



## APPENDIX **D**

# 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, page D-2](#)
- [System Messages, page D-2](#)
- [Using the CLI to Troubleshoot Problems, page D-5](#)
- [Configuring the Syslog Facility and Log Level, page D-7](#)
- [Uploading Core Dumps from the Controller, page D-9](#)
- [Monitoring Memory Leaks, page D-10](#)
- [Troubleshooting CCXv5 Client Devices, page D-11](#)
- [Using the Debug Facility, page D-27](#)

# Interpreting LEDs

## Interpreting Controller LEDs

Refer to the quick start guide for your specific controller for a description of the LED patterns. You can find the guides at this URL:

<http://www.cisco.com/en/US/products/hw/wireless/index.html>

## Interpreting Lightweight Access Point LEDs

Refer to the hardware installation guide for your specific access point for a description of the LED patterns. You can find the guides at this URL:

<http://www.cisco.com/en/US/products/hw/wireless/index.html>

# System Messages

Table D-1 lists some common system messages and their descriptions. For a complete list of system messages, refer to the *Cisco Wireless LAN Controller System Message Guide, Release 4.2*.

**Table D-1** System Messages and Descriptions

Error Message	Description
apf_utils.c 680: Received a CIF field without the protected bit set from mobile xx:xx:xx:xx:xx:xx	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.
dtl_arp.c 480: Got an idle-timeout message from an unknown client xx:xx:xx:xx:xx:xx	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 normally 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.
STATION_DISASSOCIATE	Client may have intentionally terminated usage or may have experienced a service disruption.
STATION_DEAUTHENTICATE	Client may have intentionally terminated usage or it could indicate an authentication issue.
STATION_AUTHENTICATION_FAIL	Check disable, key mismatch or other configuration issues.

**Table D-1 System Messages and Descriptions (continued)**

<b>Error Message</b>	<b>Description</b>
STATION_ASSOCIATE_FAIL	Check load on the Cisco Radio or signal quality issues.
LRAD_ASSOCIATED	The associated Cisco 1000 Series lightweight access point is now managed by this Cisco Wireless LAN Controller.
LRAD_DISASSOCIATED	Cisco 1000 Series lightweight access point may have associated with a different Cisco Wireless LAN Controller or may have become completely unreachable.
LRAD_UP	Cisco 1000 Series lightweight access point is operational, no action required.
LRAD_DOWN	Cisco 1000 Series lightweight access point may have a problem or is administratively disabled.
LRADIF_UP	Cisco Radio is UP.
LRADIF_DOWN	Cisco Radio may have a problem or is administratively disabled.
LRADIF_LOAD_PROFILE_FAILED	Client density may have exceeded system capacity.
LRADIF_NOISE_PROFILE_FAILED	The non-802.11 noise has exceed configured threshold.
LRADIF_INTERFERENCE_PROFILE_FAILED	802.11 interference has exceeded threshold on channel -- check channel assignments.
LRADIF_COVERAGE_PROFILE_FAILED	Possible coverage hole detected - check Cisco 1000 Series lightweight access point history to see if common problem - add Cisco 1000 Series lightweight access points if necessary.
LRADIF_LOAD_PROFILE_PASSED	Load is now within threshold limits.
LRADIF_NOISE_PROFILE_PASSED	Detected noise is now less than threshold.
LRADIF_INTERFERENCE_PROFILE_PASSED	Detected interference is now less than threshold.
LRADIF_COVERAGE_PROFILE_PASSED	Number of clients receiving poor signal are within threshold.
LRADIF_CURRENT_TXPOWER_CHANGED	Informational message.
LRADIF_CURRENT_CHANNEL_CHANGED	Informational message.
LRADIF_RTS_THRESHOLD_CHANGED	Informational message.
LRADIF_ED_THRESHOLD_CHANGED	Informational message.
LRADIF_FRAGMENTATION_THRESHOLD_CHANGED	Informational message.
RRM_DOT11_A_GROUPING_DONE	Informational message.
RRM_DOT11_B_GROUPING_DONE	Informational message.
ROGUE_AP_DETECTED	May be a security issue. Use maps and trends to investigate.

**Table D-1 System Messages and Descriptions (continued)**

Error Message	Description
ROGUE_AP_REMOVED	Detected rogue access point has timed out. The unit might have shut down or moved out of the coverage area.
AP_MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
LINK_UP	Positive confirmation message.
LINK_DOWN	Port may have a problem or is administratively disabled.
LINK_FAILURE	Port may have a problem or is administratively disabled.
AUTHENTICATION_FAILURE	Attempted security breach. Investigate.
STP_NEWROOT	Informational message.
STP_TOPOLOGY_CHANGE	Informational message.
IPSEC_ESP_AUTH_FAILURE	Check WLAN IPsec configuration.
IPSEC_ESP_REPLAY_FAILURE	Check for attempt to spoof IP Address.
IPSEC_ESP_POLICY_FAILURE	Check for IPsec configuration mismatch between WLAN and client.
IPSEC_ESP_INVALID_SPI	Informational message.
IPSEC_OTHER_POLICY_FAILURE	Check for IPsec configuration mismatch between WLAN and client.
IPSEC_IKE_NEG_FAILURE	Check for IPsec IKE configuration mismatch between WLAN and client.
IPSEC_SUITE_NEG_FAILURE	Check for IPsec IKE configuration mismatch between WLAN and client.
IPSEC_INVALID_COOKIE	Informational message.
RADIOS_EXCEEDED	Maximum number of supported Cisco Radios exceeded. Check for controller failure in the same Layer 2 network or add another controller.
SENSED_TEMPERATURE_HIGH	Check fan, air conditioning and/or other cooling arrangements.
SENSED_TEMPERATURE_LOW	Check room temperature and/or other reasons for low temperature.
TEMPERATURE_SENSOR_FAILURE	Replace temperature sensor ASAP.
TEMPERATURE_SENSOR_CLEAR	Temperature sensor is operational.
POE_CONTROLLER_FAILURE	Check ports — possible serious failure detected.
MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
SWITCH_UP	Controller is responding to SNMP polls.
SWITCH_DOWN	Controller is not responding to SNMP polls, check controller and SNMP settings.

**Table D-1 System Messages and Descriptions (continued)**

Error Message	Description
RADIUS_SERVERS_FAILED	Check network connectivity between RADIUS and the controller.
CONFIG_SAVED	Running configuration has been saved to flash - will be active after reboot.
MULTIPLE_USERS	Another user with the same username has logged in.
FAN_FAILURE	Monitor Cisco Wireless LAN Controller temperature to avoid overheating.
POWER_SUPPLY_CHANGE	Check for power-supply malfunction.
COLD_START	Cisco Wireless LAN Controller may have been rebooted.
WARM_START	Cisco Wireless LAN Controller may have been rebooted.

## 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:

Name	Priority	CPU Use	Reaper
reaperWatcher	( 3/124)	0 %	( 0/ 0)% I
osapiReaper	(10/121)	0 %	( 0/ 0)% I
TempStatus	(255/ 1)	0 %	( 0/ 0)% I
emWeb	(255/ 1)	0 %	( 0/ 0)% T 300
cliWebTask	(255/ 1)	0 %	( 0/ 0)% I
UtilTask	(255/ 1)	0 %	( 0/ 0)% T 300

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:

Name	Priority	BytesInUse	BlocksInUse	Reaper
reaperWatcher	( 3/124)	0	0	( 0/ 0)% I
osapiReaper	(10/121)	0	0	( 0/ 0)% I
TempStatus	(255/ 1)	308	1	( 0/ 0)% I
emWeb	(255/ 1)	294440	4910	( 0/ 0)% T 300
cliWebTask	(255/ 1)	738	2	( 0/ 0)% I
UtilTask	(255/ 1)	308	1	( 0/ 0)% T 300

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 an array of information related to the state of the system, including the current configuration, last crash file, CPU utilization, and memory utilization.
4. **show running-config**—Shows the full current configuration of the controller. Access point configuration settings are not included. This command shows only values configured by the user. It does not show system-configured default values. This command is different from the **show run-config** command, which outputs a portion of the current configuration plus a lot of extra dynamic information. In contrast, the **show running-config** command provides a clean configuration output of the controller in command format.

Here is a brief sample of the output:

```
radius auth add 1 10.50.3.104 1812 ascii ****

radius backward compatibility enable

radius admin-authentication disable

radius cred-cache enable

radius callStationIdType macAddr

radius acct retransmit-timeout 1 4

radius acct network 1 disable

radius auth rfc3576 enable 1

radius auth retransmit-timeout 1 6
```

```
radius auth network 1 disable  
radius auth management 1 disable  
radius auth ipsec enable
```



**Note** If you want to see the passwords in clear text, enter **config passwd-cleartext enable**. 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.



**Note** You cannot use TFTP to upload the output of this command. Rather, you can cut and paste the output as necessary.

## Configuring the Syslog Facility and Log Level

This section provides instructions for configuring the syslog facility and the log level. Follow these steps to perform the configuration using the controller CLI.

**Step 1** To configure a remote host for sending syslog messages, enter this command:

```
config logging syslog host host_IP_address
```



**Note** To remove a remote host that was configured for sending syslog messages, enter this command:  
**config logging syslog host** *host\_IP\_address* **delete**

**Step 2** To set the facility for outgoing syslog messages to the remote host, 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 3** To set the severity level for filtering syslog messages to the remote host, enter this command:

```
config 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 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 remote syslog host. For example, if you set the syslog level to 4, only those messages whose severity is between 0 and 4 are sent to the remote syslog host.

---

**Step 4** To save your changes, enter this command:

```
save config
```

**Step 5** To see the logging parameters and buffer contents, enter this command:

**show logging**

Information similar to the following appears:

```

Logging to buffer :
- Logging filter level..... errors
- Number of lines logged..... 51747
- Number of lines dropped..... 419704
Logging to console :
- Logging filter level..... errors
- Number of lines logged..... 0
- Number of lines dropped..... 471451
Logging to syslog :
- Logging filter level..... alerts
- Syslog facility..... syslog
- Number of lines logged..... 51737
- Number of lines dropped..... 419714
- Number of remote syslog hosts..... 0
  - Host 0..... Not Configured
Logging of traceback..... Enabled
- Traceback logging level..... errors
Logging of process information..... Enabled
Logging of source file informational..... Enabled
Timestamping of messages..... Enabled
- Timestamp format..... Date and Time
...

```

## 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. This section provides instructions to do so using the controller CLI.

### Using the CLI to Upload Controller Core Dumps

Using the controller CLI, follow these steps to enable the controller to automatically upload a core dump file of the controller.

**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, and



**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**
- 

## 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).

---

Using the controller CLI, follow these steps to monitor the controller for memory leaks.

---

- 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.
- 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 KB):  
**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 KB, 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 KB.
- Step 3** To save your changes, enter this command:  
**save config**

**Step 4** To view 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 5** To view 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(0xabcd),poison(0xreadceef),
entrysize(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 179a7afc 00000001
(179a7b00): 00000003 00000006 00000001 00000004 00000001 00000009 00000009 0000020d
(179a7b20): 00000001 00000002 00000002 00000001 00000004 00000000 00000000 5d7b9aba
(179a7b40): cbddf004 192f465e 7791acc8 e5032242 5365788c alb7cee6 00000000 00000000
(179a7b60): 00000000 00000000 00000000 00000000 00000000 ceeff00d readf00d 00000080
(179a7b80): 00000000 00000000 17958dc0 00000000 1175608c 00000078 00000000 readceef
(179a7ba0): 179a7ba4 00000001 00000003 00000006 00000001 00000004 00000001 00003763
(179a7bc0): 00000002 00000002 00000010 00000001 00000002 00000000 0000001e 00000013
(179a7be0): 0000001a 00000089 00000000 00000000 000000d8 00000000 00000000 17222194
(179a7c00): 1722246c 1722246c 00000000 00000000 00000000 00000000 00000000 ceeff00d
(179a7c20): readf00d 00000080 00000000 00000000 179a7b78 00000000 1175608c 00000078
```

**Step 6** 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

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 6-35 for more information on CCX.



**Note**

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.

## 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**

---

Cisco recommends that you enable the diagnostic channel feature only for non-anchored SSIDs that use the management interface.

---

## 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.

## 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.

## Using the GUI to Configure the Diagnostic Channel

Follow these steps to configure the diagnostic channel using the controller GUI.

**Step 1** Click **WLANs** to open the WLANs page.

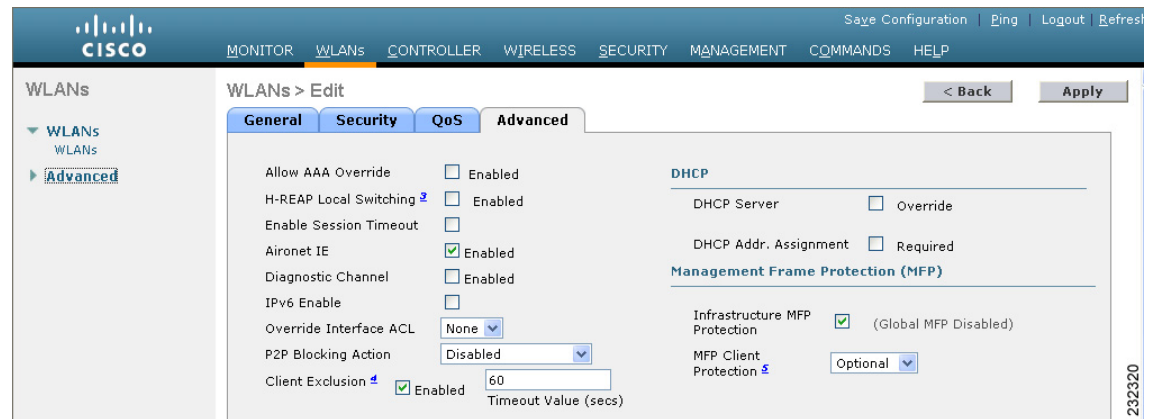
**Step 2** Create a new WLAN or click the profile name of an existing WLAN.



**Note** Cisco recommends that you create a new WLAN on which to run the diagnostic tests.

**Step 3** When the WLANs > Edit page appears, click the **Advanced** tab to open the WLANs > Edit (Advanced) page (see [Figure D-1](#)).

**Figure D-1** WLANs > Edit (Advanced) Page



**Step 4** If you want to enable diagnostic channel troubleshooting on this WLAN, check the **Diagnostic Channel** check box. Otherwise, leave this check box unchecked, which is the default value.



**Note** You can use the CLI to initiate diagnostic tests on the client. See the [“Using the CLI to Configure the Diagnostic Channel”](#) section on page D-14 for details.

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

**Step 6** Click **Save Configuration** to save your changes.

## Using the CLI to Configure the Diagnostic Channel

Using the controller CLI, follow these steps to configure the diagnostic channel.

**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..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Enabled
...
```

**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 host name, 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. Note however that 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.

- 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 l.....
00000040: 03 19 00 41 50 32 33 2d 31 30 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 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
Last Frame Number:..... 1120
Direction:..... 1
Timestamp:..... 0d 00h 50m 39s 878289us
Frame Length:..... 147
Frame Data:
00000000: 80 00 00 00 ff ff ff ff ff ff 00 0d ed c3 a0 22 .....".MP..x...
00000010: 00 0d ed c3 a0 22 00 bd 4d 50 a5 f7 78 08 00 00 .....".MP..x...
00000020: 64 00 01 00 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 84 00 0f 00 ff l.....
00000040: 03 19 00 72 6f 67 75 65 2d 74 65 73 74 31 00 00 ...rogue-test1..
00000050: 00 00 00 00 00 00 23 96 06 00 40 96 00 10 00 dd .....#...@.....
00000060: 06 00 40 96 01 01 00 dd 05 00 40 96 03 04 dd 05 ..@.....@.....
00000070: 00 40 96 0b 01 dd 18 00 50 f2 02 01 01 81 00 03 .@.....P.....

00000080: a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f 00 d2 ...'.BC^.b2/...
00000090: b4 ab 84 ...
```

LOG Frames:

```
Frame Number:..... 3
Last Frame Number:..... 1120
Direction:..... 1
Timestamp:..... 0d 00h 50m 39s 881513us
Frame Length:..... 189
```

```

Frame Data:
00000000: 80 00 00 00 ff ff ff ff ff ff 00 12 44 bd 80 30 .....D..0
00000010: 00 12 44 bd 80 30 60 f7 46 c0 8b 4b d1 05 00 00 ..D..0`.F..K...
00000020: 64 00 11 08 00 01 00 01 08 8c 12 98 24 b0 48 60 d.....$.H`
00000030: 6c 05 04 00 02 00 00 85 1e 00 00 89 00 0f 00 ff l.....
00000040: 03 19 00 41 50 34 30 2d 31 37 00 00 00 00 00 00 ...AP40-17.....
00000050: 00 00 00 00 00 00 26 dd 18 00 50 f2 01 01 00 00 .....&...P....
00000060: 50 f2 05 01 00 00 50 f2 05 01 00 00 40 96 00 28 P....P....@... (
00000070: 00 dd 06 00 40 96 01 01 00 dd 05 00 40 96 03 04 ....@.....@...

00000080: dd 16 00 40 96 04 00 05 07 a4 00 00 23 a4 00 00 ...@.....#...
00000090: 42 43 00 00 62 32 00 00 dd 05 00 40 96 0b 01 dd BC..b2.....@....
000000a0: 18 00 50 f2 02 01 01 85 00 03 a4 00 00 27 a4 00 ..P.....'...
000000b0: 00 42 43 5e 00 62 32 2f 00 0b 9a 1d 6f          .BC^.b2/.....o
...

```

---

## Using the GUI to Configure Client Reporting

Follow these steps to configure client reporting using the controller GUI.

- 
- Step 1** Click **Monitor > Clients** to open the Clients page.
  - Step 2** Click the MAC address of the desired client. The Clients > Detail page appears (see [Figure D-2](#)).

Figure D-2 Clients &gt; Detail Page

The screenshot displays the Cisco Wireless LAN Controller configuration page for a client. The page is titled "Clients > Detail" and includes a navigation menu on the left with options like Summary, Access Points, Statistics, CDP, Rogues, Clients, and Multicast. The main content area is divided into several sections:

- Client Properties:** A table listing client details such as MAC Address (00:40:96:a7:5d:55), IP Address (192.168.175.190), Client Type (Regular), User Name, Port Number (1), Interface (management), VLAN ID (0), CCX Version (CCXv5), E2E Version (Not Supported), Mobility Role (Local), Mobility Peer IP Address (N/A), Policy Manager State (RUN), Mirror Mode (Disable), and Management Frame Protection (No).
- AP Properties:** A table listing access point details such as AP Address (00:0b:85:62:65:90), AP Name (ap:62:65:90), AP Type (802.11a), WLAN Profile (ssid1), Status (Associated), Association ID (1), 802.11 Authentication (Open System), Reason Code (0), Status Code (0), CF Pollable (Not Implemented), CF Poll Request (Not Implemented), Short Preamble (Not Implemented), PBCC (Not Implemented), Channel Agility (Not Implemented), Timeout (0), and WEP State (WEP Disable).
- Security Information:** A table listing security-related details such as Security Policy Completed (Yes), Policy Type (N/A), Encryption Cipher (None), and EAP Type (N/A).
- Quality of Service Properties:** A table listing QoS-related details such as WMM State (Enabled), U-APSD Support (Disabled), QoS Level (Silver), Diff Serv Code Point (DSCP) (disabled), 802.1p Tag (disabled), Average Data Rate (disabled), Average Real-Time Rate (disabled), Burst Data Rate (disabled), and Burst Real-Time Rate (disabled).
- Client Statistics:** A table listing client performance statistics such as Bytes Received (641114), Bytes Sent (13583884), Packets Received (9910), Packets Sent (9136), Policy Errors (0), RSSI (-51), SNR (53), Sample Time (Thu Aug 30 11:14:54 2007), Excessive Retries (0), Retries (0), Success Count (0), Fail Count (0), and Tx Filtered (0).

At the top right of the page, there are buttons for "Save Configuration", "Ping", "Logout", and "Refresh". Below the "Clients > Detail" header, there are buttons for "< Back", "Apply", "Link Test", "Remove", "Send CCXv5 Req", and "Display".

**Step 3** To send a report request to the client, click the **CCXv5 Req** button.

**Step 4** To view the parameters from the client, click **Display**. The Client Reporting page appears (see [Figure D-3](#)).

212216



Figure D-4 Profile Details Page

The screenshot displays the 'Profile Details' page in the Cisco Wireless LAN Controller interface. The page is titled 'Profile Details' and includes a '< Back' button. The configuration is for a profile named 'ssid1'. The 'Radio Channels' are set to 1 through 11. The 'Data Rates (Mbps)' are configured for two radio types: DSSS with a rate list of 1.0 and 2.0, and HRDSSS(802.11b). Under '802.11 Security Settings', all fields (Authentication, EAP Method, Key Management, Encryption) are set to 'None'. The 'Radio Options' section shows a table with columns for Radio Type, Preamble, CCA Method, and Data, with values for Retries, Fragment Threshold, Short preamble, and Energy Detect + Carrier. The 'Preferred APs' and 'Proprietary Options' sections are also visible, with 'Tx Powers (dBm)' set to DSSS and Automatic.

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

## Using the CLI to Configure Client Reporting

Using the controller CLI, follow these steps to configure client reporting.

- 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)

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:
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:b2:8d: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:5.5 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ..... Rate:11.0 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

```

## Using the CLI to Configure Roaming and Real-Time Diagnostics

Using the controller CLI, follow these steps to configure roaming and real-time diagnostics.

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

**config 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:

**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
Event Timestamp=0d 00h 00m 19s 882921us
Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,
Transition Time=3234(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:c2, Target BSSID=00:0b:85:81:06:d2,
Transition Time=3281(ms)
Transition Reason: First association to WLAN
Transition Result: Success
Event Timestamp=0d 00h 00m 26s 637084us
Source BSSID=00:0b:85:81:06:d2, Target BSSID=00:0b:85:81:06:c2,
Transition Time=3313(ms)
```

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
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 01s 624375us
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
```

Information similar to the following appears for a log response with a *log\_type* of syslog:

```
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
Event Timestamp=0d 00h 19m 42s 278987us
Client SysLog = '<11> Jun 19 11:49:47 uraval3777 Mandatory
elements missing in the OID response'
Event Timestamp=0d 00h 19m 42s 278990us
Client SysLog = '<11> Jun 19 11:49:50 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
Event Timestamp=0d 00h 19m 42s 278993us
Client SysLog = '<11> Jun 19 11:49:53 uraval3777 Mandatory
elements missing in the OID response'
Event Timestamp=0d 00h 19m 42s 278996us
Client SysLog = '<11> Jun 19 11:49:56 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
Event Timestamp=0d 00h 19m 42s 279000us
Client SysLog = '<11> Jun 19 11:50:00 uraval3777 Mandatory
elements missing in the OID response'
Event Timestamp=0d 00h 19m 42s 279003us
Client SysLog = '<11> Jun 19 11:50:03 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
Event Timestamp=0d 00h 19m 42s 279009us
Client SysLog = '<11> Jun 19 11:50:09 uraval3777 Mandatory
elements missing in the OID response'
Event Timestamp=0d 00h 19m 42s 279012us
Client SysLog = '<11> Jun 19 11:50:12 uraval3777 Mandatory
elements missing in the OID response'
```

**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
dot11RTSSuccessCount                = 7
dot11RTSFailureCount                = 8
dot11ACKFailureCount                = 9
```

```
dot11ReceivedFragmentCount      = 10
dot11MulticastReceivedFrameCount = 11
dot11FCSErrorCount              = 12
dot11TransmittedFrameCount      = 13
```

---

## 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
  - Ethernet type
  - VLAN ID
- EoIP payload IP header ACL
  - Source address
  - Destination address
  - Protocol
  - Source port (if applicable)
  - Destination port (if applicable)

- LWAPP payload 802.11 header ACL
  - Destination address
  - Source address
  - BSSID
  - SNAP header type
- LWAPP 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.

Follow these steps to use the debug facility.

---

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

**debug 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 this command: **debug packet logging disable**.

---

**Step 2** Use these commands to configure packet-logging ACLs:

- **debug packet logging acl driver** *rule\_index action npu\_encap port*

where

- *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, rbc, 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, xtp, ddp, idpr-cmtp, rspf, vmtp, 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-tsmux, rtelnet, pop-2, pop-3, sunrpc, auth, sftp, uucp-path, nntp, ntp, netbios-ns, netbios-dgm, netbios-ssn, imap2, snmp, snmp-trap, cmip-man, cmip-agent, xdmcp, nextstep, bgp, prospero, irc, smux, at-rtmp, at-nbp, at-echo, at-zis, qmtp, z3950, ipx, imap3, ulistserv, https, snpp, saft, npmp-local, npmp-gui, and hmmp-ind.
- *dst\_port* is the UDP/TCP two-byte destination port (for example, telnet, 23) or “any.” The controller accepts 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 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 this command: **debug packet logging acl clear-all**.

**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 D-5](#) shows an example of hex2pcap output, and [Figure D-6](#) shows an example of text2pcap output.

**Figure D-5** Sample Hex2pcap Output

```

tx len=118, encap=n/a, port=1
[0000]: 000C316E 7F80000B 854008c0 08004500 ..ln....@.@..E.
[0010]: 00680000 40004001 5FBE0164 6C0E0164 .h..@.@.>.dl..d
[0020]: 6C010800 08D9E500 00000000 00000000 l....Ye.....
[0030]: 00000000 00000000 00000000 00001C1D .....
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789;.<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                                NOPQRS
rx len=118, encap=ip, port=1
[0000]: 000B8540 08C0000C 316E7F80 08004500 ...@.@..ln....E.
[0010]: 00680000 4000FF01 A0BD0164 6C010164 .h..@....=.dl..d
[0020]: 6C0E0000 10D9E500 00000000 00000000 l....Ye.....
[0030]: 00000000 00000000 00000000 00001C1D .....
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789;.<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                                NOPQRS

```

212235

**Figure D-6** Sample Text2pcap Output

```

tx len=118, encap=n/a, port=1
0000 00 0C 31 6E 7F 80 00 0B 85 40 08 c0 08 00 45 00 ..ln....@.@..E.
0010 00 68 00 00 40 00 40 01 5F BE 01 64 6C 0E 01 64 .h..@.@.>.dl..d
0020 6C 01 08 00 08 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789;.<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                                NOPQRS
rx len=118, encap=ip, port=1
0000 00 0B 85 40 08 C0 00 0C 31 6E 7F 80 08 00 45 00 ...@.@..ln....E.
0010 00 68 00 00 40 00 FF 01 A0 BD 01 64 6C 01 01 64 .h..@....=.dl..d
0020 6C 0E 00 00 10 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789;.<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                                NOPQRS

```

232343

**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
```

