (if applicable)
  - Destination port (if applicable)

- **CAPWAP payload 802.11 header ACL**
  - Destination address
  - Source address
  - BSSID
  - SNAP header type

- **CAPWAP payload IP header ACL**
  - Source address
  - Destination address
  - Protocol
  - Source port (if applicable)
  - Destination port (if applicable)

At each level, you can define multiple ACLs. The first ACL that matches the packet is the one that is selected.

**Configuring the Debug Facility (CLI)**

**Step 1**
To enable the debug facility, enter this command:

```
dump packet logging enable {rx | tx | all} packet_count display_size
```

where

- **rx** displays all received packets, **tx** displays all transmitted packets, and **all** displays both transmitted and received packets.
- **packet_count** is the maximum number of packets to log. You can enter a value between 1 and 65535 packets, and the default value is 25 packets.
- **display_size** is the number of bytes to display when printing a packet. By default, the entire packet is displayed.

**Note**
To disable the debug facility, enter `debug packet logging disable` command.

**Step 2**
Configure packet-logging ACLs by entering these commands:

- `debug packet logging acl driver rule_index action npu_encap port`
- **rule_index** is a value between 1 and 6 (inclusive).
- **action** is permit, deny, or disable.
- **npu_encap** specifies the NPU encapsulation type, which determines how packets are filtered. The possible values include dhcp, dot11-mgmt, dot11-probe, dot1x, eoip-ping, iapp, ip, lwapp, multicast, orphan-from-sta, orphan-to-sta, rbcp, wired-guest, or any.
- **port** is the physical port for packet transmission or reception.

- **debug packet logging acl eth** `rule_index action dst src type vlan`

where
- **rule_index** is a value between 1 and 6 (inclusive).
- **action** is permit, deny, or disable.
- **dst** is the destination MAC address.
- **src** is the source MAC address.
- **type** is the two-byte type code (such as 0x800 for IP, 0x806 for ARP). This parameter also accepts a few common string values such as “ip” (for 0x800) or “arp” (for 0x806).
- **vlan** is the two-byte VLAN ID.

- **debug packet logging acl ip** `rule_index action src dst proto src_port dst_port`

where
- **proto** is a numeric or any string recognized by getprotobyname(). The controller supports the following strings: ip, icmp, igmp, ggp, ipencap, st, tcp, egp, pup, udp, hmp, xns-idp, rdp, iso-tp4, ttp, dtp, idpr-cmtp, rsvp, vmtip, ospf, ipip, and encap.
- **src_port** is the UDP/TCP two-byte source port (for example, telnet, 23) or “any.” The controller accepts a numeric or any string recognized by getservbyname(). The controller supports the following strings: tcpmux, echo, discard, systat, daytime, netstat, qotd, msp, chargen, ftp-data, ftp, fsp, ssh, telnet, smtp, time, rlp, nameserver, whois, re-mail-ck, domain, mtp, bootps, bootpc, tftp, gopher, rje, finger, www, link, kerberos, supdup, hostnames, iso-tsap, csnet-ns, 3com-tmux, rtelnet, pop-2, pop-3, sunrpc, auth, smtp, uucp-path, nntp, tn32f, netbios-ns, netbios-dgm, netbios-ssn, imap2, snmp, snmp-trap, cmip-man, cmip-agent, xdmcp, nextstep, bgp, prospero, irc, smux, at-tcp, at-nbp, at-echo, at-zis, qtnmp, z3950, ipx, imp3, ulistserv, https, snmp, saft, nmp-local, nmp-gui, and hmnp-ind.
- **dst_port** is the UDP/TCP two-byte destination port (for example, telnet, 23) or “any.” The controller supports a numeric or any string recognized by getservbyname(). The controller supports the same strings as those for the **src_port**.

- **debug packet logging acl eoip-eth** `rule_index action dst src snap_type vlan`
- **debug packet logging acl eoip-ip** `rule_index action src dst proto src_port dst_port`
- **debug packet logging acl lwapp-dot11** `rule_index action dst src bssid snap_type`

where
- **bssid** is the Basic Service Set Identifier.
- **snap_type** is the Ethernet type.

- **debug packet logging acl lwapp-ip** `rule_index action src dst proto src_port dst_port`

**Note** To remove all configured ACLs, enter **debug packet logging acl clear-all** command.
Step 3

To configure the format of the debug output, enter this command:

```
debug packet logging format {hex2pcap | text2pcap}
```

The debug facility supports two output formats: hex2pcap and text2pcap. The standard format used by IOS supports the use of hex2pcap and can be decoded using an HTML front end. The text2pcap option is provided as an alternative so that a sequence of packets can be decoded from the same console log file. Figure 18-12 shows an example of hex2pcap output, and Figure 18-13 shows an example of text2pcap output.

**Figure 18-12 Sample Hex2pcap Output**

```
tx len=118, enccap=n/a, port=1
[0000]: 00c031e8 7f00000e 854008c0 08004500 ...ln....0.0...E.
[0010]: 00600000 40004001 5fe0e164 6c0e0164 .h...0.0_.D..d
[0020]: 6c000000 00000000 00000000 1....Y............
[0030]: 00000000 00000000 00000000 0001clid ...............
[0040]: 121f2321 22232325 26272829 2a2f2c2d ...
[0050]: 2e2f3031 32333435 36373839 3a3e3c3d ./0123456789:;=
[0060]: 3b3f4041 42344445 46474849 4a4b4c4d >?@abcdefghijklm
[0070]: 4b455051 5253  NCPQRS
```

**Figure 18-13 Sample Text2pcap Output**

```
tx len=118, enccap=n/a, port=1
0000 00 0c 31 6f 7f 00 00 00 65 40 08 00 08 00 45 00 ...ln.....0.0...E.
0010 00 60 00 00 40 00 40 01 5f 0e 01 64 6c 0e 01 64 .h...0.0_.D..d
0020 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 1d ...............
0040 1f 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d ...
0050 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d ./0123456789:;=
0060 3b 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d >?@abcdefghijklm
0070 4e 4f 50 51 52 53  NCPQRS
```

Step 4

To determine why packets might not be displayed, enter this command:

```
debug packet error {enable | disable}
```

Step 5

To display the status of packet debugging, enter this command:

```
show debug packet
```
Information similar to the following appears:

Status........................................... disabled
Number of packets to display................. 25
Bytes/packet to display....................... 0
Packet display format......................... text2pcap

Driver ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled

Ethernet ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled

IP ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled

EoIP-Ethernet ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled

EoIP-IP ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled

LWAPP-Dot11 ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled

LWAPP-IP ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
Configuring Wireless Sniffing

This section contains the following topics:
- Information About Wireless Sniffing, page 18-47
- Guidelines and Limitations, page 18-28
- Prerequisites for Wireless Sniffing, page 18-47
- Configuring Sniffing on an Access Point (GUI), page 18-48
- Configuring Sniffing on an Access Point (CLI), page 18-49

Information About Wireless Sniffing

The controller enables you to configure an access point as a network “sniffer,” which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on time stamps, signal strength, packet sizes, and so on. Sniffers allow you to monitor and record network activity and to detect problems.

Guidelines and Limitations

- Supported third-party network analyzer software applications are as follows:
  - Wildpackets Omnipeek or Airopeek
  - AirMagnet Enterprise Analyzer
  - Wireshark
- The latest version of Wireshark can decode the packets by going to the Analyze mode. Select decode as, and switch UDP5555 to decode as AIROPEEK.
- You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller, or a controller network module that runs software release 6.0 or later releases. To disable IP-MAC address binding, enter the `config network ip-mac-binding disable` command in the controller CLI. For more information, see the “Configuring IP-MAC Address Binding” section on page 4-64.
- You must enable WLAN 1 in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller, or a controller network module that runs software release 6.0 or later releases. If WLAN 1 is disabled, the access point cannot send packets.

Prerequisites for Wireless Sniffing

To perform wireless sniffing, you need the following hardware and software:
- A dedicated access point—An access point configured as a sniffer cannot simultaneously provide wireless access service on the network. To avoid disrupting coverage, use an access point that is not part of your existing wireless network.
- A remote monitoring device—A computer capable of running the analyzer software.
- Windows XP or Linux operating system—The controller supports sniffing on both Windows XP and Linux machines.
Configuring Sniffing on an Access Point (GUI)

Step 1
Choose Wireless > Access Points > All APs to open the All APs page.

Step 2
Click the name of the access point that you want to configure as the sniffer. The All APs > Details for page appears.

Step 3
From the AP Mode drop-down list, choose Sniffer.

Step 4
Click Apply to commit your changes.

Step 5
Click OK when warned that the access point will be rebooted.

Step 6
Choose Wireless > Access Points > Radios > 802.11a/n (or 802.11b/g/n) to open the 802.11a/n (or 802.11b/g/n) Radios page.

Step 7
Hover your cursor over the blue drop-down arrow for the desired access point and choose Configure. The 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page appears.

Step 8
Select the Sniff check box to enable sniffing on this access point, or leave it unselected to disable sniffing. The default value is unchecked.

Step 9
If you enabled sniffing in Step 8, follow these steps:

a. From the Channel drop-down list, choose the channel on which the access point sniffs for packets.

b. In the Server IP Address text box, enter the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark.

Step 10
Click Apply to commit your changes.

Step 11
Click Save Configuration to save your changes.
Configuring Sniffing on an Access Point (CLI)

Step 1  To configure the access point as a sniffer, enter this command:

```plaintext
config ap mode sniffer Cisco_AP
```
where `Cisco_AP` is the access point configured as the sniffer.

Step 2  When warned that the access point will be rebooted and asked if you want to continue, enter `Y`. The access point reboots in sniffer mode.

Step 3  To enable sniffing on the access point, enter this command:

```plaintext
config ap sniff {802.11a | 802.11b} enable channel server_IP_address Cisco_AP
```
where

- `channel` is the radio channel on which the access point sniffs for packets. The default values are 36 (802.11a/n) and 1 (802.11b/g/n).
- `server_IP_address` is the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark.
- `Cisco_AP` is the access point configured as the sniffer.

**Note**  To disable sniffing on the access point, enter the `config ap sniff {802.11a | 802.11b} disable Cisco_AP` command.

Step 4  To save your changes, enter this command:

```plaintext
save config
```

Step 5  To view the sniffer configuration settings for an access point, enter this command:

```plaintext
show ap config {802.11a | 802.11b} Cisco_AP
```

Information similar to the following appears:

```
Cisco AP Identifier.......................... 17
Cisco AP Name................................. AP131:46f2.98ac

AP Mode ...................................... Sniffer
Public Safety .................................. Global: Disabled, Local: Disabled
Sniffing ...................................... No

```

Troubleshooting Access Points Using Telnet or SSH

This section contains the following topics:

- Information About Troubleshooting Access Points Using Telnet or SSH, page 18-50
- Guidelines and Limitations, page 18-50
- Troubleshooting Access Points Using Telnet or SSH (GUI), page 18-50
- Troubleshooting Access Points Using Telnet or SSH (CLI), page 18-51
Information About Troubleshooting Access Points Using Telnet or SSH

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller.

- To avoid potential conflicts and security threats to the network, the following commands are unavailable while a Telnet or SSH session is enabled: config terminal, telnet, ssh, rsh, ping, traceroute, clear, clock, crypto, delete, fsck, lwapp, mkdir, radius, release, reload, rename, renew, rmdir, save, set, test, upgrade.
- Commands available during a Telnet or SSH session include debug, disable, enable, help, led, login, logout, more, no debug, show, systat, undebug, and where.

Note
For instructions on configuring Telnet or SSH sessions on the controller, see the “Configuring Telnet and SSH Sessions” section on page 3-35.

Guidelines and Limitations

You can configure Telnet or SSH by using the controller CLI in software release 5.0 or later releases or using the controller GUI in software release 6.0 or later releases.

Troubleshooting Access Points Using Telnet or SSH (GUI)

Step 1  Choose Wireless > Access Points > All APs to open the All APs page.
Step 2  Click the name of the access point for which you want to enable Telnet or SSH.
Step 3  Choose the Advanced tab to open the All APs > Details for (Advanced) page.
Troubleshooting Access Points Using Telnet or SSH

Step 4  Select the **Telnet** check box to enable Telnet connectivity on this access point. The default value is unchecked.

Step 5  Select the **SSH** check box to enable SSH connectivity on this access point. The default value is unchecked.

Step 6  Click **Apply** to commit your changes.

Step 7  Click **Save Configuration** to save your changes.

**Troubleshooting Access Points Using Telnet or SSH (CLI)**

Step 1  To enable Telnet or SSH connectivity on an access point, enter this command:

```
config ap {telnet | ssh} enable Cisco_AP
```

The default value is disabled.

**Note** To disable Telnet or SSH connectivity on an access point, enter the `config ap {telnet | ssh} disable Cisco_AP` command.

Step 2  To save your changes, enter this command:

```
save config
```

Step 3  To see whether Telnet or SSH is enabled on an access point, enter this command:

```
show ap config general Cisco_AP
```

Information similar to the following appears:

```
Cisco AP Identifier......................... 5
Cisco AP Name................................ AP33
Country code................................ Multiple Countries:US,AE,AR,AT,AU,BH
```
Reg. Domain allowed by Country................... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number................................. 2
MAC Address...................................... 00:19:2f:11:16:7a
IP Address Configuration.......................... Static IP assigned
IP Address....................................... 10.22.8.133
IP NetMask...................................... 255.255.248.0
Gateway IP Addr................................. 10.22.8.1
Domain........................................... 
Name Server...................................... 
Telnet State..................................... Enabled
Ssh State........................................ Enabled

Debugging the Access Point Monitor Service

This section contains the following topics:

- Information About Debugging the Access Point Monitor Service, page 18-52
- Debugging Access Point Monitor Service Issues (CLI), page 18-52

Information About Debugging the Access Point Monitor Service

The controller sends access point status information to the Cisco 3300 Series Mobility Services Engine (MSE) using the access point monitor service.

The MSE sends a service subscription and an access point monitor service request to get the status of all access points currently known to the controller. When any change is made in the status of an access point, a notification is sent to the MSE.

Debugging Access Point Monitor Service Issues (CLI)

If you experience any problems with the access point monitor service, enter this command:

```
dbg service ap-monitor {all | error | event | nmsp | packet} {enable | disable}
```

where

- **all** configures debugging of all access point status messages.
- **error** configures debugging of access point monitor error events.
- **event** configures debugging of access point monitor events.
- **nmsp** configures debugging of access point monitor NMSP events.
- **packet** configures debugging of access point monitor packets.
- **enable** enables the debug service ap-monitor mode.
- **disable** disables the debug service ap-monitor mode.
Troubleshooting OfficeExtend Access Points

This section contains the following topics:

- Information About Troubleshooting OfficeExtend Access Points, page 18-53
- Troubleshooting Common Problems, page 18-53

Information About Troubleshooting OfficeExtend Access Points

This section provides troubleshooting information if you experience any problems with your OfficeExtend access points.

Interpreting OfficeExtend LEDs

The LED patterns are different for 1130 series and 1140 series OfficeExtend access points. See the Cisco OfficeExtend Access Point Quick Start Guide for a description of the LED patterns. You can find this guide at this URL:


Positioning OfficeExtend Access Points for Optimal RF Coverage

When positioning your OfficeExtend access point, consider that its RF signals are emitted in a cone shape spreading outward from the LED side of the access point. Be sure to mount the access point so that air can flow behind the metal back plate and prevent the access point from overheating.

![Figure 18-16 OfficeExtend Access Point Radiation Patterns](image)

Troubleshooting Common Problems

Most of the problems experienced with OfficeExtend access points are one of the following:

- The access point cannot join the controller because of network or firewall issues.

  **Resolution:** Follow the instructions in the “Viewing Access Point Join Information (GUI)” section on page 9-40 to view join statistics for the OfficeExtend access point, or find the access point’s public IP address and perform pings of different packet sizes from inside the company.
• The access point joins but keeps dropping off. This behavior usually occurs because of network problems or when the network address translation (NAT) or firewall ports close because of short timeouts.
  **Resolution:** Ask the teleworker for the LED status.

• Clients cannot associate because of NAT issues.
  Resolution: Ask the teleworker to perform a speed test and a ping test. Some servers do not return big packet pings.

• Clients keep dropping data. This behavior usually occurs because the home router closes the port because of short timeouts.
  Resolution: Perform client troubleshooting in WCS to determine if the problem is related to the OfficeExtend access point or the client.

• The access point is not broadcasting the enterprise WLAN.
  **Resolution:** Ask the teleworker to check the cables, power supply, and LED status. If you still cannot identify the problem, ask the teleworker to try the following:
  - Connect to the home router directly and see if the PC is able to connect to an Internet website such as http://www.cisco.com/. If the PC cannot connect to the Internet, check the router or modem. If the PC can connect to the Internet, check the home router configuration to see if a firewall or MAC-based filter is enabled that is blocking the access point from reaching the Internet.
  - Log on to the home router and check to see if the access point has obtained an IP address. If it has, the access point’s LED normally blinks orange.

• The access point cannot join the controller, and you cannot identify the problem.
  **Resolution:** A problem could exist with the home router. Ask the teleworker to check the router manual and try the following:
  - Assign the access point a static IP address based on the access point’s MAC address.
  - Put the access point in a demilitarized zone (DMZ), which is a small network inserted as a neutral zone between a company’s private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.
  - If problems still occur, contact your company’s IT department for assistance.

• The teleworker experiences problems while configuring a personal SSID on the access point.
  **Resolution:** Clear the access point configuration and return it to the factory-default settings by clicking **Clear Config** on the access point GUI or by entering the **clear ap config** Cisco_AP command and then follow the steps in the “Configuring a Personal SSID on an OfficeExtend Access Point” section on page 9-67 to try again. If problems still occur, contact your company’s IT department for assistance.

• The home network needs to be rebooted.
  **Resolution:** Ask the teleworker to follow these steps:
  a. Leave all devices networked and connected, and then power down all the devices.
  b. Turn on the cable or DSL modem, and then wait for 2 minutes. (Check the LED status.)
  c. Turn on the home router, and then wait for 2 minutes. (Check the LED status.)
  d. Turn on the access point, and then wait for 5 minutes. (Check the LED status.)
  e. Turn on the client.
Troubleshooting Mesh Access Points

Mesh MAP Backhaul Deselection on Ethernet Backhaul at Runtime

When a mesh access point that joined the controller uses radio backhaul with the intent to use Ethernet as mesh backhaul, an inappropriate operation sequence could occur, when you enter the flapping mac-address.

Note

This troubleshooting tip is not applicable if Ethernet is not used for mesh AP backhaul.

To configure a mesh map Ethernet port (on the same subnet or VLAN of the Mesh RAP) as the mesh backhaul at runtime, follow these steps:

Step 1  Choose Configure > Access Points > All APs > select the AP name, click on Reset AP Now to reset mesh AP.

Step 2  Connect the Ethernet cable between the switch and the mesh AP.