Häufig gestellte Fragen zu Wireless LAN Controller (WLC)-Fehlern und Systemmeldungen

Inhalt

Einführung

Dieses Dokument enthält Informationen zu den am häufigsten gestellten Fragen (FAQs) zu Fehlermeldungen und Systemmeldungen für die Cisco Wireless LAN (WLAN) Controller (WLCs).

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Häufig gestellte Fragen zu Fehlermeldungen

F. Mit der Umstellung von mehr als 200 Access Points (APs) von der Cisco IOS® Software auf das Lightweight AP Protocol (LWAPP) mit einem Cisco 4404 WLC haben wir begonnen. Wir haben die Umwandlung von 48 APs abgeschlossen und erhalten eine Nachricht auf dem WLC mit folgenden Angaben: **[FEHLER] spam_lrad.c 4212: APs können nicht beitreten, da die maximale Anzahl von APs an Schnittstelle 1 erreicht ist.** Warum tritt der Fehler auf?

Antwort: Sie müssen zusätzliche AP-Manager-Schnittstellen erstellen, um mehr als 48 APs unterstützen zu können. Andernfalls erhalten Sie den folgenden Fehler:

```
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.
```

Konfigurieren mehrerer AP-Manager-Schnittstellen und Konfigurieren von primären/Backup-Ports, die von anderen AP-Manager-Schnittstellen nicht verwendet werden. Sie *müssen* eine zweite AP-Manager-Schnittstelle erstellen, um zusätzliche APs zu aktivieren. Stellen Sie jedoch sicher, dass sich die Konfigurationen der primären Ports und Backup-Ports für die einzelnen Manager nicht überschneiden. Wenn also AP-Manager 1 Port 1 als primären und Port 2 als Backup verwendet, muss AP-Manager 2 Port 3 als primären und Port 4 als Backup verwenden.

F. Ich habe einen Wireless LAN Controller (WLC) 4402 und verwende 1240 Lightweight Access Points (LAPs). Ich versuche, die 128-Bit-Verschlüsselung auf dem WLC zu aktivieren. Wenn ich die 128-Bit-WEP-Verschlüsselung auf dem WLC wähle, erhalte ich den Fehler, dass 128-Bit auf den 1240ern nicht unterstützt wird:

[FEHLER] spam_lrad.c 12839: Kein Erstellen von SSID auf CISCO AP xx:xx:xx:xx:xx:xx, da das WEP128-Bit nicht unterstützt wird. Warum erhalte ich diesen Fehler?

Antwort: Die auf den WLCs gezeigten Schlüssellängen sind tatsächlich die Anzahl der Bits, die im gemeinsamen geheimen Bereich enthalten sind und die 24 Bit des Initialization Vector (IV) nicht enthalten. Viele Produkte, zu denen die Aironet-Produkte gehören, nennen es einen 128-Bit-WEP-Schlüssel. In Wirklichkeit ist es ein 104-Bit-Schlüssel mit 24-Bit IV. Die Schlüsselgröße von 104 Bit muss auf dem WLC für die 128-Bit-WEP-Verschlüsselung aktiviert werden.

Wenn Sie die 128-Bit-Schlüssellänge auf dem WLC auswählen, handelt es sich um eine 152-Bit-WEP-Schlüsselverschlüsselung (128 + 24 IV). Nur Cisco LAPs der Serie 1000 (AP1010, AP1020, AP1030) unterstützen die Verwendung der WLC 128 Bit-WEP-Schlüsseleinstellung.

F. Warum erhalte ich die **WEP-Schlüssellänge von 128 Bit wird auf den APs mit den Modellen 11xx, 12xx und 13xx nicht unterstützt? WLAN wird nicht an diese Access Points weitergeleitet.** Fehlermeldung beim Versuch, WEP auf einem WLC zu konfigurieren?

Antwort: Wenn Sie auf einem Wireless LAN-Controller Static WEP als Sicherheitsmethode für Layer 2 auswählen, stehen Ihnen diese Optionen oder die WEP-Schlüsselgröße zur Verfügung.

- nicht festgelegt
- 40 Bit
- 104 Bit
- 128 Bit

Diese Schlüsselgrößenwerte enthalten nicht den 24-Bit-Initialisierungsvektor (IV), der mit dem WEP-Schlüssel verknüpft ist. Für ein 64-Bit-WEP müssen Sie also **40 Bit** als WEP-Schlüsselgröße auswählen. Der Controller fügt diesem die 24-Bit-IV hinzu, um einen 64-Bit-WEP-Schlüssel zu erstellen. Wählen Sie für einen 128-Bit-WEP-Schlüssel auch **104 Bit aus**.

Controller unterstützen auch 152-Bit-WEP-Schlüssel (128 Bit + 24 Bit IV). Diese Konfiguration wird von den APs des Modells 11xx, 12xx und 13xx nicht unterstützt. Wenn Sie also versuchen, WEP mit 144 Bit zu konfigurieren, gibt der Controller die Meldung aus, dass diese WEP-Konfiguration nicht auf die APs des Modells 11xx, 12xx und 13xx übertragen wird.

F. Clients können sich nicht bei einem WLAN authentifizieren, das für WPA2 konfiguriert ist, und der Controller zeigt **apf_80211c:1923 APF-1-PROC_RSN_WARP_IE_FAILED an: RSN und WARP IE konnten nicht verarbeitet werden. Station, die nicht RSN (WPA2) für WLAN verwendet, für die RSN.MobileStation:00:0c:f1:0c:51:22 erforderlich ist, SSID:<>** Fehlermeldung. Warum erhalte ich diesen Fehler?

Antwort: Dies ist vor allem auf Kompatibilitätsprobleme auf Client-Seite zurückzuführen. Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

- Überprüfen Sie, ob der Client für WPA2 Wi-Fi-zertifiziert ist, und überprüfen Sie die Konfiguration des Clients für WPA2.
- Überprüfen Sie im Datenblatt, ob das Client-Dienstprogramm WPA2 unterstützt. Installieren Sie alle vom Anbieter veröffentlichten Patches, um WPA2 zu unterstützen. Wenn Sie das Windows-Dienstprogramm verwenden, stellen Sie sicher, dass Sie den WPA2-Patch von Microsoft installiert haben, um WPA2 zu unterstützen.
- Aktualisieren Sie den Treiber und die Firmware des Clients.

- Deaktivieren Sie Aironet-Erweiterungen im WLAN.

F. Sobald ich den WLC neu starte, erhalte ich den **Mon Jul 17 15:23:28 2006 MFP Anomaly Detected - 3023 Invalid MIC event(s) gefunden, als durch das Funkmodul 00:XX:XX:XX:XX verletzt und von der dot11-Schnittstelle an Steckplatz 0 AP0 erkannt:XX:XX:XX:XX in 300 Sekunden bei Beobachtung von Testantworten, Beacon Frames-**Fehlermeldung. Warum tritt dieser Fehler auf, und wie löse ich ihn aus?

Antwort: Diese Fehlermeldung wird angezeigt, wenn Frames mit falschen MIC-Werten von MFP-fähigen LAPs erkannt werden. Weitere Informationen zum MFP finden Sie unter Infrastructure Management Frame Protection (MFP) mit WLC und LAP Configuration Example. Gehen Sie wie folgt vor:

1. Überprüfen und entfernen Sie nicht autorisierte oder ungültige APs oder Clients in Ihrem Netzwerk, die ungültige Frames erzeugen.
2. Deaktivieren Sie den Infrastruktur-MFP, wenn MFP für andere Mitglieder der Mobilitätsgruppe nicht aktiviert ist, da LAPs Verwaltungs-Frames von LAPs anderer WLCs in der Gruppe hören können, bei denen MFP nicht aktiviert ist. Weitere Informationen zur Mobilitätsgruppe finden Sie in den Häufig gestellten Fragen zu Wireless LAN Controller (WLC) Mobility Groups.
3. Die Behebung dieser Fehlermeldung ist in den WLC-Versionen 4.2.112.0 und 5.0.148.2 verfügbar. Aktualisieren Sie die WLCs auf eine dieser Versionen.
4. Versuchen Sie als letzte Option, die LAP, die diese Fehlermeldung generiert, erneut zu laden.

F. Der Client AIR-PI21AG-E-K9 kann mithilfe von Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) erfolgreich einem Access Point (AP) zugeordnet werden. Wenn der zugeordnete Access Point ausgeschaltet ist, roam der Client jedoch nicht zu einem anderen Access Point. Diese Meldung wird kontinuierlich im Controller-Meldungsprotokoll angezeigt: **"Freitag, 2. Juni, 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: Kann Benutzer nicht in das System einbinden - ist der Benutzer möglicherweise bereits am System angemeldet? Freitag, 2. Juni, 14:48:49 2006 [SECURITY] apf_ms.c 2557: Benutzername für mobil 00:40:96:ad:75:f4 konnte nicht gelöscht werden.** Warum?

Antwort: Wenn die Client-Karte Roaming ausführen muss, sendet sie eine Authentifizierungsanfrage, behandelt jedoch nicht die Schlüssel (informiert den Access Point/Controller nicht und antwortet nicht auf erneute Authentifizierungen).

Dies ist in der Cisco Bug ID CSCsd02837 dokumentiert (nur registrierte Kunden). Dieser Fehler wurde mit dem Installationsassistenten für Cisco Aironet 802.11a/b/g-Client-Adapter 3.5 behoben.

Im Allgemeinen tritt der `Benutzername für mobile` Nachrichten `nicht mehr gelöscht werden kann` auch aus einem der folgenden Gründe auf:

- Der spezifische Benutzername wird auf mehr als einem Client-Gerät verwendet.
- Die für dieses WLAN verwendete Authentifizierungsmethode hat eine externe anonyme Identität. In PEAP-GTC oder EAP-FAST kann beispielsweise ein generischer Benutzername als externe (sichtbare) Identität definiert werden, und der tatsächliche Benutzername ist im TLS-Tunnel zwischen Client- und Radius-Server verborgen, sodass der Controller ihn nicht

sehen und verwenden kann. In solchen Fällen kann diese Meldung angezeigt werden. Dieses Problem tritt häufiger bei einigen Drittanbietern und älteren Firmware-Clients auf.

F. Wenn ich den neuen Wireless Services Module (WiSM)-Blade im 6509-Switch installiere und PEAP (Protected Extensible Authentication Protocol) mit dem Microsoft IAS-Server implementiere, erhalte ich den folgenden Fehler: ***01.03.23.526: %LWAPP-5-CHANGED: LWAPP hat den Status "ERKENNUNG" geändert *1. März 00:00:23.700: %SYS-5-RELOAD: LWAPP CLIENT fordert Neuladen Grund: KRYPTO-INIT FEHLGESCHLAGEN. *01.03.23.700: %LWAPP-5-CHANGED: LWAPP hat sich in "DOWN *Mar 1 00:00:23.528" geändert: %LWAPP-5-CHANGED: LWAPP hat den Status "ERKENNUNG" geändert *1. März 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG:lwapp_crypto_init_ssc_keys_and_certs no certs in der SSC-privaten Datei *00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: *01.03.23.557: lwapp_crypto_init: PKI_StartSession ist fehlgeschlagen *März 1, 00:00:23.706: %SYS-5-RELOAD: Wird vom LWAPP-CLIENT angefordert. .** Warum?

Antwort: RADIUS- und dot1x-Debug zeigen, dass der WLC eine Zugriffsanforderung sendet, aber keine Antwort vom IAS-Server gibt. Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Überprüfen und überprüfen Sie die IAS-Serverkonfiguration.
2. Überprüfen Sie die Protokolldatei.
3. Installieren Sie Software, wie Ethereal, die Ihnen Authentifizierungsdetails geben kann.
4. Beenden und starten Sie den IAS-Dienst.

F. Die Lightweight Access Points (LAPs) können nicht beim Controller registriert werden. Was könnte das Problem sein? Auf dem Controller werden folgende Fehlermeldungen angezeigt: **Do. 03:20:47 2028: LWAPP Join-Request enthält kein gültiges Zertifikat in CERTIFICATE_PAYLOAD ab AP 00:0b:85:68:f4:f0. Do. 03:20:47 2028: Öffentlicher Schlüssel für AP 00:0B:85:68:F4:F0 konnte nicht freigegeben werden.**

Antwort: Wenn der Access Point (AP) die LWAPP-Join Request (Lightweight Access Point Protocol) an den WLC sendet, fügt er sein X.509-Zertifikat in die LWAPP-Nachricht ein. Außerdem wird eine zufällige Sitzungs-ID generiert, die in der LWAPP-Join-Anforderung enthalten ist. Wenn der WLC die LWAPP-Join-Anforderung empfängt, validiert er die Signatur des X.509-Zertifikats mit dem öffentlichen Schlüssel der APs und überprüft, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde. Darüber hinaus werden das Startdatum und die Uhrzeit für das Gültigkeitsintervall der AP-Zertifikate überprüft und das Datum und die Uhrzeit mit dem Datum und der Uhrzeit des Datums verglichen.

Dieses Problem kann durch eine falsche Takteinstellung auf dem WLC auftreten. Um die Uhr auf dem WLC festzulegen, geben Sie die Befehle **show time** und **config time ein**.

F. Ein LWAPP-AP (Lightweight Access Point Protocol) kann seinem Controller nicht beitreten. Das WLC-Protokoll (Wireless LAN Controller) zeigt eine ähnliche Meldung an: **LWAPP Join-Request enthält kein gültiges Zertifikat in CERTIFICATE_PAYLOAD ab AP 00:0b:85:68:ab:01.** Warum?

Antwort: Sie können diese Fehlermeldung erhalten, wenn der LWAPP-Tunnel zwischen dem AP und dem WLC einen Netzwerkpfad mit einer MTU unter 1.500 Byte durchläuft. Dies verursacht die Fragmentierung der LWAPP-Pakete. Dies ist ein bekannter Fehler im Controller. Weitere Informationen finden Sie unter Cisco Bug ID CSCsd39911 (nur registrierte Kunden).

Die Lösung besteht darin, die Controller-Firmware auf 4.0(155) zu aktualisieren.

F. Ich versuche, ein Gast-Tunneling zwischen meinem internen Controller und dem virtuellen Anker-Controller in der De-Militarized Zone (DMZ) einzurichten. Wenn ein Benutzer jedoch versucht, eine Verbindung zu einer Gast-SSID herzustellen, kann er die IP-Adresse nicht wie erwartet von der DMZ erhalten. Der Benutzerdatenverkehr wird daher nicht an den Controller der DMZ weitergeleitet. Die Ausgabe des Befehls debug mobile Handoff zeigt eine ähnliche Meldung an: **Nicht übereinstimmende Sicherheitsrichtlinien für WLAN <WLAN-ID>. Anker-Exportanforderung von der Switch-IP: <Controller-IP-Adresse> ignoriert.** Was ist das Problem?

Antwort: Gast-Tunneling bietet zusätzliche Sicherheit für den Gastzugriff auf das Wireless-Netzwerk des Unternehmens. Dadurch wird sichergestellt, dass Gastbenutzer nicht auf das Unternehmensnetzwerk zugreifen können, ohne zuvor die Firewall des Unternehmens durchlaufen zu haben. Wenn ein Benutzer einem WLAN zuordnet, das als Gast-WLAN festgelegt ist, wird der Benutzerdatenverkehr an den WLAN-Controller getunnelt, der sich außerhalb der Unternehmens-Firewall in der DMZ befindet.

In diesem Szenario kann es mehrere Gründe dafür geben, dass dieses Gasttunnel nicht wie erwartet funktioniert. Wie die Ausgabe des **Befehls debug** impliziert, liegt das Problem möglicherweise in einer der für dieses WLAN konfigurierten Sicherheitsrichtlinien im internen WLAN sowie in den DMZ-Controllern. Überprüfen Sie, ob die Sicherheitsrichtlinien und andere Einstellungen, z. B. die Timeout-Einstellungen für Sitzungen, zugeordnet wurden.

Ein weiterer häufiger Grund für dieses Problem ist, dass der DMZ-Controller nicht an sich selbst für das jeweilige WLAN verankert ist. Damit ein Gast-Tunneling ordnungsgemäß funktioniert und die DMZ die IP-Adresse des Benutzers (eines Benutzers, der zu einem Gast-WLAN gehört) verwalten kann, muss für dieses WLAN unbedingt eine ordnungsgemäße Verankerung erfolgen.

F. Auf dem Wireless LAN Controller 2006 (WLC), aber nicht auf den 4400 WLCs sehe ich viele Meldungen **"CPU Receive Multicast Queue is full on Controller" (CPU-EmpfangsMulticast-Warteschlange ist voll auf Controller).** Warum? Ich habe Multicast auf den Controllern deaktiviert. Worin besteht der Unterschied im Multicast Queue Limit zwischen den WLC-Plattformen 2006 und 4400?

Antwort: Da Multicast auf den Controllern deaktiviert ist, können die Nachrichten, die diesen Alarm auslösen, ARP-Nachrichten (Address Resolution Protocol) sein. Zwischen den 2000 WLCs und den 4400 WLCs besteht kein Unterschied in der Warteschlangentiefe (512 Pakete). Der Unterschied besteht darin, dass die 4400-NPU ARP-Pakete filtert, während alles in der Software für das Jahr 2006 erfolgt. Dies erklärt, warum der WLC 2006 zwar die Meldungen, aber nicht den 4400 WLC sieht. Ein 44xx-WLC verarbeitet Multicast-Pakete über Hardware (über CPU). Ein 2000 WLC verarbeitet Multicast-Pakete über Software. Die CPU-Verarbeitung ist effizienter als die Software. Daher wird die Warteschlange der 4400 schneller gelöscht, während der WLC des Jahres 2006 ein wenig zu kämpfen hat, wenn er viele dieser Meldungen sieht.

F. Ich sehe den **"[SECURITY] apf_foreignap.c 763: STA [00:0A:E4:36:1F:9B] Ein Paket an Port 1 empfangen, aber kein externer Access Point für diesen Port konfiguriert."** Fehlermeldung in einem meiner Controller. Was bedeutet dieser Fehler, und welche Schritte sollte ich unternehmen, um ihn zu beheben?

Antwort: Diese Meldung wird angezeigt, wenn der Controller eine DHCP-Anfrage für eine MAC-Adresse empfängt, für die er keinen Statuscomputer hat. Dies wird häufig über eine Bridge oder ein System beobachtet, das eine virtuelle Maschine wie VMWare ausführt. Der Controller überwacht DHCP-Anfragen, da er DHCP-Snooping ausführt, sodass er weiß, welche Adressen Clients mit seinen Access Points (APs) verbunden sind. Der gesamte Datenverkehr für die Wireless-Clients wird über den Controller geleitet. Wenn das Ziel eines Pakets ein Wireless-Client ist, wird es an den Controller weitergeleitet und dann über den LWAPP-Tunnel (Lightweight Access Point Protocol) an den AP und den Client weitergeleitet. Eine Möglichkeit, diese Meldung abzuschwächen, besteht darin, nur die VLANs zuzulassen, die auf dem Controller im Trunk verwendet werden, der zum Controller mit dem Befehl **switchport vlan allow** auf dem Switch geht.

F. Warum wird diese Fehlermeldung in der Konsole angezeigt? `Msg 'Set Default Gateway' der Systemtabelle fehlgeschlagen, Id = 0x0050b986 Fehlerwert = 0xfffffc`?

Antwort: Dies kann auf eine hohe CPU-Last zurückzuführen sein. Wenn die Controller-CPU stark geladen ist, z. B. wenn sie Dateikopien oder andere Aufgaben ausführt, hat sie keine Zeit, alle ACKs zu verarbeiten, die die NPU als Antwort auf Konfigurationsmeldungen sendet. In diesem Fall generiert die CPU Fehlermeldungen. Die Fehlermeldungen wirken sich jedoch nicht auf den Service oder die Funktionalität aus.

Dies ist im Abschnitt Heavily Loaded Controller CPU in den Versionshinweisen für Cisco Wireless LAN Controller und Lightweight Access Points für Version 3.2.116.21 dokumentiert.

F. Ich erhalte folgende WEP-Schlüsselfehlermeldungen (Wired Equivalent Privacy) auf meinem Wireless Control System (WCS): `Der an der Station konfigurierte WEP-Schlüssel ist möglicherweise falsch. Station MAC Address ist 'xx:xx:xx:xx:xx:xx', AP Base Radio MAC ist 'xx:xx:xx:xx:xx:xx' und Steckplatz-ID '1'`. Ich verwende WEP jedoch nicht als Sicherheitsparameter in meinem Netzwerk. Ich verwende nur Wi-Fi Protected Access (WPA). Warum erhalte ich diese WEP-Fehlermeldungen?

Antwort: Wenn alle Ihre Sicherheitskonfigurationen perfekt sind, dann werden die Nachrichten, die Sie gerade erhalten, aufgrund von Bugs angezeigt. Im Controller gibt es einige bekannte Fehler. Informationen hierzu finden Sie in den Cisco Bug-IDs CSCse17260 (nur registrierte Kunden) und CSCse1202 (nur registrierte Kunden), in denen "Der an der Station konfigurierte WEP-Schlüssel ist möglicherweise mit WPA- bzw. TKIP-Clients falsch" angegeben ist. Tatsächlich ist **CSCse17260** ein Duplikat von **CSCse11202**. Die Behebung für **CSCse11202** ist bereits in der WLC-Version 3.2.171.5 verfügbar.

Hinweis: Die neuesten WLC-Versionen haben eine Behebung für diese Fehler.

F. Wir verwenden einen externen RADIUS-Server, um Wireless-Clients über den Controller zu authentifizieren. Der Controller sendet diese Fehlermeldung regelmäßig: `keine Radius-Server reagieren`. Warum werden diese Fehlermeldungen angezeigt?

Antwort: Wenn eine Anforderung vom WLC an den RADIUS-Server gesendet wird, verfügt jedes Paket über eine Sequenznummer, auf die der WLC eine Antwort erwartet. Wenn keine Antwort vorliegt, wird eine Meldung angezeigt, dass der `Radius-Server nicht reagiert`.

Die Standardzeit für die Rückmeldung des WLC vom RADIUS-Server beträgt 2 Sekunden. Diese

Einstellung wird in der WLC-GUI unter **Sicherheit > Authentication-Server** festgelegt. Das Maximum ist 30 Sekunden. Daher kann es hilfreich sein, diesen Timeoutwert auf den Maximalwert festzulegen, um dieses Problem zu beheben.

Manchmal führen die RADIUS-Server **"stille Rückwürfe"** des Anforderungspakets aus, das vom WLC kommt. Der RADIUS-Server kann diese Pakete aufgrund einer nicht übereinstimmenden Zertifikaten und aus anderen Gründen ablehnen. Dies ist eine gültige Aktion des Servers. In solchen Fällen markiert der Controller außerdem den RADIUS-Server als nicht antworten.

Um das Problem der stillen Rückwürfe zu beheben, deaktivieren Sie die **aggressive Failover-**Funktion im WLC.

Wenn die **aggressive Failover-**Funktion in WLC aktiviert ist, ist der WLC zu aggressiv, um den AAA-Server als nicht reagiert zu markieren. Dies sollte jedoch nicht geschehen, da der AAA-Server möglicherweise nicht nur auf diesen Client reagiert (indem er stumm verworfen). Es kann eine Antwort auf andere gültige Clients sein (mit gültigen Zertifikaten). Der WLC kann jedoch weiterhin angeben, dass der AAA-Server nicht reagiert und nicht funktioniert.

Um dies zu vermeiden, deaktivieren Sie die **aggressive Failover-**Funktion. Führen Sie dazu den Befehl **Config** RADIUS **Aggressive-Failover Disable** (**aggressiv-Failover-Deaktivierung für den Konfigurationsradius** von der Controller-CLI aus. Wenn diese Option deaktiviert ist, wird der Controller nur dann zum nächsten AAA-Server umgeleitet, wenn drei aufeinander folgende Clients keine Antwort vom RADIUS-Server erhalten.

F. Mehrere Clients können keine Verbindung zu einem LWAPP herstellen, und der Controller protokolliert `IAPP-3-MSGTAG015: iappSocketTask: iappRecvPkt hat` Fehlermeldung `zurückgegeben.` Warum geschieht das?

Antwort: Dies ist in der Regel auf ein Problem mit den Intel Adaptern zurückzuführen, die CCX v4 unterstützen, aber eine Client-Paketversion vor 10.5.1.0 ausführen. Wenn Sie die Software auf 10.5.1.0 oder höher aktualisieren, wird dieses Problem behoben. Weitere Informationen zu dieser Fehlermeldung finden Sie unter Cisco Bug ID CSCsi91347 (nur registrierte Kunden).

F. Diese Fehlermeldung wird auf dem Wireless LAN Controller (WLC) angezeigt: `Max EAP-Identity Request Retries (21) für STA 00:05:4e:42:ad:c5 erreicht.` Warum?

Antwort: Diese Fehlermeldung wird angezeigt, wenn der Benutzer versucht, eine Verbindung zu einem EAP-geschützten WLAN-Netzwerk herzustellen, und die vorkonfigurierte Anzahl von EAP-Versuchen fehlgeschlagen ist. Wenn der Benutzer sich nicht authentifiziert, schließt der Controller den Client aus, und der Client kann keine Verbindung zum Netzwerk herstellen, bis der Ausschlusszeitgeber abläuft oder vom Administrator manuell überschrieben wird.

Mit Exclusion werden Authentifizierungsversuche eines einzelnen Geräts erkannt. Wenn dieses Gerät eine maximale Anzahl von Ausfällen überschreitet, darf diese MAC-Adresse nicht mehr verknüpft werden.

Ausschluss erfolgt:

- Nach 5 aufeinander folgenden Authentifizierungsfehlern für gemeinsam genutzte Authentifizierungen (6. Versuch ist ausgeschlossen)
- Nach 5 aufeinander folgenden Verbindungsfehlern für die MAC-Authentifizierung (6. Versuch

ist ausgeschlossen)
- Nach drei aufeinander folgenden EAP/802.1X-Authentifizierungsfehlern (4. Versuch ist ausgeschlossen)
- Alle externen Richtlinienserver-Fehler (NAC)
- Beliebige Instanz von IP-Adressen
- Nach drei aufeinander folgenden Webauthentifizierungsfehlern (4. Versuch ist ausgeschlossen)

Der Timer für die Ausschlusszeit eines Clients kann konfiguriert werden, und der Ausschluss kann auf Controller- oder WLAN-Ebene aktiviert oder deaktiviert werden.

F. Diese Fehlermeldung wird auf dem Wireless LAN Controller (WLC) angezeigt: `Eine Warnung zu einem Kategorie-Switch wird mit dem Schweregrad 1 von Switch WLCSCH01/10.0.16.5 generiert. Die Meldung der Warnung lautet Controller '10.0.16.5'. RADIUS-Server reagieren nicht auf Authentifizierungsanforderungen.` Worum geht es?

Antwort: Dies kann an der Cisco Bug-ID CSCsc05495 liegen. Aufgrund dieses Fehlers fügt der Controller regelmäßig ein falsches AV-Pair (Attribut 24, "state") in Authentifizierungsanforderungsnachrichten ein, die gegen einen RADIUS-RFP verstoßen und Probleme bei einigen Authentifizierungsservern verursachen. Dieser Fehler wurde in 3.2.179.6 behoben.

F. Ich erhalte unter Monitor > 802.11b/g Radios eine Störungsmeldung für das Rauschprofil. Ich möchte verstehen, warum ich diese FEHLGESCHLAGENE Nachricht sehe?

Antwort: Der Status "Rauschprofil FEHLGESCHLAGEN/PASSED" wird nach dem Testergebnis des WLC und im Vergleich zum aktuellen Grenzwert festgelegt. Der Rauschwert ist standardmäßig auf -70 festgelegt. Der FEHLER-Status gibt an, dass der Schwellenwert für diesen bestimmten Parameter oder Access Point (AP) überschritten wurde. Sie können die Parameter im Profil anpassen. Es wird jedoch empfohlen, die Einstellungen zu ändern, nachdem Sie das Netzwerkdesign und dessen Auswirkungen auf die Netzwerkleistung verstanden haben.

Die Grenzwerte für das Radio Resource Management (RRM) PASSED/FAILED (Funkressourcenmanagement, RRM) sind global für alle APs auf den **globalen Parametern 802.11a > Auto RF** und **802.11b/g Global Parameters > Auto RF-**Seiten festgelegt. Die RRM PASSED/FAILED-Grenzwerte für diesen Access Point werden auf der Seite **802.11 AP-Schnittstellen > Leistungsprofil** einzeln festgelegt.

F. Ich kann Port 2 nicht als Backup-Port für die AP-Manager-Schnittstelle festlegen. Die Fehlermeldung `Konnte die Portkonfiguration nicht festlegen.` Ich kann Port 2 als Backup-Port für die Verwaltungsschnittstelle festlegen. Der derzeit aktive Port für beide Schnittstellen ist Port 1. Warum?

Antwort: Ein AP-Manager verfügt über keinen Backup-Port. Früher wurde es in früheren Versionen unterstützt. Seit Version 4.0 und höher wird der Backup-Port für die AP-Manager-Schnittstelle nicht unterstützt. In der Regel sollte an jedem Port ein einzelner AP-Manager konfiguriert werden (keine Backups). Wenn Sie Link Aggregation (LAG) verwenden, gibt es nur einen AP-Manager.

Die statische (oder permanente) AP-Manager-Schnittstelle muss dem Distribution System-Port 1 zugewiesen werden und über eine eindeutige IP-Adresse verfügen. Sie kann keinem Backup-Port

zugeordnet werden. Sie wird in der Regel im selben VLAN oder IP-Subnetz wie die Verwaltungsschnittstelle konfiguriert, dies ist jedoch nicht erforderlich.

F. Ich sehe diese Fehlermeldung: **Der AP '00:0b:85:67:6b:b0' hat von Station '00:13:02:8d:f6:41' einen WPA-MIC-Fehler beim Protokoll '1' erhalten. Zählermessungen wurden aktiviert, und der Datenverkehr wurde 60 Sekunden lang unterbrochen.** Warum?

Antwort: Die in Wi-Fi Protected Access (WPA) integrierte Message Integrity Check (MIC) umfasst einen Frame-Zähler, der einen Man-in-the-Middle-Angriff verhindert. Dieser Fehler bedeutet, dass jemand im Netzwerk versucht, die vom ursprünglichen Client gesendete Nachricht erneut abzuspielen, oder dass der Client fehlerhaft ist.

Wenn ein Client die MIC-Prüfung wiederholt nicht durchführt, deaktiviert der Controller das WLAN auf der AP-Schnittstelle, auf der die Fehler für 60 Sekunden erkannt werden. Der erste MIC-Fehler wird protokolliert, und es wird ein Timer initiiert, um die Durchsetzung der Gegenmaßnahmen zu ermöglichen. Tritt innerhalb von 60 Sekunden nach dem letzten Ausfall ein nachfolgender MIC-Fehler auf, muss sich ein STA, dessen IEEE 802.1X-Einheit als Supplicant fungiert hat, selbst deauthentifizieren oder alle STAs mit einer Sicherheitszuordnung deauthentifizieren, wenn seine IEEE 802.1X-Einheit als Authentifizierer fungiert.

Darüber hinaus empfängt oder übermittelt das Gerät keine TKIP-verschlüsselten Datenframes und empfängt oder übermittelt keine unverschlüsselten Datenframes außer IEEE 802.1X-Nachrichten über einen Zeitraum von mindestens 60 Sekunden, nachdem das Gerät den zweiten Fehler entdeckt hat. Wenn es sich bei dem Gerät um einen Access Point handelt, werden in diesem Zeitraum von 60 Sekunden neue Verknüpfungen mit TKIP deaktiviert. Nach Ablauf des 60-Sekunden-Zeitraums nimmt der Access Point den normalen Betrieb wieder auf und ermöglicht die (erneute) Zuweisung von STAs.

Dadurch wird ein möglicher Angriff auf das Verschlüsselungsschema verhindert. Diese MIC-Fehler können in WLC-Versionen vor 4.1 nicht deaktiviert werden. Bei Wireless LAN Controller ab Version 4.1 gibt es einen Befehl zum Ändern der Abtastzeit bei MIC-Fehlern. Der Befehl lautet **config wlan security tkip hold-down <0-60 Sekunden> <wlan id>**. Verwenden Sie den Wert 0, um die MIC-Fehlererkennung für Gegenmaßnahmen zu deaktivieren.

F. Diese Fehlermeldung wird in meinen Controller-Protokollen angezeigt: **[ERROR] dhcp_support.c 357: DHCP_bind(): servPort dhcpstate ist fehlgeschlagen.** Warum?

Antwort: Diese Fehlermeldungen werden meist angezeigt, wenn der Service-Port des Controllers DHCP aktiviert hat, aber keine IP-Adresse von einem DHCP-Server empfängt.

Standardmäßig ist auf der Schnittstelle des physischen Service-Ports ein DHCP-Client installiert, der über DHCP nach einer Adresse sucht. Der WLC versucht, eine DHCP-Adresse für den Service-Port anzufordern. Wenn kein DHCP-Server verfügbar ist, schlägt eine DHCP-Anfrage für den Service-Port fehl. Dadurch werden die Fehlermeldungen generiert.

Die Lösung besteht darin, eine statische IP-Adresse für den Service-Port zu konfigurieren (selbst wenn der Service-Port getrennt ist) oder einen DHCP-Server zur Verfügung zu haben, um dem Service-Port eine IP-Adresse zuzuweisen. Laden Sie dann den Controller bei Bedarf neu.

Der Service-Port ist für die Out-of-Band-Verwaltung des Controllers und der Systemwiederherstellung sowie für die Wartung bei einem Netzwerkausfall reserviert. Er ist auch der einzige aktive Port, wenn sich der Controller im Startmodus befindet. Der Service-Port kann

keine 802.1Q-Tags enthalten. Daher muss es mit einem Access-Port am Nachbarswitch verbunden werden. Die Verwendung des Service-Ports ist optional.

Die Service-Port-Schnittstelle steuert die Kommunikation über und wird dem Service-Port vom System statisch zugeordnet. Sie muss eine IP-Adresse in einem anderen Subnetz als Management, AP-Manager und alle dynamischen Schnittstellen haben. Außerdem kann er nicht einem Backup-Port zugeordnet werden. Der Service-Port kann DHCP verwenden, um eine IP-Adresse abzurufen, oder ihm kann eine statische IP-Adresse zugewiesen werden, aber ein Standard-Gateway kann der Service-Port-Schnittstelle nicht zugewiesen werden. Über den Controller können statische Routen für den Remote-Netzwerkzugriff auf den Service-Port definiert werden.

F. Meine Wireless-Clients können keine Verbindung zum WLAN-Netzwerk herstellen. Das WiSM, mit dem der Access Point (AP) verbunden ist, meldet folgende Meldung: **Big NAV Dos-Angriff vom AP mit Base Radio MAC 00:0g:23:05:7d:d0, Steckplatz-ID 0 und Quell-MAC 00:00:00:00:00:00.** Was bedeutet das?

Antwort: Als Voraussetzung für den Zugriff auf das Medium überprüft die MAC-Schicht den Wert des Netzwerkzuweisungsvektors (NAV). Das NAV ist ein in jeder Station vorhandener Zähler, der die Zeit darstellt, die der vorherige Frame senden muss. Die NAV muss 0 sein, bevor eine Station versuchen kann, einen Frame zu senden. Vor der Übertragung eines Frames berechnet eine Station die zum Senden des Frames benötigte Zeit basierend auf der Länge und der Datenrate des Frames. Die Workstation platziert einen Wert, der diese Zeit im Feld "Dauer" im Header des Frames darstellt. Wenn Stationen den Frame empfangen, überprüfen sie diesen Wert für das Zeitintervall und verwenden ihn als Grundlage für die Festlegung der zugehörigen NAVs. Dieser Prozess reserviert das Medium für die Sendestation.

Ein hoher NAV weist auf einen überhöhten NAV-Wert hin (Virtual Carrier Sense Mechanismus für 802.11). Wenn die gemeldete MAC-Adresse 00:00:00:00:00:00 lautet, wird sie wahrscheinlich getäuscht (möglicherweise ein echter Angriff), und Sie müssen dies durch eine Paketerfassung bestätigen.

F. Nachdem der Controller konfiguriert und neu gestartet wurde, können wir nicht mehr im sicheren Web-Modus (HTTPS) auf den Controller zugreifen. Diese Fehlermeldung wird beim Zugriff auf den sicheren Web-Modus des Controllers angezeigt: **Sicheres Web: Webauthentifizierungszertifikat nicht gefunden (Fehler).** Was ist der Grund für dieses Problem?

Antwort: Dieses Problem kann verschiedene Ursachen haben. Ein häufiger Grund kann die Konfiguration der virtuellen Schnittstelle des Controllers betreffen. Um dieses Problem zu beheben, entfernen Sie die virtuelle Schnittstelle, und generieren Sie sie mit dem folgenden Befehl erneut:

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

Starten Sie anschließend den Controller neu. Nach dem Neustart des Controllers generieren Sie das Webauth-Zertifikat lokal auf dem Controller mit dem folgenden Befehl:

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

In der Ausgabe dieses Befehls sollte folgende Meldung angezeigt werden: `Das Webauthentifizierungszertifikat wurde erstellt.`

Jetzt sollten Sie beim Neustart auf den sicheren Web-Modus des Controllers zugreifen können.

F. Controller melden diese IDS DisAssociation Flood Signature-Angriffs-Warnung gegen gültige Clients, in denen die MAC-Adresse des Angreifers die des Access Points (AP) ist, der diesem Controller angeschlossen ist: **Warnung: IDS 'Disassoc Flood' Signature-Angriff erkannt auf AP '<AP Name>' Protokoll '802.11b/g' auf Controller 'x.x.x.x'. Die Signaturbeschreibung lautet "DisAssociation Flood" (Trennungsflucht), mit der Rangfolge "x". Die MAC-Adresse des Angreifers lautet 'hh:hh:hh:hh:hh:hh', Kanalnummer ist 'x' und Anzahl der Erkennungen ist 'x'.** Warum geschieht das?

Antwort: Grund hierfür ist die Cisco Bug ID CSCsg81953 (nur registrierte Kunden) .

IDS DisAssociation Flood-Angriffe auf gültige Clients werden manchmal gemeldet, wenn die MAC-Adresse des Angreifers die eines AP ist, der mit diesem Controller verbunden ist.

Wenn ein Client dem Access Point zugeordnet ist, die Kommunikation jedoch aufgrund der Entfernung der Karte, des Roaming außerhalb der Reichweite usw. zum Access Point beendet wird, wartet der Access Point bis zum Timeout im Leerlauf. Sobald die Zeitüberschreitung im Leerlauf erreicht ist, sendet der Access Point diesem Client einen separaten Frame. Wenn der Client den Trennrahmen nicht bestätigt, überträgt der Access Point den Frame mehrmals (etwa 60 Frames). Das IDS-Subsystem des Controllers hört diese Neuübertragungen und Warnmeldungen mit dieser Nachricht.

Dieser Fehler wurde in Version 4.0.217.0 behoben. Aktualisieren Sie Ihre Controller-Version auf diese Version, um diese Warnmeldung gegen gültige Clients und APs zu überwinden.

F. Ich erhalte diese Fehlermeldung im Syslog des Controllers: **[WARNUNG] apf_80211c 2408: Nachricht mit einer ungültigen unterstützten Rate von Station <xx:xx:xx:xx:xx:xx:xx> [ERROR] apf_utils.c 198 erhalten: Fehlende unterstützte Rate.** Warum?

Antwort: Tatsächlich weisen Meldungen `für fehlende unterstützte Übertragungsrate` darauf hin, dass der WLC für bestimmte erforderliche Datenraten unter den Wireless-Einstellungen konfiguriert ist, die NIC-Karte jedoch nicht die erforderliche Rate aufweist.

Wenn für den Controller Datenraten wie 1 und 2M für erforderlich festgelegt sind, die NIC-Karte jedoch nicht über diese Datenraten kommuniziert, können Sie diese Art von Nachrichten empfangen. Dies ist ein Fehlverhalten der Netzwerkkarte. Wenn dagegen der Controller 802.11g aktiviert ist und der Client eine 802.11b(only)-Karte ist, ist dies eine legitime Nachricht. Wenn diese Meldungen keine Probleme verursachen und die Karten immer noch eine Verbindung herstellen können, können diese Meldungen ignoriert werden. Wenn die Meldungen kartenspezifisch sind, stellen Sie sicher, dass der Treiber für diese Karte auf dem neuesten Stand ist.

F. Dieser Syslog **AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Dekodierungs-Msg: konnte nicht übereinstimmen WLAN ID <id>** Fehlermeldung wird in unserem Netzwerk gesendet. Warum geschieht das und wie kann ich es stoppen?

Antwort: Diese Nachricht wird von den LAPs gesendet. Dies wird angezeigt, wenn Sie die WLAN-Überschreibungsfunktion für ein WLAN konfiguriert haben und dieses WLAN nicht angekündigt wird.

Konfigurieren Sie `config ap syslog host global 0.0.0.0.0`, um es zu beenden, oder Sie können eine bestimmte IP-Adresse angeben, wenn Sie einen Syslog-Server haben, sodass die Nachricht nur an den Server gesendet wird.

F. Ich erhalte diese Fehlermeldung auf meinem WLAN-Controller (WLC): **[FEHLER] Datei: apf_mm.c: Leitung: 581 Mitteilen der Kollision für mobile 00:90:7a:05:56:8a, löschen.** Warum?

Antwort: Im Allgemeinen weist diese Fehlermeldung darauf hin, dass der Controller Kollisionen für einen Wireless-Client angekündigt hat (d. h. dass separate Access Points ankündigen, dass sie über den Client verfügen), und dass der Controller keine Übergabe von einem Access Point zum nächsten erhalten hat. Es ist kein Netzwerkstatus zu warten. Löschen Sie den Wireless-Client, und lassen Sie den Client es erneut versuchen. Wenn dieses Problem häufig auftritt, kann ein Problem mit der Mobilitätskonfiguration vorliegen. Andernfalls kann es sich um eine Anomalie handeln, die sich auf einen bestimmten Client oder eine bestimmte Bedingung bezieht.

F. Mein Controller löst diese Warnmeldung aus: **Abdeckungsschwelle von "12" verletzt.** Was ist dieser Fehler, und wie kann er behoben werden?

Antwort: Diese Warnmeldung wird ausgelöst, wenn ein Client-Signal-Rausch-Verhältnis (SNR) unter den SNR-Schwellenwert für eine bestimmte Funkeinheit fällt. 12 ist der Standard-SNR-Schwellenwert für die Erkennung von Abdeckungslücken.

Der Algorithmus zur Erkennung und Korrektur von Abdeckungslöchern bestimmt, ob eine Abdeckungslücke besteht, wenn die SNR-Stufen des Clients unter einen bestimmten SNR-Schwellenwert liegen. Dieser SNR-Schwellenwert variiert anhand von zwei Werten: AP-Übertragungsleistung und Controller-Abdeckungsprofilwert.

Der Client-SNR-Grenzwert wird detailliert durch die Übertragungsleistung jedes Access Points (in dBm dargestellt) definiert, abzüglich des konstanten Werts von 17 dBm, abzüglich des vom Benutzer konfigurierbaren Werts für das Abdeckungsprofil (dieser Wert ist standardmäßig auf 12 dB festgelegt).

- **Client SNR Cutoff-Wert (|dB|) = [AP-Übertragungsleistung (dBm) - Konstante (17 dBm) - Abdeckungsprofil (dB)]**

Auf diesen benutzerdefinierten Wert für das Abdeckungsprofil kann wie folgt zugegriffen werden:

1. Navigieren Sie in der WLC-GUI zur Hauptüberschrift Wireless, und wählen Sie links die **Netzwerkoption** für den WLAN-Standard (802.11a oder 802.11b/g) aus. Wählen Sie dann oben rechts im Fenster **Auto RF** (Automatisch) aus.
2. Auf der Seite "Globale Parameter der automatischen RF-Instanz" finden Sie den Abschnitt "Schwellenwerte für Profile". In diesem Abschnitt finden Sie den Wert Coverage (3 bis 50 dBm). Dieser Wert ist der vom Benutzer konfigurierbare Abdeckungsprofilwert.
3. Dieser Wert kann bearbeitet werden, um den Client-SNR-Schwellwert zu beeinflussen. Die andere Möglichkeit, diesen SNR-Grenzwert zu beeinflussen, besteht darin, die Übertragungsleistung zu erhöhen und die Abdeckungslöcher-Erkennung auszugleichen.

F. Ich verwende ACS 4.1 und einen Wireless LAN Controller 4402 (WLC). Wenn der WLC versucht, einen Wireless-Client mit der MAC-Authentifizierung für ACS 4.1 zu authentifizieren, antwortet der ACS nicht mit dem ACS und meldet folgende Fehlermeldung: "*Interner Fehler ist aufgetreten* ". Alle meine Konfigurationen sind korrekt. Warum tritt dieser interne Fehler auf?

Antwort: In ACS 4.1 gibt es eine authentifizierungsbezogene Cisco Bug-ID CSCsh62641 (nur registrierte Kunden), in der der ACS die `interne Fehlermeldung` angibt, `die` aufgetreten ist.

Dieser Fehler könnte das Problem sein. Für diesen Bug gibt es einen Patch auf der ACS 4.1 Download (nur registrierte Kunden) Seite, der das Problem beheben sollte.

F. Der Cisco Wireless LAN Controller (WLC) der Serie 4400 wird nicht gestartet. Diese Fehlermeldung wird auf dem Controller angezeigt: `** Keine Verwendung von ide 0:4 für Fatload ** Fehler (kein IRQ) dev 0 blk 0: Status 0x51 Fehlermeldung: 10 ** Kann nicht von Gerät 0 lesen.` Warum?

Antwort: Der Grund für diesen Fehler kann ein Hardwareproblem sein. Öffnen Sie ein TAC-Ticket, um dieses Problem weiter zu beheben. Um ein TAC-Ticket zu erstellen, benötigen Sie einen gültigen Vertrag mit Cisco. Wenden Sie sich an den technischen Support, um das Cisco TAC zu kontaktieren.

F. Der WLAN-Controller (WLC) weist Speicherpufferprobleme auf. Wenn die Speicherpuffer voll sind, stürzt der Controller ab und muss neu gestartet werden, um ihn wieder online zu stellen. Diese Fehlermeldungen werden im Meldungsprotokoll angezeigt: `Mo. 9. April 10:41:03 2007 [FEHLER] dtl_net.c 506: Aus den Systempuffern Mo 9. Apr. 10:41:03 2007 [ERROR] sysapi_if_net.c 537: Neue Mbuf kann nicht zugewiesen werden. Mo. 9. Apr. 10:41:03 2007 [ERROR] sysapi_if_net.c 219: MbufGet: keine kostenlosen Mbufs.` Warum?

Antwort: Grund hierfür ist die Cisco Bug-ID CSCsh93980 (nur registrierte Kunden) . Dieser Fehler wurde in WLC Version 4.1.185.0 behoben. Aktualisieren Sie Ihren Controller auf diese Softwareversion oder eine spätere Version, um diese Meldung zu überwinden.

F. Wir führten das Upgrade des Codes für unseren Wireless LAN Controller (WLC) 4400s auf 4.1 durch, und unser Syslog wurde durch folgende Meldungen bombardiert: `03. Mai 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), erhalten mit ungültigem SPA 192.168.1.233/TPA 192.168.1.233.` Was bedeuten diese Meldungen?

Antwort: Dies kann auftreten, wenn WLAN als DHCP erforderlich markiert ist. In solchen Fällen dürfen nur Stationen, die über DHCP eine IP-Adresse erhalten, eine Verbindung herstellen. Statische Clients dürfen keine Verbindung zu diesem WLAN herstellen. WLC fungiert als DHCP Relay Agent und zeichnet die IP-Adresse aller Stationen auf. Diese Fehlermeldung wird generiert, wenn WLC eine ARP-Anfrage von einer Station empfängt, bevor der WLC DHCP-Pakete von der Station empfangen und die IP-Adresse aufgezeichnet hat.

F. Wenn Sie Power over Ethernet (PoE) auf dem Cisco 2106 Wireless LAN Controller verwenden, sind die AP-Funkmodule nicht aktiviert. Der `Access Point kann`

nicht die ausreichende Inline-Stromversorgung überprüfen. Funksteckplatz deaktiviert.
Fehlermeldung wird angezeigt. Wie kann ich das beheben?

Antwort: Diese Fehlermeldung tritt auf, wenn es sich bei dem Switch, der den Access Point hochfährt, um einen Pre-Standard Switch handelt, der Access Point jedoch nicht den Pre-Standard Mode of Input Power (Vorstandardmodus für Eingangsleistung) unterstützt.

Bei einem Cisco Pre-Standard Switch handelt es sich um einen Switch, der keine intelligente Energieverwaltung (IPM) unterstützt, aber über ausreichende Leistung für einen Standard Access Point verfügt.

Sie müssen den **Pre-Standard**-Stromversorgungsmodus des Access Points aktivieren, der dieser Fehlermeldung unterzogen wird. Dies kann über die Controller-CLI mit der **Konfigurationsoption "ap power" vor dem Standard {enable} erfolgen. | disable} {all} | Cisco_AP}**-Befehl.

Dieser Befehl sollte bei Bedarf bereits konfiguriert werden, wenn Sie von einer früheren Version auf die Softwareversion 4.1 aktualisieren. Es ist jedoch möglich, dass Sie diesen Befehl für neue Installationen oder für das Zurücksetzen des Access Points auf die Werkseinstellungen eingeben müssen.

Diese Cisco Switches sind mit dem Vorstandard 15 Watt erhältlich:

- 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

F. Der Controller generiert **dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED: Es konnte kein ARP-Eintrag für xx:xx.-xxx.x zum Netzwerkprozessor hinzugefügt werden. Der Eintrag existiert nicht.** Syslog-Meldung ähnlich dieser. Was bedeutet diese Syslog-Meldung?

Antwort: Während ein Wireless-Client eine ARP-Antwort sendet, muss die Network Processor Unit (NPU) diese Antwort kennen. Die ARP-Antwort wird also an die NPU weitergeleitet, aber die WLC-Software sollte nicht versuchen, diesen Eintrag dem Netzwerkprozessor hinzuzufügen. Wenn dies der Fall ist, werden diese Meldungen generiert. Dies hat keine Auswirkungen auf die Funktionalität des WLC, aber der WLC generiert diese Syslog-Meldung.

F. Ich habe einen neuen Cisco 2106 WLC installiert und konfiguriert. Der WLC zeigt an, dass der Temperatursensor ausgefallen ist. Wenn Sie sich unter "Controller Summary" (Controller-Zusammenfassung) bei der Webschnittstelle anmelden, wird neben der internen Temperatur "**Sensor failed**" (Sensor fehlgeschlagen) angezeigt. Alles andere scheint normal zu funktionieren.

Antwort: Der Ausfall eines internen Temperatursensors ist kosmetisch und kann durch ein Upgrade auf die WLC-Version 4.2.61.0 behoben werden.

WLC 2106 und WLC 526, **die am oder nach dem 01.07.2007** installiert sind, können den Temperatursensorchip eines anderen Anbieters verwenden. Dieser neue Sensor funktioniert einwandfrei, ist jedoch nicht mit Software nach Version 4.2 kompatibel. Daher kann ältere Software die Temperatur nicht lesen und zeigt diesen Fehler an. Alle anderen Controller-Funktionen sind von diesem Fehler nicht betroffen.

Es gibt eine bekannte Cisco Bug ID CSCsk97299 (nur registrierte Kunden), die mit diesem Problem zusammenhängt. Dieser Fehler wird in der Versionshinweis von WLC Version 4.2 erwähnt.

F. Ich erhalte den Befehl `radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND: Es konnte keine entsprechende RADIUS-Server für WLAN <WLAN-ID> gefunden werden. Es konnte keine Standard-Server-` "Meldung für ALLE SSIDs gefunden werden. Diese Meldung wird auch für SSIDs angezeigt, die keine AAA-Server verwenden.

Antwort: Diese Fehlermeldung bedeutet, dass der Controller nicht in der Lage war, den Standard-Radius-Server zu kontaktieren, oder dass dieser nicht definiert wurde.

Ein möglicher Grund für dieses Verhalten ist die Cisco Bug ID CSCsk08181 (nur registrierte Kunden) , die in Version 4.2 behoben wurde. Aktualisieren Sie Ihren Controller auf Version 4.2.

F. Die `Nachricht: 10.Juli 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL: Die Quell-MAC-Adresse von Schnittstelle 1 wurde nicht gefunden.` auf dem Wireless LAN Controller (WLC) wird eine Fehlermeldung angezeigt. Was bedeutet das?

Antwort: Das bedeutet, dass der Controller einen Fehler hatte, während er ein CPU-Sourcing-Paket schickte.

F. Diese Fehlermeldungen werden auf dem Wireless LAN Controller (WLC) angezeigt:

- `10. Juli 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Konfigurationsdatei 'cliWebInitParms.cfg' konnte nicht gelesen werden.`
- `10. Juli 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Konfigurationsdatei "rfidInitParms.cfg" konnte nicht gelesen werden.`
- `10. Juli 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Konfigurationsdatei 'dhcpParms.cfg' konnte nicht gelesen werden.`
- `10. Juli 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Konfigurationsdatei 'bcastInitParms.cfg' konnte nicht gelesen werden.`
- `18. März 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Löschen der Datei fehlgeschlagen: sshpmInitParms.cfg. Entfernen der Datei fehlgeschlagen. - Prozess: Name:fp_main_task, ID:11ca7618`
- `18. März 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Löschen der Datei fehlgeschlagen: bcastInitParms.cfg. Entfernen der Datei fehlgeschlagen. - Prozess: Name:fp_main_task, ID:11ca7618`

Was bedeutet diese Fehlermeldung?

Antwort: Diese Meldungen sind Informationsmeldungen und Teil des normalen Bootvorgangs. Diese Meldungen werden angezeigt, weil mehrere verschiedene Konfigurationsdateien nicht gelesen oder gelöscht wurden. Wenn bestimmte Konfigurationsdateien nicht gefunden werden oder die Konfigurationsdatei nicht gelesen werden kann, sendet die Konfigurationssequenz für jeden Prozess diese Meldung, z. B. keine DHCP-Serverkonfiguration, keine Tags (RF-ID) usw. Hierbei handelt es sich um Nachrichten mit geringem Schweregrad, die problemlos ignoriert werden können. Diese Meldungen unterbrechen den Betrieb des Controllers nicht.

F. **HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAIN: Nicht in der Lage, unberechtigten Benutzer 00:14:XX:02:XX:XX im geschlossenen Zustand zu belassen - kein verfügbarer Access Point, der enthalten sein soll.** Fehlermeldung wird angezeigt. Was bedeutet das?

Antwort: Dies bedeutet, dass der Access Point, der die Funktion zum Eindämmen in Bedrohungen ausgeführt hat, nicht mehr verfügbar ist und der Controller keinen geeigneten Access Point für die Durchführung der nicht autorisierten Eingrenzung finden kann.

F. Die **DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] Die** Systemmeldung **"ARP (op 1)", die mit dem ungültigen SPA 192.168.1.152/TPA 192.168.0.206-**System **empfangen wurde,** wird auf dem Wireless LAN Controller angezeigt. Was bedeutet diese Meldung?

Antwort: Es ist möglich, dass das System ARP-Spoofing oder Vergiftung erkannt hat. Diese Nachricht impliziert jedoch nicht notwendigerweise, dass schädliche ARP-Spoofing-Ereignisse aufgetreten sind. Die Meldung wird angezeigt, wenn diese Bedingungen zutreffen:

- Ein WLAN wird mit DHCP Required konfiguriert, und ein Client-Gerät sendet nach der Zuweisung zu diesem WLAN eine ARP-Nachricht, ohne zuvor DHCP auszufüllen. Hierbei kann es sich um ein normales Verhalten handeln. Dies kann z. B. dann passieren, wenn der Client statisch adressiert ist oder wenn der Client über einen gültigen DHCP-Lease aus einer vorherigen Verbindung verfügt. Die Fehlermeldung kann wie im folgenden Beispiel aussehen:
  `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`
  Diese Bedingung hat zur Folge, dass der Client keinen Datenverkehr senden oder empfangen kann, bis er DHCPs über den WLC durchführt.Weitere Informationen finden Sie im Abschnitt zu DTL-Nachrichten im Cisco Wireless LAN Controller System Message Guide.

F. LAPs verwenden zum Hochfahren kein Power over Ethernet (POE). Die Protokolle auf dem Wireless LAN-Controller werden angezeigt:

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

Worum geht es?

Antwort: Dies kann auftreten, wenn die PoE-Einstellungen (Power over Ethernet) nicht richtig konfiguriert wurden. Wenn ein Access Point, der in den Lightweight-Modus umgewandelt wurde, z. B. ein Access Point der Serie AP1131 oder AP1242 oder ein Access Point der Serie 1250, über einen Power Injector mit einem Cisco Pre-Intelligent Power Management (Pre-IPM)-Switch betrieben wird, müssen Sie Power over Ethernet (PoE) konfigurieren.

Weitere Informationen zur Konfiguration von Power over Ethernet (PoE) finden Sie unter Konfiguration von Power over Ethernet (PoE) .

F. Sie sehen diese Meldung auf dem 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**

Was bedeutet das?

Antwort: Lightweight Access Points verwenden einen bestimmten Algorithmus, um einen Controller zu finden. Der Vorgang der Erkennung und Verknüpfung wird ausführlich in der Lightweight AP (LAP)-Registrierung bei einem Wireless LAN Controller (WLC) beschrieben.

Diese Fehlermeldung wird auf dem WLC angezeigt, wenn eine Erkennungsanfrage eingeht, nachdem die maximale AP-Kapazität erreicht wurde.

Wenn der primäre Controller für eine LAP nicht konfiguriert ist oder eine neue, sofort einsatzbereite LAP verwendet wird, sendet er LWAPP-Erkennungsanfragen an alle erreichbaren Controller. Wenn die Erkennungsanforderungen einen Controller erreichen, der mit seiner vollen AP-Kapazität ausgeführt wird, erhält der WLC die Anforderungen und stellt fest, dass er die maximale AP-Kapazität erreicht, antwortet nicht auf die Anforderung und gibt diesen Fehler weiter.

F. Wo finde ich weitere Informationen zu den LWAPP-Systemmeldungen?

Antwort: Weitere Informationen zu den LWAPP-Systemmeldungen finden Sie im Cisco Wireless LAN Controller System Message Guide 4.2.

F. Die Fehlermeldung `Webauth-Dateien` wird auf dem Wireless LAN Controller (WLC) angezeigt. Was bedeutet das?

Antwort: WLC kann kein Paket für benutzerdefinierte Webauthentifizierung/Passthrough laden, wenn eine der gebündelten Dateien mehr als 30 Zeichen im Dateinamen enthält, der die Dateierweiterung enthält. Das angepasste Web-Authentifizierungspaket darf für Dateinamen maximal 30 Zeichen lang sein. Stellen Sie sicher, dass die Dateinamen im Paket nicht größer als 30 Zeichen sind.

F. Wireless LAN Controller (WLCs), die 5.2- oder 6.0-Code mit einer großen Anzahl von AP-Gruppen ausführen, werden in der Web-GUI möglicherweise nicht alle konfigurierten AP-Gruppen angezeigt. Worum geht es?

Antwort: Die fehlenden AP-Gruppen können angezeigt werden, wenn Sie den Befehl **show wlan ap-groups** verwenden.

Versuchen Sie, der Liste eine weitere AP-Gruppe hinzuzufügen. Beispielsweise wurden 51 AP-Gruppen bereitgestellt, und die 51. fehlen (Seite 3). Fügen Sie die 52. Gruppe hinzu, und Seite 3 sollte in der Web-GUI angezeigt werden.

Um dieses Problem zu beheben, aktualisieren Sie auf WLC Version 7.0.220.0.

Zugehörige Informationen

- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.0
- Häufig gestellte Fragen zur WiSM-Fehlerbehebung
- Häufig gestellte Fragen zur Fehlerbehebung für Wireless LAN Controller (WLC)
- Wireless-Support-Seite
- Technischer Support und Dokumentation - Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.