



Troubleshooting a Mesh Network

Last Revised: March 2008

This document addresses problems that can arise in a mesh network operating with Cisco 1500 (1505, 1510) and 1520 (1522, 1524) series mesh access points and a Cisco Wireless LAN Controller operating with Cisco Unified Wireless Software (CUWN) releases 4.1.19x. Suggested solutions to those problems are also provided.

The following troubleshooting issues are addressed and listed in the order in which they should be diagnosed:

- [Power Fluctuations, page 2](#)
- [Radio Frequency \(RF\) Problems and Fluctuations, page 4](#)
- [LWAPP Discovery Request Never Sent by Access Point, page 9](#)
- [LWAPP Join Failures, page 13](#)
- [LWAPP Up, Cannot Ping Access Points, page 16](#)
- [LWAPP Failure Debugging, page 20](#)
- [Performance Notes, page 22](#)



Note

- Refer to the *Cisco Wireless Control System Configuration Guide* for details on accessing and reviewing SNMP trap logs and message logs (msglogs) mentioned in this section. The latest versions are found at the following link:
http://www.cisco.com/en/US/products/ps6305/tsd_products_support_series_home.html.
- Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 4.2* for details on accessing and reviewing logs using the controller GUI or CLI. The latest versions are found at the following link:
http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html
- Refer to the Release Notes for mesh networks, versions 4.1.90.5, 4.1.191.24M and 4.1.192.17M for detailed feature description, release compatibility and upgrade information at the following link:
http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Power Fluctuations

This section addresses possible AC and Power over Ethernet (PoE) power problems or anomalies with a mesh access point.

AC Power Problems

Table 1 AC Power Fluctuations

Possible cause	Solution/Debug steps
<p>Not enough power.</p> <p>Note Intermittent power availability, low AP uptime and AP resets are all indicators of inadequate power availability.</p>	<p>1) Verify that the PoE port on the switch or router is disabled by checking the PoE LED. If the LED is on continuously or fluttering, disable PoE on the port.</p> <p>Note Cisco mesh access points (1500 series) are not compliant with 802.3af, which allows an access point to take power from a switch or router. PoE must always be disabled on the switch or router associated with the AP.</p> <p>2) Check voltage level.</p> <p>3) Verify that streetlight “bank switching” is not in use where the access point is installed.</p> <p>4) Check for variations in power during the day and at night.</p> <p>5) Connect the detachable LED indicator to the access point to verify that power is present (LED on = power)</p> <p>6) Verify that the Ethernet port LED is active for the port that connects to the access point.</p> <p>7) If the unit you are troubleshooting is a 1520 series access point then check the power failure trap.</p>

PoE Problems

Table 2 PoE Power Fluctuations

Possible cause	Solution/Debug steps
Power injector is not providing power.	<p>1) Verify that the PoE port on the switch or router is disabled by checking the PoE LED. If the LED is continuous or fluttering, disable PoE on the port.</p> <p>Note Cisco mesh access points (1500 series) are not compliant with 802.3af, which allows an access point to take power from a switch or router. PoE must always be disabled on the switch or router associated with the AP and a Cisco external power injector must be present.</p> <p>2) Verify that the LED of the power injector is on.</p> <p>3) Verify that the physical input and output cable connections of the PoE injector are correct.</p> <p>Note The PoE injector <i>input</i> port should be connected to the network switch or router port. The PoE injector <i>output</i> port should be connected to the Ethernet port of the access point.</p> <p>4) Connect an Ethernet sniffer with an Ethernet hub to ensure packets are transmitting from a 1510 or 1505. If the mesh access point is an 1522 or 1524, then check the power LED on the access point first.</p> <p>5) Verify that the total distance between the network device, the power injector and the access point meet the 802.3 specification.</p> <p>Distance between power injector, and the AP should be no more than 328 ft.</p> <ul style="list-style-type: none">- Switch to injector (max 128 ft)- Injector to AP (max 200 ft)

Radio Frequency (RF) Problems and Fluctuations

This section addresses problems with radio transmission in the mesh network that might cause a wireless link to not establish, to go down or be available intermittently.

Details on how to diagnose the problem both remotely and locally are summarized in the table below.

Table 3 **RF Problems and Fluctuations**

Possible cause	Solution/Debug steps
<i>High-level, remote diagnostics</i>	
No neighbors found.	<ol style="list-style-type: none">1) Check the access point antenna.2) Check to see if the AP power is ON using the detachable LED indicator.3) Verify that the path to the AP is not obstructed by metal poles.
No valid parents found.	<ol style="list-style-type: none">1) Check for RF asymmetric behavior.2) Check for local interference.3) Install APs as far from transformers as possible.

Table 3 **RF Problems and Fluctuations (continued)**

Possible cause	Solution/Debug steps
<p>Insufficient Signal to Noise (SNR) values to keep the link up.</p>	<p>1) Conduct a link test on the problem link:</p> <p>In Cisco WCS, conduct the link test in both directions: parent-to-child and child-to-parent (Monitor > Maps > <i>Map Name</i> and mouse over the problem link in the map)</p> <p>2) In the controller GUI, run the AP-to-AP link test.</p> <p>Note If link test shows asymmetric values between the two different directional link tests, there might be problems with the link at one end. Check the RF cables at each end, if applicable; and, in Cisco WCS, run a Busiest APs Report to view utilization (Path: Reports > Performance Reports > <i>Busiest APs Report</i>).</p> <p>3) Run the Worst SNR Report in Cisco WCS (Reports > Mesh Reports > <i>Mesh Worst SNR Links</i>).</p> <p>4) Run a throughput test (lperf) on the link for 24 hours to determine link robustness and vitality.</p> <p>5) Check the AP max retransmissions value in the trap logs.</p> <p>6) Recheck distances between access points</p> <ul style="list-style-type: none"> • MAP deployment cannot exceed 35 feet in height above the street. • Typical 5 GHz RAP-to-MAP distances are 1000–4000 feet. • Typical 5 GHz MAP-to-MAP distances are 500–1000 feet. • Typical 2.4 GHz MAP-to-client distances are 300–500 feet. <p>7) Look for obstructions (trees, buildings, etc.) in the path between the two access points.</p> <p>8) Find the AP by entering show mesh neigh details to determine the time the lost AP was <i>last heard</i> from a known good AP neighbor.</p> <p>9) Enable the secondary backhaul feature (1510s only) to provide a temporary, alternate path to address interference issues on the primary backhaul. For configuration details see the “Routing Around Interference” section in Chapter 7 of the <i>Cisco Wireless LAN Controller Configuration Guide, 4.1</i>.</p>

Table 3 **RF Problems and Fluctuations (continued)**

Possible cause	Solution/Debug steps
SNR is greater than 60 dBm or APs are too close together.	<p>1) Check distances between APs and their antennas.</p> <p>Note Verify that the distance between APs (within the US) is 40 ft or greater when OMNI directional antennas are attached (ETSI => 10 ft) to reduce high packet error rate (PER) and prevent possible hardware problems.</p>
High packet error rate (PER).	<p>1) In Cisco WCS, run the Mesh Packet Error Rate Report (Reports > Mesh Reports > <i>Mesh Packet Error Stats</i>).</p> <p>2) Run a link test from the controller or WCS.</p> <ul style="list-style-type: none"> - If good SNR but high PER, then check for interference. <p>3) Verify load in the network.</p> <p>4) Check distances between APs and their antenna placement.</p> <p>Note Verify that the distance between APs (within the US) is 40 ft. or greater when OMNI directional antennas are attached (ETSI => 10 ft.) to reduce high PER and prevent possible hardware problems.</p>
Traffic load is too heavy on a link.	<p>1) Verify the SNMP traps for queue overflows and verify reported overflows using an Ethereal sniffer.</p> <ul style="list-style-type: none"> - Bronze queue overflow indicates too much broadcast or multicast traffic on a link. - Gold and platinum queue overflows might affect AWPP and LWAPP operation. <p>2) Run channel utilization or throughput reports using WCS.</p> <p>3) Please ensure proper RF channel planning of RAPs to avoid co-channel interference.</p>

Table 3 **RF Problems and Fluctuations (continued)**

Possible cause	Solution/Debug steps
<i>Low-level, local diagnostics</i>	
Ineffective antenna.	1) Check that antenna is screwed in correctly and in all the way. 2) If antenna is in a vertical upward position, verify that the drain plug is inserted, if applicable. 3) If antenna is in a vertical downward position, verify that the drain plug is not inserted, if applicable. 4) Verify that the correct antenna is installed. Both the 2.4 and 5 GHz antennas use the same N-type connector and could accidentally be swapped.
Interference.	1) Use a wireless 802.11 sniffer to measure packets per second (PPS). See the throughput vs. utilization chart (Figure 1) in the “ Performance Notes ” section on page 22. 2) Move AP from its current location.
Radio is out of range of another network connected radio.	1) See if the radio path is obstructed by buildings, trees or other objects. 2) Verify that the radio is within the following suggested distances: <ul style="list-style-type: none"> • MAP deployment cannot exceed 35 ft in height above the street. • Typical 5 GHz RAP-to-MAP distances are 1000–4000 ft. • Typical 5 GHz MAP-to-MAP distances are 500–1000 ft. • Typical 2.4 GHz MAP-to-client distances are 300–500 ft. • RAP locations are typically towers or tall buildings. • MAP locations are typically short building tops or streetlights.

Table 3 **RF Problems and Fluctuations (continued)**

Possible cause	Solution/Debug steps
<p>Recommended data rate of 18 Mbps (1505 and 1510) or 24 Mbps (1522 and 1524) is not in use.</p> <p>Note The rate of 18 Mbps (24 Mbps for 1522 and 1524) is the optimal backhaul rate because it aligns with the maximum coverage of the wireless LAN portion of the client wireless LAN of the MAP; that is, the distance between MAPs using 18 Mbps backhaul should allow for seamless WLAN client coverage between the MAPs.</p> <p>A lower bit rate might allow a greater distance between APs, but there are likely to be gaps in the wireless LAN client coverage, and the capacity of the backhaul network is reduced.</p> <p>An increased bit rate for the backhaul network either requires more APs, or results in a reduced SNR between APs, limiting mesh reliability and interconnection.</p>	<p>1) Enter show config to see current rate or using the controller GUI, select Data Rate from the blue drop-down menu for a given AP on the following controller page (Wireless > All APs > <i>Cisco-AP</i> > Details)</p>
<p>Recommended number of backhaul hops is exceeded.</p> <p>Note Number of backhaul hops is limited to eight, but three to four hops are recommended to maintain sufficient backhaul throughput because each MAP uses the same radio for transmission and reception of backhaul traffic. This means that throughput is approximately halved over every hop. For example, the maximum throughput for an 18 Mbps backhaul is approximately 10 Mbps for the first hop, 5 Mbps for the second hop, and 2.5 Mbps for the third hop.</p>	<p>1) Run the Cisco WCS worst node hops report (Reports > Mesh Reports > <i>Mesh Worst Node Hops</i>)</p>
<p>Recommended latency is not met.</p>	<p>1) Ping each AP radio IP address. Reported ping route time (a round-trip value) should be less than 100 msec for clients; otherwise, they will look for another AP to associate with.</p> <p>Note Use the ping test link found in the WCS GUI.</p>
<p>Defective radio.</p>	<p>1) Contact technical support and request a Return Material Authorization (RMA).</p>

LWAPP Discovery Request Never Sent by Access Point

This section highlights conditions associated with unsuccessful LWAPP joins by the access point and no receipt of a discovery request at the controller.

To monitor the messages being exchanged between access points and the controller, enter the following command and monitor (or capture) the information for at least 15 minutes.

(Cisco Controller) > **debug lwapp events enable**

- The **debug lwapp events enable** display provides information to help troubleshoot all of the possible problems listed in [Table 4](#).
- If after monitoring the **debug lwapp events enable** display for 15 minutes and, neither the NO DISCOVER RESPONSE nor the NO JOIN REQUEST event appears, enter the following CLI commands on the controller if you see this:

spamMeshRadiusProcessResponse: AP Authorization Failure for <MAC Address>

- Enter **debug disable-all** to turn off the **debug lwapp events enable** command
- Enter **config wlan mac filtering enable wlan-id** to enable the MAC filter on the WLAN



Note The MAC filter is enabled by default in release 4.1.181 and later.

- Enter **config macfilter add mac-addr wlan-id** to add the access point's MAC address to the WLAN's MAC filter

Table 4 **LWAPP Discovery Request Never Sent by Access Point**


Possible cause	Solution/Debug steps
MAC filter is enabled and blocking.	<p>1) Enter the debug lwapp events enable command and monitor for 15 minutes.</p> <ul style="list-style-type: none"> • If after 15 minutes, neither the NO DISCOVER RESPONSE nor the NO JOIN REQUEST event appears, enter the following CLI commands on the controller if you see the following message display: spamMeshRadiusProcessResponse: AP Authorization Failure for <MAC address> <ul style="list-style-type: none"> – Enter debug disable-all to turn off the debug lwapp events enable command – Enter config wlan mac filtering enable wlan-id to enable the MAC filter on the WLAN <p> Note The MAC filter is enabled by default in release 4.1.181.0 and later.</p> <ul style="list-style-type: none"> – Enter config macfilter add mac-addr wlan-id to add the access point's MAC address to the WLAN's MAC filter.
A RAP has joined but MAPs have not.	<p>1) Configure at least one access point in the mesh network as a RAP.</p> <p>Note Default setting for all access points is as a MAP</p>
Incorrect VLAN configuration.	<p>1) Verify that the access point and its associated controller are on the same VLAN by pinging from various logical switch and subnet points.</p>
Incorrect access point authorization settings.	<p>1) Enter CLI commands show auth-list and show aaa to verify settings.</p>
EAP and 802.1x authentication failure.	<p>1) Verify status by entering the following CLI commands from the controller:</p> <p>debug mesh security all enable</p> <p>debug aaa all enable</p> <p>debug dot1x all enable</p>

Table 4 **LWAPP Discovery Request Never Sent by Access Point (continued)**

Possible cause	Solution/Debug steps
EAP and 802.1x authentication timeout.	<p>1) Verify status using the following CLI commands on the controller:</p> <p>show eap adv timers</p> <p>debug mesh security all enable</p> <p>debug aaa all enable</p> <p>debug dot1x all enable</p>
Parent changed in the middle of security verification.	<p>1) Verify status using the following CLI commands on the controller:</p> <p>debug mesh security all enable</p> <p>debug aaa all enable</p> <p>debug dot1x all enable</p> <p>In some cases, the following CLI command on the controller might also be useful:</p> <p>debug client <i>MAP-MAC-address</i></p> <p>Note If problems are identified in the command displays, then wait for convergence to complete (see Table 8)</p> <p> If none of these commands indicates any problems, look for RF or power problems.</p>
RAP has lost its Ethernet connection.	<p>1) Check the physical connection between the RAP and the Ethernet port on the switch or router.</p>
RAP occasionally connects as a MAP.	<p>1) Check the physical connection between the RAP and the Ethernet port on the switch or router.</p>

Table 4 **LWAPP Discovery Request Never Sent by Access Point (continued)**

Possible cause	Solution/Debug steps
<p>PoE from the switch or router is enabled.</p> <p>Note Connections are generally erratic or inconsistent.</p>	<p>1) Verify that the PoE port on the switch or router is disabled by checking the PoE LED or configuration with the CLI. If the LED is continuous or fluttering, disable PoE on the port.</p> <p>Note Cisco mesh access points (1500 series) are not compliant with 802.3af, which allows an access point to take power from a switch or router. PoE must always be disabled on the switch or router associated with the AP.</p> <p>Note Cisco external power injectors are mandatory for PoE configurations.</p> <p>2) Verify that the recommended distance (< = 128 ft) between the switch or router and the PoE injector is not exceeded.</p>
<p>Duplicate IP addresses on the access point.</p> <p>Note Connections are generally erratic or inconsistent.</p>	<p>1) Reconfigure the access point by removing the static IP address, if applicable.</p> <p>2) Have DHCP server assign the access point IP address.</p> <p>Note Ensure that the DHCP server is configured and accessible on the same subnet as the access point.</p>

LWAPP Join Failures

This section highlights conditions associated with receipt of Discovery Requests and the non-receipt of LWAPP Joins from the access point.

To monitor the messages being exchanged between APs and the controller, enter the following command and monitor (or capture) the information for at least 15 minutes.

(Cisco Controller) > **debug lwapp events enable**

- The **debug lwapp events enable** text display provides information to help troubleshoot all of the possible join problems listed in [Table 5](#).
- If after monitoring the **debug lwapp events enable** text display for 15 minutes and, neither the NO DISCOVER RESPONSE nor the NO JOIN REQUEST event is seen, enter the following CLI commands on the controller, if you see the following display:

spamMeshRadiusProcessResponse: AP Authorization Failure for <mac>

- Enter **debug disable-all** to turn off the **debug lwapp events enable** command.
- Enter **config wlan mac filtering enable wlan-id** to enable the MAC filter on the WLAN.



Note The MAC filter is enabled by default in release 4.1.181.0 and later.

- Enter **config macfilter add mac-addr wlan-id** to add the access point's MAC address to the WLAN's MAC filter.

Table 5 LWAPP Join Failures

Possible cause	Solution/Debug steps
Incorrect regulatory domain is configured on the access point.	1) Enter show country on the controller to view country setting. 2) Enter show msglog to view country setting. 3) Check label on access point for assigned country code. 4) Configure correct country code.
A RAP has joined but MAPs have not.	1) Configure at least one access point in the mesh network as a RAP. Note Default setting for all access points is as a MAP.

Table 5 **LWAPP Join Failures (continued)**


Possible cause	Solution/Debug steps
MAC filter is enabled and blocking.	<p>1) Verify that the MAC address was correctly entered into the MAC filter on the controller.</p> <p>Note To limit MAC address entry errors, you can cut and paste addresses from the debug LWAPP events CLI command display.</p> <p>2) Enter debug lwapp events enable and monitor for 15 minutes.</p> <ul style="list-style-type: none"> • If after 15 minutes, and neither the NO DISCOVER RESPONSE nor the NO JOIN REQUEST event displays, enter the following CLI commands on the controller if you see the following message display: <pre>spamMeshRadiusProcessResponse: AP Authorization Failure for <MAC address></pre> <ul style="list-style-type: none"> - Enter debug disable-all to turn off the debug lwapp events enable command. - Enter config wlan mac filtering enable wlan-id to enable the MAC filter on the wireless LAN. <p> Note The MAC filter is enabled by default in release 4.1.181.0 and later.</p> <ul style="list-style-type: none"> - Enter config macfilter add mac-addr wlan-id to add the access point's MAC address to the WLAN's MAC filter.

Table 5 **LWAPP Join Failures (continued)**

Possible cause	Solution/Debug steps
<p>APs are associating with the wrong controller</p> <p>Note Incorrect associations often occur when multiple controllers exist on the same subnet and if the AAA server is configured to allow all MAC addresses to associate.</p>	<p>1) Enter the MAC address of the AP into the MAC filter of all controllers on the subnet. After the access point associates with one of the controllers, define the selected controller as the primary controller.</p> <p>Note An access point attempts to associate with the first controller that provides a Discovery Response if it has not been previously connected to a controller or primed to a specific controller.</p> <p>[Primed = Assigned to a primary, secondary or tertiary controller.]</p> <p>See the quick start guides for the Cisco 1500 and 1520 series access points at the following URLs for details on priming a controller.</p> <p>http://www.cisco.com/en/US/docs/wireless/access_point/1500/quick/guide/ap1500qs.html</p> <p>http://www.cisco.com/en/US/docs/wireless/access_point/1520/quick/guide/ap1520qsg.html</p> <p>2) In the Controller GUI, verify that the Authorize APs against AAA option (Security > AAA > AP Policies) is disabled.</p> <p>Note When Authorize APs against AAA is enabled, it allows an AP to associate to a controller regardless of other settings (it overrides MAC filter settings).</p>
<p>DHCP server is not providing an IP address.</p>	<p>1) Verify that the DHCP is defined on the controller.</p> <p>2) Verify that Option 43 is configured on the DHCP server.</p> <p>Note See the <i>Cisco Aironet 1500 Series Outdoor Mesh Hardware Installation Guide</i> for details on configuring Option 43 at initial install at:</p> <p>http://www.cisco.com/en/US/docs/wireless/access_point/1500/installation/guide/1500_axg.html#wpxref62208</p>

Table 5 **LWAPP Join Failures (continued)**

Possible cause	Solution/Debug steps
ARP request is not successful. No resolved address was received and cached.	<ol style="list-style-type: none"> 1) Enter show route gateway summary to verify the gateway configuration and path. 2) Perform diagnostics on switch or router using ethereal tools to verify status of ARP requests.
A bridge group name (BGN) is configured for the RAP but not for MAPs.	<ol style="list-style-type: none"> 1) Assign a BGN to the MAP. <p>Note MAPs will only connect to a controller with a default BGN.</p>
A bridge group name mismatch exists between a RAP and a MAP.	<ol style="list-style-type: none"> 1) Reconfigure the MAP bridge group name to match the BGN of the appropriate RAP. <p>Note You have up to 30 minutes to make this adjustment before the RAP reboots.</p>
Controller has defaulted to the manufacturing time setting or is not set correctly causing the certification to fail.	<ol style="list-style-type: none"> 1) Set correct time on the controller by entering the following commands: <ul style="list-style-type: none"> config time manual <i>mm/dd/yy</i> config time timezone <i>delta-hours</i> (delta-hours = difference in current time in hours from the universal coordinated time) 2) Configure the NTP server.

LWAPP Up, Cannot Ping Access Points

This section highlights possible scenarios in which a mesh access point (MAP) cannot be pinged by a controller.

Table 6 **LWAPP Up, Cannot Ping Access Points**

Possible cause	Solution/Debug steps
An invalid configuration on the gateway router is causing a discrepancy in the source address and ARP for inbound traffic. For example, if a router port maps to both a default gateway router and a hot standby router (active or not), it results in a different gateway router source address being referenced for upstream and downstream traffic.	Use a sniffer to identify the source address and ARP activity on the first and subsequent hops in the mesh network. Make the required configuration changes on the default gateway.

Access Point Disappears

This section summarizes possible reasons why an access point might disappear from a mesh network.

- When an access point disappears, it is not viewable from the controller GUI or CLI 60 seconds after its disappearance.
- On Cisco WCS, the icon remains on the map display until the next polling period (default of 15 minutes) but is not available (greyed out). Limited historical information is available during this time.

Table 7 **Access Point Disappears**

Possible cause	Solution/Debug Steps
RAP admin status was disabled then re-enabled.	<p>1) Wait several minutes for MAPs to reassociate with the controller.</p> <p>Note MAPs ignore admin status enable and disable.</p>
Parent of access point has rebooted.	<p>1) Wait the approximate times specified in Table 8.</p>
Access point has excluded its parent.	<p>1) To check for parent exclusion, look for the <i>ciscoLwappMeshChildExcludedParent</i> SNMP trap and the following Cisco WCS message: “Parent AP being excluded by child AP due to failed authentication, AP current parent MAC address “{yy.yy.yy.yy.yy.yy},” previous parent MAC address “{xx.xx.xx.xx.xx.xx}.”</p>
Link is lost because of poor SNR or radio hardware failure.	<p>1) Check the node-to-node LinkSNR. See Table 9 for the minimum LinkSNR required by data rate to maintain a link. See Table 10 for supporting LinkSNR calculation details.</p> <p>The following diagnostic information is available:</p> <ul style="list-style-type: none"> • Controller CLI (show mesh path). • Controller GUI (Wireless > Access Points > All APs > AP Name > Neighbor Info (drop-down menu) > Link Test (drop-down menu option for parent and child APs). • Cisco WCS (Reports > Mesh Reports > Mesh Link Stats). <p>Note Refer to the “RF Issues and Fluctuations” troubleshooting section in this document for additional diagnostic steps.</p>

Table 7 **Access Point Disappears (continued)**

Possible cause	Solution/Debug Steps
802.11a (802.11b if a 1505) network is disabled on the RAP.	<p>1) Enable the 802.11a Network Status <i>or</i> 802.11b/g Network Status option on the controller GUI at the following page using the appropriate path:</p> <ul style="list-style-type: none"> • Wireless > 802.11a > Network (1510) • Wireless > 802.11b > Network (1505)
Access point is not staying up due to either a power problem or reboot.	<p>1) Enter the following CLI command:</p> <p style="text-align: center;">show ap config general <i>ap-name</i></p> <p>Check the status of the following parameters:</p> <ul style="list-style-type: none"> - AP Uptime - LWAPP uptime - Join Date and Time - Join Taken Time <p>2) If a poletop installation, verify if:</p> <ul style="list-style-type: none"> a) Power is bank-switched. b) Power is stable (using voltmeter or visibly checking light stability at night).
A bridge group name (BGN) is configured for the RAP but not for the MAPs.	<p>1) Assign a BGN to the MAP.</p> <p>Note MAPs connect only to a controller with a default BGN.</p>
AP is stranded.	<p>1) Use a spectrum analyzer to detect the presence of any local noise, interference or AP transmission.</p> <p>2) Physically connect the AP directly to the controller, if possible, to see if the AP joins.</p> <p>3) A ground-level installation of a local controller and AP prior to its permanent installation on a pole or tower is recommended to verify that the AP will join the controller.</p>
Image is being/has been upgraded.	See Table 8 .
Controller has rebooted.	See Table 8 .
RAP has rebooted.	See Table 8 .
MAP has rejoined.	See Table 8 .
MAP has changed its parents.	See Table 8 .

[Table 8](#) provides a summary of transitional events that can occur within a mesh network along with the approximate time required for an event to propagate from the RAP to lower level MAPs in the mesh network hierarchy (RAP, MAP1, MAP2, MAP3).

Table 8 *Approximate Convergence Times for Mesh Network Transitions*

Convergence Time (Mins.)¹				
Transition Event	RAP	MAP1	MAP2	MAP3
Image Upgrade	< 4	< 9	< 15	< 20
Controller reboot	< 1	< 3	< 5	< 7
RAP reboot	< 1	< 3	< 5	< 8
MAP rejoin	< 1	< 3	< 3	< 3
MAP changes parent (same channel)	–	< 4	–	–
MAP changes parent (different channel)	–	< 4	–	–

1. The convergence times are approximate for a specific transition event to occur as it propagates from the RAP outward to the lower tiers of the network (MAP1, MAP2, and MAP3). RAP is at the top of the mesh hierarchy. MAP1 nodes are children of the RAP; MAP2 nodes are the children of MAP1 nodes; and MAP3 nodes are the children of MAP2 nodes.

Table 9 *1500 Series Backhaul Data Rates and Minimum LinkSNR Requirements*

Data Rate	Minimum Required LinkSNR (dB)
36 Mbps	26
24 Mbps	22
18 Mbps	18
12 Mbps	16
9 Mbps	15
6 Mbps	14

- The required minimum LinkSNR is driven by the data rate and the following formula: Minimum SNR + fade margin. [Table 10](#) summarizes the calculation by data rate.
 - Minimum SNR refers to an ideal state of non-interference, non-noise and a system packet error rate (PER) of no more than 10%
 - Typical fade margin is approximately 9 to 10 dB
 - We do not recommend using data rates greater than 18 Mbps (24 Mbps for 1520 series) in municipal mesh deployments as the SNR requirements do not make the distances practical

Table 10 *Minimum Required LinkSNR Calculations by Data Rate*

Data Rate	Minimum SNR (dB) +	Fade Margin =	Minimum Required LinkSNR (dB)
6	5	9	14
9	6	9	15
12	7	9	16

Data Rate	Minimum SNR (dB) +	Fade Margin =	Minimum Required LinkSNR (dB)
18	9	9	18
24	13	9	22
36	17	9	26

LWAPP Failure Debugging

After an access point has connected to the controller over LWAPP, a logical connection is created. This logical connection may shut down for a variety of reasons. A number of the more typical events reported and behaviors associated with LWAPP failures are noted in the table below.

LWAPP connection failures are generally caused by something other than RF, but intermittent interference or poor link SNR can be the cause of these failures.

To find information for the following LWAPP failures, refer to either the Trap Logs or Msglogs on the controller:

- In the controller GUI, refer to the Trap Log (Management > SNMP > Trap Logs) for messages of the following type: “AP Interface: 0 (802.11a) Operation State {Up | Down}.”
- In the controller CLI, enter **show msglogs**. Refer to the associated LWAPP troubleshooting messages below for more guidance on debugging.

Table 11 **LWAPP Failure Debugging**

Problem	Solution/Debug Steps
Access point resets.	<ol style="list-style-type: none"> 1) Power or manual reset of the AP has occurred. 2) AP has not been connected to a controller for 30 minutes or longer and the AP will reboot automatically.
Configuration changes. Reason given: Did not get a join response. Note In LWAPP there is a LWAPP join reply message for every join request. If the AP does not receive a join reply message, the LWAPP does not form and the above error message is reported.	Problem is mostly likely caused by poor SNR between APs or packet lost in the airwaves. <ol style="list-style-type: none"> 1) Run a link test between the two APs from the controller or WCS. 2) In Cisco WCS, run the Mesh Packet Error Rate Report (Path: Reports > Mesh Reports > <i>Mesh Packet Error Stats</i>). <ul style="list-style-type: none"> – If SNR is good but there is a high PER, then check for interference. 3) Verify load in the network.

Table 11 **LWAPP Failure Debugging (continued)**

Problem	Solution/Debug Steps
<p>Configuration changes. Reason given: Found configured or master controller.</p> <p>Note With a master controller set, if the AP does not have a primary or secondary controller name pre-configured, an AP will associate with the master controller.</p>	<p>1) Limit the number of associated APs on the master controller, to allow for initial association of such “strays.”</p> <p>2) AP might have switched from a secondary, tertiary (or other) controller to a master controller that was inactive when the AP first joined.</p>
<p>Configuration change. Reason given: Image upgraded.</p>	<p>1) An image upgrade was initiated from the controller or Cisco WCS and was sent to the AP.</p> <p>Note After the AP image upgrades, the AP reboots.</p>
<p>Configuration change. Reason given: Controller reboot command.</p>	<p>1) A controller reboot request was initiated from the controller.</p>
<p>Configuration changes. Reason given: Did not get config response.</p> <p>Note When a configuration change occurs, an AP should signal back and acknowledge it has gotten the configuration change.</p>	<p>Problem is mostly likely caused by poor SNR between APs or packet lost in the airwaves.</p> <p>1) Run a link test between the two APs from the controller or WCS.</p> <p>2) In Cisco WCS, run the Mesh Packet Error Rate Report (Path: Reports > Mesh Reports > <i>Mesh Packet Error Stats</i>).</p> <ul style="list-style-type: none"> – If SNR is good but there is a high PER, then check for interference. <p>3) Verify load in the network.</p>
<p>Link failure. Reason given: ECHO_REQUEST.</p> <p>Note LWAPP connection did not receive the acknowledgment (ACK) and the APs are disassociating because they are unable to reach the controller.</p>	<p>1) Lack of connectivity between the controller and the access points could be tied to either problems with network elements (wireless backhaul, switches, or routers) or because of low SNR.</p> <p>Note Refer to the beginning of this document, and begin step-by-step troubleshooting.</p>
<p>Link failure. Reason given: RRM_DATA_REQ.</p>	<p>1) Error message indicates LWAPP did not receive an ACK form the AP; and the APs are disassociating because the controller is unable to reach them.</p> <p>1) Check network connections (wireless backhaul, switches, routers).</p> <p>2) Check link for low SNR.</p>

Table 11 LWAPP Failure Debugging (continued)

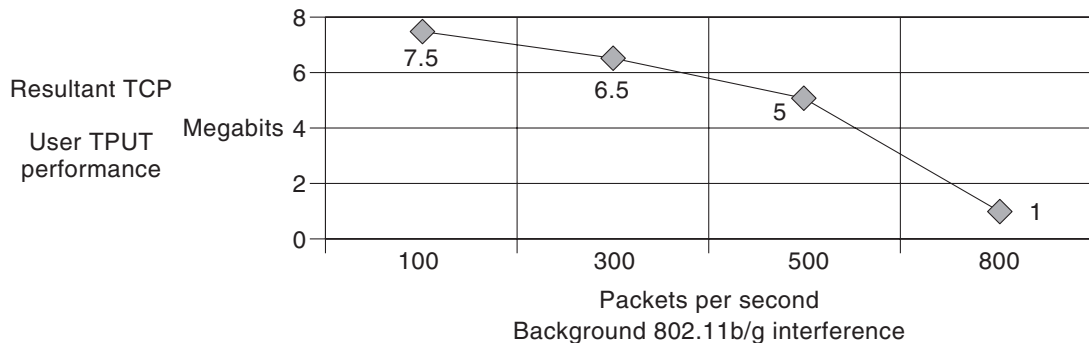
Problem	Solution/Debug Steps
<p>Link failure. Reason given: STATISTICS_INFO.</p> <p>Note Error message indicates that LWAPP could not pull statistical information from the AP. This could be due to low SNR or just packet lost in the airwaves from 802.11 behavior.</p>	<p>1) Run a link test between the two APs from the controller or WCS.</p> <p>2) In Cisco WCS, run the Mesh Packet Error Rate Report (Path: Reports > Mesh Reports > <i>Mesh Packet Error Stats</i>).</p> <ul style="list-style-type: none"> - If good SNR but high PER, then check for interference. <p>3) Verify load in the network.</p>
<p>Link failure. Reason given: CHANGE_STATE_EVENT.</p> <p>Note Link failures are, in general, tied to the non-receipt of LWAPP ACKs by the AP.</p>	<p>1) Lack of connectivity between the controller and the access points could be tied to either problems with network elements (wireless backhaul, switches, or routers) or because of low SNR.</p> <p>Note Refer to the beginning of this document, and begin step-by-step troubleshooting.</p>
<p>Maximum retransmissions timer has exceeded its setting (60 retries).</p>	<p>1) Refer to the beginning of this document, and begin step-by-step troubleshooting.</p>

Performance Notes

Typical throughput and performance are based on backhaul performance delivered to the RAP, the number of mesh hops, the noise and interference on the mesh wireless backhaul and on the wireless access side as well as client transmit uplink power. Tools such as wireless 802.11 sniffers and software spectrum analyzers can be used to troubleshoot local on-site issues.

Additionally, Cisco WCS and the controller already have noise and interference feedback tools built-in to the controller AP monitor and WCS Report pages; in general, these tools display Pass or Fail results based on default criteria.

Figure 1 Transmission Control Protocol (TCP) Throughput vs. Channel Utilization



231679

CCDE, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0803R)

Copyright © 2008 Cisco Systems, Inc. All rights reserved
