Een Lightweight AP troubleshooten dat niet wordt verbonden met een WLC

Inhoud

- Inleiding
- Voorwaarden
  - Vereisten
  - Gebruikte componenten
  - Conventies
- Overzicht van het WLC-proces voor detectie en aanmelding
- Debuggen vanaf de controller
  - debug capwap gebeurtenissen activeren
  - debug pm pki inschakelen
- Debuggen vanaf het toegangspunt
- LAP sluit zich niet aan bij de controller, waarom?
  - Bekijk eerst de basisbeginselen
- Veldmelding: Verlopen certificaat - FN63942
- Mogelijke problemen om te zoeken: voorbeelden
  - Probleem 1: De controllertijd valt buiten de geldigheid van het certificaat
  - Probleem 2: Mismatch op het gebied van regelgeving
  - Probleem 3: AP-autorisatielijst ingeschakeld op de WLC; LAP niet in de autorisatielijst
  - Probleem 4: Er is een certificaat of een openbare sleutel corruptie op de AP
  - Probleem 5: Controller ontvangt het AP-detectiebericht op verkeerd VLAN (u ziet het detectiebericht debuggen, maar geen respons)
  - Probleem 6: AP kan niet toetreden tot WLC, firewall blokkerend noodzakelijke poorten
  - Probleem 7: Dubbel IP-adres in het netwerk
  - Probleem 8: LAP's met mesh afbeelding niet in staat om WLC te verenigen
  - Probleem 9: Slecht adres Microsoft DHCP
- Gerelateerde informatie

Inleiding

Dit document beschrijft de detectie en het aanmeldingsproces van AireOS draadloze LAN-controller (WLC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de configuratie van Lichtgewicht access points (LAP's) en Cisco AireOS WLC's
- Basiskennis van Lichtgewicht access point protocol (CAPWAP)

Gebruikte componenten

Dit document concentreert zich op AireOS WLCs en behandelt geen Catalyst 9800 alhoewel het Josep proces grotendeels gelijkaardig is.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

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

Overzicht van het WLC-proces voor detectie en aanmelding

In een Cisco Unified Wireless-netwerk moeten de LAP's eerst een WLC ontdekken en zich bij een WLC aansluiten voordat ze draadloze clients kunnen onderhouden.

Dit stelt echter een vraag: hoe vonden de LAP's het IP-adres van het beheer van de controller als het op een ander subnet staat?

Als u de LAP niet vertelt waar de controller is via DHCP-optie 43, Domain Name System (DNS)-resolutie van Cisco-capwap-controller.local_domain, of de controller statisch configureren, weet de LAP niet waar in het netwerk de beheerinterface van de controller te vinden.

Naast deze methoden kijkt de LAP automatisch op het lokale subnetnet voor controllers met een 255.255.255.255.255 lokale uitzending. Ook herinnert de LAP zich het IP-adres van het beheer van de controller en de controllers die aanwezig zijn als mobiliteitspeers, zelfs bij herstart. Echter, zodra de AP zich aansluit bij een andere WLC, herinnert het zich alleen het IP van die nieuwe WLC en zijn mobiele peers en niet de vorige. Daarom, als u de LAP eerst op het lokale subnet van de beheersinterface zet, vindt het de controlemechanismebeheersinterface en herinnert het adres. Dit heet priming. Dit helpt niet om de controller te vinden als u later een LAP vervangt. Daarom raadt Cisco het gebruik van de DHCP-optie 43 of DNS-methoden aan.

De LAP's verbinden altijd eerst met het beheerinterfaceadres van de controller met een detectieaanvraag. De controller vertelt vervolgens aan de LAP het IP-adres van Layer 3 AP-Manager (dat ook standaard het beheer kan zijn), zodat de LAP een verzoek kan versturen naar de AP-Manager interface.

AP gaat door dit proces bij opstarten:

- **De LAP laarzen en DHCPs een IP adres als het niet eerder een statisch IP adres werd toegewezen.**

- **De LAP stuurt detectieverzoeken naar controllers via de verschillende detectiealgoritmen en maakt een controllerlijst.**

In essentie leert het LAP zoveel mogelijk managementinterfaceadressen voor de controllerlijst via:

a. **DHCP-optie 43 (goed voor wereldwijde bedrijven waar kantoren en controllers op verschillende continenten staan).**

b. **DNS-ingang voor** cisco-capwap-controller (goed voor lokale bedrijven - kan ook worden gebruikt om te vinden waar gloednieuwe APs toetreden) Als u CAPWAP gebruikt, zorg ervoor dat er een DNS-ingang voor cisco-capwap-controlleris.

- **IP-adressen beheren van controllers die de LAP eerder onthoudt.**
- **Een Layer 3-uitzending op het subnetnummer.**
- **Statisch ingestelde informatie.**
- **Controllers aanwezig in de mobiliteitsgroep van WLC de AP laatst aangesloten.**

Van deze lijst, de gemakkelijkste methode om voor plaatsing te gebruiken is de LAPs op zelfde Subnet te hebben zoals de beheersinterface van het controlemechanisme en de uitzending van LAPs Layer 3 toe te staan om het controlemechanisme te vinden. Deze methode moet worden gebruikt voor bedrijven die een klein netwerk hebben en geen lokale DNS-server bezitten.

De volgende gemakkelijkste methode van plaatsing is een DNS ingang met DHCP te gebruiken. U kunt meerdere items met dezelfde DNS-naam hebben. Hierdoor kan de LAP meerdere controllers ontdekken. Deze methode moet worden gebruikt door bedrijven die al hun controllers op één locatie hebben en een lokale DNS-server bezitten. Of als het bedrijf meerdere DNS-achtervoegsels heeft en de controllers zijn gescheiden door een achtervoegsel.

DHCP-optie 43 wordt door grote bedrijven gebruikt om de informatie via DHCP te lokaliseren. Deze methode wordt gebruikt door grote ondernemingen die één DNS-achtervoegsel hebben. Cisco is bijvoorbeeld eigenaar van gebouwen in Europa, Australië en de Verenigde Staten. Om ervoor te zorgen dat de LAP's zich alleen lokaal bij controllers aansluiten, kan Cisco geen DNS-ingang gebruiken en moet Cisco de DHCP-optie 43 gebruiken om de LAP's te vertellen wat het IP-adres voor beheer van hun lokale controller is.

Tot slot wordt de statische configuratie gebruikt voor een netwerk dat geen DHCP-server heeft. U kunt de informatie die nodig is om zich aan te sluiten bij een controller statisch configureren door de consolepoort en de CLI van de AP's. Voor informatie over het statisch configureren van controller-informatie met behulp van de AP CLI, gebruikt u deze opdracht:

```
AP#capwap ap primary-base <WLCName> <WLCIP>
```

Raadpleeg het configuratievoorbeeld van DHCP-optie 43 **voor informatie over het configureren van DHCP-optie 43 op een DHCP-server**

- Verzend een detectieaanvraag naar elke controller in de lijst en wacht op het antwoord op de controller met de systeemnaam, de IP-adressen van de AP-manager, het aantal AP's dat al aan elke AP-Manager interface is gekoppeld en de totale overcapaciteit voor de controller.

- Bekijk de controllerlijst en verstuur een gezamenlijk verzoek naar een controller in deze volgorde (alleen als de AP een ontdekkingsantwoord heeft ontvangen):

a. Primaire controller systeemnaam (eerder geconfigureerd op LAP).

b. Secundaire controllersysteemnaam (eerder geconfigureerd op LAP).

c. Tertiaire Controller systeemnaam (eerder geconfigureerd op LAP).

d. Primaire controller (als de LAP niet eerder is geconfigureerd met primaire, secundaire of tertiaire controllernamen. Gebruikt om altijd te weten welke controller een gloednieuwe LAPs toetreden).

e. Als geen van de vorige omstandigheden worden gezien, de lastverdeling over controlemechanismen door gebruik van de waarde van de overtollige capaciteit in de ontdekkingsreactie.

Als twee controllers dezelfde overtollige capaciteit hebben, verstuur dan het verzoek om samenvoeging naar de eerste controller die reageerde op het verzoek om ontdekking met een ontdekkingsantwoord. Als één controller meerdere AP-managers heeft op meerdere interfaces, kies dan de AP-Manager interface met het minste aantal AP's.

De controller reageert op alle ontdekkingsverzoeken zonder een certificaat of AP-referenties. Aanmeldingen moeten echter een geldig certificaat hebben om een antwoord van de controller te ontvangen. Als de LAP geen reactie van zijn keuze ontvangt, probeert de LAP de volgende controller in de lijst, tenzij de controller een geconfigureerd controller is (primair/secundair/tertiair).

- Wanneer het antwoord ontvangen wordt, controleert het toegangspunt of het dezelfde afbeelding heeft als de controller. Als dit niet het geval is, downloadt het toegangspunt de afbeelding van de controller en start het opnieuw op om de nieuwe afbeelding te laden, en start het proces opnieuw vanaf Stap 1.

- Als het dezelfde software-afbeelding heeft, vraagt het de configuratie aan van de controller en beweegt het naar de geregistreerde status op de controller.

Nadat u de configuratie hebt gedownload, kan de AP opnieuw laden om de nieuwe configuratie toe te passen. Daarom kan een extra herlading optreden en is dit een normaal gedrag.

Debuggen vanaf de controller

Er zijn een paar **debug** opdrachten op de controller die u kunt gebruiken om dit hele proces op de CLI te zien:

- **debug capwap events enable**: Toont detectiepakketten en sluit zich aan bij pakketten.

- **debug capwap packet enable**: Toont informatie op pakketniveau over de detectie en sluit zich aan bij pakketten.

- **debug pm pki enable**: Toont het validatieproces van het certificaat.

- **debug disable-all**: Hiermee schakelt u debugs uit.

Met een terminaltoepassing die uitvoer naar een logbestand kan opnemen, console in of beveiligde shell (SSH)/Telnet naar uw controller en voer deze opdrachten in:

<#root>

config session timeout 120

config serial timeout 120

show run-config

(and spacebar thru to collect all)

debug mac addr <ap-radio-mac-address>

(in xx:xx:xx:xx:xx format)

debug client <ap-mac-address>

debug capwap events enable

debug capwap errors enable

debug pm pki enable

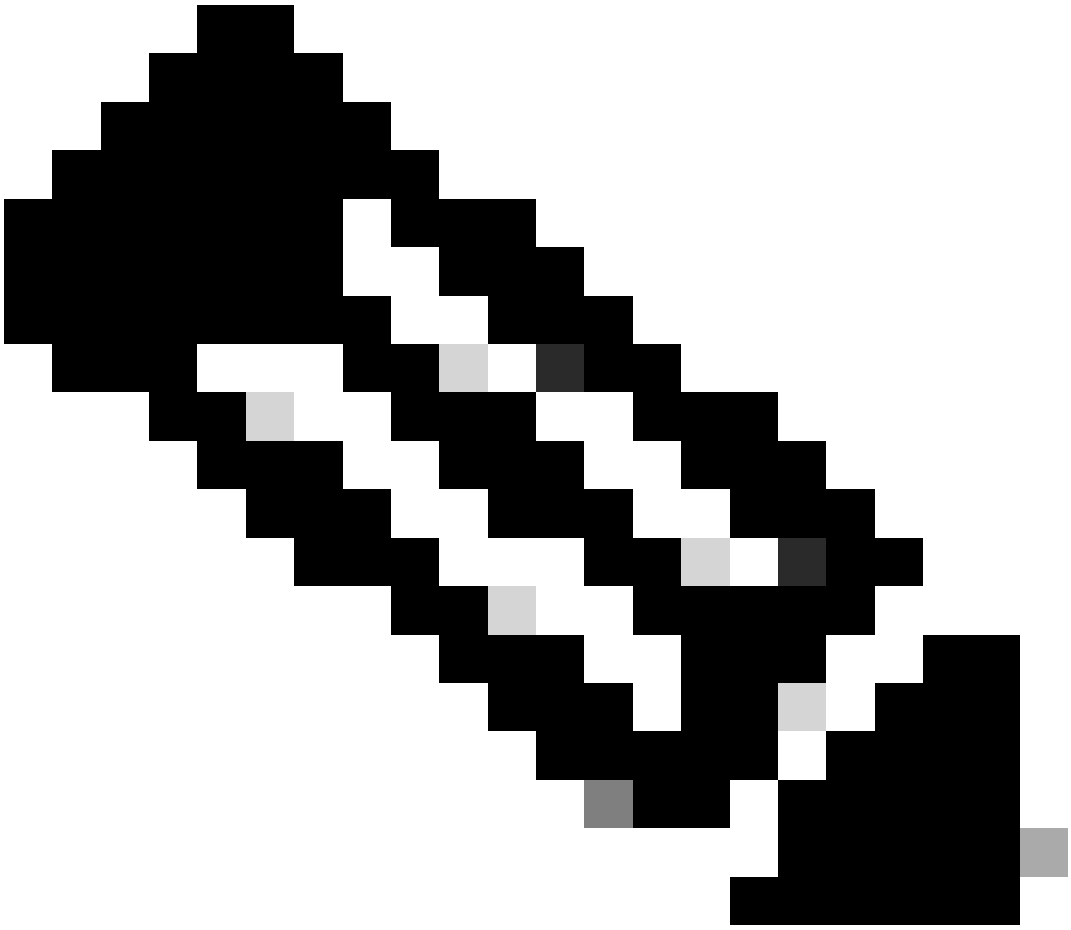
Nadat de debugs zijn opgenomen, gebruikt u de opdrachtdebug disable-all om alle debugs uit te schakelen.

De volgende secties tonen de uitvoer van deze **debug** opdrachten wanneer de LAP zich bij de controller registreert.

debug capwap gebeurtenissen activeren

Deze opdracht geeft informatie over de CAPWAP-gebeurtenissen en fouten die optreden bij de CAPWAP-detectie en het aanmeldingsproces.

Dit is de **debug capwap events enable** opdrachtoutput voor een LAP met hetzelfde beeld als de WLC:



Opmerking: sommige regels van de output zijn naar de tweede regel verplaatst vanwege ruimtebeperkingen.

<#root>

debug capwap events enable

```
*spamApTask7: Jun 16 12:37:36.038: 00:62:ec:60:ea:20 Discovery Request from 172.16.17.99:46317
```

!--- CAPWAP discovery request sent to the WLC by the LAP.

```
*spamApTask7: Jun 16 12:37:36.039: 00:62:ec:60:ea:20 Discovery Response sent to 172.16.17.99 port 46317
```

!--- WLC responds to the discovery request from the LAP.

```
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317
```

!--- LAP sends a join request to the WLC.

```
*spamApTask7: Jun 16 12:38:33.039: 00:62:ec:60:ea:20 Join Priority Processing status = 0, Incoming Ap's
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.472: 00:62:ec:60:ea:20 Join Version: = 134256640

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 apType = 46 apModel: AIR-CAP2702I-E-K9

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join resp: CAPWAP Maximum Msg element len = 90

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join Response sent to 172.16.17.99:46317
*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 CAPWAP State: Join
```

!--- WLC responds with a join reply to the LAP.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Configuration Status from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 CAPWAP State: Configure

!--- LAP requests for the configuration information from the WLC.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP info for AP 00:62:ec:60:ea:20 -- stati
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP 172.16.17.99 ===> 172.16.17.99 for AP
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Running spamDecodeVlanProfMapPayload for00:62:ec:6
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Setting MTU to 1485
*spamApTask7: Jun 16 12:38:44.019: 00:62:ec:60:ea:20 Configuration Status Response sent to 172:16:17:99

!--- WLC responds by providing all the necessary configuration information to the LAP.

*spamApTask7: Jun 16 12:38:46.882: 00:62:ec:60:ea:20 Change State Event Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Radio state change for slot: 0 state: 2 cause: 0 d
*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Change State Event Response sent to 172.16.17.99:4
.
.
.
.

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 CAPWAP State: Run

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Sending the remaining config to AP 172.16.17.99:46
.
.
.
.

!--- LAP is up and ready to service wireless clients.

*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmInterferen

```
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmNeighbourC
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmReceiveCtr
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for CcxRmMeas pay
```

!--- WLC sends all the RRM and other configuration parameters to the LAP.

Zoals vermeld in de vorige paragraaf, eens een LAP zich registreert bij de WLC, controleert het om te zien of het hetzelfde beeld heeft als de controller. Als de afbeeldingen op de LAP en de WLC verschillend zijn, downloaden de LAP's eerst de nieuwe afbeelding van de WLC. Als de LAP hetzelfde beeld heeft, blijft het de configuratie en andere parameters van de WLC downloaden.

U ziet deze berichten in de **debug capwap events enable** opdrachtoutput als de LAP een afbeelding van de controller downloadt als onderdeel van het registratieproces:

```
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Sending image data block of length 1324 and msgLen
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Image Data Request sent to 172.16.17.201:46318
*spamApTask6: Jun 17 14:23:28.693: 00:62:ec:60:ea:20 Image data Response from 172.16.17.201:46318
```

Wanneer de image-download is voltooid, start de LAP opnieuw op en voert de ontdekking uit en sluit zich opnieuw aan bij het algoritme.

debug pm pki inschakelen

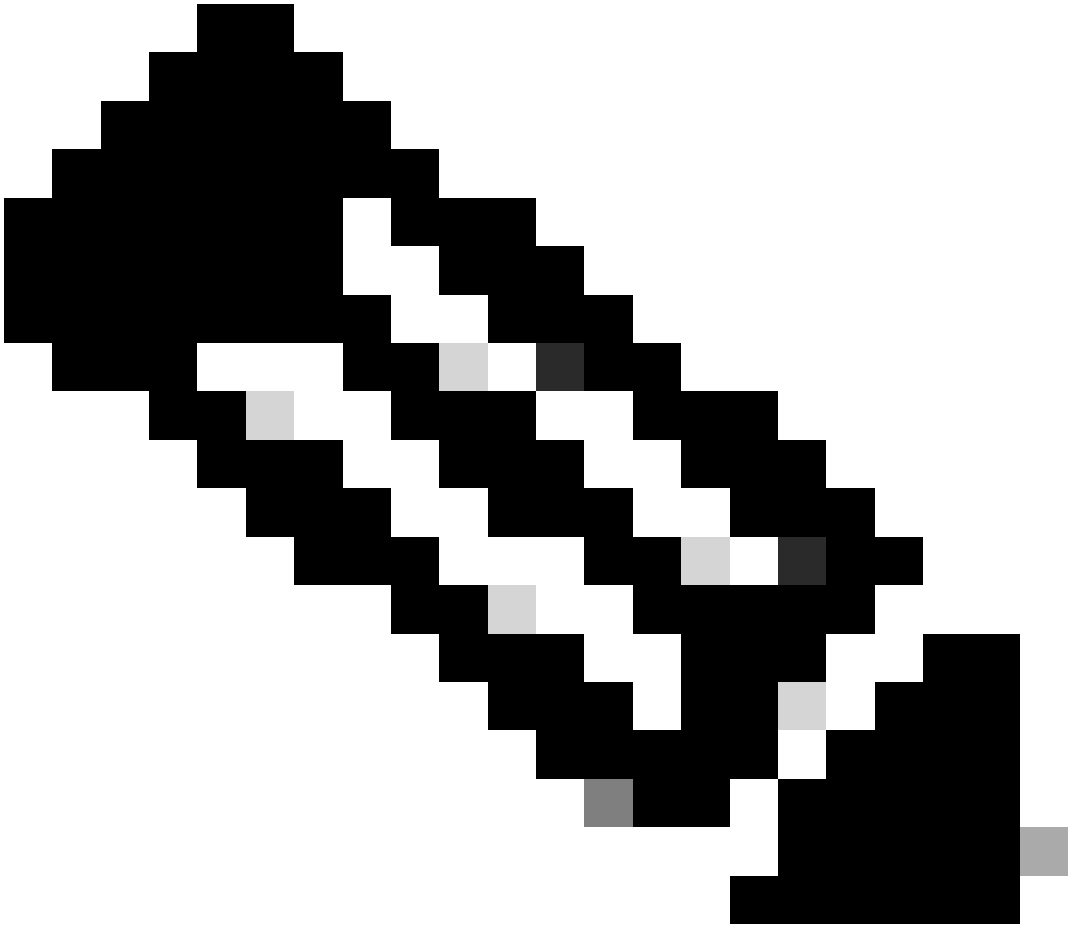
Als deel van het Josef proces, verklaart de WLC elke LAP door te bevestigen dat zijn certificaat geldig is.

Wanneer de AP de CAPWAP Join Verzoek naar de WLC verstuurt, wordt het X.509-certificaat in het CAPWAP-bericht ingesloten. De AP genereert ook een willekeurige sessie-ID die ook is opgenomen in de CAPWAP Join Verzoek. Wanneer de WLC het CAPWAP Join Verzoek ontvangt, bevestigt het de handtekening van het X.509- certificaat met de AP openbare sleutel en controleert dat het certificaat door een vertrouwde op certificaatautoriteit werd verstrekt.

Het kijkt ook naar de begindatum en de tijd voor de geldigheidsperiode van het AP-certificaat en vergelijkt die datum en tijd met zijn eigen datum en tijd (vandaar dat de controllerklok moet worden ingesteld dicht bij de huidige datum en tijd). Als het X.509-certificaat is gevalideerd, genereert de WLC een willekeurige AES-encryptiesleutel. De WLC plumpt de AES-sleutels in zijn crypto-engine zodat het toekomstige

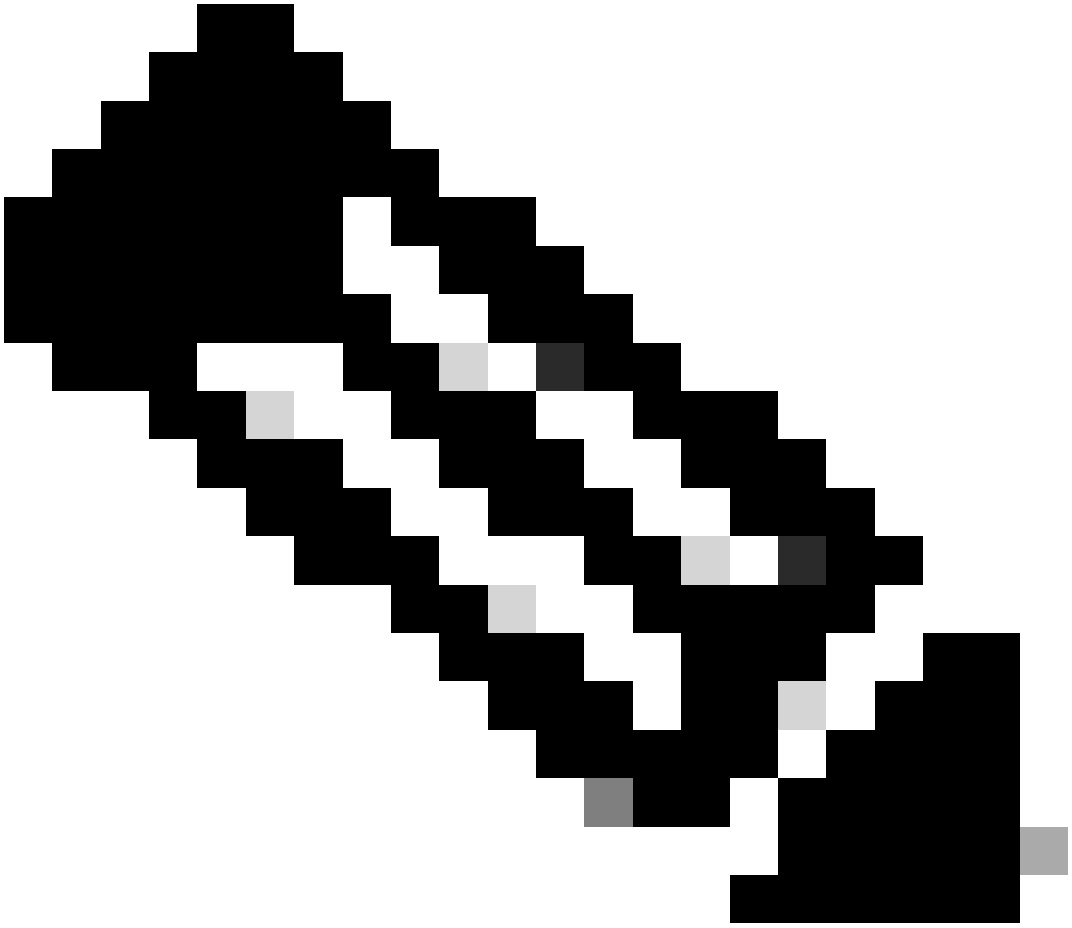
CAPWAP Control Berichten kan versleutelen en ontsleutelen die met de AP zijn uitgewisseld. Merk op dat gegevenspakketten in de duidelijke in de CAPWAP-tunnel tussen de LAP en de controller worden verzonden.

Het **debug pm pki enable** bevel toont het certificatiebevestigingsproces dat bij de toetreden fase op het controlemechanisme voorkomt. De **debug pm pki enable** opdracht geeft ook de AP-hashtoets weer bij het Josep-proces als het AP een zelfondertekend certificaat (SSC) heeft dat is gemaakt door het LWAP-conversieprogramma. Als het toegangspunt is voorzien van een productiecertificaat (MIC), ziet u geen hashsleutel.



Opmerking: alle AP's die na juni 2006 zijn geproduceerd, hebben een MIC.

Hier is de uitvoer van de **debug pm pki enable** opdracht wanneer de LAP met een MIC zich bij de controller voegt:



Opmerking: sommige regels van de output zijn naar de tweede regel verplaatst vanwege ruimtebeperkingen.

<#root>

```
*spamApTask4: Mar 20 11:05:15.687: [SA] OpenSSL Get Issuer Handles: locking ca cert table

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: x509 subject_name /C=US/ST=Californ
CN=AP3G2-1005cae83a42/emailAddress=support@cisco.com
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

issuer_name /O=Cisco Systems/CN=Cisco Manufacturing CA

```
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Cert Name in subject is AP3G2-1005c

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Extracted cert issuer from subject


*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

Cert is issued by Cisco Systems.

```
*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultMfgCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row
*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 260e5e69 for certname cscoDefaultMfgCaCert

*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultMfgCaCert in row 5 x

*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultNewRootCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultNewRootCaCert in

*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 28d7044e for certname cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultNewRootCaCert in row
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification return code: 1
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification result text: ok
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row

*spamApTask4: Mar 20 11:05:15.691: [SA]
```

Verify User Certificate: OPENSSL X509_Verify: AP Cert Verfied Using >cscoDefaultMfgCaCert<

```
*spamApTask4: Mar 20 11:05:15.691: [SA] OpenSSL Get Issuer Handles:
```

Check cert validity times (allow expired NO)

```
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultIdCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching ID cert cscoDefaultIdCert in row 2
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle: called with 0x1b0b9380

*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle:
```

freeing public key

Debuggen vanaf het toegangspunt

Als de controller debugs niet aangeven een verzoek samenvoegen, kunt u het proces vanaf het toegangspunt debuggen als het toegangspunt een consolepoort heeft. U kunt het opstartproces van het toegangspunt met deze opdrachten zien, maar u moet eerst de inschakelmodus inschakelen (standaardwachtwoord is Cisco).

- **debug dhcp detail** : Geeft informatie over DHCP-optie 43 weer.
- **debug ip udp**: Toont alle UDP-pakketten die door het toegangspunt zijn ontvangen en verzonden.
- debug capwap client event : Geeft capswapgebeurtenissen voor het toegangspunt weer.
- **debug capwap client error**: Geeft capswapfouten voor AP weer.

- **debug dtls client event**: Geeft DTLS-gebeurtenissen voor het toegangspunt weer.

- **debug dtls error enable**: Toont DTLS-fouten voor het toegangspunt.

- **undebug all**: Maakt debugs op het AP uit.

Hier is een voorbeeld van de uitvoer van de debug capwapopdrachten. Deze gedeeltelijke output geeft een idee van de pakketten die door AP bij het laarsproces worden verzonden om bij een controlemechanisme te ontdekken en zich aan te sluiten.

<#root>

```
AP can discover the WLC via one of these options :
```

!--- AP discovers the WLC via option 43

```
*Jun 28 08:43:05.839: %CAPWAP-5-DHCP_OPTION_43: Controller address 10.63.84.78 obtained through DHCP
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.78 with discovery type set
```

!--- capwap Discovery Request using the statically configured controller information.

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.32 with discovery type set
```

!--- Capwap Discovery Request sent using subnet broadcast.

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 255.255.255.255 with discovery type
```

!--- capwap Join Request sent to AP-Manager interface on DHCP discovered controller.

```
*Jun 28 08:40:29.031: %CAPWAP-5-SENDJOIN: sending Join Request to 10.63.84.78
```

LAP sluit zich niet aan bij de controller, waarom?

Bekijk eerst de basisbeginselen

- Kunnen AP en WLC communiceren?
- Zorg ervoor dat het toegangspunt een adres van DHCP krijgt (controleer de leases van de DHCP-server op het MAC-adres van het toegangspunt).
- Pingel het toegangspunt van de controller.
- Controleer of de STP-configuratie op de switch correct is, zodat pakketten naar de VLAN's niet worden geblokkeerd.
- Als pings succesvol zijn, zorg ervoor dat de AP ten minste één methode heeft waarmee om ten minste één WLC-console of telnet/ssh in de controller te ontdekken om debugs uit te voeren.
-

Elke keer dat het toegangspunt opnieuw opstart, initieert het de WLC-detectiesequentie en probeert het toegangspunt te vinden. Start het toegangspunt opnieuw op en controleer of het meedoet met de WLC.

Hier zijn enkele van de meest geziene kwesties toe te schrijven aan welke de LAPs niet tot de WLC toetreden.

Veldmelding: Verlopen certificaat - FN63942

In de hardware ingebouwde certificaten zijn 10 jaar geldig na de productie. Als uw AP's of WLC meer dan 10 jaar oud zijn, kunnen verlopen certificaten ervoor zorgen dat AP zich aansluit bij problemen. Meer informatie over dit onderwerp is te vinden in de melding in dit veld: Melding uit het veld: FN63942.

Mogelijke problemen om te zoeken: voorbeelden

Probleem 1: De controllertijd valt buiten de geldigheid van het certificaat

Voltooi de volgende stappen om dit probleem op te lossen:

- Opdrachten op het toegangspunt uitgevendebug dtls client error + debug dtls client event:

<#root>

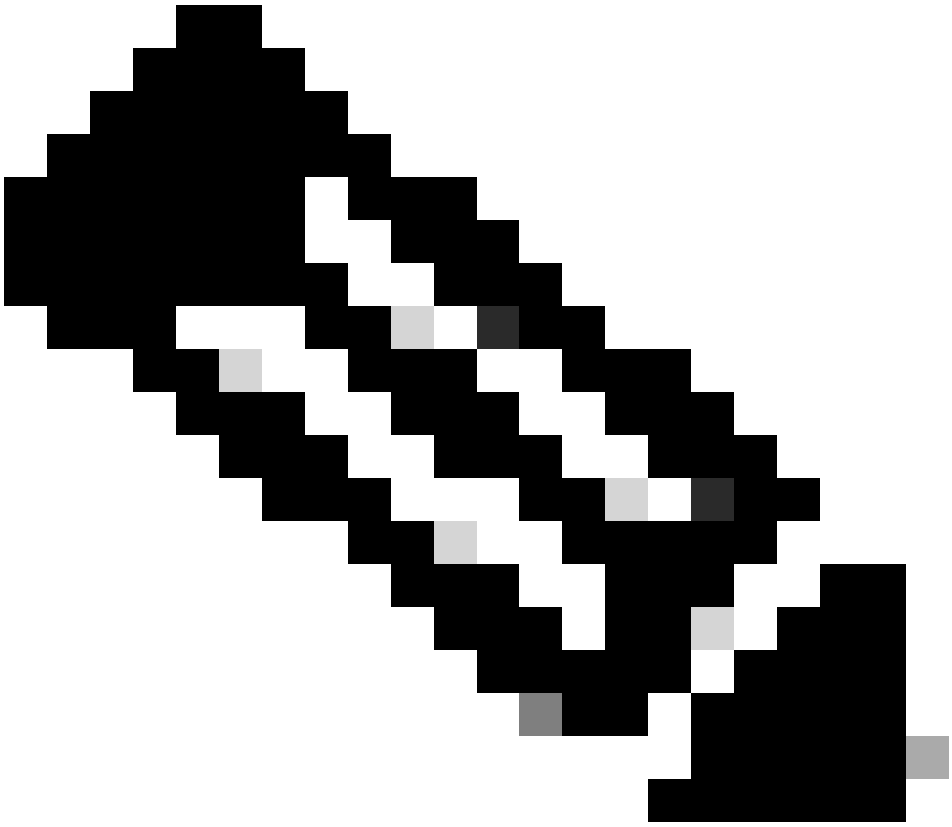
```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer certificate v
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 C
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL :
```

Bad certificate Alert

```
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_client_process_record: Error processing Certificate.
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection 0x8AE7FD0
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_free_connection: Free Called... for Connection 0x8AE
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL : Close notify Alert
```

Uit deze informatie blijkt duidelijk dat de tijd van de controller buiten de geldigheidsperiode van het certificaat van het toegangspunt valt. Daarom kan het toegangspunt zich niet registreren bij de controller. De certificaten die in AP worden geïnstalleerd hebben een vooraf bepaald geldigheidinterval. De controllertijd moet zo worden ingesteld dat deze binnen de geldigheidsperiode van het certificaat van het AP-certificaat valt.

• Geef de **show time** opdracht uit van de controller CLI om te controleren of de datum en tijd die op uw controller is ingesteld binnen deze geldigheidsperiode vallen. Als de controllertijd hoger of lager is dan dit certificaat geldigheids interval, dan verander de controlemechanismetijd om binnen dit interval te vallen.



Commands > Set Time **Opmerking**: Als de tijd niet juist is ingesteld op de controller, kies dan in de controller GUI-modus, of geef de configuratietijd-opdracht in de controller CLI uit om de controller-tijd in te stellen.

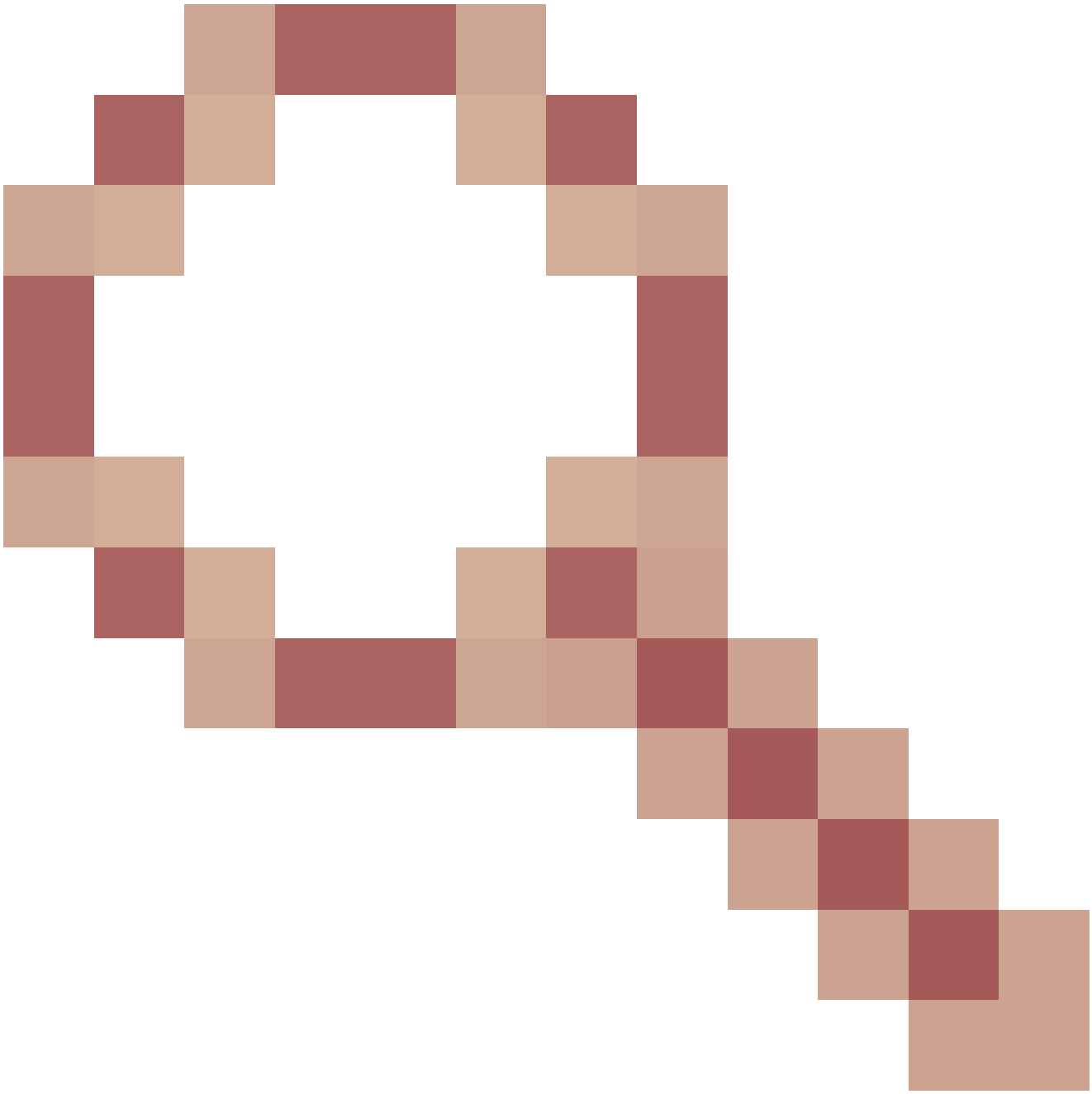
- Controleer op AP's met CLI-toegang de certificaten met de **show crypto ca certificates** opdracht van de AP CLI.

Met deze opdracht kunt u de geldigheid van het certificaat verifiëren die is ingesteld in het toegangspunt. Hierna volgt een voorbeeld:

```
AP00c1.649a.be5c#show crypto ca cert
.........................................
.........................................
.........................................
.........................................
Certificate
Status: Available
Certificate Serial Number (hex): 7D1125A900000002A61A
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA SHA2
o=Cisco
Subject:
Name: AP1G2-00c1649abe5c
e=support@cisco.com
cn=AP1G2-00c1649abe5c
o=Cisco Systems
l=San Jose
st=California
c=US
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca2.crl
Validity Date:
start date: 01:05:37 UTC Mar 24 2016
end date: 01:15:37 UTC Mar 24 2026
Associated Trustpoints: Cisco_IOS_M2_MIC_cert
Storage:
.................................
.................................
.................................
```

De gehele output wordt niet weergegeven omdat er veel validiteitsintervallen kunnen zijn die gekoppeld zijn aan de output van dit commando. Neem alleen het geldigheidinterval in overweging dat is gespecificeerd door het Associated Trustpoint: Cisco_IOS_MIC_cert met de relevante AP-naam in het naamveld. In deze voorbeelduitvoer is het de `naam: C1200-001563e50c7e`. Dit is de werkelijke geldigheidsperiode van het certificaat die in aanmerking moet worden genomen.

- Raadpleeg Cisco bug-id CSCuq19142



LAP/WLC MIC of SSC levenslang verlopen voor DTLS-fout: Cisco bug-id CSCuq19142.

Probleem 2: Mismatch op het gebied van regelgeving

U ziet dit bericht in de **debug capwap events enable** opdrachtoutput:

<#root>

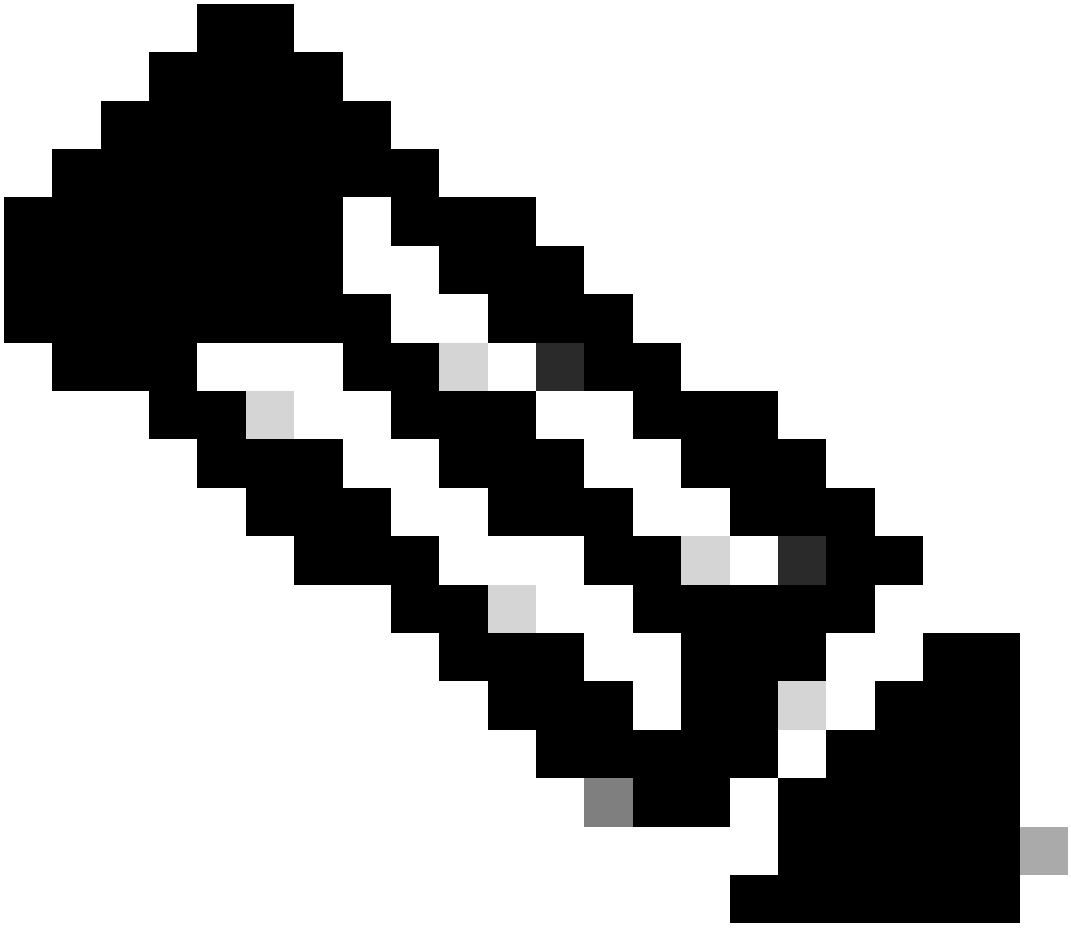
```
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
```

***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Setting MTU to1485**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Regulatory Domain Mismatch: AP 00:cc:fc:13:e5:e0 no**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Finding DTLS connection to delete for AP (192:168:4**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Disconnecting DTLS Capwap-Ctrl session 0x1d4df620 f**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 acDtlsPlumbControlPlaneKeys: lrad:192.168.47.29(603**

WLC msglog show these messages :

*spamApTask5: Jun 28 11:52:06.536: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7095 00:cc:fc:13:e5:e0: DT
closed forAP 192:168:47:28 (60389), Controller: 10:63:84:78 (5246) Regulatory Domain Mismatch

De boodschap geeft duidelijk aan dat er sprake is van een wanverhouding op het gebied van regelgeving van de LAP en de WLC. De WLC ondersteunt meerdere regulerende domeinen, maar elk regulerend domein moet worden geselecteerd voordat een AP zich kan aansluiten bij dat domein. De WLC die regulerend domein gebruikt -A kan alleen worden gebruikt met AP's die regulerend domein -A gebruiken (enzovoort). Zorg er bij de aankoop van AP’s voor dat ze hetzelfde regelgevingsdomein delen. Alleen dan kunnen de AP's zich registreren met de WLC.



Opmerking: zowel 802.1b/g als 802.11a-radio's moeten binnen hetzelfde regelgevingsdomein vallen voor één AP.

Probleem 3: AP-autorisatielijst ingeschakeld op de WLC; LAP niet in de autorisatielijst

In dergelijke gevallen ziet u dit bericht op de controller in de uitvoer van de opdrachtdebug capwap events enable:

<#root>

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received CAPWAP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
```

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received CAPWAP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce  00:0B:85:33:52:80
rxNonce  00:0B:85:51:5A:E0
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 CAPWAP Join-Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007:
```

spamRadiusProcessResponse: AP Authorization failure

for 00:0b:85:51:5a:e0

Als u een LAP gebruikt die een consolepoort heeft, ziet u dit bericht wanneer u de opdrachtdebug capwap client error geeft:

<#root>

```
AP001d.a245.a2fb#
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: spamHandleJoinTimer: Did not receive the
Join response
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG:
```

No more AP manager IP addresses remain.

Dit is opnieuw een duidelijke aanwijzing dat de LAP geen deel uitmaakt van de AP autorisatielijst op de controller.

U kunt de status van de machtigingslijst van het toegangspunt met deze opdracht weergeven:

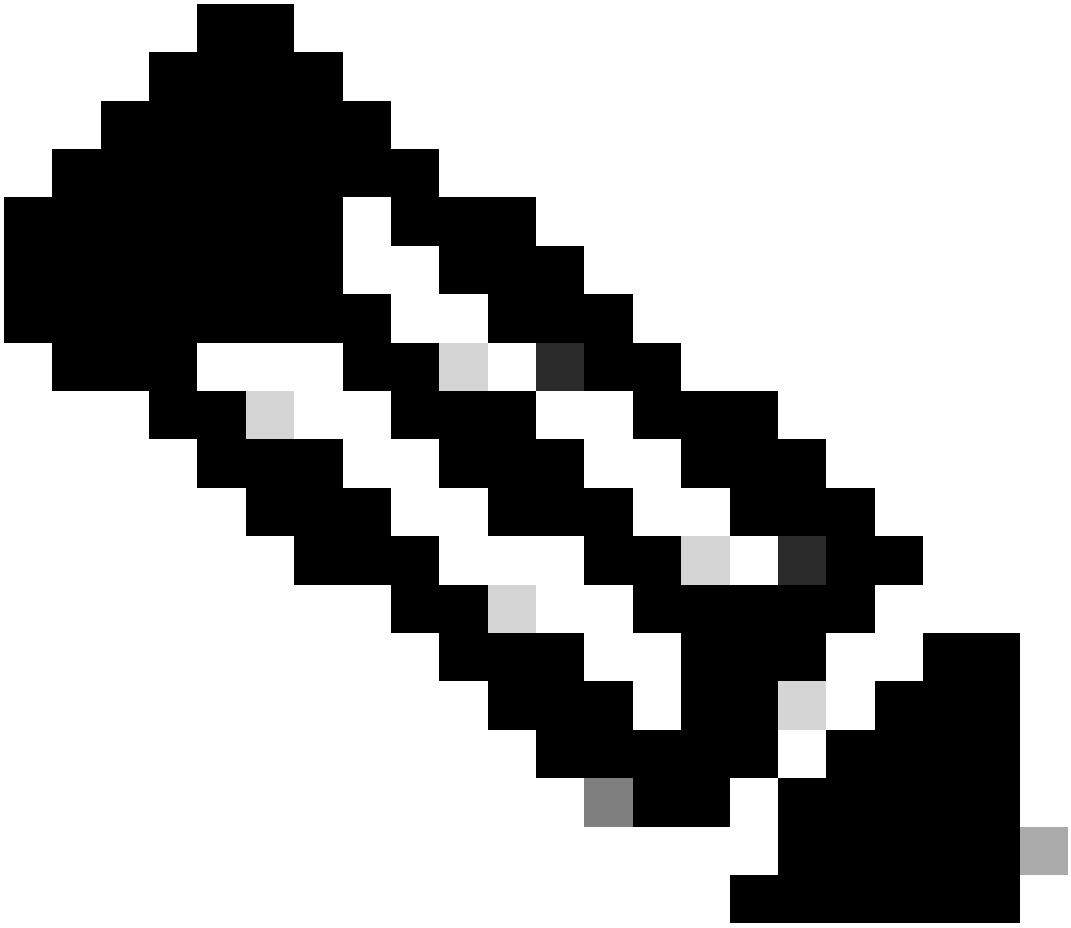
```
<#root>

(Cisco Controller) >

show auth-list

Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

Gebruik de config auth-list add mic <AP MAC Address> opdracht om een LAP toe te voegen aan de AP-autorisatielijst. Raadpleeg Lichtgewicht access point (LAP) autorisatie in een Cisco Unified Wireless Network Configuration Voorbeeld voor meer informatie over het configureren van LAP.

Probleem 4: Er is een certificaat of een openbare sleutel corruptie op de AP

De LAP sluit zich niet aan bij een controller vanwege een certificaatuitgifte.

Geef de debug capwap errors enable en **debug pm pki enable** opdrachten uit. U ziet berichten die de certificaten of de sleutels aangeven die worden beschadigd.



Opmerking: sommige regels van de output zijn verplaatst naar tweede regels vanwege ruimtebeperkingen.

<#root>

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 CAPWAP
```

Join Request does not include valid certificate in CERTIFICATE_PAYLOAD
from AP 00:0f:24:a9:52:e0

```
.
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 Deleting and removing AP 00:0f:24:a9:52:e0 from fast path
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Unable to free public key for AP
```

Gebruik een van deze twee opties om het probleem op te lossen:

- MIC AP - aanvraag een retourmateriaalautorisatie (RMA).
- LSC AP - Opnieuw provisioneren van uw LSC certificaat.

Probleem 5: Controller ontvangt het AP-detectiebericht op verkeerd VLAN (u ziet het detectiebericht debuggen, maar geen respons)

U ziet dit bericht in de debug capwap events enable opdrachtoutput:

<#root>

Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!

Dit bericht betekent dat de controller een detectieaanvraag heeft ontvangen via een IP-adres met een IP-bronadres dat niet in een geconfigureerd subnet op de controller staat. Dit betekent ook dat de controller degene is die het pakket laat vallen.

Het probleem is dat het toegangspunt niet datgene is wat de detectieaanvraag naar het IP-adres van het beheer heeft gestuurd. De controller meldt een verzoek voor broadcast-detectie van een VLAN dat niet op de controller is geconfigureerd. Dit komt typisch voor wanneer de trunks VLANs toestonden en hen niet tot draadloze VLANs beperkten.

Voltooi de volgende stappen om dit probleem op te lossen:

- Als de controller zich op een ander subnet bevindt, moeten de AP's worden **voorbereid** voor het IP-adres van de controller, of moeten de AP's het IP-adres van de controllers ontvangen met behulp van een van de detectiemethoden.

- De switch is ingesteld om bepaalde VLAN’s toe te staan niet op de controller. Beperk de toegestane VLAN’s op de trunks.

Probleem 6: AP kan niet toetreden tot WLC, firewall blokkerend noodzakelijke poorten

Als in het ondernemingsnetwerk een firewall wordt gebruikt, zorg er dan voor dat deze poorten op de firewall zijn ingeschakeld zodat de LAP zich kan aansluiten bij en kan communiceren met de controller.

U moet deze poorten inschakelen:

- Schakel deze UDP-poorten voor CAPWAP-verkeer in:
  - Gegevens - 5247
  - Controle - 5246
- Schakel deze UDP-poorten voor mobiliteitsverkeer in:
  - 16666 - 16666
  - 16667 - 16667
-

Schakel UDP-poorten 5246 en 5247 in voor CAPWAP-verkeer.

- TCP/IP-telefoon 161 en 162 voor SNMP (voor het draadloze controlesysteem [WCS])

Deze poorten zijn optioneel (afhankelijk van uw vereisten):

- UDP 69 voor TFTP
- TCP/IPsec 800 en/of 443 TCP- of HTTPS-toegang voor GUI
- TCP/IPsec 23 en/of 22 TCP/IP voor Telnet of SSH voor CLI-toegang

Probleem 7: Dubbel IP-adres in het netwerk

Dit is een andere veel voorkomende kwestie gezien wanneer de AP probeert zich aan te sluiten bij de WLC. U kunt deze foutmelding zien wanneer het toegangspunt probeert zich aan te sluiten bij de controller.

No more AP manager IP addresses remain

Een van de redenen voor deze foutmelding is wanneer er een dubbel IP-adres in het netwerk is dat overeenkomt met het IP-adres van de AP-beheerder. In een dergelijk geval houdt de LAP de initiaties van de stroomcyclus bij en kan deze zich niet bij de controller aansluiten.

De debugs tonen de WLC ontvangt LWAPP-detectieverzoeken van de AP's en stuurt een LWAPP-detectierespons naar de AP's.

WLC's ontvangen echter geen LWAPP voor verzoeken van de AP's.

Om dit probleem op te lossen, pingel de AP manager van een bekabelde host op dezelfde IP-subnetverbinding als de AP Manager. Controleer het ARP cache. Als een dubbel IP-adres wordt gevonden, verwijdert u het apparaat met het dubbele IP-adres of wijzigt u het IP-adres op het apparaat zodat het een uniek IP-adres in het netwerk heeft.

De AP kan zich dan aansluiten bij de WLC.

Probleem 8: LAP's met mesh afbeelding niet in staat om WLC te verenigen

Het lichtgewicht access point registreert niet bij de WLC. Het logbestand geeft dit het foutbericht weer:

```
AAA Authentication Failure for UserName:5475xxx8bf9c User
     Type: WLAN USER
```

Dit kan gebeuren als het lichtgewicht access point met een mesh beeld is meegeleverd en in de Bridge-modus staat. Als de LAP is besteld met mesh software erop, moet u de LAP toevoegen aan de AP autorisatielijst. Kies **Beveiliging > AP-beleid** en voeg **AP** toe aan de Autorisatielijst. De AP moet dan toetreden, de afbeelding downloaden van de controller, en vervolgens registreren met de WLC in de brugmodus. Vervolgens dient u het toegangspunt te wijzigen in de lokale modus. De LAP downloadt de afbeelding, start opnieuw op en registreert terug naar de controller in de lokale modus.

Probleem 9: Slecht adres Microsoft DHCP

Access points kunnen hun IP-adressen snel vernieuwen wanneer een poging wordt gedaan om zich aan te sluiten bij een WLC, wat ervoor kan zorgen dat Windows DHCP-servers deze IP's markeren als BAD_ADDRESS die snel de DHCP-pool kan uitputten. Controleer voor meer informatie in het hoofdstuk Client Roaming van de Cisco Wireless Controller Configuration Guide, release 8.2.

Gerelateerde informatie

- **Cisco Technical Support en downloads**
- **AP201-proces met Catalyst 9800**

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.