Beoordeel Draadloze LAN Controller (WLC) Fout en Systeem Berichten Veelgestelde vragen

Inhoud

Inleiding

Dit document beschrijft vaak gestelde vragen (FAQ) over foutmeldingen en systeemmeldingen voor Cisco Wireless LAN (WLAN)-controllers (WLC's).

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Veelgestelde vragen over foutmeldingen

Q. De conversie van meer dan 200 access points (AP's) van Cisco IOS®-software naar lichtgewicht AP-protocol (LWAP) met een Cisco 4404 WLC is gestart. De conversie van 48 AP's was voltooid en het bericht dat werd ontvangen op de WLC verklaarde: `[ERROR] spam_lrad.c 4212: AP kan niet toetreden omdat het maximum aantal AP's op interface 1 is bereikt.` Waarom treedt de fout op?

A.U moet extra AP-manager interfaces maken om meer dan 48 AP's te kunnen ondersteunen. Anders ontvangt u de fout die er zo uitziet:

```
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.
```

Configureer meerdere AP-Manager interfaces en configureer primaire/back-uppoorten die andere AP-Manager interfaces niet gebruiken. U moet een tweede AP-Manager interface maken om extra AP's te kunnen oproepen. Maar zorg ervoor dat uw primaire poort en back-up poortconfiguraties voor elke manager niet overlappen. Met andere woorden, als AP-Manager 1 poort 1 gebruikt als de primaire en poort 2 als de back-up, moet AP-Manager 2 poort 3 als de primaire en poort 4 als de back-up gebruiken.

Q. Ik heb een draadloze LAN-controller (WLC) 4402 en ik gebruik 1240 lichtgewicht access points (LAP's). Ik heb 128-bits codering op de WLC ingeschakeld. Wanneer ik 128-bit WEP-encryptie selecteer in de WLC, ontvang ik een fout die zegt dat 128-bit niet wordt ondersteund in de 1240s: `[ERROR] spam_lrad.c 12839: Niet maken SID-modus op Cisco AP xx:xx:xx:xx:xx:xx:xx:xx omdat WEP128 bit niet wordt ondersteund.` Waarom ontvang ik deze fout?

A.De belangrijkste lengten die op de WLCs worden getoond zijn eigenlijk het aantal beetjes die in het gedeelde geheim zijn en niet de 24 beetjes van de Initialiseringsvector (IV) omvatten. Bij veel producten, waaronder de Aironet-producten, wordt een 128-bits WEP-sleutel gebruikt. In werkelijkheid is het een 104-bits sleutel met 24-bits IV. De sleutelgrootte van 104-bit is wat u op de WLC moet inschakelen voor 128-bits WEP-codering.

Als u kiest voor de 128-bits sleutelgrootte op de WLC, is het eigenlijk een 152-bits (128 + 24 IV) WEP-sleutelcodering. Alleen Cisco 1000 Series LAN's (AP1010, AP1020, AP1030) ondersteunen het gebruik van de WLC 128-bits WEP-toetsinstelling.

Q. Waarom krijg ik de `WEP-sleutelgrootte van 128 bits niet ondersteund op 11xx-, 12xx- en 13xx-model AP's. WLAN kan niet naar deze access points worden gedrukt.` foutmelding wanneer ik WEP op een WLC probeer te configureren?

A.Op een draadloze LAN-controller hebt u deze opties voor de WEP-sleutelgrootte wanneer u Statische WEP kiest als de Layer 2 Security-methode.

- niet ingesteld
- 40 bits
- 104 bits
- 128 bits

Deze sleutelgroottewaarden omvatten niet de 24-bits initialiseringsvector (IV), die aaneengeschakeld is met de WEP-toets. Dus voor een 64-bits WEP moet u **40** bits als WEP-toetsgrootte kiezen. De controller voegt de 24-bits IV hieraan toe om een 64-bits WEP-sleutel te maken. Kies op dezelfde manier voor een 128-bits WEP-toets **104-bits**.

Controllers ondersteunen ook 152-bits WEP-toetsen (128-bits + 24-bits IV). Deze configuratie wordt niet ondersteund op de 11xx-, 12xx- en 13xx-modellen AP's. Wanneer u WEP probeert te configureren met 14 bits, geeft de controller een bericht dat deze WEP-configuratie niet wordt geduwd naar 11xx, 12xx en 13xx model AP's.

Q. Clients kunnen niet worden geverifieerd naar een WLAN dat is geconfigureerd voor WPA2, en de controller geeft de `apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_MISLUKT: kon de RSN en WARP IE niet verwerken. station dat geen RSN (WPA2) gebruikt voor WLAN waarvoor RSN.MobileStation:00:0c:f1:0c:51:22, SSID:<>` foutbericht nodig is. Waarom ontvang ik deze fout?

A. Dit komt meestal voor door incompatibiliteit aan de clientzijde. Probeer deze stappen om dit probleem op te lossen:

- Controleer of de client Wi-Fi is gecertificeerd voor WPA2 en controleer de configuratie van de client op WPA2.
- Controleer het gegevensblad om te zien of het client hulpprogramma WPA2 ondersteunt. Installeer elke patch die door de leverancier is vrijgegeven om WPA2 te ondersteunen. Als u Windows Utility gebruikt, zorg er dan voor dat u de WPA2-patch van Microsoft hebt geïnstalleerd om WPA2 te ondersteunen. Zie Microsoft ondersteuning voor meer informatie.
- Upgrade het clientstuurprogramma en de firmware.
- Schakel Aironet-uitbreidingen op het WLAN uit.

Q. Zodra ik de WLC herstart, krijg ik de `Mon Jul 17 15:23:28 2006 MFP Anomalie Gedetecteerd - 3023 Ongeldige MIC gebeurtenis(s) gevonden als overtreden door de radio 00:XX:XX:XX:XX en gedetecteerd door de dot11 interface in sleuf 0 van AP 00:XX:XX:XX:XX in 300 seconden bij het waarnemen van Probe reacties, Beacon Frames` foutmelding. Waarom komt deze fout voor en hoe kom ik er vanaf?

A.Deze foutmelding wordt weergegeven wanneer frames met onjuiste MIC-waarden worden gedetecteerd door in MFP enabled LAP's. Raadpleeg Infrastructure Management Frame Protection (MFP) met WLC en LAP Configuration Voorbeeld voor meer informatie over MFP. Voltooi een van deze vier stappen:

1. Controleer en verwijder alle frauduleuze of ongeldige AP's of clients in uw netwerk die ongeldige frames genereren.
2. Schakel de infrastructuur-MFP uit als MFP niet is ingeschakeld voor andere leden van de Mobility-groep, omdat LAP's beheerframes kunnen horen van LAP's van andere WLC's in de groep waarvoor MFP niet is ingeschakeld. Raadpleeg de Veelgestelde vragen over Mobiliteitsgroepen met draadloze LAN-controllers voor meer informatie over de Mobility Group.
3. De fix voor deze foutmelding is beschikbaar in de WLC releases 4.2.112.0 en 5.0.148.2. Upgrade de WLC's naar een van deze releases.
4. Als laatste optie, probeer om de LAP te herladen die deze foutmelding genereert.

Q. Client AIR-PI21AG-E-K9 kan met succes worden geassocieerd met een access point (AP) met Extensible Verification Protocol-Flexible Verification via Secure Tunneling (EAP-FAST). Wanneer het bijbehorende toegangspunt is uitgeschakeld, zwerft de client echter niet naar een ander toegangspunt. Dit bericht wordt continu weergegeven in het controllerberichtenlog: "vóór juni 2:14:48:49:2006 [SECURITY] 1x_auth_pae.c 1922: Kan gebruiker niet in het systeem worden toegelaten - wordt de gebruiker misschien al op het systeem aangemeld? Vr jun 2 14:48:49 2006 [SECURITY] apf_ms.c 2557: Kan gebruikersnaam voor mobiel 00:40:96:ad:75:f4 niet verwijderen". Waarom?

A. Wanneer de clientkaart moet zwerven, stuurt het een verificatieaanvraag, maar het behandelt niet correct sleutels (niet informeert AP/controller, antwoordt niet herverificatie).

Dit is gedocumenteerd in Cisco bug IDCSC02837. Deze bug is verholpen met Cisco Aironet 802.11a/b/g clientadapters, installatiewizard 3.5.

In het algemeen kan de gebruikersnaam voor mobiel bericht ook worden gewist om een van de volgende redenen:

- De gebruikersnaam wordt op meer dan één clientapparaat gebruikt.
- Verificatiemethode die wordt gebruikt voor dat WLAN heeft een externe anonieme identiteit. In PEAP-GTC of in EAP-FAST is het bijvoorbeeld mogelijk om een generieke gebruikersnaam te definiëren als externe (zichtbare) identiteit, en de echte gebruikersnaam is verborgen in de TLS-tunnel tussen client- en radiusserver, zodat de controller deze niet kan zien en gebruiken. In dergelijke gevallen kan dit bericht verschijnen. Dit probleem wordt vaker gezien bij een derde partij en een oude firmware-client.

  Opmerking: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-bugs, informatie en tools.

V. Wanneer ik de nieuwe Wireless Services Module (WiSM)-blade installeer in de switch 6509 en het Protected Extensible Authentication Protocol (PEAP) implementeer met de Microsoft IAS-server, ontvang ik deze fout: *Mar 1 00:00:23.526: %LWAPP-5-CHANGE: LWAPP veranderde de status in DISCOVERY *Mar 1 00:00:23.700: %SYS-5-RELOAD: Opnieuw laden gevraagd door LWAPP CLIENT.Reload Reden: MISLUKTE CRYPTO INIT. 20:00:23.700: %LWAPP-5-VERANDERD: LWAPP veranderde de staat naar DOWN *Mar 1 00:00:23.528: %LWAPP-5-VERANDERD: LWAPP veranderde de staat naar DISCOVERY *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG:lwapp_crypto_init_ssc_keys_and_certs geen certs in het SSC Private File *Mar 1 00:00:0:00:23 57: LWAPP_CLIENT_ERROR_DEBUG: *Mar 1

00:00:23.557: lwapp_crypto_init: PKI_StartSession faalde *Mar 1 00:00:23.706: %SYS-5-RELOAD: Opnieuw laden aangevraagd door LWAPP CLIENT. . Waarom?

A.RADIUS en dot1x debugs tonen aan dat de WLC een toegangsaanvraag verstuurt, maar er is geen reactie van de IAS server. Voltooi de volgende stappen om het probleem op te lossen:

1. Controleer en verifieer de IAS-serverconfiguratie.
2. Controleer het logbestand.
3. Installeer software, zoals Etheral, die u verificatiegegevens kan geven.
4. Stop en start de IAS-service.

V. De lichtgewicht access points (LAP's) registreren niet bij de controller. Wat kan het probleem zijn? Ik zie deze foutmeldingen op de controller: `Thu Feb 3 03:20:47 2028: LWAPP Join-request bevat geen geldig certificaat in CERTIFICAAT_PAYLOAD van AP 00:0b:85:68:f4:f0. Thu Feb 3 03:20:47 2028: Kan geen openbare sleutel vrijgeven voor AP 00:0B:85:68:F4:F0.`

A.Wanneer het access point (AP) het Lichtgewicht Access Point Protocol (LWAPP) Join Request naar de WLC stuurt, wordt het X.509-certificaat in het LWAPP-bericht ingesloten. Het genereert ook een willekeurige sessie-ID die is opgenomen in het LWAPP Join Verzoek. Wanneer de WLC de LWAPP Join Verzoek ontvangt, bevestigt het de handtekening van het X.509 certificaat met de openbare sleutel van APs en controleert dat het certificaat door een vertrouwd op certificaatgezag werd verstrekt. Het kijkt ook naar de begindatum en tijd voor de geldigheidsperiode van het AP-certificaat en vergelijkt die datum en tijd met zijn eigen datum en tijd.

Dit probleem kan zich voordoen door een onjuiste klokinstelling op de WLC. Om de klok op de WLC in te stellen, geeft u de `show time` en `config time` opdrachten.

Q. Een Lichtgewicht Access Point Protocol (LWAP) AP kan zich niet bij de controller aansluiten. Het logbestand Wireless LAN Controller (WLC) toont een bericht dat vergelijkbaar is met dit: `LWAPP Join-request bevat geen geldig certificaat in CERTIFICAAT_PAYLOAD van AP 00:0b:85:68:ab:01.` Waarom?

A.U kunt deze foutmelding ontvangen als de LWAP-tunnel tussen de AP en de WLC een netwerkpad doorkruist met een MTU onder 1500 bytes. Dit veroorzaakt de fragmentatie van de LWAPP-pakketten. Dit is een bekende fout in de controller. Raadpleeg het Cisco-installatieprogramma IDCSC39911.

De oplossing is om de controller firmware te upgraden naar 4.0(155).

> **Opmerking**: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-bugs, informatie en tools.

V. Ik wil gasttunneling instellen tussen mijn interne controller en de virtuele ankercontroller op de de-Militarised Zone (DMZ). Wanneer een gebruiker echter probeert te associëren met een gast-SSID, kan de gebruiker het IP-adres niet ontvangen van de DMZ, zoals verwacht. Daarom wordt het gebruikersverkeer niet getunneld naar de controller op de DMZ. De uitvoer van de opdracht debug mobile handoff toont een bericht dat vergelijkbaar is met dit: `Security Policy Mismatch voor WLAN <WLAN ID>. Anker Exportaanvraag van Switch IP: <controller IP-adres> genegeerd.` Wat is het probleem?

A.Guest tunneling biedt extra beveiliging voor de toegang van gasten tot het draadloze netwerk van het bedrijf. Dit helpt ervoor te zorgen dat gastgebruikers geen toegang hebben tot het

bedrijfsnetwerk zonder eerst door de bedrijfsfirewall te hoeven lopen. Wanneer een gebruiker verbinding maakt met een WLAN dat is aangewezen als de gast-WLAN, wordt het gebruikersverkeer getunneld naar de WLAN-controller die zich op de DMZ buiten de bedrijfsfirewall bevindt.

Nu, met het oog op dit scenario, kunnen er verscheidene redenen zijn voor deze gast het tunnelen om niet te functioneren zoals verwacht. Zoals de debugcommando-uitvoer impliceert, kan het probleem worden veroorzaakt door de mismatch in een van de beveiligingsmaatregelen die zijn geconfigureerd voor dat bepaalde WLAN in de interne en in de DMZ-controllers. Controleer of het beveiligingsbeleid en andere instellingen, zoals instellingen voor time-out van sessies, worden aangepast.

Een andere veel voorkomende reden voor dit probleem is dat de DMZ-controller niet aan zichzelf is verankerd voor dat bepaalde WLAN. Voor een gasttunneling om goed te werken en voor de DMZ om het IP-adres van de gebruiker (gebruiker die tot een gast WLAN behoort) te beheren, is het essentieel dat er een goede verankering wordt uitgevoerd voor dat bepaalde WLAN.

V. Ik zie veel **"CPU Receive Multicast Queue is vol op controller"** berichten op de 2006 draadloze LAN-controller (WLC), maar niet op de 4400 WLC's. Waarom? Ik heb multicast uitgeschakeld op de controllers. Wat is het verschil in de Multicast Queue Limit tussen de 2006 en 4400 WLC platforms?

A.Omdat multicast op de controllers is uitgeschakeld, kunnen de berichten die dit alarm veroorzaken Adresresolutie Protocol (ARP)-berichten zijn. Er is geen verschil in wachtrijdiepte (512 pakketten) tussen de 2000 WLCs en de 4400 WLCs. Het verschil is dat de 4400 NPU-filters ARP-pakketten, terwijl alles wordt gedaan in software op de 2006. Dit verklaart waarom de WLC van 2006 wel de berichten ziet, maar niet de WLC van 4400. Een 44xx WLC verwerkt multicastpakketten via hardware (via CPU). Een 2000 WLC verwerkt multicastpakketten via software. CPU verwerking is efficiënter dan software. Daarom wordt de 4400's wachtrij sneller gewist, terwijl de 2006 WLC een beetje worstelt als het veel van deze berichten ziet.

Q. Ik zie **"[SECURITY] apf_foreigap.c 763: STA [00:0A:E4:36:1F:9B] Ontvangen een pakket op poort 1 maar geen Buitenlandse AP geconfigureerd voor deze poort."** foutmelding in een van mijn controllers. Wat betekent deze fout en welke stappen moet ik nemen om deze op te lossen?

A.Dit bericht wordt gezien wanneer het controlemechanisme een DHCP- verzoek om een adres ontvangt van MAC waarvoor het geen staatsmachine heeft. Dit wordt vaak gezien van een brug of een systeem dat een virtuele machine zoals VMWare in werking stelt. De controller luistert naar de DHCP-verzoeken omdat het DHCP-snuffelen uitvoert, zodat hij weet welke adressen zijn gekoppeld aan clients die zijn aangesloten op zijn access points (AP's). Al het verkeer voor de draadloze clients gaat door de controller. Wanneer de bestemming van een pakket een draadloze client is, gaat het naar de controller en gaat vervolgens door de LWAP-tunnel (Lichtgewicht Access Point Protocol) naar de AP en uit naar de client. Eén ding dat kan worden gedaan om dit bericht te helpen verzachten is om alleen VLAN's toe te staan die op de controller worden gebruikt op de trunk die naar de controller gaat met de opdracht SwitchPort VLAN allowop de switch.

Q. Waarom zie ik deze foutmelding op de console: **Msg 'Set Default Gateway' van System Table is mislukt, Id = 0x0050b986 foutwaarde = 0xfffffffc**?

A. Dit kan het gevolg zijn van een hoge CPU-belasting. Wanneer de controller-CPU zwaar geladen is, zoals wanneer het bestand kopieert of andere taken, heeft het geen tijd om alle ACK's te verwerken die de NPU verstuurt in reactie op configuratieberichten. Wanneer dit gebeurt, genereert de CPU foutmeldingen. De foutmeldingen hebben echter geen invloed op de service of

functionaliteit.

Raadpleeg voor meer informatie Cisco draadloze LAN-controllers.

Q. Ik ontvang deze Wired Equivalent Privacy (WEP) belangrijke foutmeldingen op mijn Wireless Control System (WCS): `De WEP Key die op het station is geconfigureerd kan onjuist zijn. Het MAC-adres van het station is 'xx:xx:xx:xx:xx:xx', de basisradio van het AP is 'xx:xx:xx:xx:xx:xx' en de ID van de sleuf is '1'`. Ik gebruik WEP echter niet als beveiligingsparameter in mijn netwerk. Ik gebruik alleen WPA (Wi-Fi Protected Access). Waarom ontvang ik deze WEP foutmeldingen?

A. Als al uw veiligheid gerelateerde configuraties perfect zijn, de berichten die u nu ontvangt zijn vanwege bugs. Er zijn een paar bekende fouten in de controller. Raadpleeg Cisco-bug IDCSCse17260 en Cisco-id CSC11202, waarin staat "De WEP-sleutel die op het station is geconfigureerd, kan **met** WPA- **en TKIP-clients** onjuist zijn". Eigenlijk is Cisco bug-id **CSCse17260** een duplicaat van Cisco bug-id **CSCse11202**. De fix voor Cisco maar ID **CSCse1202** is al beschikbaar met WLC release 3.2.171.5.

> **Opmerking**: De laatste WLC releases heeft een oplossing voor deze bugs.

> **Opmerking**: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-bug-informatie en -tools.

V. Ik gebruik een externe RADIUS-server om draadloze clients te verifiëren via de controller. De controller verstuurt deze foutmelding regelmatig: `geen radiusservers reageren`. Waarom zie ik deze foutmeldingen?

A. Wanneer een verzoek van WLC aan de server van de RADIUS uitgaat, heeft elk pakket een opeenvolgingsaantal waaraan WLC een reactie verwacht. Als er geen reactie is, is er een bericht dat `aantoont` dat `de straalserver niet antwoordt.`

De standaardtijd voor WLC om terug van de server van de RADIUS te horen is 2 seconden. Dit is ingesteld vanuit de WLC GUI **onder Security > authenticatieserver**. Het maximum is 30 seconden. Daarom kan het nuttig zijn om deze time out waarde maximaal te stellen om deze kwestie op te lossen.

Soms voeren de RADIUS-servers **'stille afdankingen'** uit van het aanvraagpakket dat uit de WLC komt. De RADIUS-server kan deze pakketten afwijzen vanwege een foutieve certificaataanvraag en verschillende andere redenen. Dit is een geldige actie van de server. In dergelijke gevallen kan de controller ook aangeven dat de RADIUS-server niet reageert

Om de stille weggooi kwestie te overwinnen, maak **de agressieve** failoverfeature in WLC onbruikbaar.

Als **de agressieve** failoverfeature in WLC is ingeschakeld, is de WLC te agressief om de AAA-server te markeren als niet reagerend. Dit mag echter niet worden gedaan omdat de AAA-server niet alleen kan reageren op die bepaalde client (er wordt niet op geantwoord). Het kan een antwoord op andere geldige cliënten (met geldige certificaten) zijn. De WLC kan de AAA-server echter nog steeds markeren als niet reagerend en niet functioneel.

Om dit te overwinnen, blokkeer **de agressieve** failoverfeature. Geef **de configuratie-straal**

agressief-failover disableccommando uit van de controller CLI om dit uit te voeren. Als deze optie is uitgeschakeld, kan de controller alleen naar de volgende AAA-server overschakelen als er 3 opeenvolgende clients zijn die geen respons van de RADIUS-server ontvangen.

Q. Verschillende clients zijn niet in staat om te koppelen aan een LWAPP en de controller registreert de `IAPP-3-MSGTAG015: iappSocketTask: iappRecvPkt retourde foutmelding` . Waarom gebeurt dit?

A. Dit gebeurt meestal als gevolg van een probleem met de Intel-adapters die CCX v4 ondersteunen, maar die een client-bundelversie eerder uitvoeren dan 10.5.1.0. Als u de software upgradt naar 10.5.1.0 of hoger, dan lost dit probleem op. Raadpleeg de Cisco-bug IDCSC91347 voor meer informatie over deze foutmelding.

> **Opmerking**: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-bug-informatie en -tools.

V. Ik zie deze foutmelding op de draadloze LAN-controller (WLC): `Reached Max EAP-Identity request retries (21) voor STA 00:05:4e:42:ad:c5`. Waarom?

A.Deze foutmelding treedt op wanneer de gebruiker probeert verbinding te maken met een EAP-beveiligd WLAN-netwerk en het vooraf ingestelde aantal EAP-pogingen mislukt is. Wanneer de gebruiker niet kan worden geverifieerd, sluit de controller de client uit en kan de client geen verbinding met het netwerk maken totdat de uitsluitingstimer verloopt of handmatig door de beheerder wordt overschreven.

Uitsluiting detecteert verificatiepogingen door één apparaat. Als dat apparaat een maximum aantal storingen overschrijdt, mag dat MAC-adres niet meer aan elkaar koppelen.

Uitsluiting:

- Na 5 opeenvolgende verificatiefouten voor gedeelde verificaties (6e poging is uitgesloten)
- Na 5 opeenvolgende associatiefouten voor MAC-verificatie (6e poging is uitgesloten)
- Na 3 opeenvolgende EAP/802.1X-verificatiefouten (4e poging is uitgesloten)
- Alle externe beleidsserverfouten (NAC)
- Elke instantie voor IP-adresduplicatie
- Na 3 opeenvolgende fouten in webverificatie (4e poging is uitgesloten)

De timer voor hoe lang een client is uitgesloten, kan worden geconfigureerd en uitsluiting kan worden ingeschakeld of uitgeschakeld op controller- of WLAN-niveau.

Q. Ik zie deze foutmelding op de Wireless LAN Controller (WLC): `Een waarschuwing van categorie Switch wordt gegenereerd met ernst 1 door Switch WLCSCH01/10.0.16.5 Het bericht van de waarschuwing is Controller '10.0.16.5'. RADIUS-server(s) reageren niet op verificatieverzoeken.` Waar gaat het om?

A.Dit kan zijn vanwege Cisco bug-id CSC05495. Als gevolg van deze bug, injecteert de controller periodiek een onjuist AV-paar (kenmerk 24, "staat") in verificatieverzoekberichten die een RADIUS RFP overtreden en problemen veroorzaken voor sommige verificatieservers. Deze bug is verholpen in 3.2.179.6.

> **Opmerking**: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-bug-informatie en -tools.

Q. Ik ontvang een bericht van de mislukking van het Ruisprofiel onder Monitor > 802.11b/g Radios. Ik wil begrijpen waarom ik deze MISLUKTE boodschap zie?

A. De status van het geluidsprofiel MISLUKT/DOORGEGEVEN wordt ingesteld na het testresultaat dat door de WLC is uitgevoerd en in vergelijking met de huidige ingestelde drempelwaarde. De standaardinstelling is dat de waarde voor ruis op -70 wordt ingesteld. De MISLUKTE status geeft aan dat de drempelwaarde voor die bepaalde parameter of dat toegangspunt (AP) is overschreden. U kunt de parameters in het profiel aanpassen, maar het wordt aanbevolen de instellingen te wijzigen nadat u het netwerkontwerp duidelijk hebt begrepen en hebt vastgesteld hoe dit de prestaties van het netwerk kan beïnvloeden.

De drempelwaarden voor Radio Resource Management (RRM) DOORGEGEVEN/MISLUKT zijn globaal ingesteld voor alle AP's op de **802.11a Global Parameters > Auto** RF**en 802.11b/g Global Parameters > Auto** RF-pagina's. De drempelwaarden RRM PASSED/MISLUKT zijn voor deze AP afzonderlijk ingesteld op de **802.11 AP-interfaces > Performance** Profilepage.

V. Ik kan poort 2 niet instellen als de back-uppoort voor de AP-Manager interface. De geretourneerde foutmelding is `Kan poortconfiguratie niet instellen`. Ik kan poort 2 instellen als de back-uppoort voor de beheerinterface. De huidige actieve poort voor beide interfaces is poort 1. Waarom?

A. Een AP-manager heeft geen back-uppoort. Vroeger werd het in eerdere versies ondersteund. Sinds versie 4.0 en hoger wordt de back-uppoort voor de AP-Manager interface niet ondersteund. In de regel moet één AP-manager worden geconfigureerd op elke poort (geen back-ups). Als u Link Aggregation (LAG) gebruikt, is er slechts één AP-manager.

De statische (of permanente) AP-Manager interface moet worden toegewezen aan distributiesysteem poort 1 en moet een uniek IP-adres hebben. Het kan niet worden toegewezen aan een reservepoort. Het wordt gewoonlijk geconfigureerd op hetzelfde VLAN of IP-subnetnummer als de beheerinterface, maar dit is geen vereiste.

V. Ik zie deze foutmelding: `De AP '00:0b:85:67:6b:b0' heeft een WPA MIC-fout ontvangen op protocol '1' van Station '00:13:02:8d:f6:41'. Er zijn tegenmaatregelen genomen en het verkeer is gedurende 60 seconden stilgelegd.` Waarom?

A.Message Integrity Check (MIC), opgenomen in WPA (Wi-Fi Protected Access), bevat een frameteller die een man-in-the-middle aanval voorkomt. Deze fout betekent dat iemand in het netwerk het bericht wil terugspelen dat door de oorspronkelijke client is verzonden, of het kan betekenen dat de client defect is.

Als een client herhaaldelijk faalt in de MIC-controle, schakelt de controller het WLAN op de AP-interface uit waar de fouten gedurende 60 seconden worden gedetecteerd. De eerste MIC-fout wordt vastgelegd en er wordt een timer gestart om de tegenmaatregelen te kunnen afdwingen. Indien zich binnen 60 seconden na de meest recente storing een volgende MIC-storing voordoet, dan moet een STA waarvan de IEEE 802.1X-entiteit heeft gehandeld als een Supplicant, zichzelf ongeldig maken of alle STA's met een beveiligingsassociatie ongeldig maken indien haar IEEE 802.1X-entiteit als Authenticator heeft gehandeld.*

Bovendien ontvangt of verzendt het apparaat geen met TKIP versleutelde datakaders en ontvangt of verzendt het geen niet-versleutelde datakaders anders dan IEEE 802.1X-berichten naar of van een peer gedurende een periode van ten minste 60 seconden nadat het de tweede storing heeft gedetecteerd. Als het apparaat een AP is, verbiedt het nieuwe verenigingen met TKIP tijdens deze periode van 60 seconden; aan het eind van de periode van 60 seconden, hervat AP normale

verrichtingen en staat STAs toe om (opnieuw) te associëren.

Dit voorkomt een mogelijke aanval op het coderingsschema. Deze MIC fouten kunnen niet worden uitgeschakeld in WLC versies voor 4.1. Met Wireless LAN Controller versie 4.1 en hoger is er een opdracht om de scantijd voor MIC-fouten te wijzigen. De opdracht **bestaat uit een wachtrij voor WLAN-beveiliging <0-60 seconden> <WLAN-id>**. Gebruik de waarde 0 om MIC-storingsdetectie uit te schakelen voor tegenmaatregelen.

*Ongeldig: eindverificatie.

Q. Deze foutmelding wordt gezien in mijn controller logs: `[ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate is mislukt`. Waarom?

A. Deze foutmeldingen worden meestal weergegeven wanneer de servicepoort van de controller DHCP heeft ingeschakeld, maar geen IP-adres ontvangt van een DHCP-server.

Standaard is er een DHCP-client geïnstalleerd in de fysieke poortinterface en wordt er via DHCP naar een adres gezocht. De WLC probeert een DHCP-adres voor de servicepoort aan te vragen. Als er geen DHCP-server beschikbaar is, mislukt een DHCP-verzoek voor de servicepoort. Hierdoor worden foutmeldingen gegenereerd.

De tijdelijke oplossing is om een statisch IP-adres te configureren naar de servicepoort (zelfs als de servicepoort is losgekoppeld) of om een DHCP-server beschikbaar te hebben om een IP-adres toe te wijzen aan de servicepoort. Laad vervolgens de controller opnieuw, indien nodig.

De servicepoort is eigenlijk gereserveerd voor out-of-band beheer van de controller en systeemherstel, en onderhoud in het geval van een netwerkstoring. Het is ook de enige poort die actief is wanneer de controller in de opstartmodus staat. De servicepoort kan geen 802.1Q-tags dragen. Daarom moet het worden aangesloten op een toegangshaven op de switch van de buur. Het gebruik van de servicepoort is optioneel.

De service poort interface regelt communicatie door en wordt statisch in kaart gebracht door het systeem naar de service poort. Het moet een IP-adres hebben op een ander subnet dan het beheer, de AP-manager en alle dynamische interfaces. Het kan ook niet worden toegewezen aan een back-uppoort. De servicepoort kan DHCP gebruiken om een IP-adres te verkrijgen, of er kan een statisch IP-adres aan worden toegewezen, maar een standaardgateway kan niet worden toegewezen aan de servicepoortinterface. Statische routes kunnen worden gedefinieerd via de controller voor externe netwerktoegang tot de servicepoort.

V. Mijn draadloze clients kunnen geen verbinding maken met het draadloze LAN (WLAN)-netwerk. De WiSM waarmee het toegangspunt is verbonden meldt dit bericht: `Big NAV Dos aanval van AP met Base Radio MAC 00:0g:23:05:7d:d0, Slot ID 0 en Source MAC 00:00:00:00:00:00:000`. Wat betekent dit?

A.Als voorwaarde om tot het middel toegang te hebben, controleert de laag van MAC de waarde van zijn vector van de netwerktoewijzing (NAV). De NAV is een tegenhanger bij elk station dat de hoeveelheid tijd vertegenwoordigt die het vorige frame moet verzenden zijn frame. De NAV moet nul zijn voordat een station kan proberen een frame te verzenden. Vóór de transmissie van een frame berekent een station de tijd die nodig is om het frame te verzenden op basis van de framelengte en gegevenssnelheid. De post plaatst een waarde die deze tijd in het duurveld in de kop van het frame vertegenwoordigt. Wanneer stations het frame ontvangen, onderzoeken ze deze waarde van het duurveld en gebruiken ze deze als basis om hun corresponderende NAV's in te stellen. Dit proces reserveert het medium voor het verzendende station.

Een hoge NAV duidt op de aanwezigheid van een opgeblazen NAV-waarde (virtual carrier sense mechanisme voor 802.11). Als het gerapporteerde MAC-adres 00:00:00:00:00:00 is, wordt het waarschijnlijk gespoofd (mogelijk een echte aanval) en moet u dit bevestigen met een pakketopname.

V. Nadat ik de controller heb geconfigureerd en opnieuw ben opgestart, kan ik de controller niet in beveiligde web (https) modus gebruiken. Deze foutmelding wordt ontvangen terwijl ik probeer toegang te krijgen tot de controller beveiligde webmodus: `Secure Web: Web verificatie certificaat niet gevonden (fout).` Wat is de reden voor dit probleem?

A. Er kunnen verschillende redenen zijn die met deze kwestie verband houden. Een veel voorkomende reden kan gerelateerd zijn aan de virtuele interfaceconfiguratie van de controller. Om dit probleem op te lossen, verwijdert u de virtuele interface en genereert u deze opnieuw met deze opdracht:

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

Start vervolgens de controller opnieuw op. Nadat de controller is opgestart, moet u het webauth-certificaat lokaal opnieuw genereren op de controller met deze opdracht:

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

In de uitvoer van deze opdracht kunt u dit bericht zien:`Web Authenticatiecertificaat is gegenereerd`.

U hebt nu toegang tot de beveiligde webmodus van de controller wanneer u opnieuw opstart.

Q. Controllers melden soms dit IDS Disassociation Flood Signature aanvalsbericht tegen geldige klanten waarin het aanvaller MAC-adres dat van een access point (AP) is aangesloten bij die controller: `Waarschuwing: IDS 'Disassemc flood' Signature aanval gedetecteerd op AP '<AP name>' protocol '802.11b/g' op Controller 'x.x.x.x''. De beschrijving van de handtekening is 'disassociatievloed', met voorrang 'x'. Het adres van de aanvaller is 'hh:hh:hh:hh:hh:hh', het kanaalnummer is 'x', en het aantal detecties is 'x'.` Waarom gebeurt dit?

A.Dit komt door een Cisco-bug IDCsg81953 .

> **Opmerking**: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-bug-informatie en -tools.

IDS Disassociation Flood aanvallen tegen geldige cliënten worden soms gemeld waar het adres van de aanvaller MAC dat van AP is die aan dat controlemechanisme wordt aangesloten.

Wanneer een client is gekoppeld aan het toegangspunt, maar communicatie stopt vanwege kaartverwijdering, zwerft het buiten bereik, en zo verder, naar het toegangspunt, het toegangspunt wacht tot de time-out bij inactiviteit. Zodra de onbelaste time-out is bereikt, verstuurt de AP de client een gescheiden frame. Wanneer de client het gescheiden frame niet erkent, brengt het AP het frame meerdere malen opnieuw over (rond 60 frames). Het IDS-subsysteem van de controller hoort deze herverzendingen en waarschuwingen met dit bericht.

Deze bug is opgelost in versie 4.0.217.0. Upgrade uw Controller versie naar deze versie om dit

waarschuwingsbericht tegen geldige clients en AP's te overwinnen.

Q. Ik ontvang deze foutmelding in de syslog van de controller: **[WAARSCHUWING] apf_80211.c 2408: Ontvangen een bericht met een ongeldig ondersteund tarief van station <xx:xx:xx:xx:xx:xx:xx:xx> [ERROR] apf_utils.c 198: Missing Supported Rate.** Waarom?

A. Eigenlijk, wijzen de `Ontbrekende Ondersteunde` berichten van het `Tarief` erop dat WLC voor bepaalde vereiste gegevenstarieven onder de draadloze instellingen wordt gevormd, maar de NIC kaart mist het vereiste tarief.

Als u gegevenssnelheden hebt, zoals 1 en 2M, ingesteld voor vereist op de controller, maar de NIC-kaart communiceert niet over deze gegevenssnelheden, kunt u dit soort bericht ontvangen. Dit is NIC-kaartfout. Aan de andere kant, als uw controller 802.11g is ingeschakeld en de client een 802.11b(alleen) kaart is, is dit een legitiem bericht. Als deze berichten geen problemen veroorzaken en de kaarten nog kunnen verbinden, kunnen deze berichten worden genegeerd. Als de berichten kaartspecifiek zijn, zorg er dan voor dat de bestuurder van deze kaart up-to-date is.

Q. Deze syslog **AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decode Msg: kon niet overeenkomen WLAN-id <id>** foutmelding wordt uitgezonden op ons netwerk. Waarom gebeurt dit en hoe stop ik ermee?

A.Dit bericht wordt uitgezonden door de LAP's. Dit wordt gezien wanneer u WLAN-overschrijvingsfunctie hebt geconfigureerd voor een WLAN en dat bepaalde WLAN niet wordt geadverteerd.

`ConfigConfig ap syslog host global 0.0.0`om het te stoppen of u kunt een specifiek IP-adres zetten als u een syslog-server hebt, zodat het bericht wordt uitgezonden naar de server alleen.

V. Ik ontvang deze foutmelding op mijn draadloze LAN controller (WLC): **[ERROR] Bestand: apf_mm.c: Line: 581: Aankondig botsing aan voor mobiele 00:90:7a:05:56:8a, verwijderen.** Waarom?

A.Over het algemeen geeft deze foutmelding aan dat de controller een botsing voor een draadloze client heeft aangekondigd (dat wil zeggen dat afzonderlijke AP's aankondigen dat ze de client hebben), en dat de controller geen overdracht van één AP naar de volgende heeft ontvangen. Er is geen netwerkstaat om te onderhouden. Verwijdert de draadloze client en laat de client het nogmaals proberen. Als dit probleem zich vaak voordoet, kan er een probleem zijn met de mobiliteitsconfiguratie. Anders, kan het een anomalie zijn die met een specifieke cliënt of een voorwaarde verwant is.

Q. Mijn controller stelt dit alarmbericht: **Draagdrempel van '12' overtreden.** Wat is deze fout en hoe kan deze worden opgelost?

A.Dit alarmbericht wordt opgeroepen wanneer een client Signal-to-Noise Ratio (SNR) daalt tot een waarde die lager is dan de SNR drempelwaarde voor de betreffende radio. 12 is de standaard SNR drempelwaarde voor detectie van dekkingsgaten.

De detectie van en het correctiealgoritme voor dekkingsgaten bepalen of er een dekkingsgat bestaat wanneer de SNR-niveaus van de cliënten lager zijn dan een bepaalde SNR-drempel. Deze SNR-drempel varieert op basis van twee waarden: de verzendenergie van het toegangspunt en de profielwaarde van de controllerdekking.

In detail wordt de client-SNR-drempel gedefinieerd door de verzendenergie van elke AP

(weergegeven in dBm), minus de constante waarde van 17 dBm, minus de door de gebruiker configureerbare dekkingsprofielwaarde (deze waarde is standaard ingesteld op 12 dB).

- **Afkapwaarde client-SNR (|dB|) = [AP-transmissievermogen (dBm) - constant (17 dBm) - dekkingsprofiel (dB)]**

Deze gebruiker configureerbare dekking profiel waarde kan worden benaderd op deze manier:

1. In de WLC GUI, ga naar de belangrijkste rubriek van Draadloos en selecteer de **netwerkoptie** voor de WLAN-standaard van keuze aan de linkerkant (802.11a of 802.11b/g). Selecteer vervolgens **Auto RF** rechtsboven in het venster.
2. Op de pagina Auto RF Global parameters vindt u de sectie Profieldrempels. In dit gedeelte vindt u de Dekking (3 tot 50 dbm). Deze waarde is de door de gebruiker configureerbare waarde van het dekkingsprofiel.
3. Deze waarde kan worden bewerkt om de client-SNR-drempelwaarde te beïnvloeden. De andere manier om deze SNR drempel te beïnvloeden is de transmissiemacht te verhogen en de opsporing van het dekkingsgat te compenseren.

Q. Ik gebruik ACS v 4.1 en een 4402 draadloze LAN-controller (WLC). Wanneer de WLC probeert om een draadloze client naar ACS 4.1 te MAC-authenticeren, reageert de ACS niet met de ACS en meldt deze foutmelding: "*Interne fout is opgetreden* ". Ik heb al mijn configuraties juist. Waarom doet deze interne fout zich voor?

A. Er is een authenticatie gerelateerde Cisco bug IDCSCsh62641 in de ACS 4.1, waar de ACS geeft `de interne fout is` voorvrorbericht.

Het probleem kan zich voordoen bij deze bug. Er is een patch beschikbaar voor deze bug op de ACS 4.1 Downloads site die het probleem kan oplossen.

> **Opmerking**: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-bug-informatie en -tools.

Vraag: Cisco 4400 Series draadloze LAN-controller (WLC) kan niet worden opgestart. Deze foutmelding wordt ontvangen op de controller: `** Kan geen veld 0:4 gebruiken voor fatload ** Error (no IRQ) dev 0 blk 0: status 0x51 Error reg: 10 ** Kan niet lezen van apparaat 0.` Waarom?

A. De reden voor deze fout kan een hardwareprobleem zijn. Open een TAC-case om dit probleem verder op te lossen. U moet een geldig contract met Cisco hebben om een TAC-case te kunnen openen. Raadpleeg Technische ondersteuning om contact op te nemen met Cisco TAC.

Q. De draadloze LAN-controller (WLC) stuit op problemen met de geheugenbuffer. Wanneer de geheugenbuffers vol zijn, crasht de controller en moet opnieuw opgestart worden om het weer online te brengen. Deze foutmeldingen worden weergegeven in het berichtenlog: `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: Kan nieuwe Mbuf niet toewijzen. Mon apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 219: MbufGet: geen gratis Mbufs.` Waarom?

A.Dit komt door een Cisco-bug IDC93980. Deze bug is opgelost in WLC versie 4.1.185.0. Upgrade uw controller naar deze softwareversie of later om dit bericht te overwinnen.

> **Opmerking**: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne

Cisco-bug-informatie en -tools.

V. Ik heb de upgrade uitgevoerd van onze draadloze LAN-controller (WLC) 4400s naar 4.1-code en onze syslog werd overspoeld door berichten, zoals dit: **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) ontvangen met ongeldige SPA 192.168.1.233/TPA 192.168.1.233.** Wat duiden deze berichten op?

A.Dit kan voorkomen wanneer WLAN is gemarkeerd als DHCP vereist. In dergelijke gevallen mogen alleen stations die een IP-adres ontvangen via DHCP een koppeling maken. Statische clients mogen geen verbinding maken met dit WLAN. WLC fungeert als DHCP Relay Agent en registreert IP-adres van alle stations. Deze foutmelding wordt gegenereerd wanneer WLC ARP-verzoek van een station ontvangt voordat de WLC DHCP-pakketten van het station heeft ontvangen en zijn IP-adres heeft opgenomen.

V. Wanneer u Power over Ethernet (PoE) gebruikt op de Cisco 2106 draadloze LAN-controller, zijn de AP-radio's niet ingeschakeld. Het **toegangspunt kan niet controleren of er voldoende inline voeding is. Sleuf voor radio uitgeschakeld.** foutmelding verschijnt. Hoe kan ik dit oplossen?

A. Deze foutmelding treedt op wanneer de switch, die het toegangspunt inschakelt, een switch is die aan de standaard is onderworpen, maar het toegangspunt de modus die aan de standaard is onderworpen niet ondersteunt.

Een Cisco pre-standaard switch is een kabel die geen intelligent energiebeheer (IPM) ondersteunt, maar wel voldoende voeding heeft voor een standaard access point.

U dient de Pre-Standard-modus van stroom in te schakelen op het toegangspunt waarop deze foutmelding wordt weergegeven. Dit kan worden gedaan van de controller CLI met de configuratie ap power pre-standard {Enable | uitschakelen} {alle | Cisco_AP}opdracht.

Deze opdracht moet, indien nodig, al worden geconfigureerd als u upgrade naar softwarerelease 4.1 van een vorige release. Maar het is mogelijk dat u deze opdracht moet invoeren voor nieuwe installaties of als u het toegangspunt heeft teruggezet op fabriekswaarden.

Deze pre-standaard 15-watt switches van Cisco zijn beschikbaar:

- AIR-WLC2106-K9
- WS-C350, WS-C3560, WS-C3750 switch
- C180
- 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. De controller genereert een **dtl_arp.c:2003 DTL-3-NPUARP_ADD_MISLUKT: kan geen ARP-vermelding voor xx:xx.-xxx.x toevoegen aan de netwerkprocessor. vermelding bestaat niet.** syslog bericht vergelijkbaar met dit. Wat betekent deze syslogboodschap?

A. Terwijl één of andere draadloze client een ARP-antwoord verstuurt, moet de Network Processor Unit (NPU) dat antwoord kennen. Het ARP-antwoord wordt dus doorgestuurd naar NPU, maar WLC-software moet niet proberen om dit item toe te voegen aan de netwerkprocessor.

Als het dit doet, worden deze berichten gegenereerd. Er is geen functionaliteit invloed op de WLC als gevolg hiervan, maar de WLC genereert dit syslog bericht.

V. Ik heb een nieuwe Cisco 2106 WLC geïnstalleerd en geconfigureerd. De WLC geeft aan dat de temperatuursensor is uitgevallen. Wanneer u zich aanmeldt bij de web interface onder "controller-overzicht" staat er "`sensor defect`" naast interne temperatuur. Al het andere lijkt normaal te functioneren.

A.De interne temperatuursensorstoring is cosmetisch en kan worden opgelost met een upgrade naar WLC versie 4.2.61.0.

WLC 2106 en WLC 526 **gebouwd op of na 07/01/2007** kunnen de temperatuursensorchip van een andere leverancier gebruiken. Deze nieuwe sensor werkt prima, maar is niet compatibel met software na de release van 4.2. Daarom kan oudere software de temperatuur niet lezen en laat deze fout zien. Alle andere controllerfuncties worden niet beïnvloed door dit gebrek.

Er is een bekende Cisco-bug IDCSC97299 die betrekking heeft op dit probleem. Deze bug wordt genoemd in de release note van WLC versie 4.2.

> **Opmerking**: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-bug-informatie en -tools.

V. Ik krijg het `radius_db.c:1823 AAA-5-RADSERVER_NOT_found: Kan geen geschikte RADIUS-server voor WLAN vinden <WLAN ID> - kan geen standaardserver"` bericht voor ALLE SSID's `vinden`. Dit bericht verschijnt zelfs voor SSID's die geen AAA-servers gebruiken.

A.Deze foutmelding betekent dat de controller niet in staat was om contact op te nemen met de standaardradiusserver of dat er geen is gedefinieerd.

Een mogelijke oorzaak van dit gedrag is de Cisco-bug IDCSC08181, die in versie 4.2 is opgelost. Upgrade uw controller naar versie 4.2.

Q. Het `Bericht: Juli 10 17:55:00.725 sim.c:1061 SIM-3-MACADR._GET_FAIL: Interface 1 bron MAC-adres wordt niet gevonden.` foutmelding verschijnt op de Draadloze LAN controller (WLC). Wat betekent dit?

A.Dit betekent dat de controller een fout had tijdens het verzenden van een CPU-bronpakket.

V. Deze foutmeldingen verschijnen op de draadloze LAN-controller (WLC):

- `Jul 10 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Kan configuratie bestand 'cliWebInitParms.cfg' niet lezen`
- `Jul 10 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Kan configuratie bestand 'rfidInitParms.cfg' niet lezen`
- `Jul 10 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Kan configuratie bestand 'dhcpParms.cfg' niet lezen`
- `Jul 10 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Kan configuratie bestand 'bcastInitParms.cfg' niet lezen`
- `18 mrt 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_MISLUKT: Verwijderen van bestand: sshpmInitParms.cfg. is mislukt. -proces: Naam:fp_main_task, ID:11ca7618`
- `18 mrt 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILLIET: Verwijderen van het bestand: bcastInitParms.cfg. verwijdering van bestand mislukt. -proces: Naam:fp_main_task, ID:11ca7618`

V. Wat betekent deze foutmelding?

A. Deze berichten zijn informatieve berichten en maken deel uit van de normale opstartprocedure. Deze berichten verschijnen wegens een nalatigheid om verscheidene verschillende configuratiedossiers te lezen of te schrappen. Wanneer bepaalde configuratiebestanden niet worden gevonden of als het configuratiebestand niet kan worden gelezen, stuurt de configuratie-volgorde voor elk proces dit bericht, bijvoorbeeld geen DHCP-serverconfiguratie, geen tags (RF-id) configuratie, enzovoort. Dit zijn berichten met een lage ernst die veilig kunnen worden genegeerd. Deze berichten onderbreken de werking van de controller niet.

Q. De **HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-Cannot_TO_keep_ROUGE_CONTAINER: Kan schurk 00:14:XX:02:XX:XX in ingesloten toestand houden - geen beschikbaar AP om te bevatten.** foutmelding verschijnt. Wat betekent dit?

A.Dit betekent dat het toegangspunt dat de frauduleuze inperkingsfunctie heeft uitgevoerd, niet meer beschikbaar is en dat de controller geen geschikte toegangspunt kan vinden om de frauduleuze insluiting uit te voeren.

Q. Het **DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) ontvangen met ongeldig SPA 192.168.1.152/TPA 192.168.0.206** systeembericht verschijnt op de draadloze LAN-controller. Wat houdt dit bericht in?

A. Het is mogelijk dat het systeem ARP spoofing of vergiftiging ontdekte. Maar dit bericht impliceert niet noodzakelijk dat om het even welke kwaadwillige ARP voor de gek houden is voorgekomen. Het bericht verschijnt wanneer deze voorwaarden waar zijn:

- Een WLAN wordt geconfigureerd met DHCP vereist en een clientapparaat, nadat het is gekoppeld aan dat WLAN, verzendt een ARP-bericht zonder eerst DHCP te voltooien. Dit kan normaal gedrag zijn; het kan bijvoorbeeld gebeuren wanneer de client statisch wordt geadresseerd of wanneer de client een geldige DHCP-lease heeft van een eerdere associatie. De foutmelding kan er als volgt uitzien:

```
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
```

Het effect van deze voorwaarde is dat de client niet in staat is om dataverkeer te verzenden of ontvangen, tot het DHCP's door de WLC.

Raadpleeg het gedeelte DTL-berichten van de Berichtshandleiding voor Cisco Wireless LAN-controller voor meer informatie.

Q. LAP's maken geen gebruik van Power over Ethernet (POE) voor het inschakelen. Ik zie de logbestanden op de draadloze 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

V. Waar gaat het om?

A. Dit kan gebeuren als Power over Ethernet (POE)-instellingen niet goed zijn geconfigureerd. Wanneer een toegangspunt dat is geconverteerd naar de lichtgewicht modus, bijvoorbeeld een AP1131 of AP1242, of een access point uit de 1250 reeks, wordt gevoed door een power injector die is aangesloten op een Cisco pre-Intelligent Power Management (pre-IPM) switch, moet u Power over Ethernet (PoE) configureren, ook bekend als inline voeding.

Raadpleeg Power over Ethernet en Ethernet-ondersteuning configureren voor meer informatie.

V. U ziet dit bericht op de draadloze 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
```

V. Wat betekent dit?

A.Lichtgewicht access points traceren een bepaald algoritme om een controller te vinden. Het proces voor detectie en samenvoeging wordt gedetailleerd uitgelegd in Lichtgewicht AP (LAP)-registratie voor een draadloze LAN-controller (WLC).

Deze foutmelding is te zien op de WLC, wanneer het een detectieaanvraag ontvangt nadat het zijn maximale AP-capaciteit heeft bereikt.

Als de primaire controller voor een LAP niet is geconfigureerd of als zijn een nieuwe uit de doos LAP, stuurt het LWAPP-detectieverzoeken naar alle bereikbare controllers. Als de ontdekkingsverzoeken een controller bereiken die op zijn volledige AP-capaciteit draait, krijgt WLC de verzoeken en realiseert zich dat het op zijn maximale AP-capaciteit is en niet reageert op het verzoek en geeft deze fout.

V. Waar kan ik meer informatie vinden over de LWAPP-systeemmeldingen?

A.Raadpleeg de Berichtshandleiding voor Cisco Wireless LAN Controller System, 4.2 (beëindigd)voor meer informatie over de LWAP-systeemmeldingen.

V. De `foutmelding Error extracting (fout) van webauth-bestanden` wordt weergegeven op de draadloze LAN-controller (WLC). Wat betekent dit?

A.WLC slaagt er niet in om een Custom Web Authenticatie / Passthrough bundel te laden als een van de gebundelde bestanden meer dan 30 tekens in de bestandsnaam heeft, die de bestandsextensie omvat. De aangepaste web auth bundel heeft een limiet van maximaal 30 tekens voor bestandsnamen. Zorg ervoor dat geen bestandsnamen binnen de bundel groter zijn dan 30 tekens.

Q. Draadloze LAN-controllers (WLC's), die 5.2 of 6.0-code met een groot aantal AP-groepen uitvoeren, web GUI geeft niet alle geconfigureerde AP-groepen weer. Waar gaat het om?

A.De ontbrekende AP groepen kunnen worden gezien als u CLI gebruikt `show wlan ap-groups`uit.

Probeer één extra AP-groep aan de lijst toe te voegen. Er zijn bijvoorbeeld 51 AP-groepen geïmplementeerd en de 51st ontbreekt (pagina 3). Voeg de 52e groep toe en pagina 3 moet worden weergegeven in de Web GUI.

Om dit probleem op te lossen, upgraden naar WLC versie 7.0.20.0.

Gerelateerde informatie

- Veelgestelde vragen over WiSM-troubleshooting

- Pagina voor draadloze ondersteuning
- Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.