Review Wireless LAN Controller (WLC) Error and System Messages FAQ

Contents

Introduction

This document describes frequently asked questions (FAQ) on error messages and system messages for the Cisco Wireless LAN (WLAN) Controllers (WLCs).

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Error Messages FAQ

Q. The conversion of more than 200 access points (APs) from Cisco IOS® Software to Lightweight AP Protocol (LWAPP) with a Cisco 4404 WLC was begun. The conversion of 48 APs was completed, and the message received on the WLC stated: `[ERROR] spam_lrad.c 4212: AP cannot join because the maximum number of APs on interface 1 is reached`. Why does the error occur?

A.You must create additional AP-manager interfaces in order to support more than 48 APs. Otherwise, you receive the error that looks like this:

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
the maximum number of APs on interface 1 is reached.
```

Configure multiple AP-manager interfaces and configure primary/backup ports that other AP-manager interfaces do not use. You*must*create a second AP-manager interface in order to bring up additional APs. But make sure that your primary port and backup port configurations for each manager do not overlap. In other words, if AP-manager 1 uses port 1 as the primary and port 2 as the backup, AP-manager 2 must use port 3 as the primary and port 4 as the backup.

Q. I have a Wireless LAN Controller (WLC) 4402 and I use 1240 lightweight access points (LAPs). I enabled 128-bit encryption on the WLC. When I select 128-bit WEP encryption on the WLC, I receive an error that says that 128-bit is not supported on the 1240s: `[ERROR] spam_lrad.c 12839: Not creating SSID mde on CISCO AP xx:xx:xx:xx:xx:xx because WEP128 bit is not supported`. Why do I receive this error?

A.The key lengths shown on the WLCs are actually the number of bits that are in the shared secret and do not include the 24-bits of the Initialization Vector (IV). Many products, which

includes the Aironet products, call it a 128-bit WEP key. In reality it is a 104-bit key with 24-bit IV. The key size of 104-bit is what you must enable on the WLC for 128-bit WEP encryption.

If you choose the 128-bit key size on the WLC, it is actually a 152-bit (128 + 24 IV) WEP key encryption. Only Cisco 1000 Series LAPs (AP1010, AP1020, AP1030) support the use of the WLC 128 bit WEP key setting.

Q. Why do I get the `WEP key size of 128 bits is not supported on 11xx, 12xx and 13xx model APs. WLAN cannot be pushed to these Access Points.` error message when I try to configure WEP on a WLC?

A.On a Wireless LAN Controller, when you choose Static WEP as the Layer 2 Security method, you have these options or the WEP Key Size.

- not set
- 40 bits
- 104 bits
- 128 bits

These key size values do not include the 24-bit Initialization Vector (IV), which is concatenated with the WEP key. So, for a 64-bit WEP, you need to choose**40 bits**as the WEP key size. The controller adds the 24-bit IV to this in order to make a 64-bit WEP key. Similarly, for a 128 bit WEP key, choose**104 bits**.

Controllers also supports 152 bit WEP keys (128 bit + 24 bit IV). This configuration is not supported on the 11xx, 12xx and 13xx model APs. So when you try to configure WEP with 144 bits, the controller gives a message that this WEP configuration is not pushed to 11xx, 12xx and 13xx model APs.

Q. Clients are not able to authenticate to a WLAN that is configured for WPA2, and the controller displays the `apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED: Could not process the RSN and WARP IE. station not using RSN (WPA2) on WLAN requiring RSN.MobileStation:00:0c:f1:0c:51:22, SSID:<>` error message. Why do I receive this error?

A.This mostly occurs due to incompatibility on the client side. Try these steps in order to fix this issue:

- Check if the client is Wi-Fi certified for WPA2 and check the configuration of the client for WPA2.
- Check the data sheet in order to see if the client Utility supports WPA2. Install any patch released by the vendor to support WPA2. If you use Windows Utility, make sure that you have installed theWPA2 patch from Microsoft in order to support WPA2. See **Microsoft** support for more information.
- Upgrade the client Driver and Firmware.
- Turn off Aironet extensions on the WLAN.

Q. Once I reboot the WLC, I get the `Mon Jul 17 15:23:28 2006 MFP Anomaly Detected - 3023 Invalid MIC event(s) found as violated by the radio 00:XX:XX:XX:XX and detected by the dot11 interface at slot 0 of AP 00:XX:XX:XX:XX in 300 seconds when observing Probe responses, Beacon Frames` error message. Why does this error occur and how do I get rid of it?

A.This error message is seen when frames with incorrect MIC values are detected by MFP enabled LAPs. Refer toInfrastructure Management Frame Protection (MFP) with WLC and LAP

Configuration Examplefor more information on MFP. Complete one of these four steps:

1. Check and remove any rogue or invalid APs or clients in your network, which generate invalid frames.
2. Disable the Infrastructure MFP, if MFP is not enabled on other members of the Mobility group as LAPs can hear management frames from LAPs of other WLCs in the group that do not have MFP enabled. Refer toWireless LAN Controller (WLC) Mobility Groups FAQfor more information on Mobility Group.
3. The fix for this error message is available in the WLC releases 4.2.112.0 and 5.0.148.2. Upgrade the WLCs to either of these releases.
4. As a last option, try to reload the LAP that generates this error message.

Q. Client AIR-PI21AG-E-K9 successfully associates with an access point (AP) with Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST). However, when the associated AP is switched off, the client does not roam to another AP. This message appears continuously in the controller message log: "Fri Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: Unable to allow user into the system - perhaps the user is already logged onto the system? Fri Jun 2 14:48:49 2006 [SECURITY] apf_ms.c 2557: Unable to delete username for mobile 00:40:96:ad:75:f4". Why?

A.When the client card needs to roam, it sends an authentication request, but it does not correctly handle keys (does not inform AP/controller, does not answer reauthentication).

This is documented in Cisco bug IDCSCsd02837. This bug has been fixed with Cisco Aironet 802.11a/b/g client adapters Install Wizard 3.5.

In general, the`Unable to delete username for mobile`message also occurs due to any of these reasons:

- The particular username is used on more than one client device.
- Authentication method used for that WLAN has an external anonymous identity. For example, in PEAP-GTC or in EAP-FAST, it is possible to define a generic username as external (visible) identity, and the real username is hidden inside the TLS tunnel between client and radius server, so the controller cannot see it and use it. In such cases, this message can appear. This issue is seen more commonly with some third party and some old firmware client.

Note: Only registered Cisco users can access to internal Cisco bugs information and tools.

Q. When I install the new Wireless Services Module (WiSM) blade in the 6509 switch and implement Protected Extensible Authentication Protocol (PEAP) with the Microsoft IAS server, I receive this error: *Mar 1 00:00:23.526: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY *Mar 1 00:00:23.700: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.Reload Reason: FAILED CRYPTO INIT. *Mar 1 00:00:23.700: %LWAPP-5-CHANGED: LWAPP changed state to DOWN *Mar 1 00:00:23.528: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG:lwapp_crypto_init_ssc_keys_and_certs no certs in the SSC Private File *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: *Mar 1 00:00:23.557: lwapp_crypto_init: PKI_StartSession failed *Mar 1 00:00:23.706: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT. . Why?

A.RADIUS and dot1x debugs show that the WLC sends an access request, but there is no response from the IAS server. Complete these steps in order to troubleshoot the problem:

1. Check and verify the IAS server configuration.

2. Check the log file.
3. Install software, such as Ethereal, which can give you authentication details.
4. Stop and start the IAS service.

Q. The lightweight access points (LAPs) do not register with the controller. What can be the problem? I see these error messages on the controller: `Thu Feb 3 03:20:47 2028: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:f4:f0. Thu Feb 3 03:20:47 2028: Unable to free public key for AP 00:0B:85:68:F4:F0.`

A.When the access point (AP) sends the Lightweight Access Point Protocol (LWAPP) Join Request to the WLC, it embeds its X.509 certificate in the LWAPP message. It also generates a random session ID that is included in the LWAPP Join Request. When the WLC receives the LWAPP Join Request, it validates the signature of the X.509 certificate with the APs public key and checks that the certificate was issued by a trusted certificate authority. It also looks at the start date and time for the AP certificate validity interval and compares that date and time to its own date and time.

This problem can occur due to an incorrect clock setting on the WLC. In order to set the clock on the WLC, issue the **show time** and **config time** commands.

Q. A Lightweight Access Point Protocol (LWAPP) AP is unable to join its controller. The Wireless LAN Controller (WLC) log displays a message similar to this: `LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:ab:01.` Why?

A.You can receive this error message if the LWAPP tunnel between the AP and the WLC traverses a network path with an MTU under 1500 bytes. This causes the fragmentation of the LWAPP packets. This is a known bug in the controller. Refer to Cisco bug IDCSCsd39911.

The solution is to upgrade the controller firmware to 4.0(155).

> **Note**: Only registered Cisco users can access to internal Cisco bugs information and tools.

Q. I want to establish guest tunneling between my internal controller and the virtual anchor controller on the De-Militarized Zone (DMZ). However, when a user attempts to associate with a guest SSID, the user is unable to receive the IP address from the DMZ, as expected. Therefore, the user traffic is not tunneled to the controller on the DMZ. The output of the debug mobile handoff command displays a message similar to this: `Security Policy Mismatch for WLAN <Wlan ID>. Anchor Export Request from Switch IP: <controller Ip address> Ignored.` What is the problem?

A.Guest tunneling provides additional security for guest-user access to the corporate wireless network. This helps to ensure that guest users are unable to access the corporate network without first passing through the corporate firewall. When a user associates with a WLAN that is designated as the guest WLAN, the user traffic is tunneled to the WLAN controller that is located on the DMZ outside of the corporate firewall.

Now, in consideration of this scenario, there can be several reasons for this guest tunneling to not function as expected. As the**debug**command output implies, the problem can be with the mismatch in any of the security policies configured for that particular WLAN in the internal as well as in the DMZ controllers. Check whether the security policies as well as other settings, such as session time out settings, are matched.

Another common reason for this issue is the DMZ controller is not anchored to itself for that

particular WLAN. For a guest tunneling to work properly and for the DMZ to administer the IP address of the user (user that belongs to a guest WLAN), it is essential that proper anchoring is done for that particular WLAN.

Q. I see a lot of `"CPU Receive Multicast Queue is full on Controller"` messages on the 2006 Wireless LAN Controller (WLC), but not on the 4400 WLCs. Why? I have disabled multicast on the controllers. What is the difference in the Multicast Queue Limit between the 2006 and 4400 WLC platforms?

A.Because multicast is disabled on the controllers, the messages that cause this alarm can be Address Resolution Protocol (ARP) messages. There is no difference in queue depth (512 packets) between the 2000 WLCs and the 4400 WLCs. The difference is that the 4400 NPU filters ARP packets whereas everything is done in software on the 2006. This explains why the 2006 WLC sees the messages but not the 4400 WLC. A 44xx WLC processes multicast packets via hardware (through CPU). A 2000 WLC processes multicast packets via software. CPU processing is more efficient than software. Therefore, the 4400's queue is cleared faster, whereas the 2006 WLC struggles a bit when it sees a lot of these messages.

Q. I see the `"[SECURITY] apf_foreignap.c 763: STA [00:0A:E4:36:1F:9B] Received a packet on port 1 but no Foreign AP configured for this port."` error message in one of my controllers. What does this error mean and what steps must I take to resolve it?

A.This message is seen when the controller receives a DHCP request for a MAC address for which it does not have a state machine. This is often seen from a bridge or a system that runs a virtual machine like VMWare. The controller listens to DHCP requests because it performs DHCP snooping so it knows which addresses are associated with clients that are attached to its access points (APs). All traffic for the wireless clients pass through the controller. When the destination of a packet is a wireless client, it goes to the controller and then passes through the Lightweight Access Point Protocol (LWAPP) tunnel to the AP and off to the client. One thing that can be done to help mitigate this message is to only allow the VLANs that are used on the controller onto the trunk that goes to the controller with the**switchport vlan allow**command on the switch.

Q. Why do I see this error message on the console: `Msg 'Set Default Gateway' of System Table failed, Id = 0x0050b986 error value = 0xfffffffc`?

A.This can be due to high CPU load. When the controller CPU is heavily loaded such as when it does file copies or other tasks, it does not have time to process all of the ACKs that the NPU sends in response to configuration messages. When this occurs, the CPU generates error messages. However, the error messages do not impact service or functionality.

For more information, refer to Cisco Wireless LAN Controllers.

Q. I receive these Wired Equivalent Privacy (WEP) key error messages on my wireless control system (WCS): `The WEP Key configured at the station can be wrong. Station MAC Address is 'xx:xx:xx:xx:xx:xx', AP base radio MAC is 'xx:xx:xx:xx:xx:xx' and Slot ID is '1'`. However, I do not use WEP as the security parameter in my network. I only use Wi-Fi Protected Access (WPA). Why do I receive these WEP error messages?

A.If all your security related configurations are perfect, the messages you receive right now are because of bugs. There are some known bugs in the controller. Refer to Cisco bug IDCSCse17260 and Cisco but ID CSCse11202, which state "The WEP Key configured at the station can be wrong with**WPA and TKIP clients respectively**". Actually, Cisco bug ID **CSCse17260**is a duplicate of Cisco bug ID **CSCse11202**. The fix for Cisco but ID

CSCse11202is already available with WLC release 3.2.171.5.

Note: The latest WLC releases has a fix for these bugs.

Note: Only registered Cisco users can access internal Cisco bug information and tools.

Q. I use an external RADIUS server to authenticate wireless clients through the controller. The controller sends this error message regularly: `no radius servers are responding`. Why do I see these error messages?

A.When a request goes out from the WLC to the RADIUS server, each packet has a sequence number to which the WLC expects a response. If there is no response, there is a message that shows`radius-server not responding`.

The default time for the WLC to hear back from the RADIUS server is 2 seconds. This is set from the WLC GUI under**Security > authentication-server**. The maximum is 30 seconds. Therefore, it can be helpful to set this time out value to its maximum in order to resolve this issue.

Sometimes, the RADIUS servers perform**'silent discards'**of the request packet that comes from the WLC. The RADIUS server can reject these packets due to certificate mismatch and several other reasons. This is a valid action by the server. Also, in such cases, the controller can mark the RADIUS server as not responding

In order to overcome the silent discards issue, disable the**aggressive failover**feature in the WLC.

If the**aggressive failover**feature is enabled in WLC, the WLC is too aggressive to mark the AAA server as not responding. However, this must not be done because the AAA server cannot be responsive only to that particular client (it does silent discard). It can be a response to other valid clients (with valid certificates). However, the WLC can still mark the AAA server as not responding and not functional.

In order to overcome this, disable the**aggressive failover**feature. Issue the**config radius aggressive-failover disable**command from the controller CLI in order to perform this. If this is disabled, then the controller only fails over to the next AAA server if there are 3 consecutive clients that fail to receive a response from the RADIUS server.

Q. Several clients are unable to associate to an LWAPP and the controller logs the `IAPP-3-MSGTAG015: iappSocketTask: iappRecvPkt returned error` error message. Why does this happen?

A.This mostly happens due to an issue with the Intel adapters that support CCX v4, but that run a client bundle version earlier than 10.5.1.0. If you upgrade the software to 10.5.1.0 or later, this fixes this issue. Refer to Cisco bug IDCSCsi91347for more information on this error message.

Note: Only registered Cisco users can access internal Cisco bug information and tools.

Q. I see this error message on the Wireless LAN Controller (WLC): `Reached Max EAP-Identity Request retries (21) for STA 00:05:4e:42:ad:c5`. Why?

A.This error message occurs when the user tries to connect to a EAP protected WLAN network and has failed the preconfigured number of EAP attempts. When the user fails to authenticate, the controller excludes the client, and the client cannot connect to the network until the exclusion timer expires or is manually overridden by the administrator.

Exclusion detects authentication attempts made by a single device. When that device exceeds a maximum number of failures, that MAC address is not allowed to associate any longer.

Exclusion occurs:

- After 5 consecutive authentication failures for shared authentications (6th try is excluded)
- After 5 consecutive association failures for MAC authentication (6th try is excluded)
- After 3 consecutive EAP/802.1X authentication failures (4th try is excluded)
- Any external policy server failure (NAC)
- Any IP address duplication instance
- After 3 consecutive web authentication failures (4th try is excluded)

The timer for how long a client is excluded can be configured, and exclusion can be enabled or disabled at the controller or WLAN level.

Q. I see this error message on the Wireless LAN Controller (WLC): `An Alert of Category Switch is generated with severity 1 by Switch WLCSCH01/10.0.16.5 The message of the alert is Controller '10.0.16.5'. RADIUS server(s) are not responding to authentication requests.` What is the issue?

A.This can be because of Cisco bug ID CSCsc05495. Because of this bug, the controller periodically injects an incorrect AV-Pair (attribute 24, "state") into authentication request messages that violate a RADIUS RFP and cause problems for some authentication servers. This bug is fixed in 3.2.179.6.

Note: Only registered Cisco users can access internal Cisco bug information and tools.

Q. I receive a Noise Profile failure message under Monitor > 802.11b/g Radios. I want to understand why I see this FAILED message?

A.The Noise Profile FAILED/PASSED status is set after the test result done by the WLC and in comparison with the current set threshold. By default, the Noise value is set to -70. The FAILED state indicates that the threshold value for that particular parameter or access point (AP) has been exceeded. You can adjust the parameters in the profile, but it is recommended to change the settings after you clearly understand the network design and how it can affect the performance of the network.

The Radio Resource Management (RRM) PASSED/FAILED thresholds are globally set for all APs on the**802.11a Global Parameters > Auto RF**and**802.11b/g Global Parameters > Auto RF**pages. The RRM PASSED/FAILED thresholds are individually set for this AP on the**802.11 AP Interfaces > Performance Profile**page.

Q. I cannot set port 2 as the backup port for the AP-manager interface. The returned error message is `Could not set port configuration.` I am able to set port 2 as the backup port for the management interface. The current active port for both interfaces is port 1. Why?

A.An AP-manager does not have a backup port. It used to be supported in earlier versions. Since version 4.0 and later, the backup port for AP-manager interface is not supported. As a rule, a single AP-manager must be configured on each port (no backups). If you use Link Aggregation (LAG), there is only one AP-manager.

The static (or permanent) AP-manager interface must be assigned to distribution system port 1

and must have a unique IP address. It cannot be mapped to a backup port. It is usually configured on the same VLAN or IP subnet as the management interface, but this is not a requirement.

Q. I see this error message: `The AP '00:0b:85:67:6b:b0' received a WPA MIC error on protocol '1' from Station '00:13:02:8d:f6:41'. Counter measures have been activated and traffic has been suspended for 60 seconds.` Why?

A.Message Integrity Check (MIC) incorporated in Wi-Fi Protected Access (WPA) includes a frame counter which prevents a man-in-the-middle attack. This error means someone in the network wants to replay the message that was sent by the original client, or it can mean that the client is faulty.

If a client repeatedly fails the MIC check, the controller disables the WLAN on the AP interface where the errors are detected for 60 seconds. The first MIC failure is logged, and a timer is initiated in order to enable enforcement of the countermeasures. If a subsequent MIC failure occurs within 60 seconds of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall invalidate itself or invalidate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator.*

Furthermore, the device does not receive or transmit any TKIP-encrypted data frames and does not receive or transmit any unencrypted data frames other than IEEE 802.1X messages, to or from any peer for a period of at least 60 seconds after it detects the second failure. If the device is an AP, it disallows new associations with TKIP during this 60 seconds period; at the end of the 60 seconds period, the AP resumes normal operations and allows STAs to (re)associate.

This prevents a possible attack on the encryption scheme. These MIC errors cannot be turned off in WLC versions prior to 4.1. With Wireless LAN Controller version 4.1 and later, there is a command to change the scan time for MIC errors. The command is**config wlan security tkip hold-down <0-60 seconds> <wlan id>**. Use the value 0 in order to disable MIC failure detection for countermeasures.

*Invalidate: End authentication.

Q. This error message is seen in my controller logs: `[ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate failed.` Why?

A.These error messages are mostly seen when the service port of the controller has DHCP enabled but does not receive an IP address from a DHCP server.

By default, the physical service port interface has a DHCP client installed and looks for an address via DHCP. The WLC attempts to request a DHCP address for the service port. If no DHCP server is available, then a DHCP request for the service port fails. Therefore, this generates the error messages.

The workaround is to configure a static IP address to the service port (even if the service port is disconnected) or have a DHCP server available to assign an IP address to the service port. Then, reload the controller, if needed.

The service port is actually reserved for out-of-band management of the controller and system recovery, and maintenance in the event of a network failure. It is also the only port that is active when the controller is in boot mode. The service port cannot carry 802.1Q tags. Therefore, it must be connected to an access port on the neighbor switch. Use of the service port is optional.

The service port interface controls communications through and is statically mapped by the

system to the service port. It must have an IP address on a different subnet from the management, AP-manager, and any dynamic interfaces. Also, it cannot be mapped to a backup port. The service port can use DHCP in order to obtain an IP address, or it can be assigned a static IP address, but a default gateway cannot be assigned to the service port interface. Static routes can be defined through the controller for remote network access to the service port.

Q. My wireless clients are not able to connect to the wireless LAN (WLAN) network. The WiSM that the access point (AP) is connected to reports this message: `Big NAV Dos attack from AP with Base Radio MAC 00:0g:23:05:7d:d0, Slot ID 0 and Source MAC 00:00:00:00:00:00`. What does this mean?

A.As a condition to access the medium, the MAC Layer checks the value of its network allocation vector (NAV). The NAV is a counter resident at each station that represents the amount of time that the previous frame needs to send its frame. The NAV must be zero before a station can attempt to send a frame. Before the transmission of a frame, a station calculates the amount of time necessary to send the frame based on the frame length and data rate. The station places a value that represents this time in the duration field in the header of the frame. When stations receive the frame, they examine this duration field value and use it as the basis to set their corresponding NAVs. This process reserves the medium for the sending station.

A high NAV indicates the presence of an inflated NAV value (virtual carrier sense mechanism for 802.11). If the MAC address reported is 00:00:00:00:00:00, it probably is spoofed (potentially a real attack) and you need to confirm this with a packet capture.

Q. After I configure the controller and reboot it, I are not able to access the controller in secure web (https) mode. This error message is received while I try to access the controller secure web mode: `Secure Web: Web Authentication Certificate not found (error)`. What is the reason for this problem?

A.There can be several reasons associated with this issue. One common reason can be related to the virtual interface configuration of the controller. In order to resolve this problem, remove the virtual interface and then re-generate it with this command:

```
WLC>config interface address virtual 1.1.1.1
```

Then, reboot the controller. After the controller is rebooted, re-generate the webauth certificate locally on the controller with this command:

```
WLC>config certificate generate webauth
```

In the output of this command, you can see this message:`Web Authentication certificate has been generated`.

You are now able to access the secure web mode of the controller upon reboot.

Q. Controllers sometimes report this IDS Disassociation Flood Signature attack alert message against valid clients in which the attacker MAC address is that of an access point (AP) joined to that controller: `Alert: IDS 'Disassoc flood' Signature attack detected on AP '<AP name>' protocol '802.11b/g' on Controller 'x.x.x.x'. The Signature description is 'Disassociation flood', with precedence 'x'. The attacker mac address is 'hh:hh:hh:hh:hh:hh', channel number is 'x', and the number of detections is 'x'`. Why does this occur?

A.This is because of Cisco bug IDCSCsg81953 .

Note: Only registered Cisco users can access internal Cisco bug information and tools.

IDS Disassociation Flood attacks against valid clients are sometimes reported where the attacker MAC address is that of an AP joined to that controller.

When a client is associated to the AP but stops communicatioins because of card removal, it roams out of range, and so on, to the AP, the AP waits until the idle timeout. Once the idle timeout is reached, the AP sends that client a disassociate frame. When the client does not acknowledge the disassociate frame, the AP retransmits the frame numerous times (around 60 frames). The IDS subsystem of the controller hears these retransmits and alerts with this message.

This bug is resolved in version 4.0.217.0. Upgrade your Controller version to this version in order to overcome this alert message against valid clients and APs.

Q. I receive this error message in the syslog of the controller: `[WARNING] apf_80211.c 2408: Received a message with an invalid supported rate from station <xx:xx:xx:xx:xx:xx> [ERROR] apf_utils.c 198: Missing Supported Rate.` Why?

A.Actually, `Missing Supported Rate` messages indicate that the WLC is configured for certain required data rates under the wireless settings, but the NIC card is missing the required rate.

If you have data rates, such as 1 and 2M, set for required on the controller but the NIC card does not communicate on these data rates, you can receive this kind of message. This is NIC card misbehavior. On the other hand, if your controller is 802.11g is enabled and the client is a 802.11b(only) card, this is a legitimate message. If these messages do not cause any problems and the cards can still connect, these messages can be ignored . If the messages are card specific, then make sure the driver for this card is up to date.

Q. This syslog `AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decode Msg: could not match WLAN ID <id>` error message is broadcast on our network. Why does this occur and how do I stop it?

A.This message is broadcast by the LAPs. This is seen when you have configured WLAN override feature for a WLAN and that particular WLAN is not advertised.

Configure`config ap syslog host global 0.0.0.0`in order to stop it or you can put a specific IP address if you have a syslog server so that message is broadcast to the server alone.

Q. I receive this error message on my wireless LAN controller (WLC): `[ERROR] File: apf_mm.c : Line: 581 : Announce collision for mobile 00:90:7a:05:56:8a, deleting.` Why?

A.Generally, this error message indicates that the controller had announced collisions for a wireless client (that is, separate APs announce that they have the client), and the controller did not receive a handoff from one AP to the next. There is no network state to maintain. Delete the wireless client and have the client try again. If this problem occurs frequently, there can be a problem with mobility configuration. Otherwise, it can be an anomaly that is related to a specific client or condition.

Q. My controller raises this alarm message: `Coverage threshold of '12' violated.` What is this error and how can it be resolved?

A.This alarm message is raised when a client Signal-to-Noise Ratio (SNR) falls to a value that is

less than the SNR threshold value for the particular radio. 12 is the default SNR threshold value for coverage hole detection.

The coverage hole detection and correction algorithm determine if a coverage hole exists when clients' SNR levels are less than a given SNR threshold. This SNR threshold varies based on two values: AP transmit power and the controller coverage profile value.

In detail, the Client SNR threshold is defined by each AP's transmit power (represented in dBm), minus the constant value of 17dBm, minus the user configurable Coverage profile value (this value is defaulted to 12 dB).

- **Client SNR Cutoff Value (|dB|) = [AP Transmit Power (dBm) – Constant (17 dBm) – Coverage Profile (dB)]**

This user configurable coverage profile value can be accessed this way:

1. In the WLC GUI, go to the main heading of Wireless and select the **Network** option for the WLAN standard of choice on the left side (802.11a or 802.11b/g). Then, select **Auto RF** in the upper right of the window.
2. In the Auto RF Global parameters page, find the Profile Thresholds section. In this section, you can find the Coverage (3 to 50 dbm) value. This value is the user configurable coverage profile value.
3. This value can be edited to influence the Client SNR threshold value. The other way to influence this SNR threshold is to increase the transmit power and compensate the coverage hole detection.

Q. I use ACS v 4.1 and a 4402 Wireless LAN Controller (WLC). When the WLC attempts to MAC-authenticate a wireless client to ACS 4.1, the ACS fails to respond with the ACS and reports this error message: " *Internal error has occurred* ". I have all my configurations correct. Why does this internal error occur?

A.There is an authentication related Cisco bug IDCSCsh62641 in the ACS 4.1, where the ACS gives the`Internal error has occured`error message.

This bug can be the issue. There is a patch available for this bug on the ACS 4.1 Downloads site which can fix the problem.

Note: Only registered Cisco users can access internal Cisco bug information and tools.

Q. The Cisco 4400 Series Wireless LAN Controller (WLC) cannot boot. This error message is received on the controller: `** Unable to use ide 0:4 for fatload ** Error (no IRQ) dev 0 blk 0: status 0x51 Error reg: 10 ** Cannot read from device 0.` Why?

A.The reason for this error can be a hardware issue. Open a TAC case to further troubleshoot this problem. In order to open a TAC case, you need to have a valid contract with Cisco. Refer to Technical Support in order to contact the Cisco TAC.

Q. The wireless LAN controller (WLC) runs into memory buffer issues. Once the memory buffers are full, the controller crashes and needs to be rebooted to bring it back online. These error messages are seen in the message log: `Mon Apr 9 10:41:03 2007 [ERROR] dtl_net.c 506: Out of System buffers Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537: Cannot allocate new Mbuf. Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 219: MbufGet: no free Mbufs.` Why?

A.This is due to Cisco bug IDCSCsh93980. This bug has been resolved in WLC version 4.1.185.0. Upgrade your Controller to this software version or later in order to overcome this message.

Note: Only registered Cisco users can access internal Cisco bug information and tools.

Q. I performed the upgrade of our Wireless LAN Controller (WLC) 4400s to 4.1 code and our syslog was bombarded by messages, such as this: `May03 03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93, 0.0.0.0] ARP (op 1) received with invalid SPA 192.168.1.233/TPA 192.168.1.233`. What do these messages indicate?

A.This can occur when WLAN is marked as DHCP required . In such cases, only stations that receive an IP address through DHCP are allowed to associate. Static clients are not allowed to associate to this WLAN. WLC acts as a DHCP relay agent and records IP address of all the stations. This error message is generated when WLC receives ARP request from a station before the WLC has received DHCP packets from the station and recorded its IP address.

Q. When you use Power over Ethernet (PoE) on the Cisco 2106 Wireless LAN Controller, the AP radios are not enabled. The `AP is unable to verify sufficient in-line power. Radio slot disabled.` error message appears. How can I fix this?

A.This error message occurs when the switch, which powers up the Access Point, is a pre-standard switch but the AP does not support Pre-standard mode of input power.

A Cisco pre-standard switch is one that does not support intelligent power management (IPM) but does have sufficient power for a standard access point.

You must enable the**Pre-Standard**mode of power on the AP that is subjected to this error message. This can be done from the Controller CLI with the**config ap power pre-standard {enable | disable} {all | Cisco_AP}**command.

This command must already be configured, if required, if you upgrade to software release 4.1 from a previous release. But, it is possible that you need to enter this command for new installations, or if you reset the AP to Factory Defaults.

These Cisco pre-standard 15-watt switches are available:

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

Q. The Controller generates a `dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED: Unable to add an ARP entry for xx:xx.-xxx.x to the network processor. entry does not exist.` syslog message similar to this. What does this syslog message mean?

A.While some wireless client sends an ARP reply, the Network Processor Unit (NPU) needs to know that reply. So, the ARP reply is forwarded to NPU, but WLC software must not try to add this entry to the network processor. If it does so, these messages are generated. There is no

functionality impact on the WLC due to this, but the WLC does generate this syslog message.

Q. I have installed and configured a new Cisco 2106 WLC. The WLC indicates that the temperature sensor has failed. When you log into the web interface under "controller summary," it says "`sensor failed`" next to internal temperature. Everything else appears to function normally.

A.The internal temperature sensor failure is a cosmetic one and can be resolved with an upgrade to the WLC version 4.2.61.0.

WLC 2106 and WLC 526**built on or after 07/01/2007**can use the temperature sensor chip from another vendor. This new sensor works fine but is not compatible with software later than the 4.2 release. Hence, older software is not able to read the temperature and shows this error. All other controller functionalities are not affected by this defect.

There is a known Cisco bug IDCSCsk97299 related to this issue. This bug is mentioned in the release note of WLC version 4.2.

Note: Only registered Cisco users can access internal Cisco bug information and tools.

Q. I get the `radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND: Could not find appropriate RADIUS server for WLAN <WLAN ID> - unable to find a default server"` message for ALL SSIDs. This message appears even for SSIDs that do not use AAA servers.

A.This error message means that the controller was not able to contact the default radius server or that one was not defined.

One possible reason for this behavior is the Cisco bug IDCSCsk08181, which has been resolved in version 4.2. Upgrade your controller to version 4.2.

Q. The `Message: Jul 10 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 source MAC address is not found.` error message appears on the Wireless LAN controller (WLC). What does this indicate?

A.This means that the controller had an error while it sent a CPU sourced packet.

Q. These error messages appear on the Wireless LAN controller (WLC):

- `Jul 10 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'cliWebInitParms.cfg'`
- `Jul 10 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'rfidInitParms.cfg'`
- `Jul 10 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'dhcpParms.cfg'`
- `Jul 10 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'bcastInitParms.cfg'`
- `Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file : sshpmInitParms.cfg. file removal failed. -Process: Name:fp_main_task, Id:11ca7618`
- `Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file : bcastInitParms.cfg. file removal failed. -Process: Name:fp_main_task, Id:11ca7618`

Q. What do these error message indicate?

A.These messages are informational messages and are part of the normal boot procedure. These messages appear because of a failure to read or delete several different configuration files. When particular configuration files are not found or if the configuration file cannot be read, the config

sequence for each process sends out this message, for example, no DHCP server config, no tags (RF ID) config, and so forth. These are low-severity messages that can safely be ignored. These messages do not interrupt the operation of the controller.

Q. The `HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAIN: Unable to keep rogue 00:14:XX:02:XX:XX in contained state - no available AP to contain.` error message appears. What does this indicate?

A.This means that the AP that performed the rogue containment function is no longer available, and the controller cannot find any suitable AP to perform the rogue containment.

Q. The `DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA 192.168.1.152/TPA 192.168.0.206` system message appears on the Wireless LAN Controller. What does this message imply?

A.It is possible that the system detected ARP spoofing or poisoning. But this message does not necessarily imply that any malicious ARP spoofing has occurred. The message appears when these conditions are true:

- A WLAN is configured with DHCP Required, and a client device, after it associates to that WLAN, transmits an ARP message without first completing DHCP. This can be normal behavior; it can happen, for example, when the client is statically addressed, or when the client holds a valid DHCP lease from a prior association. The error message can look like this example:

```
DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with
invalid SPA 192.168.1.152/TPA 192.168.0.206
```

The effect of this condition is that the client is unable to send or receive any data traffic, until it DHCPs through the WLC.

Refer to the DTL Messagessection ofCisco Wireless LAN Controller System Message Guide for more information.

Q. LAPs do not use Power over Ethernet (POE) to power up. I see the logs on the Wireless LAN Controller:

```
AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD
Cause=Low in-line power
```

Q. What is the issue?

A.This can happen if Power over Ethernet (POE) settings are not configured correctly. When an access point that has been converted to lightweight mode, for example, an AP1131 or AP1242, or a 1250 series access point is powered by a power injector that is connected to a Cisco pre-Intelligent Power Management (pre-IPM) switch, you need to configure Power over Ethernet (PoE), also known as inline power.

Refer to Configure Power over Ethernet, Ethernet Supportfor more information.

Q. You see this message on the Wireless LAN Controller (WLC):

```
*Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary
discovery request from
AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6
```

Q. What does this indicate?

A.Lightweight Access Points trace a certain algorithm to find a controller. The discovery and join process is explained in detail in Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

This error message is seen on the WLC, when it receives a discovery request after it has reached its maximum AP capacity.

If the primary controller for a LAP is not configured or if its a new out of the box LAP, it sends out LWAPP discovery requests to all reachable controllers. If the discovery requests reaches a controller that runs at its full AP capacity, WLC gets the requests and realizes that it is at its maximum AP capacity and does not respond to the request and gives this error.

Q. Where can I find more information on the LWAPP system messages?

A.Refer to Cisco Wireless LAN Controller System Message Guide, 4.2 (Retired)for more information on the LWAPP System messages.

Q. The `Error extracting webauth files` error message appears on the Wireless LAN controller (WLC). What does this indicate?

A.WLC fails to load a Custom Web Authentication/Passthrough bundle if any one of the bundled files has greater than 30 characters in the filename, which includes the file extension. The customized web auth bundle has a limit of up to 30 characters for filenames. Ensure that no filenames within the bundle are greater than 30 characters.

Q. Wireless LAN controllers (WLCs), that runs 5.2 or 6.0 code with a large number of AP Groups, web GUI does not display all configured AP groups. What is the issue?

A.The missing AP groups can be seen if you use the CLI **show wlan ap-groups**command.

Try to add one additional AP Group to the list. For example, 51 AP Groups deployed, and the 51st is missing (Page 3). Add the 52nd group, and Page 3 must appear in the Web GUI.

In order to resolve this issue, upgrade to WLC version 7.0.220.0.

Related Information

- **WiSM Troubleshooting FAQ**
- **Wireless Support Page**
- **Cisco Technical Support & Downloads**