



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](#)

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 system messages and descriptions.

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.
STATION_ASSOCIATE_FAIL	Check load on the Cisco Radio or signal quality issues.

Table D-1 System Messages and Descriptions (continued)

Error Message	Description
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 password-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.
