



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**, **IDS > Manage IDS Settings**, or **IDS > Manage Network-Wide IDS 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 2-2](#)
- [Radio Interface Faults, page 2-8](#)
- [IDS \(Intrusion Detection System\) Faults, page 2-14](#)
- [Voice Faults, page 2-24](#)
- [WLSE Faults, page 2-24](#)
- [AAA Server Faults, page 2-26](#)
- [Switch Faults, page 2-31](#)
- [Router Fault, page 2-33](#)
- [WLSM Faults, page 2-33](#)

Access Point/Bridge Faults

Table 2-1 Access Point Faults

Fault Description	Explanation	Related Setting	Recommended Action
Access point <i>ssid</i> reclassified from Friendly to Rogue due to <i>rule</i>	<p>An access point that was previously determined to be Friendly has been reclassified to Rogue:</p> <p><i>ssid</i> is the Service Set Identifier of the unmanaged radio's BSS.</p> <p><i>rule</i> is one of the following:</p> <ul style="list-style-type: none"> Change in RSSI ordering between observers <p>The estimated proximity of the unmanaged radio between two observers has switched—if the WLSE thought that observer A was closer to radio R than observer B, it now thinks that observer B is closer to radio R than observer A.</p> <ul style="list-style-type: none"> Difference in relative RSSI between original and current observers exceeded threshold <p>While radio R's strength changed by factor M between observer A and observer B, it changed by factor M+T between observer B and observer C. That is, it does not</p>	<p>IDS > Manage Network-Wide IDS Settings > Rogue AP Detection > Friendly to Rogue AP Reclassification</p> <p>or</p> <p>IDS > Manage Rogues</p>	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.
Access point <i>ssid</i> reclassified from Friendly to Rogue due to <i>rule</i> (continued)	<p>appear that radio R's change in strength is merely due to a change in its power configuration.</p> <ul style="list-style-type: none"> Fewer than two observers Too long without any observations 		
AP CPU utilization is Degraded (<i>utilization %</i>)	<p>The fault threshold set for the degraded state has been exceeded.</p> <p>When this fault has been cleared, the following message displays: AP CPU utilization is Ok.</p>	Manage Fault Settings > Access Point/Bridge Thresholds > CPU Utilization	<p>Verify that the fault threshold is set correctly.</p> <p>If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.</p>

Table 2-1 Access Point Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
AP 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 > Access Point/Bridge Thresholds > 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.
AP is not registered with a WDS	The managed access point is not registered with any WDS. For Radio Manager functionality to work, all 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 <i>User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13</i> .
AP 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: AP memory utilization is Ok.	Manage Fault Settings > Access Point/Bridge Thresholds > 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.
AP 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: AP memory utilization is Ok.	Manage Fault Settings > Access Point/Bridge Thresholds > 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.
AP registered with an Unmanaged WDS: ipAddressOfTheUnManagedWDS	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	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: ssid	The WLSE detected a rogue access point (where <i>ssid</i> is the Service Set Identifier of the unmanaged radio's BSS). This is an access point that is not being managed and is unknown to the WLSE.	IDS > Manage Network-Wide IDS Settings > Rogue AP Detection or IDS > Manage Rogues	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. These faults do not automatically clear after the Rogue AP no longer appears in the network; you must manually delete or clear the fault.

Table 2-1 Access Point Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Device was not reachable via SNMP	<p>The SNMP Agent could be down.</p> <p>Using the SNMP threshold setting, you configure the WLSE to poll the sysUpTime MIB object periodically. If at any time the WLSE fails to poll this MIB object, the WLSE generates this fault.</p> <p>Also, if while polling any other MIB objects for other fault policies or thresholds associated with the device, the WLSE observes the device is SNMP unreachable, it generates this fault.</p> <p>And lastly, during rediscovery if a previously-discovered device is found to be SNMP unreachable, the WLSE generate this fault.</p> <p>When this fault is cleared, the following message displays: Device was reachable via SNMP.</p>	Manage Fault Settings > Access Point/Bridge Thresholds > SNMP Reachable	<p>Make sure SNMP is enabled on the device and that the agent is not down.</p> <p>Take a MIB walk of the device and ensure that the sysUpTime returns a non-zero value, which indicates that the device is reachable.</p>
	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	<p>The Network EAP or the Open authentication is disabled on this SSID.</p> <p>When this fault is cleared, the following message displays: EAP per SSID for Cisco Supplicant is enabled.</p>	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	<p>The Network EAP or the Open authentication is disabled on this SSID.</p> <p>When this fault is cleared, the following message displays: EAP per SSID for Non-Cisco Supplicant is enabled.</p>	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	<p>The Network EAP or the Open authentication is disabled on this SSID.</p> <p>When this fault is cleared, the following message displays: EAP per SSID for Cisco Supplicant is enabled.</p>	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.

Table 2-1 Access Point Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Ethernet bandwidth utilization is Degraded (<i>utilization %</i>)	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.
Ethernet bandwidth utilization is Overloaded (<i>utilization %</i>)	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.
Excessive frame counts: <ul style="list-style-type: none"> • Action • Association • Authentication • Deauthentication • Disassociation • Probe • Reassociation 	See IDS (Intrusion Detection System) Faults, page 2-14		
Firmware version policy violation (<i>version number</i>)	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.

Table 2-1 Access Point Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
HotStandBy is active	<p>The access point that is configured for hot standby has become active.</p> <p>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.</p> <p>When this fault is cleared, the following message displays: HotStandBy is disabled.</p>	Manage Fault Settings > Access Point/Bridge Policies > HotStandby Status	<ol style="list-style-type: none"> 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.
<p>Inconsistent device state found: <i>MIB-name table-name. OID-name problem-details</i></p>	<p>One or more configuration values of the AP/BR are either out-of-range or are in conflict with another configuration value. The fault description and corresponding swan.log entry provide details about the suspect value, including the official public MIB name of the SNMP OID for which the error was found.</p> <p>When a radio is declared to have an invalid configuration or has failed, it cannot be manipulated by Radio Management and is removed from SWAN RM operations. For example, if just the 802.11a radio on a WDS is not configured correctly, only that radio is excluded from RM operations; the 802.11b/g radio and the WDS remains fully RM-operational. This behavior can help you isolate the portions of your network that are affected by misconfigurations or failures.</p>	Not applicable.	<p>To resolve an inconsistent configuration, several possibilities exist:</p> <ul style="list-style-type: none"> • It is possible that the most recent Inventory failed for the device. Re-running inventory might clear the condition. • If the configuration value being contested is user-editable, you can correct the problem using the WLSE templates, the AP/BR GUI, or the AP/BR CLI. • If the configuration value being contested is not user-editable, this is probably an IOS error. You will need to upgrade the affected AP/BR to the most recent version of IOS. <p>For information about the MIB referenced in the fault description, see http://www.cisco.com/public/sw-cent er/netmgmt/cmtk/mibs.shtml.</p>

Table 2-1 Access Point Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
MIC is disabled for the VLAN <i>number</i>	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	Log into the access point and enable the VLAN. Then, using the WLSE fault settings, enable the MIC for that VLAN.
Radar Detected on Channel <i>origChannel</i>	On its current channel, the AP detected likely contention with a radar device, so it needs to leave that channel and find another. The AP will automatically scan for another channel, but might be unable to accept associations for one minute. This one minute delay is the required scan time on another Dynamic Frequency Selection channel that must elapse before the AP can accept associations. When this fault is cleared, the following message displays: No radar detected on new channel <i>newChannel</i>	Manage Fault Settings > Radio-802.11a Policies > Dynamic Frequency Selection (DFS)	The WLSE will automatically handle the assignment of another channel for those APs affected by the Radar Detection. However, if these faults become common, you should re-run Assisted Configuration (RPG) soon after a DFS event has occurred (or just manually deselect the DFS channel from the Assisted Config Wizard). This will reorganize the site to avoid the affected channel and make future conflicts likely.
Vlan WEP key length policy violation	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.
WDS appears down.	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.
WDS Registered with another WLSE (<i>IPaddress</i>)	The WDS is registered with a different WLSE.	Manage Fault Settings > WDS > Authentication Failures	Determine which WLSE is supposed to manage that WDS from an RM perspective. Then modify the wnm configuration on the WDS to point to the correct WLSE. For more information, see the managing devices information in the online help or the <i>User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13</i> .

Table 2-1 Access Point Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
WEP is disabled	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	Make sure you have set the policy correctly for the VLAN.
WLSE failed to authenticate with WDS.	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 <i>User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13</i> .

Radio Interface Faults

Table 2-2 Radio Interface Faults

Fault Description	Explanation	Related Setting	Recommended Action
AP is in a Degraded state <i>number</i> associated clients	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	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 <i>number</i> associated clients	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.

Table 2-2 Radio Interface Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Appeared up/down. Compensated for by Up/Down radio(s).	The indicated radio appeared up or down on this AP, so other radios were modified to maintain coverage. After self healing has been applied to the other AP, this fault indicates the radio that had the failure.	Radio Manager > Self Healing > Finish	Display the Self Healing fault details page, then select the document with the eyeglasses. A list of radios with the old and new power settings is displayed. These radios can compensate for the downed or recovered radio. If self healing is configured to automatically apply changes, then these are the values that were applied. If self healing is configured for manual application of the compensation calculations, then the recommended values are shown with an option to apply them to the indicated radios. Check the radio to determine why it is down and resolve the problem.
Broadcast SSID is enabled.	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- <i>x</i> SSID <i>ssid</i> fault.	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- <i>x</i> SSID <i>ssid</i> fault.	Manage Fault Settings > Radio-802.11x Policies > Broadcast SSID	Log in to the access point and make sure that the SSID, which is in WLSE's "Do not Broadcast SSID" list is not selected for Broadcast on the access point.
Client association rate is Degraded <i>number</i> per minute	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 <i>number</i> per minute	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.		
Compensation determination is in progress	The WLSE determined that a radio was down or back up. Self Healing is attempting to compensate for the failed or recovered radio.	Not applicable.	There is no action necessary; Self Healing is attempting to adjust the power on other neighboring radios (which can be on other floors) to maintain coverage.

Table 2-2 Radio Interface Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Compensation calculation did not complete due to errors	Errors forced the cancellation of Self Healing compensation calculations.	Not applicable.	Display the Self Healing fault details page, then select the document with the eyeglasses. The error messages displayed on this page will explain the problem. Determine the action necessary to clear the fault condition.
Compensation finished with errors	Self Healing compensation calculations finished but there were errors. For example, a power change cannot be applied to a radio because: 1) The community strings for the device are wrong for the AP. 2) AP is down or unreachable 3) Wrong configuration set on the radio	Not applicable.	Determine the action necessary to clear the fault condition. For example, if WLSE determines that five radios are needed to compensate for a down radio and only one has bad community strings, the changes to the other four radios will take place.
Compensation did not complete due to timeout of <i>timeout</i> (mins)	Self Healing compensation calculations took longer than 30 minutes.	Not applicable.	Display the Self Healing fault details page, then select the document with the eyeglasses. The error messages displayed on this page will explain the problem. Determine the action necessary to clear the fault condition.
EAP is disabled	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	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	Log in to the access point and make sure the WLSE's Infrastructure SSID matches the access point infrastructure SSID

Table 2-2 Radio Interface Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Not Monitored because: <i>reason, Ignored</i>	To qualify for Self Healing, an AP must: <ul style="list-style-type: none"> • Enable Radio Monitoring on both Serving and Non-Serving channels. • Be configured with a WDS that is authenticated with the WLSE (link status must be okay too). 		The faults will clear when the WDS/WLSE is reauthenticated and Radio Monitoring is enabled correctly.
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 Replays Discarded is OK.	IDS > Manage IDS Settings > IDS-802.11x > CCMP Replays Discarded	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.
Packet Error is in Degraded state (<i>error rate %</i>)	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 Overloaded state (<i>error rate %</i>)	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.		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	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	Explanation	Related Setting	Recommended Action
Port is down	<p>The port is operationally down.</p> <p>When this fault is cleared, the following message displays: Port is up</p>	<p>Manage Fault Settings > Radio-802.11x Thresholds > RF Port AdminStatus</p>	<p>Check the device to determine why the port is down.</p> <p>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.</p> <p>The fault RF Port AdminStatus is enabled by default and must remain enabled with a default polling time of 5 minutes. Self healing ignores any radio set as administratively down, but this can only be detected if fault polling is enabled.</p>
PSPF is disabled	<p>The PSPF port has been disabled.</p> <p>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.</p> <p>When the fault is cleared, the following message displays: The PSPF is enabled.</p>	<p>Manage Fault Settings > Access Point/Bridge Policies > PSPF Enabled</p>	<p>Log in to the access point and enable the PSPF setting.</p>
Requires healing: %reason%.	<p>The indicated radio appeared up or down on this AP. Self Healing has been started.</p> <p>After compensation results have been for other radios, this fault indicates the radio that had the failure.</p>	<p>Not applicable.</p>	<p>There is no action necessary; Self Healing will attempt to adjust the power on other radios on the floor to maintain coverage.</p> <p>Possible reasons self healing is required:</p> <ul style="list-style-type: none"> • An applicable radio is avoiding or no longer avoiding radar. • An AP has unregistered or re-registered with its WDS • A radio that had its beacons heard by other radios has not been heard by any radio (and vice-versa)

Table 2-2 Radio Interface Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action		
<p>Retry Count rate is Degraded <i>number</i> per minute</p> <p>Retry Count rate is Overloaded <i>number</i> per minute</p>	<p>The retry count rate alarm indicates if the wireless medium is congested. The alarm will be raised if the MSDU retransmission rate per minute is greater than the specified threshold. For example, if the overloaded state is set to greater than 90, a fault will be raised for an interface that has more than 90 MSDUs that required retransmission in a minute.</p> <p>When the fault is cleared, the following message displays: Retry Count rate is OK.</p>	<p>Manage Fault Settings > Radio-802.11x Thresholds > Max Retry Count</p>	<p>Verify the threshold settings. There could be too many clients or access points located near the radio interface for which fault is raised. Clear the alarm and increase the threshold, or reduce the polling time.</p>		
<p>RF bandwidth utilization is Degraded (<i>utilization %</i>)</p>	<p>The fault threshold set for the degraded state has been exceeded.</p> <p>When the fault is cleared, the following message displays: RF bandwidth utilization is OK</p>	<p>Manage Fault Settings > Radio-802.11x Thresholds > RF Port Utilization</p>	<p>Verify that the fault threshold is set correctly.</p> <p>If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.</p>		
<p>RF bandwidth utilization is Overloaded (<i>utilization %</i>)</p>	<p>The fault threshold set for the overloaded state has been exceeded.</p> <p>When the fault is cleared, the following message displays: RF bandwidth utilization is OK</p>			<p>Serving and non-serving channel Radio Monitoring must be enabled</p>	<p>For Self Healing to work, all radios on the floor must be configured with Radio Monitoring. The fault will indicate which radios need to be configured with both serving and non serving radio monitoring.</p> <p>When the fault is cleared, the following message displays: Qualifies for Self Healing Monitoring.</p>
<p>Serving and non-serving channel Radio Monitoring must be enabled</p>	<p>For Self Healing to work, all radios on the floor must be configured with Radio Monitoring. The fault will indicate which radios need to be configured with both serving and non serving radio monitoring.</p> <p>When the fault is cleared, the following message displays: Qualifies for Self Healing Monitoring.</p>	<p>Not applicable.</p>	<p>Enable Radio Monitoring for both serving and non-serving channels.</p> <p>Or, use the Location Manager tool, Verify RM Capability.</p>		

Table 2-2 Radio Interface Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
WEP Error is in Degraded state (<i>error rate %</i>)	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 (<i>error rate %</i>)	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		
WEP key length policy violation	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.

IDS (Intrusion Detection System) Faults

Table 2-3 IDS Faults

Fault Description	Explanation	Related Setting	Recommended Action
802.11-B/G Interference Detected - or - 802.11-A Interference Detected	The WLSE detected a non-802.11 interference.	IDS > Manage Network-Wide IDS 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: <i>ssid</i>	An ad-hoc network was formed by some wireless clients (where <i>ssid</i> is the Service Set Identifier of the UnmanagedRadio's BSS). One of your infrastructure APs or other clients sent this information to the WLSE via your WDS setup.	IDS > Manage Network-Wide IDS 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 2-3 IDS Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
<p>Ad-hoc network <i>ssid</i> reclassified from Friendly to Rogue due to <i>rule</i></p>	<p>An ad-hoc network that was previously determined to be Friendly has been reclassified to Rogue.</p> <p><i>ssid</i> is the Service Set Identifier of the unmanaged radio's BSS.</p> <p><i>rule</i> is one of the following:</p> <ul style="list-style-type: none"> • Change in RSSI ordering between observers <p>The estimated proximity of the unmanaged radio between two observers has switched—if the WLSE thought that observer A was closer to radio R than observer B, it now thinks that observer B is closer to radio R than observer A.</p> <ul style="list-style-type: none"> • Difference in relative RSSI between original and current observers exceeded threshold <p>While radio R's strength changed by factor M between observer A and observer B, it changed by factor M+T between observer B and observer C. That is, it does not appear that radio R's change in strength is merely due to a change in its power configuration.</p> <ul style="list-style-type: none"> • Fewer than two observers • Too long without observations 	<p>IDS > Manage Network-Wide IDS Settings > Ad-hoc Network Detection > Friendly to Rogue AP Reclassification</p> <p>or</p> <p>IDS > Manage Rogues</p>	<p>Use the fault details page to mark it friendly if the network is known, or to delete it from the WLSE database if it is unknown.</p>

Table 2-3 IDS Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Bad MIC while MFP enabled	This fault is raised against the AP that is <i>observed</i> generating the violation.	Not applicable.	Investigate the possibility that a rogue AP is conducting a spoofing attack against the managed network. Also, make sure that an MFP configuration error (see MFP Configuration error (Detect disabled; should be enabled) , page 2-19) is not the root cause of the MFP Validation error. It is also possible that communications problems between the WDS and its registered APs have prevented MFP key rotation messages from reaching either the detector or generator AP.
Bad Sequence Number while MFP enabled	This fault is raised against the AP that is <i>observed</i> generating the violation.	Not applicable.	See Bad MIC while MFP enabled , page 2-16).
CCMP DecryptErrorsClient is detected	The fault threshold has been exceeded for the number of decryption errors detected by the CCMP play mechanism on the interface.	IDS > Manage IDS Settings > CcmpDecryptErrorsClient	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.
CCMP Replay Client is detected	The fault threshold set has been exceeded. When this fault is cleared, the following message displays: There is no CCMP Replay detected	IDS > Manage IDS Settings > General Settings > CcmpReplaysClient	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 Degraded <i>number</i> per minute	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Client association rate is OK.	IDS > Manage IDS Settings > IDS-802.11x > 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 2-3 IDS Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Client authentication error rate is Degraded <i>number</i> per minute	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.	IDS > Manage IDS Settings > IDS-802.11x > 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 <i>number</i> per minute	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.		
Client TKIP RemoteMICFailure is detected	A wireless client has detected a MIC failure. The MIB value that is polled is cDot11WidsTkipRemoteMicFailures. When this fault is cleared, the following message displays: There is no TKIP RemoteMICFailure detected.	IDS > Manage IDS Settings > General IDS Settings > TkipRemoteMicFailureClient	Occasionally MIC failures can occur during key rotation. To diagnose the problem, you should: <ul style="list-style-type: none"> • Check the IOS version. • Enable 802.1x logs on the AP. • Perform an SNMP walk of cDot11WidsProtectFailClientTable to determine which clients are reporting the TKIP MIC failure. If just one client is reporting the failure, it could be a client issue
EAPOL FLOOD is detected (Flood count: <i>floodcount</i>)	The fault threshold has been exceeded. When this fault is cleared, the following message displays: There is no EAPOL Flood detected.	IDS > Manage IDS Settings > General IDS Settings > EAPOL Detection	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
Excessive Action Frames in Channel: <i>channel</i> [Frames: <i>framecount</i> ,Interval: <i>windowsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Action Frames not present in Channel.	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Action Frames from STA: <i>station</i> [Frames: <i>framecount</i> ,Interval: <i>windowsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Action Frames from STA: <i>station</i> not present	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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 2-3 IDS Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Excessive Association Frames in Channel: <i>channel</i> [Frames: <i>framecount</i> ,Interval: <i>wind owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Association Frames not present in Channel: <i>channel</i>	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Association Frames from STA: <i>station</i> [Frames: <i>framecount</i> ,Interval: <i>wind owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Association Frames from STA: <i>station</i> not present	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Authentication Frames in Channel: <i>channel</i> [Frames: <i>framecount</i> ,Interval: <i>wind owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Authentication Frames not present in Channel.	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Authentication Frames from STA: <i>station</i> [Frames: <i>framecount</i> ,Interval: <i>wind owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Authentication Frames from STA: <i>station</i> not present	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Deauthentication Frames in Channel: <i>channel</i> [Frames: <i>framecount</i> ,Interval: <i>wind owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Deauthentication Frames not present in Channel.	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Deauthentication Frames from STA: <i>station</i> [Frames: <i>framecount</i> ,Interval: <i>wind owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Deauthentication Frames from STA: <i>station</i> not present	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Disassociation Frames in Channel: <i>channel</i> [Frames: <i>framecount</i> ,Interval: <i>wind owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Disassociation Frames not present in Channel.	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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 2-3 IDS Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Excessive Disassociation Frames from STA: <i>station</i> [Frames: <i>framecount</i> ,Interval: <i>wind</i> <i>owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Disassociation Frames from STA: <i>station</i> not present	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Probe Frames in Channel: <i>channel</i> [Frames: <i>framecount</i> ,Interval: <i>wind</i> <i>owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Probe Frames not present in Channel.	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Probe Frames from STA: <i>station</i> [Frames: <i>framecount</i> ,Interval: <i>wind</i> <i>owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Probe Frames from STA: <i>station</i> not present	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Reassociation Frames in Channel: <i>channel</i> [Frames: <i>framecount</i> ,Interval: <i>wind</i> <i>owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Reassociation Frames not present in Channel.	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
Excessive Reassociation Frames from STA: <i>station</i> [Frames: <i>framecount</i> ,Interval: <i>wind</i> <i>owsize</i>]	The fault thresholds been exceeded. When this fault is cleared, the following message displays: Excessive Reassociation Frames from STA: <i>station</i> not present	IDS > Manage IDS Settings > General IDS Settings > Excessive Management Frame Detection	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.
MFP Configuration error (Detect disabled; should be enabled)	This fault is raised against an AP that contains an MFP-related configuration error. Note No fault is raised against an AP that does <i>not</i> support MFP.	Not applicable.	Restart the affected AP.
MFP Timebase Invalid (bad SNTP)	This fault is raised against an AP that has a bad timebase.	Configure > Templates > Services > SNTP	Configure the AP to reference an SNTP server.
No MIC while MFP Enabled	This fault is raised against the AP that is <i>observed</i> generating the violation.	Not applicable.	See Bad MIC while MFP enabled, page 2-16).

Table 2-3 IDS Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Number of CCMP Replay Discarded is Degraded.	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: Number of CCMP Replays Discarded is OK.	IDS > Manage IDS Settings > IDS-802.11x >CCMP Replays Discarded	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 Replays Discarded is OK.		
Number of EAPOL Flood Count is Degraded	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: EAPOL Flood Count is OK.	IDS > Manage IDS Settings > General IDS Settings > EAPOL Detection	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 EAPOL Flood Count is Overloaded	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: EAPOL Flood Count is OK.		
Number of TKIP counter measure is Degraded.	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: Number of TKIP Counter Measure is OK.	IDS > Manage IDS Settings > IDS-802.11x >TKIP Counter Measure Invoked	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 Counter Measure is OK.		

Table 2-3 IDS Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Number of TKIP Local MIC failures is Degraded.	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: Number of TKIP Local MIC failures is OK.	IDS > Manage IDS Settings > IDS-802.11x >TKIP Local MIC failures	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 Local MIC failures 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 Local MIC failures is OK.		
Number of TKIP Remote MIC failures is Degraded.	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: Number of TKIP Remote MIC failures is OK.	IDS > Manage IDS Settings > IDS-802.11x >TKIP Remote MIC failures	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 Remote MIC failures 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 Remote MIC failures is OK.		
Number of TKIP replay errors is Degraded.	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.	IDS > Manage IDS Settings > IDS-802.11x >TKIP Replays Detected	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.		

Table 2-3 IDS Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Radio Role must be “roleScanner” to support Frame Monitoring (was <i>x</i>).	<p>This fault is raised when a radio is initially configured for Frame Monitoring (where <i>x</i> is the integer value of the SNMP OID cd11IfStationRole from the CISCO-DOT11-IF-MIB), but then someone configures the radio out of scanning-only mode. As a side effect, this also disables Frame Monitoring.</p> <p>When this fault is cleared, the following message displays: Radio Role is “roleScanner” and supports Frame Monitoring.</p>	Radio Mgr > Frame Monitoring	<p>Review your network to determine the action necessary to clear the fault condition.</p> <p>Although this situation might simply be that an administrator no longer needs to monitor or scan a portion of their site any longer, it could also be an intruder who has somehow gained console access to a Scanning AP and is attempting to “blind” IDS services for a portion of a site.</p>
TKIP Replay is detected	<p>The fault threshold set has been exceeded.</p> <p>When this fault is cleared, the following message displays: There is no TKIP Replay detected.</p>	IDS > Manage IDS Settings > General IDS Settings > TkipReplayClient	<p>Verify that the fault threshold is set correctly.</p> <p>If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.</p>
TKIP LocalMICFailure is detected	<p>The fault threshold set has been exceeded.</p> <p>When this fault is cleared, the following message displays: There is no TKIP LocalMICFailure detected.</p>	IDS > Manage IDS Settings > General IDS Settings > TkipLocalMicFailure Client	<p>Verify that the fault threshold is set correctly.</p> <p>If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.</p>
Unexpected MIC while MFP Disabled	This fault is raised against the AP that is <i>observed</i> generating the violation.	Not applicable.	See Bad MIC while MFP enabled, page 2-16).

Table 2-3 IDS Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Unregistered Client(s) present	<p>One or more unregistered clients have been detected in the wireless network, and are unsuccessfully attempting to authenticate with the APs.</p> <p>The unregistered client fault is triggered when an AP in scanning mode detects a number of probe requests and association requests from a station, client, or access point, which crosses the configured threshold in the configured time.</p> <p>The registration attempts are not being made to the scanning AP; the attempts are being made to regular APs that the scanning AP notices.</p> <p>The scanning AP counts the packets per station.</p> <p>(The fault is generated based on the configured Client Registration Request Count within a 15-minute period. The default is 100 registrations, but can be changed to 200, 300, 400 or 500.)</p> <p>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).</p>	IDS > Manage IDS Settings > General IDS Settings > Unregistered Client	<p>Set the priority of the fault to be generated and the threshold for the failed authentication attempts by the client.</p> <p>Make a physical check near the scanning AP that reported this fault to see if there are any rogue clients.</p>
Wireless Client MAC spoofing detected	<p>The WLSE has detected a spoofed MAC address.</p> <p>Whenever the WDS detects an authentication taking place for a known MAC address, it verifies that the same user ID is being used. If the user ID does not match, the authentication is rejected and a fault is issued.</p> <p>When this fault is cleared, the following message displays: No Wireless Client MAC Spoofing Detected.</p>	IDS > Manage IDS Settings > General IDS Settings > Wireless Client MAC Spoofing	Review your network to determine the action necessary to clear the fault condition.

Voice Faults

Table 2-4 Voice Faults

Fault Description	Explanation	Related Setting	Recommended Action
Voice Bandwidth Exceeded [Bandwidth In Use: <i>current%</i> , Threshold: <i>threshold%</i>]	<p>This is a warning that is triggered only when the voice bandwidth in use exceeds the threshold limit.</p> <p>The higher the percentage of bandwidth being used, the less is available for new phone calls to be placed or to roam in. The default configured bandwidth for voice is 75%. After reaching 100% of the configured bandwidth in use, no additional calls can be accepted.</p>	<p>Faults > Manage Fault Settings, then Edit the Default profile. Select RADIO-802.11a THRESHOLDS > Voice Bandwidth.</p>	<p>You can (at the expense of data traffic clients such as laptops) increase the amount of bandwidth reserved for voice traffic. But a better solution would be to find a solution that would reduce the voice traffic on the congested cell.</p>

WLSE Faults

Table 2-5 WLSE Faults

Fault Description	Explanation	Related Setting	Recommended Action
Auto Resite Survey Performance Degradations	<p>There is at least one floor with a 20% difference in the base and current performance values on one or more floors configured for Auto Re-Site Survey.</p> <p>The fault will clear when there are no longer any buildings or any floors with 20% differences in the performance values.</p>	Radio Manager > Auto Re-Site Survey	<p>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.</p> <p>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.</p>
Data may not have been successfully restored from active.	The standby WLSE has detected a failure in the active WLSE and is becoming active before it successfully synchronized with the active WLSE.	Not applicable.	Make sure the WLSEs are correctly configured and functioning properly.

Table 2-5 WLSE Faults

Fault Description	Explanation	Related Setting	Recommended Action
Duplicate IP Detection	<p>During discovery, an AP with a duplicate IP is found and placed in the Duplicate IP folder under Devices > Managed > Manage/Unmanage.</p> <p>This folder contains access points that are in the <i>pending</i> state. A device becomes pending and is placed in this folder when:</p> <ul style="list-style-type: none"> • 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. <p>The IP address shown for a device in this folder is the last known address for the device, before the address change occurred.</p>	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 <i>User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.13.</i> or in the online help.
Fault Engine is overloaded with excessive polling.	<p>The WLSE fault engine is overloaded due a large number of fault policy and threshold polling occurring at one time. This generally occurs when the WLSE is configured to monitor large number of fault policies and thresholds on large number of devices.</p> <p>This fault will clear when the polling rate drops below the internally set threshold.</p>	Not applicable.	<ul style="list-style-type: none"> • Make sure the WLSE has connectivity to the network. • Reduce the amount of fault polling by disabling certain policies and thresholds.
Lost connectivity with router.	The WLSE is unable to ping the default router.	Not applicable.	<p>Make sure that:</p> <ul style="list-style-type: none"> • Connectivity from the WLSE to the gateway router is okay. • The gateway router is functioning properly.
Lost connectivity with standby on ip_address.	The standby WLSE indicated by the IP address is down.	Not applicable.	<p>Make sure that:</p> <ul style="list-style-type: none"> • The standby WLSE is up and running. • The standby WLSE is network accessible. • Redundancy has been correctly setup on the Active WLSE.

Table 2-5 WLSE Faults

Fault Description	Explanation	Related Setting	Recommended Action
Other node is running a different version. Redundancy will be turned off.	A mismatch of WLSE software version has been detected between the active and the standby WLSEs.	Not applicable.	Make sure the correct WLSE software has been installed on both the active and standby WLSEs.
Redundancy active mode enabled	The WLSE sending this message is now active.	Not applicable.	Confirm that both WLSEs are functioning respectively as Active and Standby.
Redundancy standby mode.	The WLSE sending this message is now in standby mode.	Not applicable.	Confirm that both WLSEs are functioning respectively as Active and Standby.
Redundancy turned off.	Redundancy has been disabled.	Not applicable.	Make sure the WLSEs are correctly configured and functioning properly.
Regained connectivity with router.	The WLSE that sent this message is now able to ping the default router.	Not applicable.	Confirm that both WLSEs are functioning respectively as Active and Standby.
Regained connectivity with standby on ip_address	The Standby WLSE is up.	Not applicable.	Confirm that both WLSEs are functioning respectively as Active and Standby.
System check failed on ip_address for reason: reason.	The system check failed.	Not applicable.	Make sure the WLSEs are correctly configured and functioning properly.

AAA Server Faults

Table 2-6 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	Server is reachable but 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.

Table 2-6 AAA Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
EAP-FAST server is not available	EAP-FAST	<p>Can be caused by any of the following reasons:</p> <ul style="list-style-type: none"> • WLSE IP Address is not configured as a NAS on the server. • Shared secret key does not match the key configured on the server. • Server is unreachable. <p>When this fault has been cleared, the following message displays: EAP-MD5 server is available</p>	Manage Fault Settings > AAA > EAP-FAST > Response Time	<p>Check server configuration to make sure that:</p> <ul style="list-style-type: none"> • WLSE IP address is configured as NAS on the server. • Shared secret key matches the key configured on the server
EAP-FAST server is Degraded	EAP-FAST	<p>The fault threshold set for the degraded state has been exceeded.</p> <p>When this fault has been cleared, the following message displays: EAP-FAST server is OK</p>	Manage Fault Settings > AAA > EAP-FAST > Response Time	<p>Verify that the fault threshold is set correctly.</p> <p>If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.</p>
EAP-FAST server is Overloaded	EAP-FAST5	<p>The fault threshold set for the overloaded state has been exceeded.</p> <p>When this fault has been cleared, the following message displays: EAP-FAST server is OK</p>	Manage Fault Settings > AAA > EAP-FAST > Response Time	<p>Verify that the fault threshold is set correctly.</p> <p>If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.</p>
EAP-MD5 server is not available	EAP-MD5	<p>Can be caused by any of the following reasons:</p> <ul style="list-style-type: none"> • WLSE IP Address is not configured as a NAS on the server. • Shared secret key does not match with the key configured on the server. • Server is unreachable. <p>When this fault has been cleared, the following message displays: EAP-MD5 server is available</p>	Manage Fault Settings > AAA > EAP-MD5 > Response Time	<p>Check the server configuration to make sure that:</p> <ul style="list-style-type: none"> • The WLSE IP address is configured as NAS on the server. • The shared secret key matches the key configured on the server

Table 2-6 AAA Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
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	Fault threshold 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	Can be caused by any of the following: <ul style="list-style-type: none"> You enabled this policy and are using a non-Cisco client with EAP. WLSE IP Address is not configured as a NAS on the server. Shared secret key does not match the key configured on the server. 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: <ul style="list-style-type: none"> The WLSE IP address is configured as NAS on the server. The shared secret key matches the key configured on the server
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.

Table 2-6 AAA Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
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 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.
PEAP server is not available	PEAP	Can be caused by any of the following reasons: <ul style="list-style-type: none"> • PEAP monitoring is not enabled. • WLSE IP Address is not configured as a NAS on the server. • Shared secret key does not match with the key configured on the server. • 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: <ul style="list-style-type: none"> • PEAP monitoring is enabled under Manage Fault Settings > AAA > PEAP > Response time. • WLSE IP address is configured as NAS on the authentication server. • If both NICs in the WLSE are assigned an IP, both should be added as NAS in the PEAP authentication server. • Shared secret key matches the key configured on the server. • 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.

Table 2-6 AAA Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
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.
RADIUS server is not available	PEAP	Can be caused by any of the following reasons: <ul style="list-style-type: none"> • WLSE IP Address is not configured as a NAS on the server. • Shared secret key does not match with the key configured on the server. • 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: <ul style="list-style-type: none"> • 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 2-7 Switch Faults

Fault Description	Explanation	Related Setting	Recommended Action
CPU utilization is Degraded (<i>utilization %</i>)	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 (<i>utilization %</i>)	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.
Port is administratively set to down	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 > Switch > Port Status	Confirm that the switch port has been deliberately shut down, and that it is not down due to some other accidental operation.

Table 2-7 Switch Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Port is down.	The port is operationally down. When this fault is cleared, the following message displays: Port is UP.	Manage Fault Settings > Switch > Port Status	Check the switch to determine why the port is down.
Switch memory utilization is Degraded (<i>utilization %</i>)	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 (<i>utilization %</i>)	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.
Switch Port bandwidth utilization is Degraded (<i>utilization %</i>)	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 (<i>utilization %</i>)	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 2-8 Router Fault

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

WLSM Faults

Table 2-9 WLSM Faults

Fault Description	Explanation	Related Setting	Recommended Action
Device was not reachable via SNMP	<p>The SNMP Agent on the WLSM is down.</p> <p>When this fault has been cleared, the following message displays: Device was reachable via SNMP.</p>	Manage Fault Settings > WLSM > SNMP Reachable	Make sure that the SNMP agent is active.
WLSM HSRP state has changed to Active	<p>A switchover has occurred and the standby WLSM has become active.</p> <p>If the WLSM goes back to standby state, the WLSE will automatically clear the fault.</p> <p>Note See the Recommended Actions column for information regarding clearing the fault manually or acknowledging the fault when the the WLSM does not go back to the standby state.</p>	Manage Fault Settings > WLSM > HSRP Standby to Active	<p>Investigate the reason for the switchover. For example it could have been caused by any of the following reasons: the active WLSM might have become defective, it may have been physically pulled out of the chassis, or the configuration may have been modified.</p> <p>After the reason for the switchover has been determined, schedule an inventory job to synchronize the current HSRP states of the WLSMs. After inventory is complete, either move the fault to the Acknowledge state or clear it.</p>

