FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine

Release 2.9

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: OL-5921-01

CONTENTS

CHAPTER 1 **FAQs and Troubleshooting** 1-1

- General FAQs and Troubleshooting 1-1
- Faults FAQs and Troubleshooting 1-11
- Devices FAQs and Troubleshooting 1-15
- Configuration FAQs and Troubleshooting 1-22
- Firmware FAQs and Troubleshooting 1-27
- Reports FAQs and Troubleshooting 1-33
- Radio Manager FAQs and Troubleshooting 1-36
- Location Manager FAQs and Troubleshooting 1-43
- Administration FAQs and Troubleshooting 1-48

CHAPTER 2 **Fault Descriptions** 2-1

- Access Point /Bridge Faults 2-1
- Radio Interface Faults 2-7
- WLSE Faults 2-15
- AAA Server Faults 2-16
- Switch Faults 2-21
- Router Fault 2-22

INDEX

FAQs and Troubleshooting

This FAQ and troubleshooting guide consists of the following sections:

- General Questions—See General FAQs and Troubleshooting, page 1-1
- Faults—Faults FAQs and Troubleshooting, page 1-11
- Devices—Devices FAQs and Troubleshooting, page 1-15
- Configuration—Configuration FAQs and Troubleshooting, page 1-22
- Firmware—Firmware FAQs and Troubleshooting, page 1-27
- Reports—Reports FAQs and Troubleshooting, page 1-33
- Radio Manager—Radio Manager FAQs and Troubleshooting, page 1-36
- Location Manager—Location Manager FAQs and Troubleshooting, page 1-43
- Administration—Administration FAQs and Troubleshooting, page 1-48

General FAQs and Troubleshooting

- General FAQs, page 1-1
- General Troubleshooting, page 1-4

General FAQs

- Q.Can several users be logged on and managing the same access point at once?
- Q.Does the WLSE support Network Address Translation (NAT)?
- Q.Is Telnet enabled or disabled by default on the WLSE?
- Q.Which ports and protocols does the WLSE use?
- Q.Can I use a different HTTP port to manage the access point?
- Q.Can SSH be disabled?
- Q.Can I run a job to convert a number of access points from non-IOS to IOS?
- Q.Devices are being displayed by IP address instead of hostname. Can I change this?
- Q.How can I get information about the WLSE's operating system and hardware?

- Q.Can I install WLSE 2.9 software on a CiscoWorks 1105 appliance?

Q. Can several users be logged on and managing the same access point at once?

A. Yes, several users can view data and reports on the same access point. More than one user can create configuration and firmware update jobs for the same access point and these will be run in the order they are scheduled. Configuration templates may be modified by more than one user at the same time and the last write will overwrite the others.

Q. Does the WLSE support Network Address Translation (NAT)?

A. No.

Q. Is Telnet enabled or disabled by default on the WLSE?

A. Telnet is disabled by default for security reasons. SSH is enabled by default.

Q. Which ports and protocols does the WLSE use?

A. The WLSE uses the following ports and protocols. Table 1-1 lists the ports used by the WLSE, and Table 1-2 lists the ports hosted by the WLSE.

Table 1-1 Ports Used by WLSE

Destination Port Number	Protocol and WLSE Service	Port Hosted By
TCP 21	FTP—IOS AP configuration	FTP server
TCP 22	SSH—IOS AP configuration	Access point
TCP 23	TELNET—IOS AP configuration	Access point
TCP 25	SMTP—fault notification	SMTP server
UDP 53	DNS—IOS AP configuration	DNS server
TCP 80	HTTP—non-IOS (VxWorks) access point configuration	Access point
TCP 9851	WHISK—repository for upgrading WLSE software	Windows repository server
UDP 161	SNMP—discovery, inventory, configuration of APs	Access point, other devices
UDP 162	SNMPTRAP—fault notification	Trap server
UDP 514	SYSLOG—fault notification	Syslog server
UDP 1645 and 1646	RADIUS—AAA synthetic authentication (ACS versions prior to 3.2.3)	Cisco ACS server
UDP 1812 and 1813	RADIUS—AAA synthetic authentication (ACS 3.2.3 version)	Cisco ACS server
UDP 1812 and 1813	RADIUS—WLCCP authentication	Local RADIUS access point
UDP 1812	LEAP—AP1100 or AP 1210 configured as a LEAP AAA server on the WLSE.	AP 1100 or AP 1210

Table 1-1 Ports Used by WLSE (continued)

Destination Port Number	Protocol and WLSE Service	Port Hosted By
TCP 21	FTP—IOS AP configuration	FTP server
TCP 22	SSH—IOS AP configuration	Access point
TCP 23	TELNET—IOS AP configuration	Access point
TCP 25	SMTP—fault notification	SMTP server
UDP 53	DNS—IOS AP configuration	DNS server
UDP 1812	EAP-FAST—AP 1100 or AP 1210 configured as an EAP-FAST AAA server on the WLSE.	AP 1100 or AP 1210
UDP 2887	WLCCP—Wireless Domain Service (WDS) radio management	Master WDS access point

Table 1-2 Ports Hosted by WLSE

Destination Port Number	Protocol and WLSE Service	Source
TCP 443	HTTPS—WLSE secure Web port	Client browser
TCP 1741	HTTP—WLSE Web port	Client browser
UDP ephemeral	TFTP—firmware image transfer	Access point
UDP 69	TFTP—firmware image transfer	Access point

Q. Can I use a different HTTP port to manage the access point?

A. Yes, the HTTP port can be changed on the access point. The change will be reflected in WLSE after the next inventory cycle, or if you choose to run inventory now for the devices on which HTTP port was changed. This is assuming the inventory is done by SNMP and not HTTP.

Q. Can SSH be disabled?

A. It cannot be disabled on the WLSE itself, but you can use the firewall command to deny all SSH connections. For example, the following CLI command will cause the WLSE to reject all incoming SSH connections on the Ethernet 0 interface but allows connections through other protocols and other ports:

```
firewall ethernet0 private ssh
```

Q. Can I run a job to convert a number of access points from non-IOS to IOS?

A. Yes, you can run a firmware job, using a special IOS upgrade image that is available on Cisco.com. For more information, see the document *Converting Access Points to IOS*.

Q. Devices are being displayed by IP address instead of hostname. Can I change this?

A. Select **Devices > Discover > DISCOVER > Advanced Options**. In the Name Format field, enter %hostname% as the name format.

Q. How can I get information about the WLSE's operating system and hardware?

A. For information about the operating system, WLSE model name, CPU and disk capacity, run the **show version** CLI command. For other information about the hardware, see the Technical Specifications appendix in the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*.

Q. Can I install WLSE 2.9 software on a CiscoWorks 1105 appliance?

A. No. WLSE 2.9 software can be installed on a CiscoWorks 1130 or 1130-19 only.

General Troubleshooting

This section provides the following troubleshooting information:

- Symptom After the WLSE reboots, the login screen appears, followed by an Internal Server Error message.
- Symptom A search for an access point using APs Based on Client IP, displays the following message, “search yielded no results.”
- Symptom When I try to access an access point web page through the WLSE, the following error message appears: Action Cancelled.
- Symptom Cannot recover after incorrect setup program entry.
- Symptom Cannot log into the system.
- Symptom Cannot log in as a system administrator.
- Symptom After the WLSE starts up, the setup login prompt appears. Use the setup program. The WLSE cannot connect to the network.
- Symptom Cannot connect to the WLSE using a Web browser.
- Symptom The system time or date is incorrect.
- Symptom The system cannot boot from the hard drive during a reboot.
- Symptom Cannot connect to system with Telnet or Telnet interaction is slow.
- Symptom The Internal Server Error message appears in the Web interface.
- Symptom Cannot boot from the recovery CD.
- Symptom Cannot successfully connect to the WLSE by using a console.
- Symptom Pop-up windows are blocked and screens are not refreshed.

Symptom After the WLSE reboots, the login screen appears, followed by an Internal Server Error message.

Possible Cause The servlet engine in the WLSE is starting up.

Recommended Action Wait for 20 to 30 seconds, then log in again.

Symptom A search for an access point using APs Based on Client IP, displays the following message, "search yielded no results."

Possible Cause The device you are searching for is an IOS device. This type of search only works for non-IOS devices.

Recommended Action None.

Symptom When I try to access an access point web page through the WLSE, the following error message appears: Action Cancelled.

Possible Cause The SNMP user on the access point does not have enough rights.

Recommended Action Log in to the access point web interface, select **Setup > Security > User Information**, and make sure that the user corresponding to the SNMP community (which is set up in the WLSE under **Discovery > Device Credentials**) has been granted rights for the following: firmware, admin, and snmp.

Symptom Cannot recover after incorrect setup program entry.

Possible Cause You entered incorrect text during the initial setup and want to fix the entry.

Recommended Action Exit setup by pressing **Ctrl-c**. Then run **erase config** to remove the incorrect installation information and rerun the setup program. If you use the erase config command to erase the previous WLSE configuration, and run the setup program again, you will be required to get a new certificate. Use the **mkcert** command or **Administration > Appliance > Security > SSL (HTTPS)**.

Symptom Cannot log into the system.

Possible Cause You did not run the setup program to create an initial system configuration or you lost all the user account passwords.

Recommended Action

1. Did you run the setup program after booting the system for the first time?

   If no, run the setup program.

   If yes, continue to the next step.
2. Do you know the password for any system user accounts?

   If no, see Symptom Cannot log in as a system administrator., page 1-6.

   If yes, continue to the next step.
3. If you are certain you entered a valid username and password, contact Cisco's Technical Assistance Center for assistance.

Symptom Cannot log in as a system administrator.

Possible Cause All administrator passwords have been lost.

Recommended Action Perform the following procedure (requires reconfiguring the WLSE's network setup):

1. Connect a console to the serial/console port on the back panel.
2. Power the system off, then power it back on. Boot messages appear and then the following prompt appears:

```
-----------------------------------
0: CiscoBre
1: CiscoBreR
-----------------------------------
```

3. Use the Up Arrow and Down Arrow keys to select 1 to boot into CiscoBreR, then press Enter. The following prompt appears:

```
[root@CiscoMaintImage/]#
```

4. Enter the following command. This erases the WLSE's configuration, returns the WLSE to factory defaults, and reloads the WLSE.

```
[root@CiscoMaintImage/]# erase config
```

5. After the WLSE starts up, the setup login prompt appears. Use the setup program to reconfigure the system. This allows you to add a password for the admin user.

   For information about the setup program, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Symptom After the WLSE starts up, the setup login prompt appears. Use the setup program. The WLSE cannot connect to the network.

Possible Cause

- The network cable is not connected to the Ethernet 0 port.
- The Ethernet 0 interface is disabled or misconfigured.
- The system is configured correctly, but the network is down or misconfigured.
- DNS is misconfigured. Ping commands will result in a 50-70% failure rate in Pings from the WLSE (Web interface and CLI).

Recommended Action

1. Verify that the network cable is connected to the Ethernet 0 port and the Ethernet indicator is lit.

- If the network cable is not connected, connect it.
- If the network cable is connected but the Ethernet indicator is not lit, these are the probable causes:

  The network cable is faulty.

  The network cable is the wrong type (for example, a cross-over type, rather than the required straight-through type).

  The port on the default gateway to which the system connects is down.

- If the network cable is connected and the Ethernet indicator is on but the system cannot connect to the network, continue to the next step.

2. Use the **ping** command to perform the following tests:

- Try to ping a well-known host on the network. A DNS server is a good target host.

  If the ping command gets a response, the system is connected to the network. If the system cannot connect to a particular host, the problem is either with the network configuration or that host. Contact your network administrator for assistance.

  If the ping command does not get a response, continue.

- Attempt to connect to another host on the same subnet as the system.

  If the ping command can connect to a host on the same subnet, but cannot connect to a host on a different subnet, the default gateway is probably down.

  If the ping command cannot connect to any hosts, continue to the next step.

3. Use the **show interfaces** command to determine if the Ethernet 0 interface is disabled or misconfigured.

   For more information on the **show interfaces** command, see the CLI appendix in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

   If the Ethernet 0 interface is disabled, enable it. If it is misconfigured, configure it correctly. For more information, see the **interface** command description in the CLI appendix in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

   If the interface is enabled and correctly configured, continue to the next step.

4. Contact your network administrator to verify that there are no conditions on the network that prevent the system from connecting to the network.

   If conditions prevent the system from connecting to the network, have your network administrator correct them.

5. If no conditions are preventing the system from connecting to the network, contact Cisco's Technical Assistance Center.

Symptom Cannot connect to the WLSE using a Web browser.

Possible Cause

- The system cannot connect to the network.
- HTTP or HTTPS is not enabled
- If connecting via HTTP, the IP address was not appended with **:1741**.
- The client system is not configured.

Recommended Action

1. Make sure that the system can connect to the network. Attempt to connect the system using a Web browser.

   If you cannot connect, continue.

2. If you are attempting to connect via HTTP, verify that:

   The IP address is appended with **:1741**.

   HTTP or HTTPs is enabled.

3. Verify that you are using a supported browser and the browser is configured correctly, and attempt to connect to the WLSE. For more information about browsers, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine* or the "Getting Started" section in the online help.
4. If you still cannot connect through the browser, continue to step 5.
5. At the system console, or through Telnet, verify that the Web Server and tomcat are running by entering the following:

   ```
   # services status
   ```

   If they are running, go to step 8. If they are not running continue to step 6.

6. Stop the system services by entering the following:

   ```
   # services stop
   ```

7. Restart the system services by entering the following:

   ```
   # services start
   ```

8. Try to connect the system using a Web browser.

   If you cannot connect, continue to the next step.

9. Reboot the system by entering the **reload** command.

   For more information on the **reload** command, see the CLI appendix in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

10. If you still cannot connect to the system using a Web browser, contact Cisco's Technical Assistance Center for assistance.

Symptom The system time or date is incorrect.

Possible Cause

- NTP is misconfigured.
- The system clock is set incorrectly.

Recommended Action Make sure NTP is configured correctly and that the system clock is set correctly.

For information about maintaining the system time and date, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

Symptom The system cannot boot from the hard drive during a reboot.

Possible Cause

- The disk has a physical error.
- The disk image is corrupted.

Recommended Action If the WLSE cannot boot from the hard drive, the hard drive needs to be reimaged. Use the Recovery CD to reimage your WLSE. For more information, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

Symptom Cannot connect to system with Telnet or Telnet interaction is slow.

Possible Cause

- Telnet is disabled or configured incorrectly.
- The WLSE cannot recognize host names.

  If you are not using name recognition, slow or non-existent telnet interaction is an expected problem.

Note Telnet is disabled by default. SSH is enabled by default.

Recommended Action

If the problem is not the network, perform the following steps. Connect to the console port if you cannot Telnet to the WLSE.

1. Check the Telnet settings to be sure Telnet is enabled and configured correctly. For more information, see the following

   To check the Telnet settings, or to enable or disable Telnet on specific domains or IP addresses, use the **telnetenable** CLI command. For more information on this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help

   To enable or disable Telnet on individual ports, use the **firewall** CLI command. For more information on this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help
2. If you have specified hosts using the **telnetenable** CLI command, make sure the host from which you are attempting to Telnet is on the list.
3. If you are using a DNS server, perform the following step:

   Configure the system to use a functioning DNS server by entering:

   ```
   # ip name-server ip-address
   ```

   where *ip-address* is the IP address of the DNS server.
   If you are using the import CLI command, proceed to the next step.
4. Verify that the system can get DNS services from the network by entering the following command:

   ```
   # nslookup dns-name {hostname | ip-address}
   ```

   where *dns-name* is the DNS name of a host on the network that is registered in DNS and *hostname* and *ip-address* is the same IP address specified in 2. The command returns the IP address of the host.
5. If the system cannot resolve DNS names to IP addresses, the DNS server it is using is not working properly.

   Resolve the network DNS problem, then continue.

6. If you are using the **import** CLI command to resolve host names, verify that the WLSE can resolve host names by entering the following command:

   ```
   ping hostname
   ```

   where *hostname* is a host name that has been mapped to an IP address, or imported in a host file, using the **import** command.

7. If the system can resolve DNS names to IP addresses but you still cannot connect to the system using Telnet, or Telnet interaction with the system is extremely slow, contact Cisco's Technical Assistance Center.

Symptom The Internal Server Error message appears in the Web interface.

Possible Cause In a redundant WLSE pair, the active WLSE has lost contact with the standby WLSE.

Recommended Action The standby WLSE is not up yet and returns this error when the active WLSE makes a request of it. This message will disappear when the standby WLSE has started up.

Symptom Cannot boot from the recovery CD.

Possible Cause The CD may look like it is firmly on the spindle, but it may not be.

Recommended Action Press the CD firmly onto the spindle. Also, see the following symptom (Symptom Cannot successfully connect to the WLSE by using a console., page 1-10).

Symptom Cannot successfully connect to the WLSE by using a console.

Possible Cause The monitor and/or keyboard are attached to the video port and USB port.

Recommended Action Attach the console to the console/serial port.

Symptom Pop-up windows are blocked and screens are not refreshed.

Possible Cause A pop-up blocker is running in the browser.

Recommended Action Disable the pop-up blocker while using the WLSE web interface or add the WLSE to the pop-up allowed list.

Faults FAQs and Troubleshooting

- Faults FAQs, page 1-11
- Faults Troubleshooting, page 1-12

Faults FAQs

- Q.Does acknowledging a fault clear it?
- Q.What traps are sent from the WLSE?
- Q.What trap types are forwarded by the WLSE?
- Q.Does a MIB or trap definition file exist for the WLSE?
- Q.What information is emailed in a fault notification?
- Q.Can I use the Associated Client setting for non-IOS access points even through the threshold is listed per interface?
- Q.Why I am not receiving any email fault notifications for low prioritiy faults?
- Q.What does it mean when there is an ellipsis (...) in a fault description for self healing?
- Q.After I change the refresh rate in the Display Faults screen, why does it revert back to the default of 300 seconds when I log out, then log back in again?
- Q.Why is a fault that is set to one priority level reported as a different priority level?

Q. Does acknowledging a fault clear it?

A. No, it only removes it from the Active list. For a description of fault states, see the information on understanding fault states in the online help.

Q. What traps are sent from the WLSE?

A. Traps are sent based on fault policy and threshold settings on the WLSE. The WLSE only sends out v2c traps, so make sure your trap listener is configured to accept v2c traps.

Solaris 2.8- based NetView 7.1 receives and displays the SNMP v2c fault notification traps from WLSE, but Windows-based NetView 7.1 supports only v1 traps and cannot receive and display any v2c traps from the WLSE.

Q. What trap types are forwarded by the WLSE?

A. No traps are forwarded from other devices.

Q. What information is emailed in a fault notification?

A. For a description see the online help.

Q. Does a MIB or trap definition file exist for the WLSE?

A. Yes, from the Cisco.com download site, download MIB CISCO-DEVICE-EXCEPTION-REPORTING-MIB.my and load it into the trap receiver.

Q. Can I use the Associated Client setting for non-IOS access points even through the threshold is listed per interface?

A. Yes. You can use either interface setting to set the threshold for a non-IOS access point. The fault generated under **Faults > View Faults** will reference the access point, not the radio interface.

Q. Why I am not receiving any email fault notifications for low prioritiy faults?

A. No email notification is sent for lower priority faults if higher priority faults already exists for that fault.

Q. What does it mean when there is an ellipsis (...) in a fault description for self healing?

A. The description is too long to fit in the allotted space. However a full description can be viewed by accessing the logs under **Radio Manager > Self Healing > Review Current**, then click Self Healing Run Log.

Q. After I change the refresh rate in the Display Faults screen, why does it revert back to the default of 300 seconds when I log out, then log back in again?

A. Changes to the refresh timer are applied only to a particular session. This is done by design.

Q. Why is a fault that is set to one priority level reported as a different priority level?

A. When more than one fault is reported against a device, the fault priorities are aggregated, and the maximum priority of all the active faults for that device is displayed. For example, if the device has a P1, a P2, and a P3 fault against it, only the P1 is displayed in the Severity column. However, when you click on the Description for that fault, all three priorities are displayed with an explanatoin for each.

Faults Troubleshooting

- Symptom After adding a AAA server in a Release 2.9 WLSE, the fault ‘AAA server is Not available’ is generated for that AAA server.
- Symptom A polling interval for a fault is increased from one minute to a higher value, yet the fault reappears after one minute, not in the new polling time.
- Symptom The Display Fault view is blank.
- Symptom Email fails to arrive at its destination.
- Symptom No VLAN fault information is displayed for IOS access points.
- Symptom No email notifications are being received for low priority faults.
- Symptom SNMP Unreachable faults are displayed more frequently than the set polling interval.
- Symptom The WLSE does not generate an ‘SNMP Unreachable’ fault when the device is unreachable.
- Symptom The following error message appears in the faults.log: ConditionProcessor MESSAGE: MOState: unknown state ViolatingPolicy for fsm SNMPReachable mo={MOID[c=1,d=141,i=141]}

Symptom After adding a AAA server in a Release 2.9 WLSE, the fault 'AAA server is Not available' is generated for that AAA server.

Possible Cause There are several reasons for this error messages: the wrong secret (a secret that does not match what is configured on the AAA server) was entered; the WLSE IP address is not configured as a NAS on the server, or the server is unreachable.

Recommended Action Enter the correct secret; the one that is configured on the AAA server or configure the WLSE IP address as NAS on the server.

Symptom A polling interval for a fault is increased from one minute to a higher value, yet the fault reappears after one minute, not in the new polling time.

Possible Cause The new polling time did not register.

Recommended Action Disable fault polling on the relevant policy or threshold, then manually clear the fault. Change the fault polling interval on the policy or threshold to the new setting, then enable fault polling on the relevant policy or threshold.

Symptom The Display Fault view is blank.

Possible Cause There are no faults to report based on the filtering criteria you entered.

Recommended Action Not applicable.

Symptom Email fails to arrive at its destination.

Possible Cause The SMTP server is not configured properly.

Recommended Action Configure the SMTP server by selecting Administration > Appliance > Configure Mailroute.

Symptom No VLAN fault information is displayed for IOS access points.

Possible Cause WEP keys have not been configured in each VLAN. When the WEP keys are configured in the IOS access points, VLAN information is accessible by SNMP.

Recommended Action Configure the WEP keys for the corresponding VLAN.

Symptom No email notifications are being received for low priority faults.

Possible Cause No email notification is sent for lower priority faults if higher priority faults already exists for that fault

Recommended Action None.

Symptom SNMP Unreachable faults are displayed more frequently than the set polling interval.

Possible Cause When the WLSE polls for any faults, it also checks if the device is SNMP reachable. If the device is unreachable, it will generate an SNMP Unreachable fault no matter what SNMP Reachable poll interval is.

Recommended Action None.

Symptom The WLSE does not generate an 'SNMP Unreachable' fault when the device is unreachable.

Possible Cause This is observed only with a WLSE that has been upgraded from WLSE 2.7.

Recommended Action

1. Find the device for which the faults state machine might be corruptedas follows:
   a. View the faults.log under **Admin > Appliance > View Log File**.
   b. Look out for the following error messages in the log file:

      ```
      2004/12/01 20:23:00 ConditionProcessor MESSAGE: MOState:  unknown state
      ViolatingPolicy for fsm SNMPReachable mo={MOID[c=1,d=141,i=141]}
      ```

   c. Note the DEVICEID. For example the DEVICEID in the error message is 141 (d=141).
2. Determine the IP address corresponding to the DEVICEID as follows:
   a. Enter http://<wlse-ip>:1741/debug/dbquery.jsp in your browser.
   b. Enter the following in the Database Query Utility window:

      select IPADDRESS from DEVICES_MG where DEVICEID=<id>

      where DEVICE ID is the ID noted in Step 1. For example, 141.
   c. Note the IP address of the device.
3. Repeat Steps 1 and 2 for all the DEVICEIDs.
4. Delete the devices from the WLSE.
5. Rediscover and manage the devices.

Symptom The following error message appears in the faults.log: ConditionProcessor MESSAGE: MOState: unknown state ViolatingPolicy for fsm SNMPReachable mo={MOID[c=1,d=141,i=141]}

Possible Cause This is observed only with a WLSE that has been upgraded from WLSE 2.7.

Recommended Action

1. Find the device for which the faults state machine might be corrupted as follows:
   a. View the faults.log under **Admin > Appliance > View Log File**.
   b. Look out for the following error messages in the log file:

      ```
      2004/12/01 20:23:00 ConditionProcessor MESSAGE: MOState:  unknown state
      ViolatingPolicy for fsm SNMPReachable mo={MOID[c=1,d=141,i=141]}
      ```

   c. Note the DEVICEID. For example the DEVICEID in the error message is 141 (d=141).
2. Determine the IP address corresponding to the DEVICEID as follows:
   a. Enter http://<wlse-ip>:1741/debug/dbquery.jsp in your browser.

b. Enter the following in the Database Query Utility window:

   select IPADDRESS from DEVICES_MG where DEVICEID=<id>

   where DEVICE ID is the ID noted in Step 1. For example, 141.

c. Note the IP address of the device.

3. Repeat Steps 1 and 2 for all the DEVICEIDs.
4. Delete the devices from the WLSE.
5. Rediscover and manage the devices.

Devices FAQs and Troubleshooting

- Devices FAQs, page 1-15
- Devices Troubleshooting, page 1-17

Devices FAQs

- Q.Why is hostname (device name), sysContact, and sysLocation information not updated in the WLSE after I change these parameters on the access point?
- Q.What is an invalid CDP seed?
- Q.Can I discover devices if CDP is disabled?
- Q.What are the extra inventories listed in the Run Now folder?
- Q.What are the results of adding or removing an interface from an access point?
- Q.Can the WLSE discover access points that are connected to non-Cisco switches?
- Q.Can I register an access point as an AAA server to be monitored by the WLSE?
- Q.How does the WLSE handle duplicate IP addresses on APs internally?

Q. Why is hostname (device name), sysContact, and sysLocation information not updated in the WLSE after I change these parameters on the access point?

A. The hostname (device name), sysContact, and sysLocation parameters are updated during discovery, not during inventory. Make sure you schedule a periodic discovery under **Devices > Discover > DISCOVER > Discovery Wizard**.

Q. What is an invalid CDP seed?

A. An invalid seed is a device that does not run Cisco Discovery Protocol (CDP), such as a PC or workstation). Such a device does not function as a seed because it does not allow the WLSE to traverse the network and find other devices. In the discovery run log, invalid seeds are shown as SNMP unreachable.

Q. Can I discover devices if CDP is disabled?

A. If CDP is disabled on network devices, you can still discover access points by entering the IP addresses of all of them on the WLSE as seed values. However, the WLSE cannot discover switches directly attached to such access points, and switch-related reports will be empty.

Q. What are the extra inventories listed in the Run Now folder?

A. The radio management module runs periodic immediate inventories.

Q. What are the results of adding or removing an interface from an access point?

A. If you physically remove an interface (for example, removing 11b from a dual-interface AP 1200), the WLSE will automatically detect the change during the next inventory cycle. If you physically *add* an interface, you must delete the device and rediscover it. Otherwise, the inventory data might be invalid.

Q. Can the WLSE discover access points that are connected to non-Cisco switches?

A. You cannot use CDP to discover the APs, but you can import them from a file or enter them all as seed devices in the WLSE. Alternatively, if you have configured Wireless Domain Services, the APs may automatically be discovered if they are within the range of the participating APs.

Q. Can I register an access point as an AAA server to be monitored by the WLSE?

A. Yes, you can register an AP 1100 or AP 1210 as an AAA server. However, if you register an AP as an AAA server, you can no longer use the WLSE to manage that AP as a wireless device.

Q. How does the WLSE handle duplicate IP addresses on APs internally?

A. The WLSE must be able to handle situations in which an AP is assigned an address that is already assigned to another device that has been discovered by the WLSE. The WLSE handles these situations by sending appropriate internal events, placing the device that previously had the address in the Duplicate IP folder and updating the database. Detection of duplicate addresses occurs during periodic checking for rebooted APs and during discovery. The following rules apply when an IP address changes for an existing device:

1. If the IP address was assigned to an unmanaged AP, the AP will be marked deleted and later removed from the WLSE. This unmanaged AP can be rediscovered if it still exists and then would have a different IP address.
2. If the IP address was assigned to a different managed AP, that AP will be moved to the pending state and placed in the Duplicate IP folder. That AP will be considered unmanaged by the WLSE until the WLSE finds the right IP address for it. The WLSE sends an unmanage event for the AP.
3. If an AP having the same identity exists in the WLSE and is in the pending state, the WLSE assigns the IP address to the device in the database and moves the AP to the managed state. The WLSE sends a manage event.
4. If an AP with the same identity has a different IP address, the WLSE updates the device with the new IP address and sends an IP address change event.
5. If the AP with the same identity does not exist in the database, it is considered a new device and discovery is initiated.
6. If the AP is already assigned the right IP address, nothing is done.

For more information on how you should handle devices in the Duplicate IP folder, see the online help for the Devices tab.

Devices Troubleshooting

This section contains the following troubleshooting information:

Discovery Troubleshooting

- Symptom Devices were discovered but are not displayed in the GUI; for example, in Reports.
- Symptom There is a time discrepancy in the scheduled discovery jobs.
- Symptom Access points are placed in Misconfigured Devices group after discovery and dot11mib fault is displayed.
- Symptom Access points are placed in Misconfigured Devices group even though they have been configured with the correct ISO views.
- Symptom The SNMP Query Authorization Exception is recorded in the discovery log.
- Symptom An error message appears in the discovery run log.
- Symptom An IOS access point configured with an iee802dot11 view is not discovered.
- Symptom After changing the device name format, device names are not updated in the device tree.
- Symptom After a device is moved from unmanaged to managed, the name format is not applied.
- Symptom Instead of a proper device name or IP address, the WLSE is displaying device names as "%dns%, "%hostname%", or "%description%".
- Symptom After creating a custom device name format, truncation of device names in displays makes it difficult or impossible to distinguish one device from another.
- Symptom Access points with 12.2(13)JA or 12.2(15)JA firmware are not discovered and are placed in the Misconfigured Devices folder under Group Management.
- Symptom The name of an AAA server is displayed as %hostname% instead of the name entered by the user when the AAA server was added.
- Symptom The Managed Devices display does not reflect the latest information (such as a change in the IP address of a device or a change in device state).

Inventory Troubleshooting

- Symptom Frequent client inventories are causing too much network traffic or degrading WLSE performance.
- Symptom Inventory is taking longer than expected and a message about no logs available appears in the inventory log.

Symptom Devices were discovered but are not displayed in the GUI; for example, in Reports.

Possible Cause The devices have not been moved to the Managed state.

Recommended Action Select **Administration > Discover > Managed Devices**. Move the devices from New or Unmanaged to Managed.

Intermediate switches with no access points directly connected to them are shown to be discovered in the Administration > Tasks History > Discovery logs but will not show up in **Administration > Discover > Managed Devices > Manage/Unmanage**.

Symptom There is a time discrepancy in the scheduled discovery jobs.

Possible Cause The local or system time is not set correctly on the WLSE.

Recommended Action

a. Reset the WLSE system time (UTC) using CLI commands as follows:

   Enter **services stop** to stop services.

   Enter the **clock** command to reset the time.

   Enter **services start** to restart the services.

b. Set the local browser time. Select **Administration > Appliance > Time/NTP/Name**.

Symptom Access points are placed in Misconfigured Devices group after discovery and dot11mib fault is displayed.

Possible Cause IOS access points are not configured correctly with an ISO view. Also, see the following Symptom: Symptom Access points are placed in Misconfigured Devices group even though they have been configured with the correct ISO views., page 1-19.

Recommended Action Perform the following tasks on the IOS access points and the WLSE. Either configure the devices individually or create a configuration template with the relevant custom values and create a job for the devices.

To configure access points individually:

a. Use Telnet or SSH to log in to the device, then enter enable mode.

b. In global configuration mode, enter the following commands in sequence:

```
# snmp-server view iso iso included
# snmp-server community community_string view iso RO
```

   where *community_string* is the AP's read-only community string. This is the same string that should exist in the WLSE's SNMP credentials screen (**Devices > Discover > Device Credentials > SNMP Communities**). If it is not entered there, see the following instructions for entering device credentials in the WLSE.

c. Exit from the global configuration mode, and enter the following command:

   # write memory

To configure access points by using a template:

a. Use the procedures in the configuration template instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9* to create a template.

b. Enter the following custom values in the template:

   snmp-server view iso iso included

   snmp-server community *community_string* **view iso RO**

c. Run a configuration job on the APs in the Misconfigured Devices group:

   — Select the template created in the previous step.

   —Either select the Misconfigured Devices group or the devices in the group.

   —Schedule the job to run at the desired time.

d. After the configuration job finishes successfully, the dot11 mib fault will be cleared after the next discovery cycle. You can run a manual discovery immediately after the configuration job finishes; select Devices > Discover > Run Inventory > Run Now.

Perform the following steps on the WLSE:

a. If the AP's ISO community string has not been entered on the WLSE, select **Devices > Discover > Device Credentials > SNMP Communities**. Then, enter the same community strings that you configured on the devices in the previous procedure.

   Otherwise, the devices will be placed back in the Misconfigured Devices group after the next discovery cycle.

b. Rediscover the APs by using them as seed devices in an immediate discovery. Select **Devices > Discover > Discover > Discovery Wizard.** Then select **Automatic Discovery Based on CDP > Run Now**. For more information on discovery, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Symptom Access points are placed in Misconfigured Devices group even though they have been configured with the correct ISO views.

Possible Cause Unknown.

Recommended Action Delete the access points from the WLSE and run a new discovery.

Symptom The SNMP Query Authorization Exception is recorded in the discovery log.

Possible Cause The community string on the access point does not have admin and firmware rights.

Recommended Action In the configuration template or on the access point, assign the missing rights to the community string. For more information, see the information on setting up devices in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*.

Symptom An error message appears in the discovery run log.

Table 1-3 Discovery Run Log Messages

Message	Possible Cause	Recommended Action
`No seeds defined.`	Although discovery is initially enabled and runs every 24 hours, it will not run unless you add seed devices.	See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

x.x.x.x `is reachable but unable to provide the information you requested. For IOS access points, make sure the SNMP community does not have an object identifier associated with it.`	The community string might not have an SNMP ISO view associated with it, and the WLSE cannot poll some attributes.	Configure the AP's community string as follows:
		`# snmp-server view iso iso included`
		`# snmp-server community` *community_string* `view iso RO`
		where *community_string* is the AP's read-only community string.

Table 1-3 Discovery Run Log Messages

Message	Possible Cause	Recommended Action
`Inventory collection was not run for updated devices, run on-demand inventory or wait for the next scheduled inventory`	An automatic inventory does not run for rediscovered devices.	Run an on-demand inventory or wait for the next scheduled inventory. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.
x.x.x.x `does not respond to ieeedot11 attributes.`	The IOS access point has not been configured with an IOS view. After the device is properly configured, you can run discovery or wait for the next scheduled discovery. After discovery, the device will be placed in the proper group(s).	See the symptom, Symptom Access points are placed in Misconfigured Devices group after discovery and dot11mib fault is displayed.
`IP conflict for` *ip_address* `(`*hostname*`). Identifier or ethernet MAC is` *identifier or MAC address*`. A device already exists under this IP address. If the original device was replaced, please delete it first and run discovery again.`	A newly discovered device has the same IP address as a previously discovered device. The new device will not be discovered until the conflict is resolved. The identifier shown is for the previously discovered device. For access points, the identifier shown is the Ethernet MAC address.	If you want both devices to be managed, assign a different IP address to the newly discovered device. If you substituted a new device for a previous device and want to retain the IP address, delete the old device. In either case, run discovery again or wait for the next scheduled discovery. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.
`Unable to auto-manage device: x.x.x.x due to MAC filter values or time period for auto-management has expired.`	A new device is being discovered but could not be auto-managed because the MAC filter values exclude the device or the time period selected for auto-management has expired.	See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Symptom An IOS access point configured with an iee802dot11 view is not discovered.

Possible Cause The community string should be configured with an ISO view.

Recommended Action

1. In the Web interface of the AP, select Services > SNMP.
2. Select the Read/Write community string associated with an iee802dot11 view. In the Object Identifier field, enter “iso.” Select Read-Only or Read-Write and click **Apply**.
3. On the WLSE, select Devices > Discover > DISCOVER > Advanced Options. Make sure auto-manage is enabled.
4. Run discovery on the device, using the community string that has the ISO view.

   Result: The WLSE discovers the device and places it in the Managed folder.

Symptom After changing the device name format, device names are not updated in the device tree.

Possible Cause If there are many devices in the device tree, it may take some time to perform the update and the page may not automatically be refreshed.

Recommended Action Navigate to some other screen and then return to the device tree. The device tree will be updated correctly to the new name format.

Symptom Instead of a proper device name or IP address, the WLSE is displaying device names as "%dns%, "%hostname%", or "%description%".

Possible Cause The default device identifier used in WLSE displays is the device's hostname. If no hostname is assigned to the device, "%hostname%" is used instead. If "%dns%" or "%description%" is being displayed, a user has changed the default device identifier format, but there is no DNS name or the user has not assigned a description to the device.

Recommended Action The default device identifier string is set under **Devices > Discover > DISCOVER > Advanced Options**. If you use the IP address as the default identifier, the device name will always be correct. If you use one of the other formats as the default identifier, make sure the requirements are met. For more information, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9* on Cisco.com.

Symptom After creating a custom device name format, truncation of device names in displays makes it difficult or impossible to distinguish one device from another.

Possible Cause In device trees, only 30 characters can be displayed. In some other displays, device names are truncated as well.

Recommended Action Reconstruct the name format string so that the unique portion of the name comes first; for example, place the IP address first.

Symptom After a device is moved from unmanaged to managed, the name format is not applied.

Possible Cause When devices are moved from unmanaged to managed, the current name format choice is not applied until the next inventory runs.

Recommended Action Run an inventory on the device. Select **Devices > Discover > Inventory > Run Inventory**.

Symptom Access points with 12.2(13)JA or 12.2(15)JA firmware are not discovered and are placed in the Misconfigured Devices folder under Group Management.

Possible Cause If an ieee802dot11 view is configured on these access points, the WLSE does not discover them.

Recommended Action Either configure an iso view on the access points, or do not configure any view. Then, rediscover the access points. WLSE discovers these devices because all MIBs are accessible from such devices, whether an iso view is configured or no view is configured.

Symptom The name of an AAA server is displayed as %hostname% instead of the name entered by the user when the AAA server was added.

Possible Cause This sometimes occurs after updating the system software to 2.9.1 or 2.11.

Recommended Action Select **Devices > Discover > AAA Server** and remove the AAA server. Then, add the server again.

Symptom The Managed Devices display does not reflect the latest information (such as a change in the IP address of a device or a change in device state).

Possible Cause The device tree under MANAGED DEVICES shows the state of the system at the time you select the Managed Devices option. Therefore, if device details change or the device changes to another state after you display the page, these changes are not automatically displayed.

Recommended Action If you refresh the page by using the browser controls or navigate to another page and then return to Managed Devices, the page will be updated to show changes that have occurred.

Symptom Frequent client inventories are causing too much network traffic or degrading WLSE performance.

Possible Cause Running frequent client inventories when managing large numbers of access points (1,000 or more) generates a great deal of traffic and may degrade WLSE performance.

Recommended Action Increasing the Wireless Client Poll Interval in **Devices > Discover > Inventory > Polling** will reduce the polling frequency. If you need more frequent client polling for a subset of your access points, use the Scheduled Inventory feature instead (**Devices > Discover > Inventory > Run Inventory**).

Symptom Inventory is taking longer than expected and a message about no logs available appears in the inventory log.

```
No logs available. Waiting for resources to start job.
```

Possible Cause If there are also SNMP timeouts on the network, inventory jobs will take much longer. Other jobs may be using all of the available resources. Also, the next scheduled inventory will not run until the current inventory finishes.

Recommended Action None.

Configuration FAQs and Troubleshooting

- Configuration FAQs, page 1-23
- Configuration Troubleshooting, page 1-25

Configuration FAQs

- Q.What happens when I apply a configuration to a device with an existing configuration?
- Q.Can I stop a running job?
- Q.If a template is valid for an access point with an 802.11g radio, can I also apply that template to an access point with an 802.11b radio?
- Q.If a template is valid for a 1310 wireless bridge in bridge mode, can I also apply that template to a 1310 wireless bridge in access point mode?
- Q.Can I apply a template to a 1310 wireless bridge that is in workgroup bridge mode?
- Q.If I create a configuration template that includes WEP key settings how can I verify that they were set on the access point.
- Q.Can you undo a configuration update?
- Q.How long is the configuration job history kept in the WLSE?
- Q.What mechanism do configuration jobs use to initiate a configuration upload?
- Q.What kinds of job logs are available?
- Q.What is startup configuration?
- Q.If I make changes to the startup template, will those modifications be automatically uploaded to the access points that already had that startup template applied?
- Q.What is auto configuration?
- Q.Can I give a configuration job a name that is used for a firmware or radio management job?

Q. What happens when I apply a configuration to a device with an existing configuration?

A. The two configurations are merged unless you have specified that you want to overwrite the existing configuration when you ran the job. If you choose to overwrite the configuration, two things will occur: the selected configuration template will replace the startup-config on the selected device(s) and the device(s) will be rebooted after the copy to startup-config succeeds.

Q. Can I stop a running job?

A. No. A job that is already running cannot be stopped.

Q. If a template is valid for an access point with an 802.11g radio, can I also apply that template to an access point with an 802.11b radio?

A. No. You can only apply a template valid for an access point with an 802.11g radio to an access point with an 802.11g radio.

Q. If a template is valid for a 1310 wireless bridge in bridge mode, can I also apply that template to a 1310 wireless bridge in access point mode?

A. No. You can only apply a template valid for a 1310 wireless bride in bridge mode, to a 1310 wireless bridge in bridge mode.

Q. Can I apply a template to a 1310 wireless bridge that is in workgroup bridge mode?

A. No. The WLSE does not support configuration of workgroup bridges.

Q. If I create a configuration template that includes WEP key settings how can I verify that they were set on the access point.

(The access point does not show WEP key settings on its web interface)?

A. For security reasons, the access point does not show or send WEP key information. One of the ways to verify the update is to look at the WEP Key length. The only way to verify the contents of the WEP key is to try associating a client that uses that WEP key.

Q. Can you undo a configuration update?

A. Yes, but only for successful jobs and device versions 12.01T and later. The Undo feature cannot be used for IOS devices.

To undo a job, view the Job Run Details table under Configuration > Jobs, select the job you want to undo, and click Undo. For more specific information, see the online help.

Q. How long is the configuration job history kept in the WLSE?

A. The default time is 30 days. You can change this by navigating to Devices > Discover > Inventory > Polling > Job History Truncation Interval. Also, by default, for the recurring jobs, the last 30 runs are maintained in the database.

Q. What mechanism do configuration jobs use to initiate a configuration upload?

A. WLSE configuration jobs for IOS devices use Telnet or SSH. Configuration jobs for non-IOS devices can use either HTTP or SNMP as the mechanism to initiate a configuration template upload to an access point.

- The HTTP mechanism is valid for all supported device versions. The following setup parameters must be in place for HTTP mechanism to function properly:
  - HTTP credentials for the device (with admin and firmware privileges on the access point) must match those entered on the WLSE HTTP device credentials screen.
  - TFTP server settings on the access point (Setup > FTP), must refer to the WLSE's IP address.

Note Both username and password in the device credentials are case sensitive.

- The SNMP mechanism is valid for versions 12.01T and later. The following setup parameters must be in place for SNMP to function properly:
  - SNMP credentials for the device (with admin and firmware privileges on the access point) must match those entered on the WLSE SNMP device credentials screen.
  - There is no need to change TFTP server settings for the SNMP mechanism, although you can use the SNMP mechanism to change the TFTP server settings on the AP to be used in the HTTP mechanism. Enter valid credentials in the Security > Local Admin Access template screen.

  The SNMP job mechanism can be used to update TFTP settings, which are needed by HTTP-based jobs. This setting is available under Service > FTP in the configuration templates screens.

Q. What kinds of job logs are available?

A. There are two kinds of job logs: Job run log and the jobvm log.

- The job run log is where events are logged for a particular job's run. This log can be used to check what went wrong with the job and make any required corrections. The job run log can be viewed by selecting a particular job from the job list, then clicking **Job Run Detail**. From the window that pops up, select a particular run for the job, then click **Job Run Log**.

- The jobvm.log is a global log for all types of jobs. It is used mainly for development troubleshooting. The jobvm.log can be viewed by selecting Administration > Appliance > View Log File, then clicking **jobvm.log**.

Q. What is startup configuration?

Startup configuration is used right after a device (access point) reboots. It requires DHCP server to be properly set up to allow the access point to pick its startup configuration from WLSE. For this to work, you must set up the following:

a. Enter the <`IP address of the WLSE`> in the **Boot Server Host Name** field (option number 066) on the DHCP server.

b. Enter `<startup file name>` in the **BootfileName** field (option number 067) on the DHCP server.

For additional information, or for information about configuring a router as a DHCP server, see the online help.

Q. What is auto configuration?

A. Auto configuration is used after the device has been discovered and inventory has been collected for it. This template can be applied based on criteria you define while saving your auto-configuration template.

Q. If I make changes to the startup template, will those modifications be automatically uploaded to the access points that already had that startup template applied?

A. No. If you make modifications to the startup template, you will have to reapply the template.

Q. Can I give a configuration job a name that is used for a firmware or radio management job?

A. No. Job names cannot be duplicated.

Configuration Troubleshooting

- Symptom When I upgrade from WLSE Release 2.7 to 2.9, my AP 1210 template no longer works for all AP1210 devices.
- Symptom .The banner command in an IOS custom template fails or is incomplete.
- Symptom An imported non-IOS template fails to include a MAC address..
- Symptom HTTP configuration jobs are picking up the wrong template.
- Symptom An IOS template job failed.
- Symptom Configuration jobs fail because the Telnet/SSH credentials are not valid, even though credentials have been entered on the WLSE.

Symptom When I upgrade from WLSE Release 2.7 to 2.9, my AP 1210 template no longer works for all AP1210 devices.

Possible Cause .When the device type selected in the automanage template for Release 2.7 is AP1210, it will not work for single radio AP 1210's in Release 2.9.

Recommended Action Edit the auto manage criteria for the auto manage template to include both AP 1210 for dual radios, as well as AP 1210-SR for single radio device types.

Symptom .The banner command in an IOS custom template fails or is incomplete.

Possible Cause The banner command fails because it contains 240 or more characters.

Possible Cause A delimiter in the banner string, can cause a partial banner to be applied to the device. For example, if the following command is typed in the custom template using the letter "c" as the delimiter: **`banner motd c This is to check banner c`**, the following is displayed when previewed: "`banner motd c This is to c`." The banner displays incorrectly because there is a word in the banner (check) that begins with the same character used as the delimiter.

Recommended Action Use less than 240 characters in the banner string, and do not use characters for delimiters if the characters are also used in the text of the banner.

Symptom An imported non-IOS template fails to include a MAC address.

Possible Cause The template was imported from a device with the Allowed or disallowed MAC address filter included

Recommended Action .Import the template with the full option. If it is imported with the Non-IP option, the MAC address will not be imported.

Symptom HTTP configuration jobs are picking up the wrong template.

Possible Cause If the access point's FTP setting is for another WLSE server, and it has the same as the setting for startup configuration on the DHCP server, then the HTTP config job for the access point picks up the wrong template from wrong WLSE server, but job status is shows as successful.

Recommended Action Make sure the access point's FTP setting is for correct WLSE server.

Symptom An IOS template job failed.

Possible Cause The template has the hostname configured instead of the IP address, and the DNS name resolution is not configured correctly on the access point.

Recommended Action Use the IP address or configure the DNS name correctly on the access point.

Symptom Configuration jobs fail because the Telnet/SSH credentials are not valid, even though credentials have been entered on the WLSE.

Possible Cause The credentials entered on the WLSE do not exactly match the data entered in Devices > Discovery > Device Credentials > Telnet/SSH User/Password.

Recommended Action Make sure that the Telnet/SSH credentials data entered on the WLSE show the correct device login response. Match the device login sequence with the credential fields, as shown in Symptom Firmware jobs fail because the Telnet/SSH credentials are not valid., page 1-32.

Firmware FAQs and Troubleshooting

- Firmware FAQs, page 1-27
- Firmware Troubleshooting, page 1-29

Note For troubleshooting information on converting non-IOS access points to IOS, see the document *Converting Access Points to IOS* on Cisco.com.

Firmware FAQs

- Q.How can firmware images be imported?
- Q.Are firmware jobs run by using both HTTP and SNMP?
- Q.What kinds of job logs are available?
- Q.How many devices can I have in one firmware job?
- Q.Can I give a firmware job a name that is used for a configuration or radio management job?

Q. How can firmware images be imported?

A. Firmware images can be imported to WLSE from the desktop as well as Cisco.com. While importing any image from Cisco.com, the WLSE reads the version string and the device type for the image attributes. For imports from the desktop, you must make sure that the version and the device type strings are correctly entered in the image attributes. For example, for an AP 350, image version 12.00T, the image string must be entered as 12.01T; not 12.0 or 12.01 or 12.0T.

Q. Are firmware jobs run by using both HTTP and SNMP?

A. Non-IOS firmware jobs use both HTTP and SNMP protocols. IOS firmware upgrades and conversion from non-IOS to IOS use SNMP only.

- **Non-IOS firmware upgrades:**
  - HTTP is valid for all supported device versions. The following setup parameters must be in place for HTTP to function properly:

    HTTP credentials for the device (with admin and firmware privileges on the AP) must match those entered on the WLSE HTTP device credentials screen.

    TFTP server settings on the access point must reference the WLSE's IP address.

Note Both username and password in the device credentials are case sensitive.

- SNMP is valid for versions 12.01T and later. The following setup parameters must be in place for SNMP to function properly:

  SNMP credentials for the device (with admin and firmware privileges on the AP) must match those entered on the WLSE SNMP device credentials screen.

  There is no need to change TFTP server settings for the SNMP mechanism, although you can use the SNMP mechanism to change the TFTP server settings on the AP to be used in the HTTP mechanism. Enter valid credentials in the **Security > Local Admin Access** template screen.

Note NOTE: Make sure you provide a numeric value in the user ID field (template screen).

- **IOS firmware upgrades** (for information on conversion from non-IOS to IOS, see *Converting Access Points to IOS, 2.7*). Use SNMP only and make sure the following setup parameters are in place before running the upgrade job:

  SNMP credentials for the device (with admin and firmware privileges on the AP) must match those entered on the WLSE SNMP device credentials screen.

Q. What kinds of job logs are available?

A. There are two kinds of job logs: Job run log and the jobvm log.

- The job run log is where events are logged for a particular job's run. This log can be used to check what went wrong with the job and make any required corrections. The job run log can be viewed by selecting a particular job from the job list, then clicking **Job Run Detail**. From the window that pops up, select a particular run for the job, then click **Job Run Log**.
- The jobvm.log is a global log for all types of jobs. It is used mainly for development troubleshooting. The jobvm.log can be viewed by selecting **Administration > Appliance > View Log File**, then clicking **jobvm.log**.

Q. How many devices can I have in one firmware job?

A. There is no limit, although it is recommended that you work with device groups and set up jobs accordingly (for example, by location or building). The WLSE can run 10 jobs in parallel. While a job is running, the WLSE allocates resources for updating 20 devices in parallel. At any given time, 20 devices will be upgrading and the remainder will be waiting for resources to become available.

Creating a single job with more than 100 access points is not recommended. If you are updating the firmware on a large number of access points (especially if you are converting non-IOS access points to IOS), you might want to convert a few APs initially to get familiar with the process. Once you are familiar with the process, you can create a job with 20 devices, then increase the number of devices if no devices are failing. By running a smaller job, you will also know how much time it takes for the job to complete.

Q. Can I give a firmware job a name that is used for a configuration or radio management job?

A. No. Job names cannot be duplicated.

Firmware Troubleshooting

- Symptom When uploading an image to an access point from a from a remote TFTP server, the access point reports an Invalid checksum error or Unknown failure.
- Symptom There is a time discrepancy in a job.
- Symptom Email about job completion fails to arrive at destination.
- Symptom Firmware is not updated on all the devices included in a job.
- Symptom An SNMP job fails.
- Symptom A firmware job ends with status “not verified.”
- Symptom Firmware jobs over slow links do not succeed.
- Symptom When downloading firmware from Cisco.com, an error message about cryptography permissions appears.
- Symptom When downloading firmware from Cisco.com, an error message about connectivity failure appears.
- Symptom Firmware jobs fail because the Telnet/SSH credentials are not valid.

Symptom When uploading an image to an access point from a from a remote TFTP server, the access point reports an Invalid checksum error or Unknown failure.

Possible Cause The image filename entered in the job does not match the image filename on the remote TFTP server.

Recommended Action Make sure the filenames on the job and on the server are the same.

Symptom There is a time discrepancy in a job.

Possible Cause The time was not set correctly on the WLSE.

Recommended Action

a. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows:

   Enter **services stop** to stop services.

   Enter the **clock** command to reset the time.

   Enter **services start** to restart the services.

b. Set the time in local browser time, select Administration > Appliance > Time/NTP/Name.

For more information on setting the time, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE’s online help.

Symptom Email about job completion fails to arrive at destination.

Possible Cause The SMTP server is not specified.

Recommended Action Configure the mail route by selecting Administration > Appliance > Configure Mailroute.

Symptom Firmware is not updated on all the devices included in a job.

Possible Cause There were warnings displayed when the job was saved. Jobs for devices with warnings do not run; the job runs only for devices that do not have any warnings.

Recommended Action Solve the problems indicated in the warning messages before running the job.

Possible Cause If two firmware jobs were scheduled closely together, the second job contained some of the same devices as the first job. Those devices could not be updated because the first job was already running.

Recommended Action It is recommended that firmware jobs be run on groups of devices. Each group should be exclusive; that is, no device should be a member of more than one group.

For more information on updating firmware, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

Symptom An SNMP job fails.

Possible Cause The read community string does not have sufficient permissions.

Recommended Action The access point must have a user with at least SNMP, FIRMWARE, and ADMIN permissions for read-only access.

Access points with software releases prior to 12.01(T) must have a user with SNMP, FIRMWARE, ADMIN, and IDENT permissions for read-only access.

Symptom A firmware job ends with status "not verified."

Note The "not verified" status may not mean that the job has failed. The WLSE may time out before confirming whether the upgrade succeeded. To make sure, you can run an on-demand inventory on the devices in question to find out whether the firmware upgrade was installed. For more information, see the Inventory online help, or select Devices > DISCOVER > Inventory > Run Inventory Now.

Possible Cause The device may be taking a long time to reboot.

Caution Do not take the following action for firmware jobs that you are running to convert non-IOS access points to IOS. See the special conversion instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*.

Recommended Action Increase the value of the Device Reboot Wait Timeout parameter by accessing the WLSE through the following URL:

http://*your_wlse*:1741/debug/jobprops.jsp

where *your_wlse* is the name of the WLSE.

Increase the value of the Device Reboot Wait Timeout parameter and run the job again.

Note Do not make this value extremely high. It is advisable to keep this value to something slightly higher than the actual reboot time of the slowest access point.

Symptom Firmware jobs over slow links do not succeed.

Possible Cause The access points being upgraded are connected to the WLSE over a slow link (less than 1.544 Mbps) and the job is timing out.

Caution Do not take the following action for firmware jobs that you are running to convert non-IOS access points to IOS. See the special conversion instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*.

Recommended Action

a. Access the WLSE through the following URL:

   http://*your_wlse*:1741/debug/jobprops.jsp

b. Increase the value of the Per device job operation timeout parameter. For example, for a 56kbps link, the recommended value is 2400 seconds (40 minutes). On a 128kbps link, the recommended value is 1200 seconds (20 minutes).

Symptom When downloading firmware from Cisco.com, an error message about cryptography permissions appears.

Possible Cause The first time you attempt to download firmware, the WLSE displays this message: `Error while selecting or displaying image details. Please log into cisco.com and make sure your username has acknowledged cryptography permissions for downloading IOS images.`

Recommended Action Log into Cisco.com and acknowledge the cryptography permissions. After you have acknowledged these permissions, you can import IOS images to the WLSE.

Symptom When downloading firmware from Cisco.com, an error message about connectivity failure appears.

Possible Cause DNS is not configured on the WLSE.

Recommended Action Configure DNS on the WLSE and make sure the WLSE can resolve the cisco.com domain name. For information about configuring DNS, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9* or the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Symptom Firmware jobs fail because the Telnet/SSH credentials are not valid.

Possible Cause The credentials entered on the WLSE do not exactly match the data entered in **Devices > Discovery > Device Credentials > Telnet/SSH User/Password**.

Recommended Action Make sure that the Telnet/SSH credentials data entered on the WLSE show the correct device login response. Match the device login sequence with the credential fields as follows.

Table 1-4 Telnet/SSH Credentials Required

Device Login Sequence	Telnet Credential Fields Required

`Username:`
`Password:`
`prompt>`**`enable`**
`Password:`
`enable prompt #`
	User Name
	User Password
	Enable Password

`Password:`
`prompt>`**`enable`**
`Password:`
`enable prompt#`
	User Password
	Enable Password

`Username:`
`Password:`
`enable prompt#`
	User Name
	User Password

`enable prompt#`	(no credentials required)

`Username:`
`prompt>`**`enable`**
`Password:`
`enable prompt#`
	User Name
	Enable Password

`Username:` `prompt#`	User Name

`Username:`
`Password:`
`prompt>`**`enable`**
`Username:`
`Password:`
`enable prompt#`
	User Name
	User Password
	Enable User Name
	Enable Password

Reports FAQs and Troubleshooting

- Reports FAQs, page 1-33
- Reports Troubleshooting, page 1-33

Reports FAQs

Q. Are any of the Current or Trend reports real-time reports?

A. The reports are not real time. They are based on data that is collected periodically. The frequency with which the data is collected is user configurable (see Devices > Discover > Inventory > Polling). The data shown in reports is as current as the time the data was collected from the devices.

Q. In the Group Performance Report: RF Utilization, how is the value in the As Of column calculated?

A. The As Of column indicates the starting time of the aggregation for the utilization report. Therefore, the starting time shown might be earlier than the date range selected for the report.

Reports Troubleshooting

- Symptom The Top N Busiest Clients report and the Client Statistics report display 0 (zero) values.
- Symptom Some report fields are blank.
- Symptom The client association data in the Group Client Association report differs from the data shown in the Current Client Associations report.
- Symptom The access point data in the Historical Associations report is not accurate.
- Symptom The Summary and/or Detailed report for access points is empty.
- Symptom The group report for a user-defined group contains no data.
- Symptom After running a job, the updated data does not appear in a report.
- Symptom Email fails to arrive at its destination.
- Symptom There is a time discrepancy in the scheduled email jobs.
- Symptom No VLAN information is displayed for IOS access points.
- Symptom There is a discrepancy in the first aggregation intervals after the first time the WLSE starts up or after the WLSE's software is upgraded.

Symptom Real-time reports will not launch.

Possible Cause Proxy is set.

Recommended Action Remove proxy settings.

Symptom The Top N Busiest Clients report and the Client Statistics report display 0 (zero) values.

Possible Cause Wireless client polling frequency is set to 51 minutes by default. The counters could reset between two polling cycles which would cause zero values when the reports are run.

Recommended Action Increase the polling frequency by selecting Devices > Discover > Inventory > Polling.

Caution Increasing the polling frequency could have an effect on performance.

Symptom Some report fields are blank.

Possible Cause The device is not configured properly for management by the WLSE; the ISO view has not been created.

Recommended Action See Symptom Access points are placed in Misconfigured Devices group after discovery and dot11mib fault is displayed., page 1-18 for information about how to correct the problem.

Symptom The client association data in the Group Client Association report differs from the data shown in the Current Client Associations report.

Possible Cause The data for the Group Client Association report is collected using performance attributes polling and the data shown in the Current Client Association report uses wireless client polling.

Whichever report has a higher polling frequency will contain the most up to date data. Select Devices > Discover > Inventory > Polling to view polling frequency.

Recommended Action None.

Symptom The access point data in the Historical Associations report is not accurate.

Possible Cause The wireless client was associated with an access point managed by the WLSE, but subsequently associated with an access point that was added to the network, but not yet managed by the WLSE.

Recommended Action Verify that the associated access points are in the managed devices folder by selecting Devices > Discover > Managed Devices > Manage/Unmanage.

Symptom The Summary and/or Detailed report for access points is empty.

Possible Cause The SNMP user may not have the correct rights assigned.

Recommended Action

a. Open a browser window to the access point, and select Setup > Security > User Information.
b. Make sure that the user corresponding to the SNMP community (which is set up in WLSE in Discovery > Device Credentials) has been granted rights for the following: Ident, firmware, admin, snmp, and write.

c. If not, click on the user and assign all these rights.

Symptom The group report for a user-defined group contains no data.

Possible Cause Reports cannot be displayed for a user-defined group that contains another group.

Recommended Action Display individual reports for the sub-groups or devices within the user-defined group.

Symptom After running a job, the updated data does not appear in a report.

Possible Cause A full polling cycle has not completed and the new data has not been entered in the database.

Recommended Action Verify that the polling cycle has completed as follows:

a. Select Administration > Appliance > Status > View Log File.
b. Click **jobvm.log**.
c. Scroll through the log to find the message: “Finished Inventory” for your particular job.

Symptom Email fails to arrive at its destination.

Possible Cause The SMTP server is not configured properly.

Recommended Action Configure the SMTP server by selecting Administration > Appliance > Configure Mailroute.

Symptom There is a time discrepancy in the scheduled email jobs.

Possible Cause The time is not set correctly on the WLSE.

Recommended Action

a. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows:

   Enter **services stop** to stop services.

   Enter the **clock** command to reset the time.

   Enter **services start** to restart the services.
b. Set the time in local browser time, select Administration > Appliance > Time/NTP/Name.

Symptom No VLAN information is displayed for IOS access points.

Possible Cause WEP keys have not been configured in each VLAN. When the WEP keys are configured in the IOS access points, VLAN information is accessible by SNMP.

Recommended Action Configure the WEP keys for the corresponding VLAN.

Symptom There is a discrepancy in the first aggregation intervals after the first time the WLSE starts up or after the WLSE's software is upgraded.

Possible Cause This is because the very first aggregations are based on the day and time that the WLSE's system software was installed, and the formula for computing the next aggregation is causing this discrepancy.

Recommended Action No action is required. Subsequent aggregations will occur at the normal intervals.

Radio Manager FAQs and Troubleshooting

- Radio Manager FAQs
- Radio Manager Troubleshooting

Radio Manager FAQs

Note For more frequently asked questions about using the Radio Manager, see the "Managing Your WLAN Radio Environment" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

Configuration

- Q.For each AP to report radio information back to WLSE, does each AP need to be configured as a WDS AP?
- Q.If so, do I need a separate username and password for each? If not, how many WDS APs would I need?
- Q.Do I need a separate Infrastructure SSID for the APs that are configured as WDS?

Collecting RM Data

- Q.How does AP Radio Scan affect an access point's performance?
- Q.Is there a problem if Radio Monitoring is always disabled?

Radio Parameter Generation

- Q.When Radio Manager is trying to calculate new radio parameter generations, why do I get an error about walkabout locations?

Detecting Rogue APs

- Q.How does WLSE detect rogue APs?
- Q.How often does rogue AP detection occur and can it be customized?
- Q.Can I disable transmit on an AP and yet allow it to receive signals so that it can participate in rogue AP detection?
- Q.I want to disable Radio Monitoring and detect rogue APs only when AP Radio Scan jobs are scheduled. Is this possible?

- Q.What requirements and configuration are needed before a client can participate in rogue AP detection?
- Q.Can the client be used to help triangulate a rogue AP?
- Q.How can I automatically adjust the channel and power settings on my managed APs to overcome the coverage problems introduced by rogue APs?
- Q.I understand that WLSE does not accept SNMP traps that indicate an AP detected a rogue. So why is an AP that is currently designated as the WDS generating rogue AP SNMP traps?

Interference Detection

- Q.Are the Network-Wide > Interference Detection settings of -87dbm for 10% always the same, or are they the optimal recommended values, or are they calculated depending on the environment? Should they be left alone, or are there any recommendations?

APs in Scanning-Only Mode

- Q.Why are the APs running in scanning-only mode having problems with sporadic connection loss and image upgrade failure?

Self Healing

- Q.How do “Hot Standby” and “Self-Healing” work together?
- Q.Self-Healing takes 15 minutes to cover for a failed AP, which is not suitable for a mission critical environment. Are any time tuning parameters available?
- Q.In a centralized deployment where WLSE is located in a central location and wireless network is being managed across the WAN, how does Self Healing behave when there is a WAN failure?

Miscellaneous

- Q.Can I give a radio management job a name that is used for a firmware or configuration management job?
- Q.Can I use a non-Cisco RADIUS server with radio management?

Configuration

Q. For each AP to report radio information back to WLSE, does each AP need to be configured as a WDS AP?

A. No, one WDS AP must be configured for each AP subnet. The WDS APs should be configured to know about WLSE.

For example, if you have 3 AP subnets in a building, you must set up 3 APs as WDS APs. Those 3 APs must be configured with the IP of the WLSE, and the non-WDS APs must be configured with the WLCCP username and password. These configuration settings will allow the APs to send information to the WDS APs, which the WDS APs will then forward to WLSE.

Note You could also set up a WLSM (Wireless LAN Services Module) device to manage your APs. One WLSM-WDS device can manage multiple AP subnets.

Q. If so, do I need a separate username and password for each? If not, how many WDS APs would I need?

A. No, you do not need a separate username and password for each. Each WDS AP (either 1100 or 1200) supports up to 30 APs.

Q. Do I need a separate Infrastructure SSID for the APs that are configured as WDS?

A. No, the infrastructure SSID configuration does not need to be altered.

Collecting RM Data

Q. How does AP Radio Scan affect an access point's performance?

A. With all the APs configured to the same channel and at maximum power, there is some degradation in throughput. Also, while the APs step through their various power settings, there may be some loss of coverage. This only lasts for the length of the AP scan (3to 4 minutes).

Q. Is there a problem if Radio Monitoring is always disabled?

A. If you disable Radio Monitoring, you will not have access to these features: continuous detection of rogue APs, self-healing networks, auto re-site surveys, and certain Radio Manager reports.

Q. Is the WDS radio required to be up during an AP radio scan?

A. No, but if the WDS radio is not up, the WDS will not be part of the radio scan. If you do include the WDS radio interface in the scan job, you will see some timeouts from this interface in the logs, but the scan will work on the other interfaces as expected. If you are not using a WDS to serve clients, you can turn off the radio to exclude this interface from the scan task.

Radio Parameter Generation

Q. When Radio Manager is trying to calculate new radio parameter generations, why do I get an error about walkabout locations?

A. Before Radio Manager can generate radio parameters, you must have previously collected client walkabout data or you must have defined the dimensions of your building and floor(s). If you receive an error, make sure you have entered the correct building and floor dimensions using the Building and Floor Edit Tool in Location Manager and then try running the parameter generation again.

Detecting Rogue APs

Q. How does WLSE detect rogue APs?

A. Here is a brief summary of the rogue AP detection logic:

a. A rogue AP appears and starts sending out beacons and responding to probe-requests.

b. A nearby *managed* and *RM-enabled* AP or client detects the beacon (same channel or off-channel) or probe response (off-channel). The AP or client sends back a beacon report of the rogue AP in the next scheduled RM report. The scheduled internal RM reporting interval is 90 seconds, so this step can take up to 90 seconds to complete.

c. The WLSE Radio Manager (RM) receives the beacon report, recognizes that this AP is not in the system (not a managed AP, and not a previously detected radio), and triggers the rogue AP switch-port tracing logic. The WLSE RM does not issue a rogue AP fault at this time.

d. The WLSE RM waits for 3 measurement intervals (3x90, or 270 seconds) for other surrounding APs or clients to report the same radio. This delay allows as many APs as possible to detect the rogue and helps pinpoint the rogue's location (which is reported in Step e.) When other APs or clients detect this radio, the reporting AP and the reported RSSI of the rogue AP are stored or

updated in the WLSE RM database. This period of time also allows the switch port tracing logic to try to locate the switch port to which this rogue AP might connect. This logic happens in parallel. Depending on the size of the network, the switch port tracing logic may or may not finish before the end of this interval (270 seconds).

e. The WLSE RM issues a rogue AP fault. These first steps (b - e) can take from 270 to 360 seconds (3x90 to 4x90) to generate a fault against a particular rogue AP. After the fault has been generated, the fault notifications follow the standard WLSE fault notification process. (You must set up the e-mail notification to receive it.) The fault details page is updated so that when you click on the rogue AP's location, the system will have enough information (if it is available) to do a location triangulation based on the RSSI from the different reporting APs.

f. The AP or client continues to update the rogue AP's RSSI, and the Radio Manager continues to update this information in the WLSE. This allows the WLSE to keep the rogue AP's location current and not limited to the position when it was first detected.

Q. How often does rogue AP detection occur and can it be customized?

A. Rogues can be detected within 90 seconds, but are not reported for another 180 seconds. This delay allows as many APs as possible to detect the rogue, which helps pinpoint the rogue's location. Detection frequency cannot be customized, but rogue AP detection and the fault priority that is assigned can be enabled and disabled for the network.

Q. Can I disable transmit on an AP and yet allow it to receive signals so that it can participate in rogue AP detection?

A. The solution you want is called scanning-only AP mode. Scanning-Only AP mode puts a radio interface in a dedicated mode monitoring the air space surrounding it without carrying any regular WLAN user traffic. For more information, see the scanning-only AP mode information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*.

Q. I want to disable Radio Monitoring and detect rogue APs only when AP Radio Scan jobs are scheduled. Is this possible?

A. Radio Monitoring is the preferred method for detecting rogue APs. AP Radio Scan jobs can detect rogues, but only during the scan (approximately 3 to 4 minutes); any rogues that show up after the scan are not detected. In addition, because the scan is so short, it is possible that some rogues will not be detected because they do not respond with a Probe Request during the active scan. When Radio Monitoring is enabled, the rogue will eventually be detected by the beacon frame; it is statistically possible that a beacon will not be seen during an AP scan.

Q. What requirements and configuration are needed before a client can participate in rogue AP detection?

A. Participation is automatic. Cisco and CCX clients gather radio frequency information as instructed by the APs to which they are associated. APs gather similar information. This data is aggregated at the WDS device and then analyzed by the WLSE.

Q. Can the client be used to help triangulate a rogue AP?

A. The client's data does not get factored into location triangulation; only the AP data is used.

Q. How can I automatically adjust the channel and power settings on my managed APs to overcome the coverage problems introduced by rogue APs?

A. To automatically adjust channel and power settings on managed APs after detecting rogue APs, run RM Assisted Configuration (or Auto Site Survey from the Location Manager wizard).

Q. I understand that WLSE does not accept SNMP traps that indicate an AP detected a rogue. So why is an AP that is currently designated as the WDS generating rogue AP SNMP traps?

A. The AP is generating the detected rogue trap, not the WDS functionality currently operating within the AP. This trap is based on authentication tattletale rogue detection, which is currently not reported to the WLSE.

WLSE uses radio measurements to detect the rogues. The authentication tattletale method uses a message sent from a participating client that indicates some type of authentication issue with some other AP. This other AP is considered to be rogue for one of these reasons:

- The rogue was not running 802.1x.
- Authentication with the rogue timed out.
- Bad user password.
- Authentication challenge failed.

This tattletale method is enabled on the AP itself, detected by the AP, and flagged at the AP via the trap.

Interference Detection

Q. Are the **Network-Wide > Interference Detection** settings of -87dbm for 10% always the same, or are they the optimal recommended values, or are they calculated depending on the environment? Should they be left alone, or are there any recommendations?

A. This is the default setting. If it is not adequate, you will need to experiment to find the proper setting for your environment.

APs in Scanning-Only Mode

Q. Why are the APs running in scanning-only mode having problems with sporadic connection loss and image upgrade failure?

A. In a heavy-load environment, APs running in scanning-only mode may face sporadic connection loss and image upgrade failure. To resolve these problems, use the following configuration commands to balance CPU time:

```
scheduler interval <100-xxx>
scheduler allocate <3000-xxx> <1000-xxx>
```

Many newer Cisco platforms use the command **scheduler allocate** instead of **scheduler interval**. The scheduler allocate command takes two parameters: a period in microseconds for the system to run with interrupts enabled, and a period in microseconds for the system to run with interrupts masked. Please refer to the IOS documentation for more information about these commands.

Self Healing

Q. How do “Hot Standby” and “Self-Healing” work together?

A. Hot Standby allows the customer to keep a redundant standby AP set for a primary AP. Then, if the primary AP goes down, the standby will take over—presumably, with the same or similar settings—to allow for no loss in coverage.

With Self Healing, the WLSE monitors the wireless network and if it determines a radio is down, it modifies the power settings of neighboring APs in an attempt to maintain the coverage.

If both Hot Standby and Self Healing are deployed, then Hot Standby takes precedence over Self Healing. In this case, Self Healing does not modify the neighboring APs unless the standby becomes the primary AP *and* that AP goes down as well (a double failure).

Q. Self-Healing takes 15 minutes to cover for a failed AP, which is not suitable for a mission critical environment. Are any time tuning parameters available?

A. The key issue here is determining the difference between a radio that is down and a radio that cannot be heard. This involves the radio monitoring interval, some reasonable time period, and the overhead on the APs themselves. The 15 minute time period is a setting that is thought would balance the needs for a timely response, versus false reports, versus the reporting overheard on the APs.

That said, we can tune the settings with engineering assistance if *absolutely necessary*. It will require experimentation with different settings if you want to try a setting faster than the tested 15 minutes.

Q. In a centralized deployment where WLSE is located in a central location and wireless network is being managed across the WAN, how does Self Healing behave when there is a WAN failure?

The Self Healing feature runs on the WLSE, which means that the downed radio determination is evaluated on the WLSE. The data for this determination is provided to the WLSE over the wired network via the WDS and SWAN architecture. The power setting changes are initiated from the WLSE and deployed over the wired network as well. If there is a prolonged WAN failure between the WLSE and the wireless network under management, the WLSE cannot provide the Self Healing feature.

Miscellaneous

Q. Can I give a radio management job a name that is used for a firmware or configuration management job?

A. No. Job names cannot be duplicated.

Q. Can I use a non-Cisco RADIUS server with radio management?

A. A RADIUS server that supports LEAP is required for infrastructure authentication. RADIUS servers other than Cisco ACS have not been extensively tested. Problems have been observed with the Funk Steel Belt Server.

If you do not want to turn on LEAP in your RADIUS server and you are using AP-based WDS (not WLSM-based WDS), you can turn on the Local Authentication Server (LAS) software feature on the WDS AP. Then you can use LAS for infrastructure authentication via LEAP while using the external AAA server with non-LEAP authentication for client authentication.

If you use the approach outlined above, you will need to enter the security credential of the WLSE into each LAS (WDS AP).

If you have many subnets with WDS APs, it will be easier to use a centralized AAA server with LEAP turned only only for SWAN infrastructure authentication. Use AES, PEAP, or a more advanced security scheme for client authentication.

Radio Manager Troubleshooting

- Symptom WDS has been set up on the AP and WLSE, but WDS isn't authenticating with WLSE.
- Symptom My clients are not being authenticated through WDS.

- Symptom ERROR: Aborting execution of AP Scanning task because there are no applicable Radio Interfaces that can participate.

Symptom WDS has been set up on the AP and WLSE, but WDS isn't authenticating with WLSE.

The “Not Authenticated” you see in response to the “show wlccp wds ap” command means that the WDS component has not authenticated the WLSE. There are two possible causes:

Possible Cause The device credentials in the WLSE are not correct. The user name and password should match the user names and passwords entered on the WDS AP and the AAA server.

Recommended Action To correct the credentials:

1. Select **Devices > Discover > Device Credentials > WLCCP Credentials**.
2. Change the **Radius User Name** and **Radius Password** fields to match the user names and passwords entered on the WDS AP and the AAA server.

Possible Cause The WDS AP has not been managed in the WLSE.

Recommended Action To manage the WDS AP:

1. Select **Devices > Discover > Managed/Unmanaged**.
2. Look in the **New** folder for your WDS AP.
3. Select it, then select **Manage**. The process will take 1-2 minutes.

After the WLSE is authenticated by the WDS, the WDS reports its member APs to the WLSE, so they are “discovered” by the WLSE. After these member APs have been discovered, you will need to manage them as well.

Symptom My clients are not being authenticated through WDS.

Possible Cause You have not created a server group on the WDS for client authentication.

Recommended Action To create a server group on the WDS for client authentication, you can use the AP CLI, the AP web interface, or the WLSE configuration templates for an AP-WDS, or the WLSM CLI for a WLSM-WDS. For more information, see the device setup information in the online help or the User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9.

Symptom ERROR: Aborting execution of AP Scanning task because there are no applicable Radio Interfaces that can participate.

Possible Cause This error message says that the AP scan is ending because there are no interfaces capable of participating in the scan. It is always included with one or more messages that describe why a given interface was removed from the scan. For example:

```
WARNING: Skipping device 172.xx.xx.xxx because it is not registered with any WDS
```

Recommended Action There are quite a few reasons why an interface might be removed from the scan. The WLSE examines each interface separately; after that, if all interfaces have been removed, this error is displayed.

Location Manager FAQs and Troubleshooting

- Location Manager FAQs
- Location Manager Troubleshooting

Location Manager FAQs

General

- Q.Is there is a size limitation for the building image that can be imported in Location Manager?
- Q.Why does Location Manager show a coverage map for an AP based on the configured transmit power setting even when the radios are shut down?
- Q.In Location Manager > Rogue > Unknown Radio List, why does the Switch IP Address field say Unknown?

Assisted Site Survey Wizard

- Q.Why don’t I see the building or floor node in the device tree in the Assisted Site Survey Wizard?
- Q.Why don't I see the device that I am looking for in the Assisted Site Survey device tree?
- Q.When I select devices in the Assisted Site Survey Wizard, why are some shown in red?
- Q.When I’m using the Assisted Site Survey Wizard, why is the Next button disabled after I complete step one?
- Q.In the Assisted Site Survey Wizard, why is Use Old Radio Scan Data disabled?
- Q.In the Assisted Site Survey Wizard, what does None mean in the Last Scan Time field?
- Q.In the Assisted Site Survey Wizard, why is the Next button disabled on the radio scan step?
- Q.Why did my radio scan job fail in the Assisted Site Survey Wizard?
- Q.When I’m using the Assisted Site Survey Wizard, the radio scan progress advances very slowly. How long does it radio scan normally take?
- Q.Can I skip client walkabout in the Assisted Site Survey Wizard even though the number of data shown is zero?
- Q.In the client walkabout step in the Assisted Site Survey Wizard, what is the Recall button for?
- Q.What is the difference between the Number of Location Data and Number of New Location Data fields?
- Q.In the Constraints and Goals step in the Assisted Site Survey Wizard, how do I select multiple channels in the channel list?
- Q.How long should the Constraints and Goals calculation step take in the Assisted Site Survey Wizard?
- Q.Where can I see the result of the Constraints and Goals calculation in the Assisted Site Survey Wizard?
- Q.If I don't like result of the Constraints and Goals calculation in the Assisted Site Survey Wizard, what can I do?
- Q.When I apply the configuration in the Assisted Site Survey Wizard, where do I see the results?
- Q.In the last step of the Assisted Site Survey Wizard, why is the Next button disabled?

General

Q. Is there is a size limitation for the building image that can be imported in Location Manager?

A. Although there is no limit on the file size for each image, for the best performance we suggest that the image file be less than 300KB. For optimal performance, if the image file was created using a graphic editing application, save the file for use as a "web image" if possible.

Q. Why does Location Manager show a coverage map for an AP based on the configured transmit power setting even when the radios are shut down?

A. Even when a radio is turned off, it still has a configured transmit power. The coverage display is calculated from the WLSE RM database (populated by AP radio scan, client walkabout, and RF monitoring) using a calibrated path loss model. What the display represents is an estimation of the coverage area based on the RM data, assuming the radio is turned on.

Q. In **Location Manager > Rogue > Unknown Radio List**, why does the Switch IP Address field say Unknown?

Recommended Action If the switch IP address is *Unknown*, the IP address of the switch that the unknown radio is connected to could not be determine. To find the switch port to which the rogue AP is connected, the Switch Port Location feature uses the rogue AP's BSSID that it hears over the air to make a heuristic guess of the rogue's Ethernet MAC address. This might not be possible, however, if its Ethernet MAC address and BSSID do not follow the one-off rule, where the MAC address is the same or one-off of the BSSID. For more information, see the Understanding Switch Port Location and Suppression section in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*.

Assisted Site Survey Wizard

Q. Why don't I see the building or floor node in the device tree in the Assisted Site Survey Wizard?

A. Expand the building node to see all floors that belong to the building. If you expand the building node and the floors still do not appear, close the Wizard and make sure the building and floor exist in the Location Manager navigation tree. If the building or floor does not exist in the Location Manager navigation tree, you first need to create them and then restart the Assisted Site Survey Wizard. See the topic Adding Building Information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*.

Q. Why don't I see the device that I am looking for in the Assisted Site Survey device tree?

A. Expand the building and floor nodes to see all devices that belong to a building or floor. If the device still does not appear, close the Assisted Site Survey Wizard and make sure the device appears in the Location Manager navigation tree. If the device does not appear in the Location Manager navigation tree, select **Tools > Find Device** to locate it. If you find the device, move it to the desired location. See the topic Adding Devices to the Floor Map in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*. If the device does not appear in Location Manager, it might not have been discovered by the system. See the topic Managing Device Discovery in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*. After adding the device and specifying its location, restart the Assisted Site Survey Wizard.

Q. When I select devices in the Assisted Site Survey Wizard, why are some shown in red?

A. The devices might be red if:

- The devices are not in the Managed state. Select Devices > Discover > Manage/Unmanage to verify that the devices are Managed.

- The devices are not in infrastructure mode. Go to the configuration for the individual device and verify that it is in "Infrastructure Mode" with the proper WDS assigned.

Q. When I'm using the Assisted Site Survey Wizard, why is the **Next** button disabled after I complete step one?

A. You have not selected any acceptable devices that are required for the next step. If any of the selected devices are shown in red, you need to deselect them before you can go to the next step.

Q. In the Assisted Site Survey Wizard, why is **Use Old Radio Scan Data** disabled?

A. You might not have previously run radio scan for the selected devices. You must start a new radio scan.

Q. In the Assisted Site Survey Wizard, what does *None* mean in the Last Scan Time field?

A. The selected device was not included in a previous radio scan.

Q. In the Assisted Site Survey Wizard, why is the **Next** button disabled on the radio scan step?

A. You need to run radio scan by clicking **Start**. When the radio scan is complete, you will be able to click **Next**.

Q. Why did my radio scan job fail in the Assisted Site Survey Wizard?

A. Look at the log window to find out exact failure cause. If radio scan failed:

- Make sure the devices have the correct setup for WDS. Also verify that WDS is authenticated to WLSE and that WDS has an IP address pointing to WLSE.
- Make sure the devices have the correct SNMP read/write community strings that match the WLSE setting.

Q. When I'm using the Assisted Site Survey Wizard, the radio scan progress advances very slowly. How long does it radio scan normally take?

A. Radio scan normally takes about 5 to 10 minutes to complete. If you suspect the program has stalled, check its status by selecting Radio Manager > AP Radio Scan and viewing the progress of the job.

Q. Can I skip client walkabout in the Assisted Site Survey Wizard even though the number of data shown is zero?

A. Yes, you can skip client walkabout. However, performing a client walkabout will generate better parameters for your wireless network.

Q. In the client walkabout step in the Assisted Site Survey Wizard, what is the **Recall** button for?

A. You can click **Recall** to display a list of the last five client MAC addresses that were used for the previous client walkabout. To retrieve a previously used MAC address, click **Recall** and select a MAC address from the list.

Q. What is the difference between the **Number of Location Data** and **Number of New Location Data** fields?

A. Number of Location Data is the total number of data found by client walkabout for the current session plus any previous sessions. Number of New Location Data is the total number of data found by client walkabout for the current session only. The numbers in these two fields can increase at the same time during a client walkabout.

Q. In the Constraints and Goals step in the Assisted Site Survey Wizard, how do I select multiple channels in the channel list?

A. For Windows users, control-click on the channels to add them to the selection. The selected channels are highlighted.

Q. How long should the Constraints and Goals calculation step take in the Assisted Site Survey Wizard?

A. It varies depending on the amount of radio scan and client walkabout data. The more data you have, the longer it will take to calculate.

Q. Where can I see the result of the Constraints and Goals calculation in the Assisted Site Survey Wizard?

A. If the calculation was successful, you can click **Next** to view the result.

Q. If I don't like result of the Constraints and Goals calculation in the Assisted Site Survey Wizard, what can I do?

A. Go back and specify different constraints and goals, and then recalculate the constraints and goals.

Q. When I apply the configuration in the Assisted Site Survey Wizard, where do I see the results?

A. Check Location Manager to view the configuration changes. You might need to refresh the Location Manager window by selecting View > Refresh Data. In rare cases, the wizard might have failed to apply the configuration. In that case, check your SNMP settings, particularly the WRITE community string, for the devices.

Q. In the last step of the Assisted Site Survey Wizard, why is the **Next** button disabled?

A. This is the last step in Assisted Site Survey Wizard. You can close the Wizard unless you want to repeat any previous steps.

Location Manager Troubleshooting

This section contains the following troubleshooting information:

- Symptom Location Manager does not display the location of an AP I know to be a rogue because the AP is reported to be in an unknown location.
- Symptom After completing the Assisted Site Survey, Location Manager did not update to include the applied configurations.
- Symptom It takes a very long time to import a building or floor image in to Location Manager.
- Symptom AP coverage is not displaying in Location Manager .
- Symptom When selecting View > Radio Band > Show 2.4 GHz, Location Manager does not refresh to show the 2.4 GHz radios.
- Symptom The Location Manager cannot be launched when using the Mozilla browser.

Symptom Location Manager does not display the location of an AP I know to be a rogue because the AP is reported to be in an unknown location.

Possible Cause The rogue AP was detected by APs whose locations were not specified in Location Manager, or the locations of the reporting APs were specified after the detection of the rogue AP.

Recommended Action In the Unknown Radio List window, determine which APs reported the detection. Make sure you have placed the reporting APs on a particular floor in Location Manager. Turn on Radio Monitoring for the reporting APs and after they detect the same rogue AP, the possible location of the rogue AP will be available.

Symptom After completing the Assisted Site Survey, Location Manager did not update to include the applied configurations.

Possible Cause You did not refresh the Location Manager window.

Recommended Action In the Location Manager window, select **View > Refresh** Data.

Symptom It takes a very long time to import a building or floor image in to Location Manager.

Possible Cause The resolution and pixel size of the image file is very large.

Recommended Action Because the larger an image resolution is, the longer it takes to upload to the server and the more memory it uses, it is recommended that your building and floor images be less than 1,000x1,000 pixels.

Symptom AP coverage is not displaying in Location Manager .

Possible Cause You have not imported an image map for the floor and did not enter the floor dimensions in the Building Tool.

Recommended Action Import an image map for the floor or if you do not want to use an image map, enter the floor dimensions in the Building Tool. For more information, see the instructions for adding building information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*.

Symptom When selecting **View > Radio Band > Show 2.4 GHz**, Location Manager does not refresh to show the 2.4 GHz radios.

Possible Cause The **View > Radio Band** menu filters the options (radio channel, transmit power, and data rate) that you want to display in the Location Manager window; it does not filter the display of the APs themselves.

Recommended Action Use the **View > Radio Band** menu to specify which radio band's view options to display and which information (radio channel, transmit power, and/or data rate) to display.

Symptom The Location Manager cannot be launched when using the Mozilla browser.

Possible Cause Cookies must be enabled on the browser.

Symptom Under **Edit > Preferences**, select **Privacy and Security > Cookie**s. Enable all cookies or enable cookies for the originating web site only.

Symptom Location manager will will not launch.

Possible Cause Proxy is set.

Recommended Action Remove proxy settings.

Administration FAQs and Troubleshooting

- Administration FAQs, page 1-48
- Administration Troubleshooting, page 1-49

Administration FAQs

Q. How can I verify the status of the database?

A. You can verify that the WLSE database is running by using the **show process** CLI command. If the command output includes the db2sync process, the database is running.

Q. What are the rules for WLSE user names and passwords?

A. User names can be up to 32 characters long and cannot begin with a number. You can use the alphanumeric characters (A-Z, a-z, 0-9) and numerous special characters. For a complete list of the characters allowed, see the Naming Guidelines appendix in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*. Passwords are unlimited in length and you can use all characters except the single quote, double quote, and dollar sign. Both user names and passwords are case sensitive.

Q. Can I restore a backup that I made on a WLSE running beta software to a WLSE running released software?

A. No.

Q. Can I upgrade from beta software to released software?

A. No.

Q. Are there any special considerations when performing actions on a redundant cluster?

A. Yes, there are special procedures for backup/restore, upgrading the software, and changing the web timeout. See the online help for the redundancy feature.

Administration Troubleshooting

This section contains the following troubleshooting information:

- Symptom After adding users to an external authentication server and configuring the authentication module on the WLSE, users cannot log in to the WLSE.
- Symptom Users cannot log in after failure of the alternative authentication source.
- Symptom Some users are not listed under User Admin > Manage Users.
- Symptom When using Internet Explorer 6.0 to install a new image on a WLSE from a repository located on a Windows XP machine, the progress bar does not appear in the Install Software Updates window. This problem also occurs when you use Internet Explorer 6.0 and a Windows XP system as a client to install a new image on a WLSE.
- Symptom Cannot back up the WLSE configuration to a Windows 2000 or Windows XP Server.
- Symptom Cannot log in with a username and password created in the CLI.
- Symptom The ACS Failed Login Report link is missing.
- Symptom When using the MS NT Domain authentication module, the user could not log in by using the domain password.

Symptom After adding users to an external authentication server and configuring the authentication module on the WLSE, users cannot log in to the WLSE.

Possible Cause Users do not have local accounts on the WLSE.

Recommended Action All users must have local accounts on the WLSE. Each user on the external authentication server must have a local user account matching that username. Set up the local accounts under **Administration > User Admin > Manage Users**.

Symptom Users cannot log in after failure of the alternative authentication source.

Possible Cause The WLSE falls back to the Local authentication module.

Recommended Action

- Users can log in using their local passwords.
- The system administrator can log in using the admin log in.
- All users with CLI access can log in using the CLI.
- If you still cannot log in, follow the procedure on recovering from the loss of all admin passwords in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Symptom Some users are not listed under User Admin > Manage Users.

Possible Cause Only the creator of a user can view that user's name in the list. The admin user, however, can view all users.

Recommended Action None.

Symptom When using Internet Explorer 6.0 to install a new image on a WLSE from a repository located on a Windows XP machine, the progress bar does not appear in the Install Software Updates window. This problem also occurs when you use Internet Explorer 6.0 and a Windows XP system as a client to install a new image on a WLSE.

Possible Cause The Internet Explorer 6.0 browser on Windows XP does not come with the Java plug-in installed.

Recommended Action Before using a Windows XP machine as a r*emote repository* to update WLSE software, perform the following on the repository:

a. Install the JRE version 1.3.1_08 or later browser plug-in.
b. In the browser, select Tools > Internet Options > Privacy. Lower the slider all the way down to achieve the **Accept All Cookies** setting.

Before using a Windows XP machine as a *client* to update WLSE software, install the JRE 1.3.1_08 or later browser plug-in on the client machine.

You can download the plug-in from third-party sources such as Sun Microsystems or IBM.

Symptom Cannot log in with a username and password created in the CLI.

Possible Cause The password is too long.

Recommended Action Reset the password by using the CLI **username** command, or log in by using the first 8 characters of the password. Passwords should be from 5 to 8 characters long.

Symptom Cannot back up the WLSE configuration to a Windows 2000 or Windows XP Server.

Possible Cause The backup directory is not writable.

Recommended Action Set the directory to UNIX mode and make it write-enabled. For more information, see the backup and restore instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9*.

Symptom The ACS Failed Login Report link is missing.

Possible Cause Someone has deleted the link.

Recommended Action This link requires a special procedure for recreating it:

a. Navigate to **Administration > Links** and click **Add to Links...**
b. In the Name field, enter **`ACS Failed Login Report`**, then click **Save**. The ACS Failed Login Report link is recreated.
c. Click **Edit**. All of the required fields are displayed.
d. Enter the URL of the ACS server, the administrator username created when the ACS software was installed, and the password for the administrator.
e. To display the report in the right pane of the WLSE interface, deselect **Open in New Window**.
f. Click **Save**.

Symptom When using the MS NT Domain authentication module, the user could not log in by using the domain password.

Possible Cause The incorrect hostname format may be entered for the primary domain controller

Recommended Action When entering the hostname for the domain controllers, you must use the WINS name (simple hostname) instead of an IP address or a fully qualified domain name.

Fault Descriptions

This section provides the following information on the faults displayed in **Faults > Display Faults**. The following information is provided:

- Fault—The fault as it appears in the Display Faults table.
- Explanation—An explanation as to why the fault occurred.
- Related Setting—The threshold or policy you assigned to devices under **Faults > Manage Fault Settings**, when applicable.
- Recommended Action—An action that can be taken to clear the displayed fault.

Fault tables are provided for each device type:

- Access Point /Bridge Faults, page 2-1
- Radio Interface Faults, page 2-7
- WLSE Faults, page 2-15
- AAA Server Faults, page 2-16
- Switch Faults, page 2-21
- Router Fault, page 2-22

Access Point /Bridge Faults

Table 2-1 Access Point Faults

Fault Description	Type	Explanation	Related Setting	Recommended Action
AP is in a Degraded state *number* associated clients	Non-IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: AP is in OK state.	Manage Fault Settings > Access Point/Bridge Thresholds > Associated Clients	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
AP is in an Overloaded state *number* associated clients	Non-IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: AP is in OK state.	Manage Fault Settings > Access Point/Bridge Thresholds> Associated Clients	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
AP is not registered with any WDS	IOS	The managed IOS access point is not registered with any WDS. For Radio Manager functionality to work, all IOS access points must register with a WDS. If an access point is not registered, it will be excluded from all the Radio Manager procedures, which will provide incorrect results.	Manage Fault Settings > Access Point/Bridge > Registration Error	Verify that the WLCCP AP credentials are configured correctly so that the AP can register with a WDS in its subnet. For more information, see the managing devices information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine Express, Release 2.9*.
AP registered with an Unmanaged WDS: ipAddressOfTheUnManagedWDS	IOS	AP is registered with a WDS but that WDS is not managed by WLSE. When this fault is cleared, the following message displays: AP registered with a managed WDS.	Manage Fault Settings > Access Point/Bridge > Registration Error	Manage the WDS.
Broadcast Key Rotation is disabled	Non-IOS and IOS	The broadcast key rotation has been disabled. When this fault is cleared, the following message displays: Broadcast Key Rotation is enabled.	Manage Fault Settings > Access Point/Bridge Policies > Key Rotation per VLAN	Log in to the access point and enable the broadcast key rotation interval.
Device state is rogue access point	IOS	The WLSE detected a rogue access point. (This is an access point that is not being managed and is unknown to the WLSE.)	Manage Network-Wide Settings > Rogue AP Detection	Use the fault details page to mark it friendly if the AP is known, or to delete it from the WLSE database if it is an unknown AP.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Device was not reachable via SNMP	Non-IOS and IOS	The SNMP Agent could be down. When this fault is cleared, the following message displays: Device was reachable via SNMP.	Manage Fault Settings > Access Point/Bridge Thresholds > SNMP Reachable	Make sure SNMP is enabled on the device and that the agent is not down. Take a MIB walk of the device to make sure sysup time is returning 0, which indicates Device is reachable.
		The SNMP community string in the access point has been changed, and then a discovery job is run.	Not applicable.	Change the SNMP community string on the WLSE to match the new community string on the access point, then run discovery again.
EAP per SSID for Cisco-Supplicant is disabled	Non-IOS and IOS	The Network EAP or the Open authentication is disabled on this SSID. When this fault is cleared, the following message displays: EAP per SSID for Cisco Supplicant is enabled.	Manage Fault Settings > Access Point/Bridge Policies > EAP Per SSID Enforced for Cisco-Supplicant	Log in to the access point and enable both Network EAP and Open authentication on that SSID.
EAP per SSID for Non-Cisco-Supplicant is disabled	Non-IOS and IOS	The Network EAP or the Open authentication is disabled on this SSID. When this fault is cleared, the following message displays: EAP per SSID for Non-Cisco Supplicant is enabled.	Manage Fault Settings > Access Point/Bridge Policies > EAP Per SSID Enforced for Non-Cisco-Supplicant	Log in to the access point and enable both Network EAP and Open authentication on that SSID.
EAP per SSID for Mixed-Cisco-Supplicant is disabled	Non-IOS and IOS	The Network EAP or the Open authentication is disabled on this SSID. When this fault is cleared, the following message displays: EAP per SSID for Cisco Supplicant is enabled.	Manage Fault Settings > Access Point/Bridge Policies > EAP Per SSID Enforced for Mixed-Cisco-Supplicant	Log in to the access point and enable both Network EAP and Open authentication on that SSID.
Ethernet bandwidth utilization is Degraded (*utilization %)*	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: Ethernet bandwidth utilization is OK.	Manage Fault Settings > Access Point/Point Thresholds > Ethernet Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Ethernet bandwidth utilization is Overloaded (*utilization %)*	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: Ethernet bandwidth utilization is OK.	Manage Fault Settings > Access Point/Bridge Thresholds > Ethernet Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Firmware version policy violation (*version number*)	Non-IOS and IOS	The wrong version number for policy checking has been entered. When this fault is cleared, the following message displays: Firmware version is valid.	Manage Fault Settings > Access Point/Bridge Policies > Firmware Version	Make sure that the firmware version that is entered in the policy setting matches the firmware version on the access point.
		The access point is running an unauthorized firmware version. When this fault is cleared, the following message displays: Firmware version is valid.		Make sure that you have entered authorized versions in the policy setting. Update the firmware on the access point to an authorized version.
HotStandBy is active	Non-IOS and IOS	The access point that is configured for hot standby has become active. The following conditions could cause the hot standby access point to become active: the primary access point is down, the Ethernet port is down, or the Radio port is down. When this fault is cleared, the following message displays: HotStandBy is disabled.	Manage Fault Settings > Access Point/Bridge Policies > HotStandby Status	For non-IOS access points: 1. Check the primary access point, the Ethernet port, or the Radio port to see why the hot standby access point has been activated. 2. Correct the condition. For example, if the Radio Port on the formerly active access point was in a disabled state, then enable it using the access point GUI. 3. Launch the GUI for access point that is currently in Active Takeover mode. 4. Select the Hot Standby section and click **Start Hot Standby mode** to reconfigure the access point to Hot Standby mode.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
				For IOS access points: 1. Check the primary access point, the Ethernet port, or the Radio port to see why the hot standby access point has been activated. 2. Correct the condition. For example, if the Radio Port on the formerly active access point was in a disabled state, then enable it using the access point GUI. 3. Launch the GUI for access point that is currently in Active Takeover mode. 4. Select Hot Standby, click **Disabled** , then click **Apply**. 5. Click **Enabled**, then enter the Radio MAC address of Monitored Radio Port, leave the Polling interval and Timeout for Each Polling fields blank,. 6. Click **Apply** to reconfigure the access point to Hot Standby mode.
HTTP access is enabled	Non-IOS	HTTP has been enabled on the access point. When this fault is cleared, the following message displays: HTTP access is disabled.	Manage Fault Settings > Access Point/Bridge Policies > HTTP Disabled	Log in to the access point and disable HTTP access.
HTTP access without login is enabled	Non-IOS	The allowBrowseWithoutLogin setting on the access point is set. When this fault is cleared, the following message displays: HTTP access without login is disabled.	Manage Fault Settings > Access Point/Bridge Policies > HTTP Authentication (NonIOS)	Log in to the access point and disable the allowBrowseWithoutLogin setting.
MIC is disabled for the VLAN *number*	IOS	MIC is not enabled for the selected VLAN on the access point. When the fault is cleared, the following message displays: MIC is enabled.	Manage Fault Settings > Access Point/Bridge Policies > MIC per Vlan (IOS)	Log into the access point and enable the VLAN. Then, using the WLSE fault settings, enable the MIC for that VLAN.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
PSPF is disabled	Non-IOS	The PSPF port has been disabled. PSPF (Publicly Secure Packet Forwarding) is a feature that prevents client devices associated to a bridge or access point from inadvertently sharing files with other client devices on the wireless network. When the fault is cleared, the following message displays: The PSPF is enabled.	Manage Fault Settings > Access Point/Bridge Policies > PSPF Enabled (Non-IOS)	Log in to the access point and enable the PSPF setting.
SNMP query received authorization error response	Non-IOS	The access point's user community strings do not have Admin, Ident, Firmware, SNMP privileges. The WLSE might not be able to access some SNMP information from the access point that requires these privileges. When the fault is cleared, the following message displays: Device was reachable via SNMP.	Manage Fault Settings > Access Point/Bridge Thresholds > SNMP Reachable	Make sure the SNMP community string set on the WLSE (Devices > Discover > Device Credentials > SNMP Communities) is the same as the string set on the access point (Setup > Security > User Information).
Telnet access is enabled	Non-IOS	Telnet has been enabled on the access point. When this fault has been cleared, the following message displays: Telnet access is disabled	Manage Fault Settings > Access Point/Bridge Policies > Telnet Disabled	Log in to the access point and disable the Telnet access setting.
User capabilities are not enforced	Non-IOS	The enableUserMgr setting is not set on the access point. When this fault has been cleared, the following message displays: User capabilities are enforced.	Manage Fault Settings > Access Point/Bridge Policies > User Manager Enforced (NonIOS)	Log in to the access point and enable the User Mgr setting.
Vlan WEP key length policy violation	Non-IOS and IOS	The WEP key length for the selected VLAN setting has been violated. When this fault has been cleared, the following message displays: Vlan WEP key length is ok.	Manage Fault Settings > Access Point/Bridge Policies > WEP Encryption per Vlan	Make sure the WEP key length selected in the policy setting matches the access point settings.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
WDS appears down.	IOS	The WLSE failed to receive "keep active" messages from the WDS. This happens when the WDS is down or when the network is down.	Manage Fault Settings > WDS > WLSE-WDS Link Status	Check the network connectivity, and the WDS status.
WEP is disabled	IOS	WEP is not enabled for the VLAN defined on the access point. (Note that the VLAN number is displayed in the Type column under Faults > Display Faults.) When the fault is cleared, the following message displays: WEP is enabled.	Manage Fault Settings > Access Point/Bridge Policies > WEP per Vlan (IOS)	Make sure you have set the policy correctly for the VLAN.
WNM failed to authenticate with WDS.	IOS	Authentication required to open a WLCCP channel between the WLSE and the WDS failed.	Manage Fault Settings > WDS > Authentication Failures	Verify that the WLSE credentials used to authenticate with the WDS are correct. For more information, see the managing devices information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine Express, Release 2.9*.

Radio Interface Faults

Table 2-2 Radio Interface Faults

Fault Description	Type	Explanation	Related Setting	Recommended Action
802.11-B/G Interference Detected - or - 802.11-A Interference Detected	IOS	The WLSE detected a non-802.11 interference.	Manage Network-Wide Settings > Interference Detection	Look at the fault description to determine which AP reported the interference, then take corrective action by removing the interference source.
Ad-hoc network creation detected	Non-IOS and IOS	An ad-hoc network was formed by some wireless clients. One of your infrastructure APs or other clients sent this information to the WLSE via your WDS setup.	Manage Network-Wide Settings > Ad-hoc Network Detection	If the information is available, the WLSE will show the clients that are participating in the network (and that it can detect) in the fault details page. Use the Location Manager to find these APs and verify that this is not a security issue.

Table 2-2 Radio Interface Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
AP is in a Degraded state *number* associated clients	IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: AP is in OK state.	Manage Fault Settings > Radio-802.11x Thresholds > Associated Clients (IOS)	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
AP is in an Overloaded state *number* associated clients	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: AP is in OK state.	Manage Fault Settings > Thresholds > Access Point > Associated Clients	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Auto Resite Survey Performance Degradations	IOS only	There was a 20% difference in the base and current performance values. The fault will clear when there are no longer any buildings or any floors with 20% differences in the performance values.	Network-Wide Settings > Auto Re-Site Survey	Select the document with the eyeglasses in the detail view of the fault condition. A list of all buildings and floors that have performance degradations is displayed. First, check the details for the floor and if needed, run Radio Manager Assisted Configuration. Then select Auto Re-Site Survey to set the new base values.
Broadcast SSID is enabled.	Non-IOS and IOS	The broadcast mode for the SSID on the interface has been disabled. When this fault is cleared, the following message displays: Broadcast SSID is disabled.	Manage Fault Settings > Radio-802.11x Policies > Broadcast Disabled	Log in to the access point and disable the broadcast mode.
Broadcast is enabled for Radio-*x* SSID *ssid* fault.	IOS	An SSID, which you do not want broadcast, is being broadcast. When this fault is cleared, the following message displays: Broadcast is disabled for Radio-*x* SSID *ssid* fault.	Manage Fault Settings > Radio-802.11x Policies > Broadcast SSID (IOS)	Log in to the access point and make sure that the that the SSID, which is in WLSE's "Do not Broadcast SSID" list is not selected for Broadcast on the access point.

Table 2-2 Radio Interface Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Number of CCMP Replay Discarded is degraded.	IOS	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: Number of CCMP Replay Discarded is OK.	Manage Fault Settings > Radio-802.11x Policies > CCMP Replay Discarded (IOS)	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Number of CCMP Replay Discarded is overloaded.		The fault threshold set for the overloaded state has been exceeded. When the fault is cleared, the following message displays: Number of CCMP Replay Discarded is OK.		
Client association rate is Degraded *number* per minute	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: Client association rate is OK.	Manage Fault Settings > Radio-802.11x Thresholds > Association Rate	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Client association rate is Overloaded *number* per minute	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: Client association rate is OK.	Manage Fault Settings > Radio-802.11x Thresholds > Association Rate	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Client authentication error rate is Degraded *number* per minute	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: Client association error rate is OK.	Manage Fault Settings > Radio-802.11x Thresholds > Authentication Error Rate	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Client authentication error rate is Overloaded *number* per minute	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: Client association error rate is OK.	Manage Fault Settings > Radio-802.11x Thresholds > Authentication Error Rate	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-2 Radio Interface Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
EAP is disabled	Non-IOS and IOS	The EAP per SSID has been disabled. When this fault is cleared, the following message displays: EAP is enabled	Manage Fault Settings > Radio-802.11x Policies > EAP Enforced for Cisco Supplicant/ Non-Cisco Supplicant/ Mixed-Cisco Supplicant	Log in to the access point and enable the Network EAP and Open authentication.
Infrastructure SSID policy violation	IOS	The infrastructure SSID does not match the infrastructure SSID set on the access point. When this fault is cleared, the following message displays: Infrastructure SSID is valid .	Manage Fault Settings > Radio-802.11x Policies > Infrastructure SSID (IOS)	Log in to the access point and make sure the WLSE's Infrastructure SSID matches the access point infrastructure SSID
Packet Error is in Degraded state (*error rate %)*	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: Packet Error is in OK state.	Manage Fault Settings > Radio-802.11x Thresholds > RF Port Packet Errors	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
		The radio interfaces on the devices may be very under utilized, which can trigger the degradation problem. For example, if a total of three packets are sent over the radio, and two of them are corrupt, the percentage would be 2/3 = 66%, and could trigger the alarm.		Remove the alarm from the profile associated with these devices.
Packet Error is in is in Overloaded state (*error rate %)*	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: Packet Error is in OK state.	Manage Fault Settings > Radio-802.11x Thresholds > RF Port Packet Errors	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Port is administratively set to down	Non-IOS and IOS	The port has been set to Down by the administrator. When this fault is cleared, the following message displays: Port is up	Manage Fault Settings > Radio-802.11x Thresholds > RF Port Status	There is no action necessary; the port has been deliberately shut down.

Table 2-2 Radio Interface Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Port is down	Non-IOS and IOS	The port is operationally down. When this fault is cleared, the following message displays: Port is up	Manage Fault Settings > Radio-802.11x Thresholds > RF Port AdminStatus	Check the device to determine why the port is down. If you have added or removed an interface from an access point, the WLSE might generate an erroneous fault. See Q.What are the results of adding or removing an interface from an access point?, page 1-16.
PSPF is disabled	IOS	The PSPF port has been disabled. PSPF (Publicly Secure Packet Forwarding) is a feature that prevents client devices associated to a bridge or access point from inadvertently sharing files with other client devices on the wireless network. When the fault is cleared, the following message displays: The PSPF is enabled.	Manage Fault Settings > Access Point/Bridge Policies > PSPF Enabled (IOS)	Log in to the access point and enable the PSPF setting.
Radio (*macaddress(es)*) appears down - triggered self healing	IOS	The indicated radio appeared down on this AP, so other APs were modified to maintain coverage. After self healing has been applied to the other AP, this fault indicates the AP that had the failure.	Not applicable.	Select the document with the eyeglasses in the detail view of the fault condition. A list of the APs that were modified with the old and new power settings is displayed. Check the radio to determine why it is down. Then either replace it or clear the fault and rerun AP Radio Scan. Or if you like the new setup, just clear the fault.
Retry Count rate is Degraded *number* per minute	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: Retry Count rate is OK	Manage Fault Settings > Radio-802.11x Thresholds > Max Retry Count	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-2 Radio Interface Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Retry Count rate is Overloaded *number* per minute	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When the fault is cleared, the following message displays: Retry Count rate is OK	Manage Fault Settings > Radio-802.11x Thresholds > Max Retry Count	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
RF bandwidth utilization is Degraded (*utilization %)*	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: RF bandwidth utilization is OK	Manage Fault Settings > Radio-802.11x Thresholds > RF Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
RF bandwidth utilization is Overloaded (*utilization %)*	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When the fault is cleared, the following message displays: RF bandwidth utilization is OK	Manage Fault Settings > Radio-802.11x Thresholds > RF Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Self Healing finished with errors: *message*	IOS	An error occurred while attempting self healing. For example, a power change cannot be applied to an AP. 1) The community strings for the device are wrong 2) AP is down 3) Wrong configuration set on the AP	Not applicable.	Determine the action necessary to clear the fault condition.
Self Healing In Progress	IOS	The WLSE determined that a radio was down. When self healing is complete, a fault is applied against the AP that had the failure.	Not applicable.	There is no action necessary; self healing is attempting to adjust the power on other radios on the floor to maintain coverage.
Serving and non-serving channel Radio Monitoring must be enabled.	IOS	Radio Monitoring is not enabled for serving and non-serving channels. When the fault is cleared, the following message displays: Qualifies for Self Healing Monitoring.	Not applicable.	Enable Radio Monitoring for both serving and non-serving channels.

Table 2-2 Radio Interface Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Number of TKIP replay errors is degraded.	IOS	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: Number of TKIP replay errors is OK.	Manage Fault Settings > Radio-802.11x Thresholds >TKIP Replay (IOS)	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Number of TKIP replay errors is overloaded.		The fault threshold set for the overloaded state has been exceeded. When the fault is cleared, the following message displays: Number of TKIP replay errors is OK.		
Number of TKIP counter measure is degraded.	IOS	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: Number of TKIP replay errors is OK.	Manage Fault Settings > Radio-802.11x Thresholds >TKIP Counter Measure (IOS)	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Number of TKIP counter measure is overloaded.		The fault threshold set for the overloaded state has been exceeded. When the fault is cleared, the following message displays: Number of TKIP replay errors is OK.		
Unregistered Client(s) present	IOS	One or more unregistered clients are present in the wireless network and are unsuccessfully attempting to authenticate with the APs. This fault occurs when, during the observation interval, the number of failed attempts crosses the threshold defined by the administrator. This fault is cleared when no registration attempts are detected during the observation interval (the client leaves the wireless network or is not seen or reported by any Scanning APs).	Faults > Manage Network-Wide Settings > Scanning AP.	Set the priority of the fault to be generated and the threshold for the failed authentication attempts by the client. Make a physical check near the scanning AP that reported this fault to see if there are any rogue clients.

Table 2-2 Radio Interface Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
WEP Error is in Degraded state (*error rate %)*	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: WEP Error is in OK state	Manage Fault Settings > Radio-802.11x Thresholds > RF Port WEP Errors	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
WEP Error is in Overloaded state (*error rate %)*	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: WEP Error is in OK state	Manage Fault Settings > Radio-802.11x Thresholds > RF Port WEP Errors	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
WEP is disabled	Non-IOS and IOS	WEP has been disabled. When this fault has been cleared, the following message displays: WEP is enabled.	Manage Fault Settings > Radio-802.11x Policies > WEP Enforced (Non-IOS)	Log in to the access point and enable WEP.
WEP key length policy violation	Non-IOS and IOS	The WEP key length setting has been violated. When this fault has been cleared, the following message displays: WEP key length is OK.	Manage Fault Settings > Radio-802.11x Policies > WEP Key Length	Check the WEP key settings on the interface to make sure they match the WLSE settings.

WLSE Faults

Table 2-3 WLSE Fault

Fault Description	Explanation	Related Setting	Recommended Action
Dot11mib view is not enabled on some Access Points. Please consult online help for details	The device is not configured with the iso (dot11 mib) view, and cannot be managed effectively by the WLSE. This can cause some WLSE report information to be missing and some WLSE faults may not be generated. When this fault has been cleared, the following message displays: No Dot11mib view misconfigurations detected.	Manage Fault Settings > Thresholds > WLSE > Dot11mib view enabled	Configure the devices and the WLSE as described in Symptom Access points are placed in Misconfigured Devices group after discovery and dot11mib fault is displayed., page 1-18.
Duplicate IP Detection	During discovery, an AP with a duplicate IP is found and placed in the Duplicate IP folder under Devices > Managed > Manage/Unmanage. This folder contains access points that are in the *pending* state. A device becomes pending and is placed in this folder when: • The same IP address is assigned to more than one access point. • An access point's IP address changes. • You replace a managed access point. The IP address shown for a device in this folder is the last known address for the device, before the address change occurred.	Manage Fault Settings > Thresholds > WLSE > Duplicate IP detection	For information on how to move devices from the Duplicate IP folder, see the topic: Handling Duplicate IP Addresses on Access Points in the Managing Devices chapter of the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.9.* or in the online help.

AAA Server Faults

Table 2-4 AAA Server Faults

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
Authentication failed. Please check EAP-FAST, EAP-MD5, LEAP, PEAP, or RADIUS credentials	All AAA Servers	The server is reachable but the credentials are incorrect. When this fault has been cleared, the following message displays: Authentication succeeded	Manage Fault Settings > AAA > EAP-FAST/ EAP-MD5 /LEAP/ PEAP/RADIUS> Response Time	Make sure that the credentials are set correctly by selecting Devices > Discover > AAA Server.
EAP-FAST server is not available	EAP-FAST	This fault can be caused by any of the following reasons: • The WLSE IP Address is not configured as a NAS on the server. • The shared secret key does not match with the key configured on the server. • The server is unreachable. When this fault has been cleared, the following message displays: EAP-MD5 server is available	Manage Fault Settings > AAA > EAP-FAST > Response Time	Check the server configuration to make sure that: • The WLSE IP address is configured as NAS on the server. • The shared secret key matches the key configured on the server
EAP-FAST server is Degraded	EAP-FAST	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: EAP-FAST server is OK	Manage Fault Settings > AAA > EAP-FAST > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
EAP-FAST server is Overloaded	EAP-FAST 5	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: EAP-FAST server is OK	Manage Fault Settings > AAA > EAP-FAST > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-4 AAA Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
EAP-MD5 server is not available	EAP-MD5	This fault can be caused by any of the following reasons: • The WLSE IP Address is not configured as a NAS on the server. • The shared secret key does not match with the key configured on the server. • The server is unreachable. When this fault has been cleared, the following message displays: EAP-MD5 server is available	Manage Fault Settings > AAA > EAP-MD5 > Response Time	Check the server configuration to make sure that: • The WLSE IP address is configured as NAS on the server. • The shared secret key matches the key configured on the server
EAP-MD5 server is Degraded	EAP-MD5	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: EAP-MD5 server is OK	Manage Fault Settings > AAA > EAP-MD5 > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
EAP-MD5 server is Overloaded	EAP-MD5	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: EAP-MD5 server is OK	Manage Fault Settings > AAA > EAP-MD5 > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
LEAP server is not available	LEAP	This fault can be caused by any of the following reasons: • This can be caused if you have enabled this policy and you are using a non-Cisco client with EAP. • The WLSE IP Address is not configured as a NAS on the server. • The shared secret key does not match with the key configured on the server. • The server is unreachable. When this fault has been cleared, the following message displays: LEAP server is available	Manage Fault Settings > AAA > LEAP > Response Time	Check the server configuration and make sure that: • The WLSE IP address is configured as NAS on the server. • The shared secret key matches the key configured on the server

Table 2-4 AAA Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
LEAP server is Degraded	LEAP	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: LEAP server is OK.	Manage Fault Settings > AAA > LEAP > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
LEAP server is Overloaded	LEAP	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: LEAP server is OK.	Manage Fault Settings > AAA > LEAP > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
PAC is either invalid or expired. Please reimport new PAC file	EAP-FAST	PAC file used is either invalid or expired.	This fault is not generated based on a threshold violation.	Generate a new PAC file from the EAP-FAST server you are trying to monitor and make sure that the expiry time is set properly when generating the PAC file.

Table 2-4 AAA Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
PEAP server is not available	PEAP	This fault can be caused by any of the following reasons: • PEAP monitoring is not enabled. • The WLSE IP Address is not configured as a NAS on the server. • The shared secret key does not match with the key configured on the server. • The server is unreachable. • EAP-GTC is required for reports and faults. When this fault has been cleared, the following message displays: PEAP server is available	Manage Fault Settings > AAA > PEAP > Response Time	Check the server configuration and make sure that: • PEAP monitoring is enabled under Manage Fault Settings > AAA> PEAP > Response time. • The WLSE IP address is configured as NAS on the authentication server. • If both NICs in the WLSE are assigned an IP, then both should be added as NAS in the PEAP authentication server. • The shared secret key matches the key configured on the server. • The WLSE requires EAP-GTC for PEAP monitoring, which is used for PEAP-related reports and faults. They will not work with MS-CHAPV2.
PEAP server is Degraded	PEAP	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: PEAP server is OK.	Manage Fault Settings > AAA > PEAP > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
PEAP server is Overloaded	PEAP	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: PEAP server is OK	Manage Fault Settings > AAA > PEAP > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-4 AAA Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
RADIUS server is not available	PEAP	This fault can be caused by any of the following reasons: • The WLSE IP Address is not configured as a NAS on the server. • The shared secret key does not match with the key configured on the server. • The server is unreachable. When this fault has been cleared, the following message displays: RADIUS server is available	Manage Fault Settings > AAA > RADIUS > Response Time	Check your server configuration and make sure that: • The WLSE IP address is configured as NAS on the server. • The shared secret key matches the key configured on the server
RADIUS server is Degraded	PEAP	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: RADIUS server is OK.	Manage Fault Settings > AAA > RADIUS > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
RADIUS server is Overloaded	PEAP	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: RADIUS server is OK.	Manage Fault Settings > AAA > RADIUS > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Switch Faults

Table 2-5 Switch Faults

Fault Description	Explanation	Related Setting	Recommended Action
CPU utilization is Degraded *(utilization %)*	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: CPU utilization is Ok.	Manage Fault Settings > Switch > CPU Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
CPU utilization is Overloaded (*utilization %)*	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: CPU utilization is Ok.	Manage Fault Settings > Switch > CPU Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Device was not reachable via SNMP	The SNMP Agent on the switch is down. When this fault has been cleared, the following message displays: Device was reachable via SNMP.	Manage Fault Settings > Switch > SNMP Reachable	Make sure that the switch SNMP agent is active.
Module is down	The module is down. When this fault has been cleared, the following message displays: Module is up.	Manage Fault Settings > Switch > Module Status	Check the module in the switch and correct the problem.
Port could not agree with other end on duplex mode	The port could not agree with the far end on port duplex, and is in disagree(3) mode. When this fault has been cleared, the following message displays: Port duplex state is OK.	Not applicable.	Make sure the duplex mode on both ends match.
Switch memory utilization is Degraded (*utilization %)*	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: Switch memory utilization is Ok.	Manage Fault Settings > Switch > Memory Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Switch memory utilization is Overloaded (*utilization %)*	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: Switch memory utilization is Ok.	Manage Fault Settings > Switch > Memory Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-5 Switch Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Switch Port bandwidth utilization is Degraded (*utilization %)*	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: Switch port bandwidth utilization is Ok.	Manage Fault Settings > Switch > Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Switch Port bandwidth utilization is Overloaded (*utilization %)*	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: Switch port bandwidth utilization is Ok.	Manage Fault Settings > Switch > Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Router Fault

Table 2-6 Router Fault

Fault Description	Explanation	Related Setting	Recommended Action
Device was not reachable via SNMP	The SNMP Agent on the switch is down. When this fault has been cleared, the following message displays: Device was reachable via SNMP.	Manage Fault Settings > Router > SNMP Reachable	Make sure that the router SNMP agent is active.

Numerics

12.2(13)JA and 12.2(15)JA firmware, discovery of access points 1-21

A

AAA server
- Cisco ACS, ports used by 1-2
- fault descriptions 2-16
- named displayed as %hostname% 1-22
- using AP 1100 or AP 1210 as AAA server 1-16

access point
- accessing through WLSE, troubleshooting 1-5
- AP web page, accessing 1-5
- fault descriptions 2-1
- interface
  - adding, results of 1-16
  - removing, results of 1-16
- not discovered 1-20
- reports, VLAN information in 1-35

ACS Failed Login Report link, recreating 1-50

Administration tab
- FAQs 1-48
- troubleshooting 1-49

AP 1100, using as AAA server 1-16

AP 1210, using as AAA server 1-16

B

backing up and restoring WLSE configuration
- restoring backups from beta to released not allowed 1-48
- Windows 2000 or XP server 1-50

beta software, restoring backups and upgrading software not allowed 1-48

booting, WLSE 1-4, 1-8

browser
- cannot connect to WLSE 1-7
- IE, installing software updates 1-50
- Mozilla browser and Location Manager 1-48
- pop-up blocker usage 1-10

C

CDP
- discovery without using 1-15
- seed, invalid 1-15

client

inventory, troubleshooting 1-22
reports 1-34
community string
with iee802dot11 view 1-20
configuration
auto-configuration 1-25
FAQs 1-23
IOS template job failures 1-26
job history, retention of 1-24
protocols used for jobs 1-24
startup template, changes to 1-25
Telnet/SSH credentials not valid 1-27
troubleshooting 1-25
updates, undoing 1-24
WEP key settings 1-24
connecting to WLSE
using a console 1-10
using Telnet 1-9
console, connecting to WLSE 1-10

D

database
checking database status 1-48
date and time
incorrect 1-8
device name, updates to 1-15
device name format
device tree not updated 1-21
name not updated after moving device to managed 1-21
devices
type of identifier used in displays 1-3
Devices tab
FAQs 1-15
troubleshooting 1-17
discovery
APs running 12.2(13)JA or 12.2(15)JA 1-21
AP with iee802dot11 view not discovered 1-20
devices discovered, but not displayed 1-17
Misconfigured Devices group 1-18
port used for 1-2
seed devices 1-15
SNMP Authorization Exception in discovery log 1-19
time discrepancy in jobs 1-18
troubleshooting 1-17
without CDP 1-15
DNS
port for IOS AP configuration 1-2
dot11 mib fault
description of 2-15
troubleshooting 1-18
duplicate IP address 1-16

E

EAP-FAST server

port for AP 1100 or AP 1210 1-3

F

FAQs
Administration 1-48
configuration 1-23
devices 1-15
faults 1-11
firmware 1-27
general 1-1
radio manager 1-36
reports 1-33
faults
AAA server fault descriptions 2-16
access point fault descriptions 2-1
acknowledging 1-11
clearing 1-11
descriptions of 2-1
email of 1-13
FAQs 1-11
MIB file 1-11
no display 1-13
router fault description 2-22
switch fault descriptions 2-21
troubleshooting 1-12
firmware
connectivity failure 1-32
cryptography permissions, message about 1-31
email fails to arrive 1-29
FAQs 1-27
images
transfer, ports used for 1-2
job logs 1-28
job not verified 1-30
number of devices in jobs 1-28
slow links 1-31
SNMP job fails 1-30
some devices not updated 1-30
Telnet/SSH credentials not valid 1-32
time discrepancy in jobs 1-29
troubleshooting 1-27
FTP
port for IOS AP configuration 1-2

G

groups
Misconfigured Devices group 1-18

H

hostname
displaying devices by hostname 1-3
HTTP
port for VxWorks access point configuration 1-2
WLSE Web port for 1-3

HTTPS
port used for 1-3

I

iee802dot11 view 1-20
interference, detecting 1-37
Internal Server Error message in redundant WLSEs 1-10
inventory
effects on traffic and performance 1-22
extra inventories 1-16
FAQs 1-15
length of time required 1-22
port used for 1-2
IP address, duplicate 1-16

L

LEAP server
port for AP 1100 or AP 1210 1-2
Location Manager
viewing with Mozilla browser 1-48
logging in
cannot log in 1-5
cannot log in as system administrator 1-6
failure of authentication source 1-49
password created in CLI 1-50

M

Misconfigured Devices folder
devices placed in 1-21
Misconfigured Devices system group
moving devices from 1-18
Mozilla browser, viewing Location Manager 1-48

N

name format, device names 1-21
network
connection failure 1-6
Network Address Translation (NAT), not supported 1-2

P

passwords, loss of 1-6
performance
problems caused by frequent client inventory 1-22
pop-up blockers, do not use 1-10
pre-release software, restoring backups and upgrading software not allowed 1-48
protocols
SSH, disabling 1-3
Telnet, enabling 1-2
used for configuration jobs 1-24

R

radio manager
  Assisted Site Survey
    client walkabout, skipping 1-45
    configuration, not updated 1-47
    configuration, results of 1-46
    Constraints and Goals, calculations of 1-46
    devices in red 1-44
    device tree 1-44
    job, failure of 1-45
    Last Scan Time Field 1-45
    Location Data fields 1-45
    missing building or floor nodes 1-44
    multiple channels, selecting 1-46
    Next button disabled 1-45, 1-46
    radio scan slow 1-45
    Recall button 1-45
    Use Old Radio Scan Data disabled 1-45
  configuring APs 1-36
  data collection 1-36
  FAQs 1-36
  interference detection 1-37
  inventories run by 1-16
  job names 1-37
  rogue AP detection 1-36
  scanning-only APs 1-37
  troubleshooting 1-41
RADIUS
  port for WLCCP authentication 1-2
RADIUS server
  ports for 1-2
redundancy
  Internal Server Error message 1-10
  special procedures 1-48
reports
  ACS Failed Login Report link, recreating 1-50
  blank fields in 1-34
  client reports, 0 values in 1-34
  FAQs 1-33
  not real-time 1-33
  troubleshooting 1-33
  VLAN information missing 1-35
repository
  port for 1-2
rogue APs, detecting 1-36
routers, fault message for 2-22

S

search, for devices
  no results yielded 1-5
security
  authentication (WLSE)
    failure of authentication source 1-49
    troubleshooting 1-49
seed
  invalid 1-15

setup program
  incorrect entry 1-5
  network connection fails 1-6
SMTP
  port for fault notification 1-2
SNMP
  port for 1-2
SNMPTRAP
  port for fault notification 1-2
software, on WLSE
  repository
    port for 1-2
  updates
    CiscoWorks 1105 1-4
    Internet Explorer, problems using 1-50
SSH
  disabling 1-3
  port for IOS AP configuration 1-2
switches, fault descriptions 2-21
sysContact information, updates to 1-15
sysLocation information
  updates to 1-15
syslog
  port for 1-2

T

TCP ports used by WLSE 1-2
Telnet
  connecting to WLSE 1-9
  enabling 1-2
  port for IOS AP configuration 1-2
TFTP
  ports used for firmware upgrade 1-3
time
  incorrect 1-8
traps
  definition file 1-11
  not forwarded 1-11
  type of 1-11
troubleshooting
  administration 1-49
  configuration 1-25
  devices 1-17
  faults 1-12
  firmware 1-29
  radio manager 1-41
  reports 1-33

U

UDP ports used by WLSE 1-2
upgrading WLSE software
  upgrade from beta to released not allowed 1-48
users
  authentication, external 1-49
  authentication server failure 1-49
  external authentication server 1-49

not listed in UI 1-49
password created in CLI not accepted 1-50
simultaneous access to access points 1-2

V

VLANs
in reports 1-35

W

WDS
WLCCP
port for 1-3
WHISK port 1-2
WLCCP
port for 1-2
WLSE 1105, 2.9 software not supported on 1-4