

Begrijp het AP Join Proces met Catalyst 9800 WLC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[CAPWAP-sessieinstelling](#)

[DTLS-sessieinstelling](#)

[Detectiemethoden voor draadloze LAN-controllers](#)

[Selectie van draadloze LAN-controllers](#)

[CAPWAP State Machine](#)

[CAPWAP State: Detectie](#)

[CAPWAP State: DTLS Setup](#)

[CAPWAP Staat: Join](#)

[CAPWAP-status: beeldgegevens](#)

[CAPWAP-status: configureren](#)

[CAPWAP State: Uitvoeren](#)

[Configureren](#)

[Statische WLC-verkiezingen](#)

[Telnet/SSH-toegang tot het toegangspunt inschakelen](#)

[Data Link-encryptie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Bekende problemen](#)

[WLC GUI-controles](#)

[Opdrachten](#)

[Van de WLC](#)

[Van Wave 2 en Catalyst 11ax AP's](#)

[Vanaf Wave 1 access points](#)

[Radioactieve sporen](#)

Inleiding

Dit document beschrijft in detail het AP-Join-proces met Cisco Catalyst 9800 WLC.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van controle en provisioning voor draadloze access points (CAPWAP)
- Basiskennis van het gebruik van een draadloze LAN-controller (WLC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9800-L WLC, Cisco IOS® XE koppeling 17.9.3
- Catalyst 9120AXE access point

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.

Achtergrondinformatie

CAPWAP-sessieinstelling

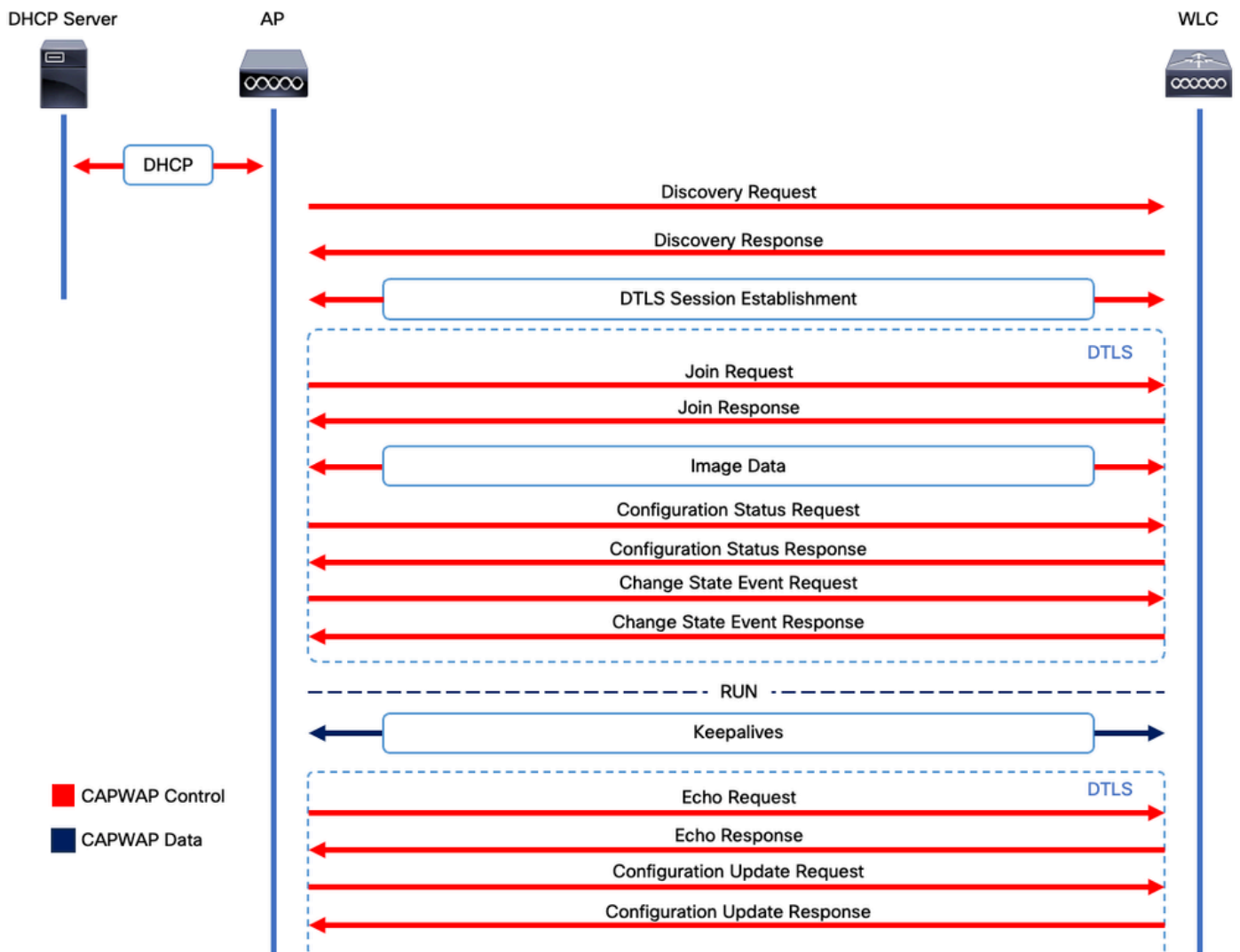
Control and Provisioning Wireless Access Point (CAPWAP) is het protocol dat het transportmechanisme biedt dat door access points (AP's) en draadloze LAN-controllers (WLC's) wordt gebruikt om controle- en dataplatforminformatie via een beveiligde communicatietunnel (voor CAPWAP-controle) uit te wisselen.

Om verder te gaan met het AP Join-proces, is het belangrijk dat u het Control and Provisioning Wireless Access Point (CAPWAP)-sessieproces begrijpt.

Houd er rekening mee dat het toegangspunt een IP-adres moet hebben voordat het CAPWAP-proces kan starten. Als het toegangspunt geen IP-adres heeft, wordt het CAPWAP Session Establishment Process niet gestart.

1. Access Point stuurt een detectieaanvraag. Zie de sectie WLC Discovery Methods voor meer informatie over dit onderwerp
2. WLC stuurt een Discovery Response
3. DTLS-sessie instellen. Hierna worden alle berichten versleuteld en weergegeven als DTLS-toepassingsgegevenspakketten in een pakketanalysetool.
4. Access Point verstuurt een Join Verzoek
5. WLC stuurt een Join Response
6. AP voert een beeldcontrole uit. Als het dezelfde beeldversie heeft als de WLC, gaat het verder met de volgende stap. Als het niet, dan downloadt het het beeld van WLC en reboots om het nieuwe beeld te laden. In dat geval wordt het proces uit stap 1 herhaald.
7. Access Point verstuurt een Configuration Status-verzoek.
8. WLC stuurt een Configuration Status Response
9. Access point gaat naar RUN state
10. Tijdens de RUN-status wordt CAPWAP Tunnelonderhoud op twee manieren uitgevoerd:

1. Keepalives worden uitgewisseld om de CAPWAP Data tunnel te onderhouden
2. AP stuurt een Echo-verzoek naar de WLC, dat moet worden beantwoord met zijn respectieve Echo Response. Dit is om de CAPWAP Control tunnel te behouden.



CAPWAP-sessievaststellingsproces



Opmerking: volgens RFC 5415 maakt CAPWAP gebruik van de UDP-poorten 5246 (voor CAPWAP Control) en 5247 (voor CAPWAP Data).

DTLS-sessieinstelling

Zodra het access point een geldige Discovery Response van de WLC ontvangt, wordt er een DTLS-tunnel tussen hen opgezet om alle volgende pakketten via een beveiligde tunnel te verzenden. Dit is het proces voor het instellen van de DTLS-sessie:

1. AP verstuurt een bericht van Client Hello
2. WLC verstuurt een Helloverifyrequest bericht met een cookie die voor validatie wordt gebruikt.
3. AP verstuurt een ClientHello bericht met een cookie die voor validatie wordt gebruikt.
4. WLC verstuurt deze pakketten in volgorde:
 1. ServerHallo
 2. Certificaat
 3. Toetsuitwisseling voor servers

4. Certificaataanvraag
5. ServerHalloGereed
5. AP verstuurt deze pakketten in volgorde:
 1. Certificaat
 2. ClientKey Exchange
 3. Certificaat controleren
 4. Specificaties wijzigen
6. WLC reageert op de ChangeCypherSpec van het AP met zijn eigen ChangedCypherSpec:
 1. Specificaties wijzigen

Na het laatste ChangedCypherSpec-bericht dat door de WLC is verstuurd, wordt de beveiligde tunnel tot stand gebracht en wordt al het verkeer dat in beide richtingen wordt verstuurd nu versleuteld.

Detectiemethoden voor draadloze LAN-controllers

Er zijn verschillende opties om de access points te laten weten dat er één WLC in het netwerk bestaat:

- DHCP-optie 43: Deze optie geeft de AP's het IPv4-adres van de WLC om toe te voegen. Dit proces is handig voor grote implementaties waarin de AP's en de WLC in verschillende sites zijn.
- DHCP-optie 52: Deze optie geeft de AP's het IPv6-adres van de WLC om toe te voegen. Het gebruik ervan is handig in hetzelfde scenario als DHCP-optie 43.
- DNS-detectie: AP's zoeken de domeinnaam Cisco-CAPWAP-CONTROLLER.localdomain. U moet uw DNS-server configureren om het IPv4- of IPv6-adres van de WLC op te lossen. Deze optie is handig voor implementaties waarin de WLC's zijn opgeslagen op dezelfde locatie als de AP's.
- Layer 3 Broadcast: De AP's verzenden automatisch een uitzendingsbericht naar 255.255.255.255. Om het even welke WLC binnen zelfde subnetto zoals AP wordt verwacht om aan dit ontdekkingsverzoek gevolg te geven.
- Statische configuratie: U kunt de opdracht `capwap ap primary-base <wlc-hostname> <wlc-IP-adres>` gebruiken om een statische ingang voor een WLC in het AP te configureren.

- **Mobility Discovery:** Als de AP eerder was aangesloten bij een WLC die deel uitmaakte van een mobiliteitsgroep, slaat de AP ook een registratie op van de WLC's die aanwezig zijn in die mobiliteitsgroep.



Opmerking: de genoemde WLC-detectiemethoden hebben geen prioriteitsvolgorde.

Selectie van draadloze LAN-controllers

Zodra de AP een **Discovery Response** heeft ontvangen van een WLC met behulp van een van de WLC-detectiemethoden, selecteert hij één controller om aan deze criteria te voldoen:

- Primaire controller (geconfigureerd met de opdracht **capwap ap primary-base <wlc-hostname> <wlc-IP-adres>**)
- Secundaire controller (geconfigureerd met de opdracht **capwap ap second-base <wlc-hostname> <wlc-IP-adres>**)

- Tertiaire controller (geconfigureerd met de opdracht **capwap ap tertiair-base <wlc-hostname> <wlc-IP-adres>**)
- Als geen Primaire, Secundaire of Tertiaire WLC eerder werd geconfigureerd, dan probeert de AP zich aan te sluiten bij de eerste WLC die reageerde op de Discovery-aanvraag met zijn eigen **Discovery Response** die de maximale capaciteit van beschikbare **APs** heeft (dat wil zeggen, de **WLC** die op een gegeven moment de meeste **APs** kan ondersteunen).

CAPWAP State Machine

In de AP-console kunt u bijhouden van de CAPWAP State machine, die de stappen beschreven in de sectie CAPWAP Session Establishment.

CAPWAP State: Detectie

Hier kunt u de **detectieaanvragen** en antwoorden zien. Neem waar hoe AP een WLC IP via **DHCP** ontvangt (Optie 43), en verzendt ook een **Ontdekkingsverzoek** naar eerder bekende WLCs:

```
<#root>
```

```
[*09/14/2023 04:12:09.7740]
```

```
CAPWAP State: Init
```

```
[*09/14/2023 04:12:09.7770]
```

```
[*09/14/2023 04:12:09.7770]
```

```
CAPWAP State: Discovery
```

```
[*09/14/2023 04:12:09.7790]
```

```
Discovery Request sent to 172.16.0.20, discovery type STATIC_CONFIG(1)
```

```
[*09/14/2023 04:12:09.7800]
```

```
Discovery Request
```

```
sent to 172.16.5.11, discovery type STATIC_CONFIG(1)
```

```
[*09/14/2023 04:12:09.7800]
```

```
Got WLC address 172.16.5.11 from DHCP.
```

```
[*09/14/2023 04:12:09.7820]
```

```
Discovery Request
```

```
sent to 172.16.0.20, discovery type STATIC_CONFIG(1)
```

```
[*09/14/2023 04:12:09.7830]
```

```
Discovery Request
```

```
sent to 172.16.5.11, discovery type STATIC_CONFIG(1)
```

```
[*09/14/2023 04:12:09.7840]
```

```
Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)
```

```
[*09/14/2023 04:12:09.7850]
```

```
[*09/14/2023 04:12:09.7850]
```

CAPWAP State: Discovery

[*09/14/2023 04:12:09.7850]

Discovery Response

from 172.16.0.20

[*09/14/2023 04:12:09.8030]

Discovery Response

from 172.16.5.11

[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.0.20

[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.11

[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.11

[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.0.20

[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.169

[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.169

Naast het ontvangen van een **Discovery Response** van zowel een statisch geconfigureerde WLC (172.16.0.20) als de WLC aangegeven via DHCP-optie 43 (172.16.5.11), ontving deze AP ook een **Discovery Response** van een andere WLC (172.16.5.169) binnen hetzelfde netwerk omdat het de uitzending Discovery bericht kreeg.

CAPWAP State: DTLS Setup.

Hier wordt de DTLS-sessie tussen de AP en de WLC uitgewisseld.

<#root>

[*09/27/2023 21:50:41.0000]

CAPWAP State: DTLS Setup

[*09/27/2023 21:50:41.7140] sudi99_request_check_and_load: Use HARSa SUDI certificaat

CAPWAP Staat: Join

Na het instellen van de DTLS sessie, wordt nu een **Join Verzoek** naar de WLC verzonden over de beveiligde sessie. Neem waar hoe dit verzoek onmiddellijk wordt beantwoord met een **Join Response** van de WLC

<#root>

[*09/27/2023 21:50:41.9880]

CAPWAP State: Join

[*09/27/2023 21:50:41.9910]

Sending Join request to 172.16.5.11

through port 5270

[*09/27/2023 21:50:41.9950]

Join Response from 172.16.5.11

[*09/27/2023 21:50:41.9950]

AC accepted join request

with result code: 0

[*09/27/2023 21:50:41.9990] Received wlcType 0, timer 30

[*09/27/2023 21:50:41.9990] TLV ID 2216 not found

[*09/27/2023 21:50:41.9990] TLV-DEC-ERR-1: No proc for 2216

CAPWAP-status: beeldgegevens

De AP vergelijkt zijn afbeelding met die van de WLC. In dit geval hebben zowel de actieve partitie van de AP als de back-uppartitie andere afbeeldingen dan de WLC, dus het haalt het **upgrade.sh** script aan, dat de AP instrueert om het juiste beeld aan de WLC te vragen en het naar zijn huidige niet-actieve partitie te downloaden.

<#root>

[*09/27/2023 21:50:42.0430]

CAPWAP State: Image Data

[*09/27/2023 21:50:42.0430]

AP image version 8.10.185.0 backup 8.10.105.0, Controller 17.9.3.50

[*09/27/2023 21:50:42.0430]

Version does not match.

[*09/27/2023 21:50:42.0680]

upgrade.sh

: Script called with args:[PRECHECK]
[*09/27/2023 21:50:42.1060] do PRECHECK,

part2 is active part

[*09/27/2023 21:50:42.1240]

upgrade.sh

: /tmp space: OK available 101476, required 40000

[*09/27/2023 21:50:42.1250] wtpImgFileReadRequest: request ap1g7, local /tmp/part.tar

[*09/27/2023 21:50:42.1310]

Image Data Request sent to 172.16.5.11

, fileName [ap1g7], slaveStatus 0

[*09/27/2023 21:50:42.1340]

Image Data Response from 172.16.5.11

[*09/27/2023 21:50:42.1340] AC accepted join request with result code: 0

[*09/27/2023 21:50:42.1450] <.....

[*09/27/2023 21:50:55.4980]

[*09/27/2023 21:51:11.6290]Discarding msg CAPWAP_WTP_EVENT_REQUEST(type

[*09/27/2023 21:51:19.7220]

[*09/27/2023 21:51:24.6880]

[*09/27/2023 21:51:37.7790]

[*09/27/2023 21:51:50.9440]> 76738560 bytes, 57055 msgs, 930 last

[*09/27/2023 21:51:59.9160] Last block stored, IsPre 0, WriteTaskId 0

[*09/27/2023 21:51:59.9160]

Image transfer completed from WLC

, last 1

Nadat de image-overdracht is voltooid, start het toegangspunt een proces voor de verificatie van de beeldondertekening om dit te valideren. Na dit te doen, installeert het script **upgrade.sh** de afbeelding in de huidige niet-actieve partitie, en ruilt de partitie die het opstart van. Tot slot herlaadt de AP zichzelf en herhaalt het proces vanaf het begin (**CAPWAP State: Discover**).

<#root>

[*09/27/2023 21:52:01.1280]

Image signing verify success.

[*09/27/2023 21:52:01.1440]

[*09/27/2023 21:52:01.1440] [9/27/2023 21:53:2] : Shadow is now in-synced with master

[*09/27/2023 21:52:01.1440]

[*09/27/2023 21:52:01.1440] [9/27/2023 21:53:2] : Verifying against bundle image btldr.img...

[*09/27/2023 21:52:01.1570]

upgrade.sh

:

part to upgrade is part1

[*09/27/2023 21:52:01.1780]

upgrade.sh

: AP version1: part1 8.10.105.0, img 17.9.3.50
[*09/27/2023 21:52:01.1960]

upgrade.sh

: Extracting and verifying image in part1...
[*09/27/2023 21:52:01.2080]

upgrade.sh

: BOARD generic case execute
[*09/27/2023 21:52:01.5280]

upgrade.sh

: Untar /tmp/part.tar to /bootpart/part1...
[*09/27/2023 21:52:01.7890]

upgrade.sh

: Sync image to disk...
[*09/27/2023 21:52:31.4970]

upgrade.sh

: status '

Successfully verified image in part1.

'
[*09/27/2023 21:52:32.5270]

upgrade.sh

: AP version2: part1 17.9.3.50, img 17.9.3.50
[*09/27/2023 21:52:32.5540]

upgrade.sh

: AP backup version: 17.9.3.50
[*09/27/2023 21:52:32.5700]

upgrade.sh

:
Finished upgrade task.

[*09/27/2023 21:52:32.5840]

upgrade.sh

: Cleanup for do_upgrade...
[*09/27/2023 21:52:32.5970]

upgrade.sh

: /tmp/upgrade_in_progress cleaned
[*09/27/2023 21:52:32.6090]

upgrade.sh

: Cleanup tmp files ...
[*09/27/2023 21:52:32.6720]

upgrade.sh

: Script called with args:[ACTIVATE]
[*09/27/2023 21:52:32.7100] do ACTIVATE, part2 is active part
[*09/27/2023 21:52:32.7640]

upgrade.sh

: Verifying image signature in part1
[*09/27/2023 21:52:33.7730]

upgrade.sh

: status 'Successfully verified image in part1.'
[*09/27/2023 21:52:33.7850]

upgrade.sh

:
activate part1, set BOOT to part1

[*09/27/2023 21:52:34.2940]

upgrade.sh

:
AP primary version after reload: 17.9.3.50

[*09/27/2023 21:52:34.3070]

upgrade.sh

: AP backup version after reload: 8.10.185.0
[*09/27/2023 21:52:34.3190]

upgrade.sh

: Create after-upgrade.log
[*09/27/2023 21:52:37.3520]

AP Rebooting: Reset Reason - Image Upgrade



Waarschuwing: Wave 1 access points kunnen mogelijk geen nieuwe afbeelding downloaden vanwege een verlopen certificaat. Raadpleeg [melding uit het veld 72524](#) voor meer informatie en lees de [IOS AP Image Download Fails Due to Expired Image Signing Certificate Afgelopen op 4 december 2022 \(CSCwd80290\) Support Document](#) om de impact en oplossing ervan te begrijpen.

Zodra het toegangspunt opnieuw wordt geladen en weer door de **CAPWAP Discover**-en **Join**-toestanden gaat, detecteert het tijdens de **Image Data**-status dat het nu de juiste afbeelding heeft.

<#root>

[*09/27/2023 21:56:13.7640]

CAPWAP State: Image Data

[*09/27/2023 21:56:13.7650]

AP image version 17.9.3.50 backup 8.10.185.0, Controller 17.9.3.50

[*09/27/2023 21:56:13.7650]

Version is the same, do not need update.

[*09/27/2023 21:56:13.7650] status '

upgrade.sh: Script called with args:[NO_UPGRADE]

,

[*09/27/2023 21:56:13.7850] do NO_UPGRADE, part1 is active part

CAPWAP-status: configureren

Nadat de AP bevestigt dat het dezelfde versie heeft als de WLC, brengt het zijn huidige configuraties aan de WLC op de hoogte. In het algemeen betekent dit dat de AP vraagt om zijn configuraties te behouden (als ze beschikbaar zijn in de WLC).

<#root>

[*09/27/2023 21:56:14.8680]

CAPWAP State: Configure

[*09/27/2023 21:56:15.8890] Telnet is not supported by AP, should not encode this payload

[*09/27/2023 21:56:15.8890] Radio [1] Administrative state DISABLED change to ENABLED

[*09/27/2023 21:56:16.0650] Radio [0] Administrative state DISABLED change to ENABLED

[*09/27/2023 21:56:16.0750] DOT11_CFG[1]: Starting radio 1

[*09/27/2023 21:56:16.1150] DOT11_DRV[1]: Start Radio1

[*09/27/2023 21:56:16.1160] DOT11_DRV[1]: set_channel Channel set to 36/20

[*09/27/2023 21:56:16.4380] Started Radio 1

[*09/27/2023 21:56:16.4880] DOT11_CFG[0]: Starting radio 0

[*09/27/2023 21:56:17.5220] DOT11_DRV[0]: Start Radio0

[*09/27/2023 21:56:16.5650] DOT11_DRV[0]: set_channel Channel set to 1/20

[*09/27/2023 21:56:16.5650] Started Radio 0

[*09/27/2023 21:56:16.5890] sensord psage_base init: RHB Sage base ptr a1030000

CAPWAP State: Uitvoeren

Op dit punt is de AP succesvol toegetreten tot de controller. Tijdens deze staat, activeert WLC een mechanisme om de configuratie met voeten te treden die door AP wordt gevraagd. Je kunt zien dat de AP **Radio en Credentials configuraties** geduwd krijgt, en het wordt ook toegewezen aan de **standaard beleidstag** aangezien de WLC geen eerdere kennis van deze AP had.

<#root>

[*09/27/2023 21:56:17.4870]

CAPWAP State: Run

[*09/27/2023 21:56:17.4870]

AP has joined controller

uwu-9800

[*09/27/2023 21:56:17.4940] DOT11_DRV[0]: set_channel Channel set to 1/20
[*09/27/2023 21:56:17.5440] sensord split_glue psage_base: RHB Sage base ptr a1030000
[*09/27/2023 21:56:17.6010] sensord split_glue sage_addr: RHB Sage base ptr a1030000
[*09/27/2023 21:56:17.6230] ptr a1030000
[*09/27/2023 21:56:17.6420]

DOT11_DRV[0]: set_channel Channel set to 1/20

[*09/27/2023 21:56:17.8120]

DOT11_DRV[1]: set_channel Channel set to 36/20

[*09/27/2023 21:56:17.9350] Previous AP mode is 0, change to 0
[*09/27/2023 21:56:18.0160] Current session mode: ssh, Configured: Telnet-No, SSH-Yes, Console-Yes
[*09/27/2023 21:56:18.1220] Current session mode: telnet, Configured: Telnet-No, SSH-Yes, Console-Yes
[*09/27/2023 21:56:18.1310] Current session mode: console, Configured: Telnet-No, SSH-Yes, Console-Yes
[*09/27/2023 21:56:18.1340]

chpasswd: password for user changed

[*09/27/2023 21:56:18.1350]

chpasswd: password for user changed

[*09/27/2023 21:56:18.1520] systemd[1]: Starting Cisco rsyslog client watcher...
[*09/27/2023 21:56:18.1610] Same LSC mode, no action needed
[*09/27/2023 21:56:18.1640] CLSM[00:00:00:00:00:00]: U3 Client RSSI Stats feature is deprecated; can no
[*09/27/2023 21:56:18.1720] systemd[1]: Stopping rsyslog client...
[*09/27/2023 21:56:18.2120] systemd[1]: Starting Cisco syslog service...
[*09/27/2023 21:56:18.2230] systemd[1]: Started Cisco syslog service.
[*09/27/2023 21:56:18.2410] systemd[1]: Started rsyslog client.
[*09/27/2023 21:56:18.2440] AP is in good condition, BLE is off
[*09/27/2023 21:56:18.2510] SET_SYS_COND_INTF: allow_usb state: 1 (up) condition
[*09/27/2023 21:56:18.2530] systemd[1]: Starting dhcpv6 client watcher...
[*09/27/2023 21:56:18.2530] systemd[1]: Stopping DHCPv6 client...
[*09/27/2023 21:56:18.2530] systemd[1]: Starting DHCPv6 client...
[*09/27/2023 21:56:18.2530] systemd[1]: Started DHCPv6 client.
[*09/27/2023 21:56:18.2530] systemd[1]: Started dhcpv6 client watcher.
[*09/27/2023 21:56:18.2560]

Set radio 0 power 4 antenna mask 15

[*09/27/2023 21:56:18.2530]

Set radio 1 power 4 antenna mask 15

[*09/27/2023 21:56:18.2530] Got WSA Server config TLVs
[*09/27/2023 21:56:18.2720]

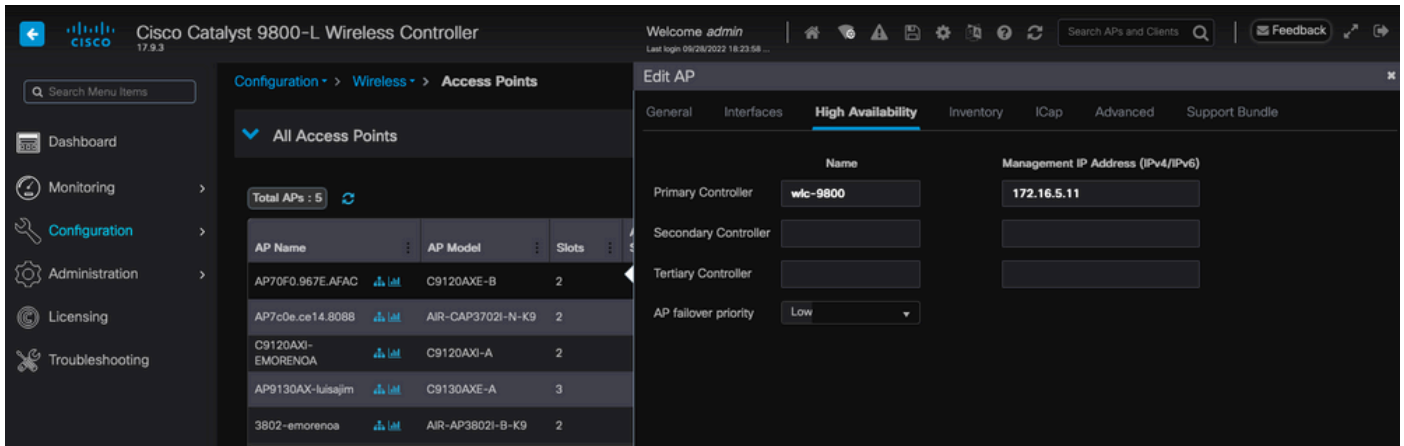
AP tag change to default-policy-tag

[*09/27/2023 21:56:18.2780] Chip flash OK

Configureren

Statische WLC-verkiezingen

In de GUI, kunt u naar **Configuration > Wireless > Access points** gaan, een AP selecteren en naar het tabblad **Hoge beschikbaarheid** navigeren. Hier kunt u de **primaire, secundaire en tertiaire** WLC's configureren zoals beschreven in het gedeelte Draadloze LAN-controllerselectie van dit document. Deze configuratie wordt uitgevoerd per access point.



The screenshot displays the Cisco Catalyst 9800-L Wireless Controller GUI. The left sidebar shows navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Wireless > Access Points' and shows a table of 'All Access Points'. The table has columns for AP Name, AP Model, and Slots. The right pane is titled 'Edit AP' and shows the 'High Availability' tab. The configuration fields are as follows:

	Name	Management IP Address (IPv4/IPv6)
Primary Controller	wlc-9800	172.16.5.11
Secondary Controller		
Tertiary Controller		
AP failover priority	Low	

Primaire, secundaire en tertiaire WLC's voor een AP.



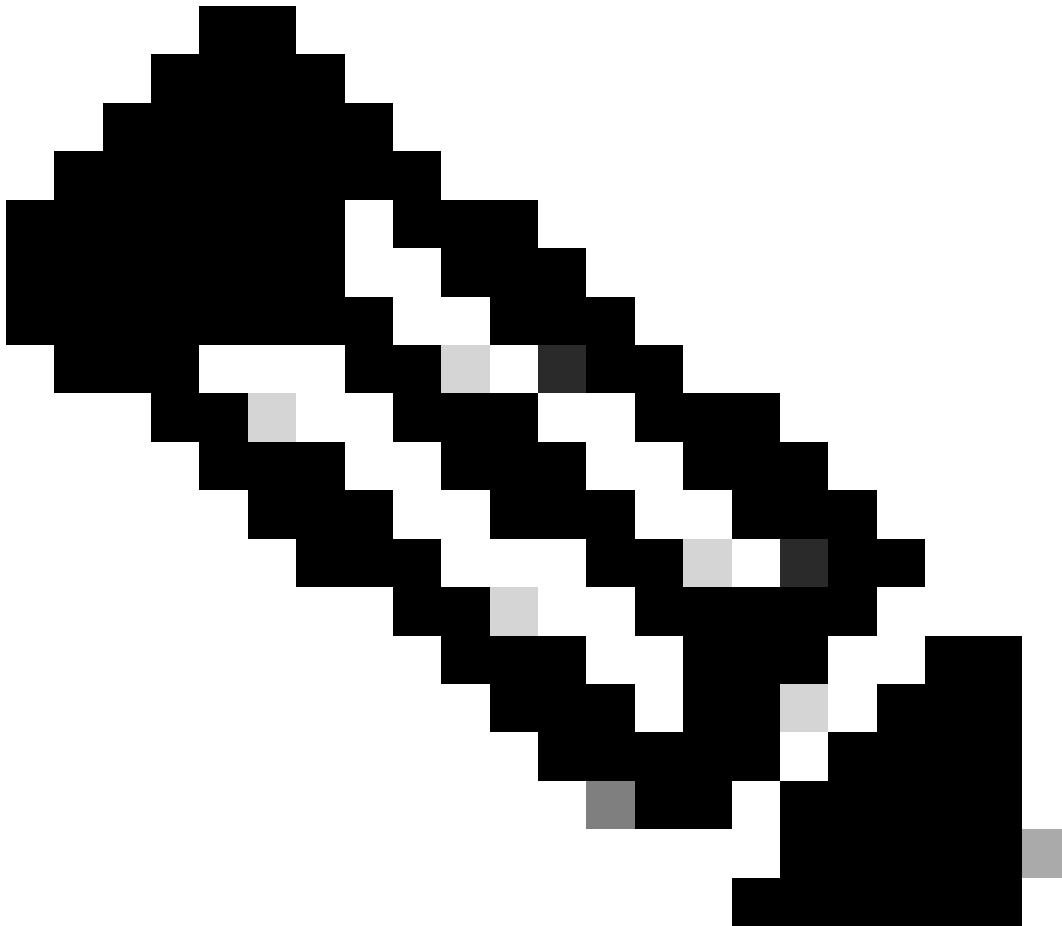
Opmerking: met Cisco IOS XE 17.9.2 kunt u Priming Profiles gebruiken om primaire, secundaire en tertiaire controllers te configureren voor een groep AP's die overeenkomen met reguliere expressie (regex) of voor een individuele AP. Raadpleeg de [Fallback](#) van het [toegangspunt naar controllers die zijn geconfigureerd onder het](#) gedeelte [Priming Profile](#) van de [Configuratiegids](#) voor meer informatie.

Houd er rekening mee dat de primaire, secundaire en tertiaire controllers die zijn geconfigureerd op het tabblad Hoge beschikbaarheid van het toegangspunt verschillen van de **back-up van primaire en secundaire** WLC's die kunnen worden geconfigureerd per **toegangspunt toetreden** onder het tabblad **CAPWAP > Hoge beschikbaarheid**. De **primaire, secundaire en tertiaire controllers** worden beschouwd als WLC's met prioriteit 1, 2 en 3, terwijl de **back-up primaire en secundaire controllers** worden beschouwd als WLC's met prioriteit 4 en 5.

Als **AP Fallback** is ingeschakeld, zoekt de AP actief naar de **Primaire controller** wanneer hij zich aansluit bij een andere **WLC**. De **AP** zoekt alleen naar **WLC's** met prioriteiten 4 en 5 als er een **CAPWAP Down**-gebeurtenis is en geen van de **back-up primaire en secundaire controllers** beschikbaar is.

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main window is titled "Edit AP Join Profile" and is divided into several tabs: General, Client, CAPWAP (selected), AP, Management, Security, ICap, and QoS. The "High Availability" section is expanded, showing "CAPWAP Timers" and "Retransmit Timers" with various time values. A red box highlights the "AP Fallback to Primary" section, which includes an "Enable" checkbox (checked), a "Backup Primary Controller" section with a name of "backup-9800" and an IPv4/IPv6 address of "172.16.28.50", and a "Backup Secondary Controller" section with a name field set to "Enter Name" and an empty IPv4/IPv6 address field.

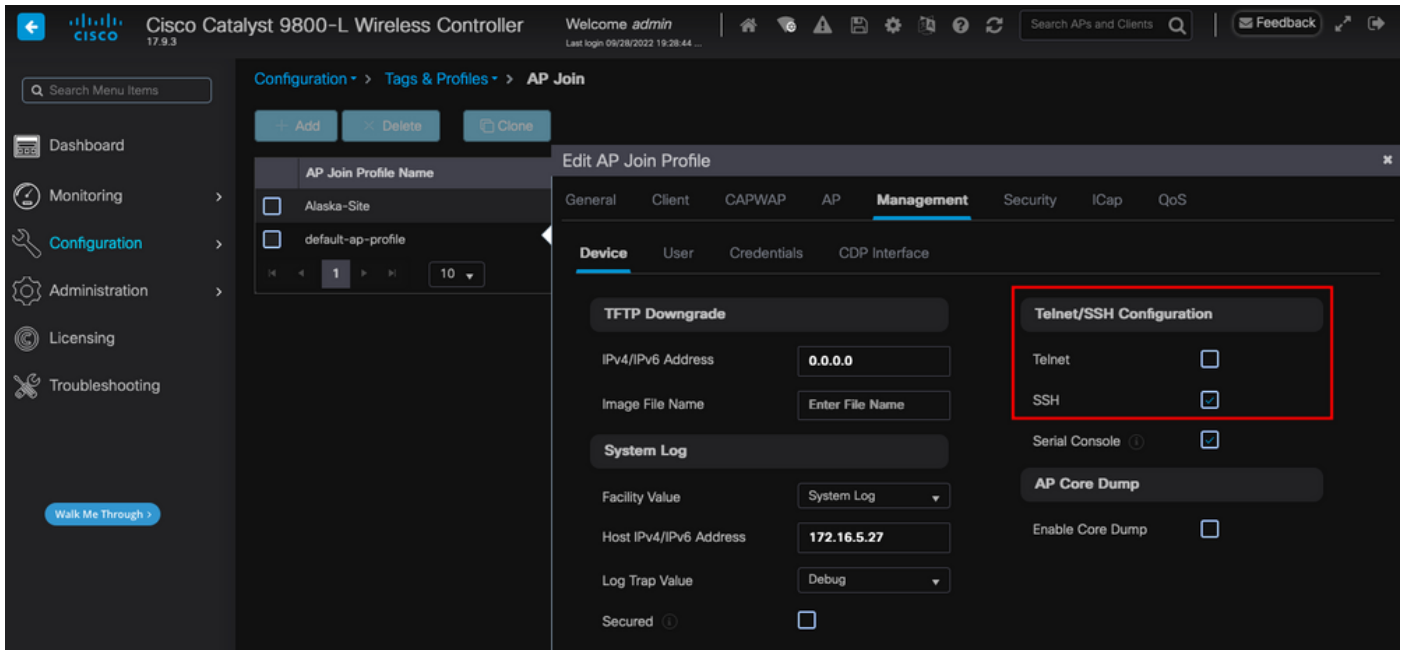
Hoge beschikbaarheid Opties in het profiel van de AP Join



Opmerking: de configuratie van back-up primaire en back-up secundaire WLC's in het AP Join Profile vult de statische primaire en secundaire vermeldingen niet in het tabblad Hoge beschikbaarheid van het access point.

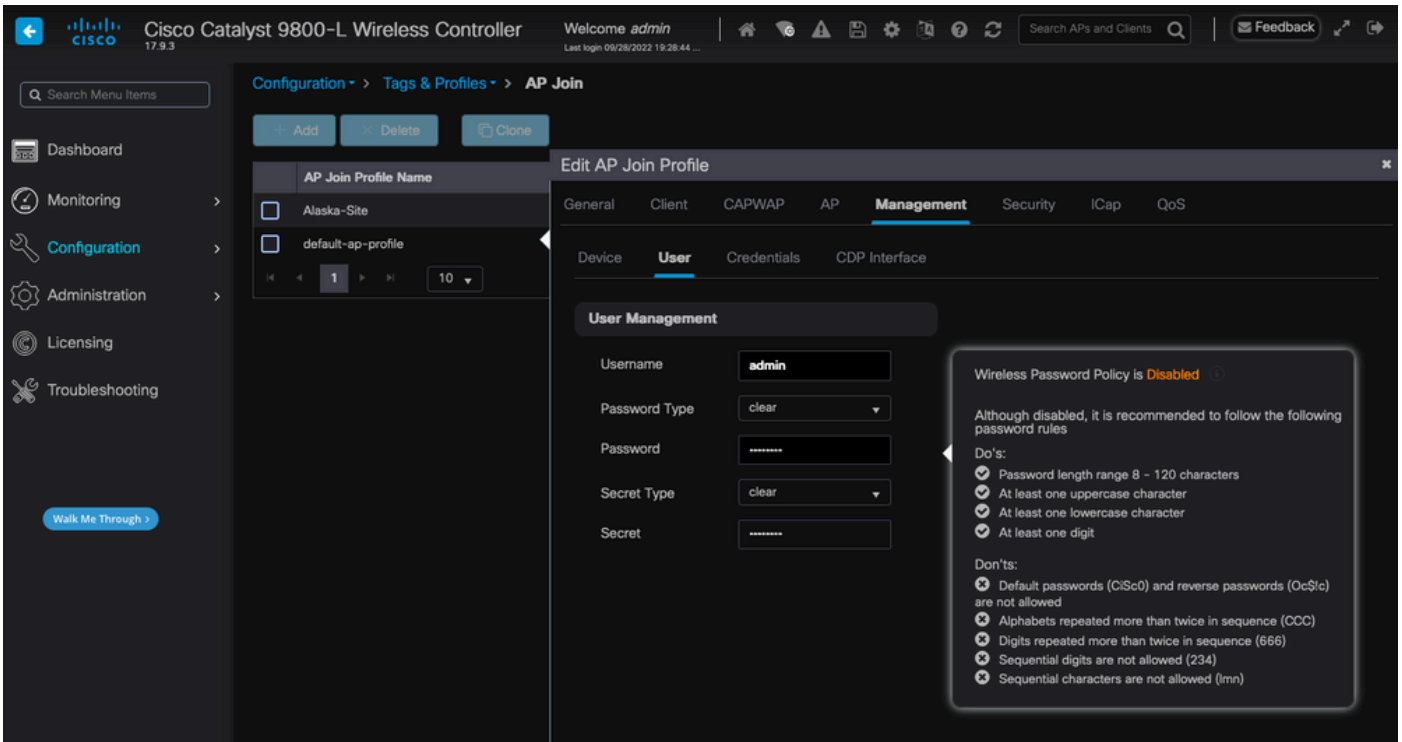
Telnet/SSH-toegang tot het toegangspunt inschakelen

Ga naar **Configuratie > Tags & profielen > AP Join > Management > Apparaat** en selecteer **SSH** en/of **Telnet**.



Telnet/SSH-toegang op het toegangspunt inschakelen voor het profiel

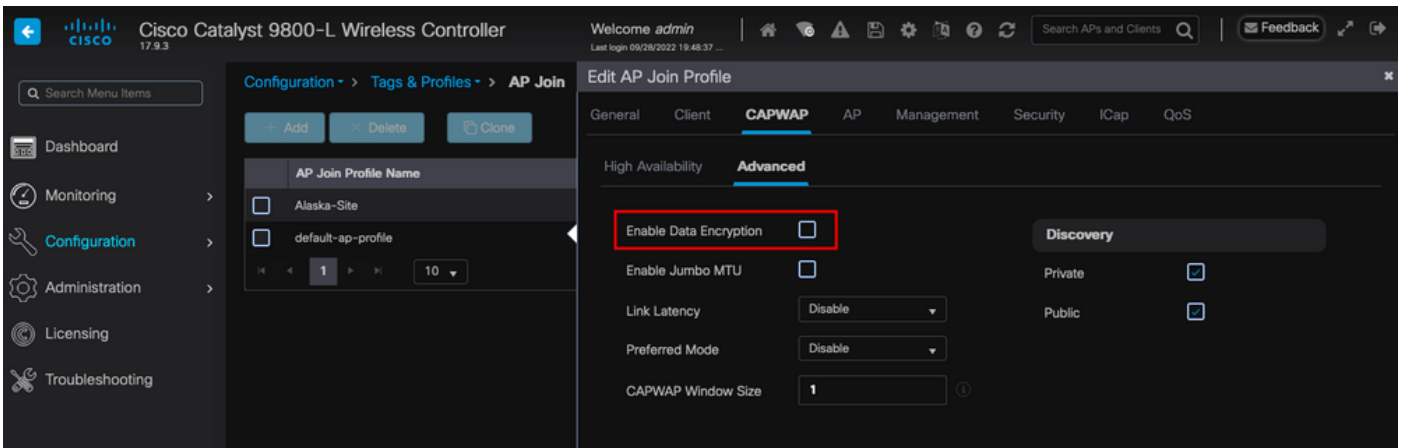
Om de SSH/Telnet Credentials te configureren navigeert u naar het tabblad **Gebruiker** in hetzelfde venster en stelt u de **gebruikersnaam**, het **wachtwoord** en het **geheim in** om toegang te krijgen tot het toegangspunt.



SSH- en Telnet-referenties voor het AP

Data Link-encryptie

Als u problemen met clients moet oplossen waarvoor u een pakketopname van het verkeer van het toegangspunt moet maken, zorg er dan voor dat **datalink-encryptie** niet is ingeschakeld onder **Configuration > Tags & profielen > AP Join > CAPWAP > Advanced**. Anders wordt uw verkeer versleuteld.



Data Link-encryptie



Opmerking: met gegevensversleuteling wordt alleen CAPWAP-gegevensverkeer versleuteld. CAPWAP Control-verkeer is al versleuteld via DTLS.

Verifiëren

Naast het bijhouden van de CAPWAP state machine in de console van de AP, kunt u ook een [ingesloten Packet Capture](#) nemen in de WLC om het AP Join proces te analyseren:

No.	Time	Time delta from Source	Destination	Protocol	Length	Destination Port	Info
886	12:58:41.288976	0.022802000	172.16.5.65	CAPWAP-Control	294	5246	CAPWAP-Control - Discovery Request
887	12:58:41.288976	0.000000000	172.16.5.11	CAPWAP-Control	147	5267	CAPWAP-Control - Discovery Response
888	12:58:41.388974	0.027998000	172.16.5.65	255.255.255.255	294	5246	CAPWAP-Control - Discovery Request
889	12:58:41.388974	0.000000000	172.16.5.11	CAPWAP-Control	147	5267	CAPWAP-Control - Discovery Response
1156	12:58:50.794957	0.195980000	172.16.5.65	DTLSv1.2	276	5246	Client Hello
1157	12:58:50.795948	0.000991000	172.16.5.11	DTLSv1.2	98	5267	Hello Verify Request
1158	12:58:50.796955	0.001007000	172.16.5.65	DTLSv1.2	296	5246	Client Hello
1159	12:58:50.798954	0.001999000	172.16.5.11	DTLSv1.2	562	5267	Server Hello, Certificate (Fragment)
1160	12:58:50.798954	0.000000000	172.16.5.65	DTLSv1.2	562	5267	Certificate (Fragment)
1161	12:58:50.798954	0.000000000	172.16.5.11	DTLSv1.2	562	5267	Certificate (Reassembled), Server Key Exchange (Fragment)
1162	12:58:50.798954	0.000000000	172.16.5.11	DTLSv1.2	349	5267	Server Key Exchange (Reassembled), Certificate Request, Server Hello Done
1163	12:58:50.859948	0.060980000	172.16.5.65	DTLSv1.2	594	5246	Certificate (Fragment)
1164	12:58:50.859948	0.000000000	172.16.5.11	DTLSv1.2	594	5246	Certificate (Reassembled), Client Key Exchange (Fragment)
1181	12:58:51.204975	0.066997000	172.16.5.65	DTLSv1.2	463	5246	Client Key Exchange (Reassembled), Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
1182	12:58:51.204975	0.000000000	172.16.5.11	DTLSv1.2	125	5267	Change Cipher Spec, Encrypted Handshake Message
1320	12:58:55.914945	0.016997000	172.16.5.11	DTLSv1.2	1487	5246	Application Data
1321	12:58:55.916944	0.001999000	172.16.5.11	DTLSv1.2	1484	5267	Application Data
1330	12:58:56.246981	0.109003000	172.16.5.65	DTLSv1.2	1439	5246	Application Data
1331	12:58:56.246981	0.000000000	172.16.5.11	DTLSv1.2	1439	5246	Application Data
1332	12:58:56.246981	0.000000000	172.16.5.65	DTLSv1.2	379	5246	Application Data
1333	12:58:56.247973	0.000992000	172.16.5.11	DTLSv1.2	354	5267	Application Data
1364	12:58:57.292984	0.040999000	172.16.5.65	DTLSv1.2	1439	5246	Application Data
1365	12:58:57.292984	0.000000000	172.16.5.11	DTLSv1.2	690	5246	Application Data
1366	12:58:57.293975	0.000991000	172.16.5.11	DTLSv1.2	354	5267	Application Data
1368	12:58:57.387965	0.069980000	172.16.5.65	DTLSv1.2	902	5246	Application Data
1369	12:58:57.388972	0.001007000	172.16.5.11	DTLSv1.2	402	5267	Application Data
1376	12:58:57.466961	0.001999000	172.16.5.65	DTLSv1.2	140	5246	Application Data
1377	12:58:57.466961	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1378	12:58:57.470968	0.001007000	172.16.5.65	CAPWAP-Data	104	5247	CAPWAP-Data Keep-Alive(Malformed Packet)
1379	12:58:57.474966	0.003998000	172.16.5.11	DTLSv1.2	133	5267	Application Data
1380	12:58:57.477972	0.003006000	172.16.5.11	CAPWAP-Data	104	5267	CAPWAP-Data Keep-Alive(Malformed Packet)
1400	12:58:57.546968	0.003997000	172.16.5.65	DTLSv1.2	140	5246	Application Data
1401	12:58:57.546968	0.000000000	172.16.5.11	DTLSv1.2	119	5246	Application Data
1402	12:58:57.547968	0.000992000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1403	12:58:57.547968	0.000000000	172.16.5.65	DTLSv1.2	121	5267	Application Data
1411	12:58:57.575958	0.002998000	172.16.5.11	DTLSv1.2	140	5246	Application Data
1412	12:58:57.575958	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1413	12:58:57.577957	0.001999000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1414	12:58:57.577957	0.000000000	172.16.5.65	DTLSv1.2	143	5246	Application Data
1415	12:58:57.577957	0.000000000	172.16.5.11	DTLSv1.2	1190	5267	Application Data
1416	12:58:57.577957	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1425	12:58:57.688959	0.078995000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1426	12:58:57.688959	0.000000000	172.16.5.11	DTLSv1.2	140	5246	Application Data
1427	12:58:57.688959	0.000000000	172.16.5.11	DTLSv1.2	119	5267	Application Data
1428	12:58:57.688959	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1429	12:58:57.688951	0.000992000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1430	12:58:57.688951	0.000000000	172.16.5.11	DTLSv1.2	222	5246	Application Data
1431	12:58:57.690958	0.001007000	172.16.5.11	DTLSv1.2	175	5267	Application Data
1432	12:58:57.690958	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1433	12:58:57.692957	0.001999000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1434	12:58:57.692957	0.000000000	172.16.5.65	DTLSv1.2	111	5246	Application Data

AP Join proces dat in een ingesloten pakketvastlegging in WLC wordt gezien

Let op hoe al het verkeer na het pakket **Change Cipher Spec** (Packet No. 1182) alleen wordt weergegeven als **Application Data** via **DTLSv1.2**. Dit zijn alle versleutelde gegevens na de **DTLS-sessie**.

Problemen oplossen

Bekende problemen

Gelieve te verwijzen naar de bekende kwesties die uw AP's zouden kunnen verhinderen om zich bij WLC aan te sluiten.

- [AP's op bootlus vanwege beschadigd beeld in Wave 2 en Catalyst 11ax access points \(CSCvx32806\)](#)
- [Meldingen uit het veld 72424: voor de met ingang van september 2022 gefabriceerde C9105/C9120/C9130 access points kunnen software-upgrades nodig zijn om zich aan te sluiten bij draadloze LAN-controllers.](#)
- [Melding uit het veld 72524: tijdens software-upgrade/downgrade blijven Cisco IOS-AP's mogelijk na 4 december 2022 in de downloadstaat vanwege het verlopen van het certificaat - Aanbevolen software-upgrade](#)
- [Cisco bug-id CSCwb13784: AP's kunnen zich niet bij 9800 aansluiten vanwege ongeldig pad MTU in AP Join request](#)
- [Cisco bug-id CSCvu22886: C9130: bericht "unlzma: write: No space left on device" bij upgrade naar 17.7 Maximale grootte vergroten van /tmp](#)

Raadpleeg altijd het gedeelte **Upgradepad** van de [Releaseopmerkingen](#) van elke versie voordat u een upgrade uitvoert.



Opmerking: vanaf Cisco IOS XE koppeling 17.7.1 accepteert de Cisco Catalyst 9800-CL draadloze controller niet meer dan 50 AP's als de slimme licentie niet is verbonden en niet is geactiveerd.

WLC GUI-controles

In uw WLC, ga naar **Monitoring > Wireless > AP Statistics > Join Statistics** kunt u de **laatste Reboot Reason** gemeld door een AP en de **laatste Disconnect Reason** geregistreerd door de WLC zien.

AP Name	AP Model	Status	IP Address	Base Radio MAC	Ethernet MAC	Last Reboot Reason (Reported by AP)	Last Disconnect Reason
9120AP	C9120AXI-A	Red	172.16.5.23	3c41.0a31.7700	6c41.0e16.e79c	No reboot reason	DTLS close alert from peer
pschell9120	C9120AXI-B	Red	172.16.5.61	3c41.0a31.7700	6c41.0e16.e79c	No reboot reason	DTLS close alert from peer
AP19F9.2096.54F0	C9106AXI-A	Red	172.16.5.32	489b.0aa7.7940	1099.2096.54f0	No reboot reason	DTLS close alert from peer
AP72F9.9676.AFAC	C9120AXI-B	Green	172.16.5.79	709D.9685.7980	709D.9676.afac	Controller reload command	Mesh AP role change
AP710e.ce14.8088	AR-CAP3702I-N-K9	Green	172.16.5.31	710e.ce14.8080	710e.ce14.8088	Image upgrade successfully	NA
C9120AXI-EMORENDA	C9120AXI-A	Green	172.16.5.65	a49b.cdaa.1980	a49b.c05a.1f58	Image upgrade successfully	DTLS close alert from peer
BRCTAC0428	C9120AXI-B	Red	172.16.46.35	c884.a172.2600	c884.a165.8530	No reboot reason	DTLS close alert from peer
AP9130AXI-tulajim	C9130AXI-A	Green	172.16.5.67	011d.2d49.d840	709D.9606.4a44	Controller reload command	Mode change to sniffer
3802-emorenda	AR-AP9802I-B-K9	Green	172.16.5.25	802b.cba7.a5c0	286f.7d1f.530e	Controller reload command	Mode change to sniffer

AP Join Statistics pagina op de WLC

U kunt op elk toegangspunt klikken en controleren of het toegangspunt deelneemt aan de statistische gegevens. Hier kunt u meer gedetailleerde informatie zien, zoals de tijd en datum waarop de AP zich voor het laatst heeft aangesloten bij de WLC.

Access Point Statistics Summary

Is the AP currently connected to controller	NOT JOINED
Time at which the AP joined this controller last time	09/27/2022 09:45:49
Type of error that occurred last	Join
Time at which the last join error occurred	09/27/2022 09:46:01

Last AP Disconnect Details

Reason for last AP connection failure	DTLS close alert from peer
Last Reboot Reason (Reported by AP)	No reboot reason

Last AP message decryption failure details

Reason for last message decryption failure	NA
--	----

Discovery Phase Statistics

Discovery requests received	106
Successful discovery responses sent	106
Unsuccessful discovery request processing	NA
Reason for last unsuccessful discovery attempt	None
Time at last successful discovery attempt	09/27/2022 09:52:27
Time at last unsuccessful discovery attempt	NA

Algemene AP Join Statistics

Ga voor meer informatie naar het tabblad Statistieken van hetzelfde venster. Hier kunt u de hoeveelheid **verzonden Join Responses** vergelijken met het aantal **ontvangen Join Requirements**, evenals de **verzonden Configuration Responses** versus de **ontvangen Configuration Requirements**.

Join Statistics

General

Statistics

Control DTLS Statistics

DTLS Session request received	8
Established DTLS session	8
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	09/27/2022 09:45:44
Time at last unsuccessful DTLS session	NA

Join phase statistics

Join requests received	8
Successful join responses sent	8
Unsuccessful join request processing	0
Reason for last unsuccessful join attempt	DTLS close alert from peer
Time at last successful join attempt	09/27/2022 09:45:49
Time at last unsuccessful join attempt	NA

Configuration phase statistics

Configuration requests received	15
Successful configuration responses sent	15
Unsuccessful configuration request processing	0
Reason for last unsuccessful configuration attempt	NA
Time at last successful configuration attempt	09/21/2022 01:39:07
Time at last unsuccessful configuration attempt	NA

Data DTLS Statistics

DTLS Session request received	0
Established DTLS session	0
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	NA
Time at last unsuccessful DTLS session	NA

Gedetailleerde AP Join Statistieken

Opdrachten

Deze opdrachten zijn handig om problemen op te lossen met AP Join problemen:

Van de WLC

- samenvatting van map weergeven
- debug capwap fout
- debug capwap-pakket

Van Wave 2 en Catalyst 11ax AP's

- debug capwap client events
- debug capwap client fout
- debug dtls-clientfout
- debug dtls-clientgebeurtenis
- debug capwap client keepalive
- herstart van testcapwap
- kapsel tap alles wissen

Vanaf Wave 1 access points

- debug capwap console client
- debug capwap client zonder opnieuw laden
- DTLS-stats tonen
- duidelijk cawap ap all-config



Opmerking: wanneer u via Telnet/SSH verbinding maakt met de AP's om problemen op te lossen, geef dan altijd de opdrachtterminalmonitor uit terwijl u het probleem reproduceert nadat u debugs op de AP's hebt ingeschakeld. Anders, kunt u geen output van de debugs zien.

Radioactieve sporen

Een goed startpunt bij problemen met AP Join is om Radioactive Traces van zowel de Radio- als Ethernet MAC-adressen te nemen van een AP die problemen heeft bij het aansluiten. Raadpleeg de [Debug & Log-verzameling op Catalyst 9800 WLC-document](#) voor meer informatie over het genereren van deze logs.

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.