

# Le contrôleur convergé NGWC AP d'Access joignent la question dépannent avec des suivis

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Produits connexes](#)

[AP joignent l'ordre](#)

[Dépannez](#)

[Étapes de base](#)

[Suivis de contrôleur](#)

[Les raisons communes pour AP joignent la panne](#)

[Problème 1 : AP sur le commutateur de gamme Catalyst 3850 n'est pas dans le VLAN de gestion Sans fil.](#)

[Problème 2 : Le modèle AP est sans support.](#)

[Problème 3 : Le permis de compte AP n'est pas activé sur le contrôleur.](#)

[Problème 4 : Le domaine réglementaire est mal adapté.](#)

[Problème 5 : Le contrôleur de mobilité sans fil n'est pas défini.](#)

[Problème 6 : AP a le code de maille là-dessus.](#)

[Problème 7 : L'AP3700 est connecté à une gamme Catalyst 3850 commute que les passages 3.3.0SE.](#)

[Problème 8 : Le temps de contrôleur est en dehors de l'intervalle de validité de certificat AP.](#)

[Problème 9 : La liste d'autorisation AP est activée sur le WLC ; AP n'est pas dans la liste d'autorisation.](#)

[Problème 10 : La stratégie MIC AP est désactivée.](#)

[Conseils généraux de tech](#)

## Introduction

Ce document décrit les commandes trace qui sont utilisées afin de dépanner le Point d'accès (AP) joignent des questions sur les contrôleurs convergés d'accès et décrit certaines des raisons communes pour AP joignent la panne.

## Conditions préalables

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Point d'accès léger Protocol (LWAPP) /Control et ravitaillement des points d'accès sans fil (CAPWAP)
- Point d'accès léger (LAP) et configurations Sans fil du contrôleur LAN (WLC) pour le fonctionnement de base

## Composants utilisés

Les informations dans ce document sont basées sur une gamme Cisco Catalyst 3850 commutent qu'expert en logiciel de la version de logiciel 3.3.0 de passages.

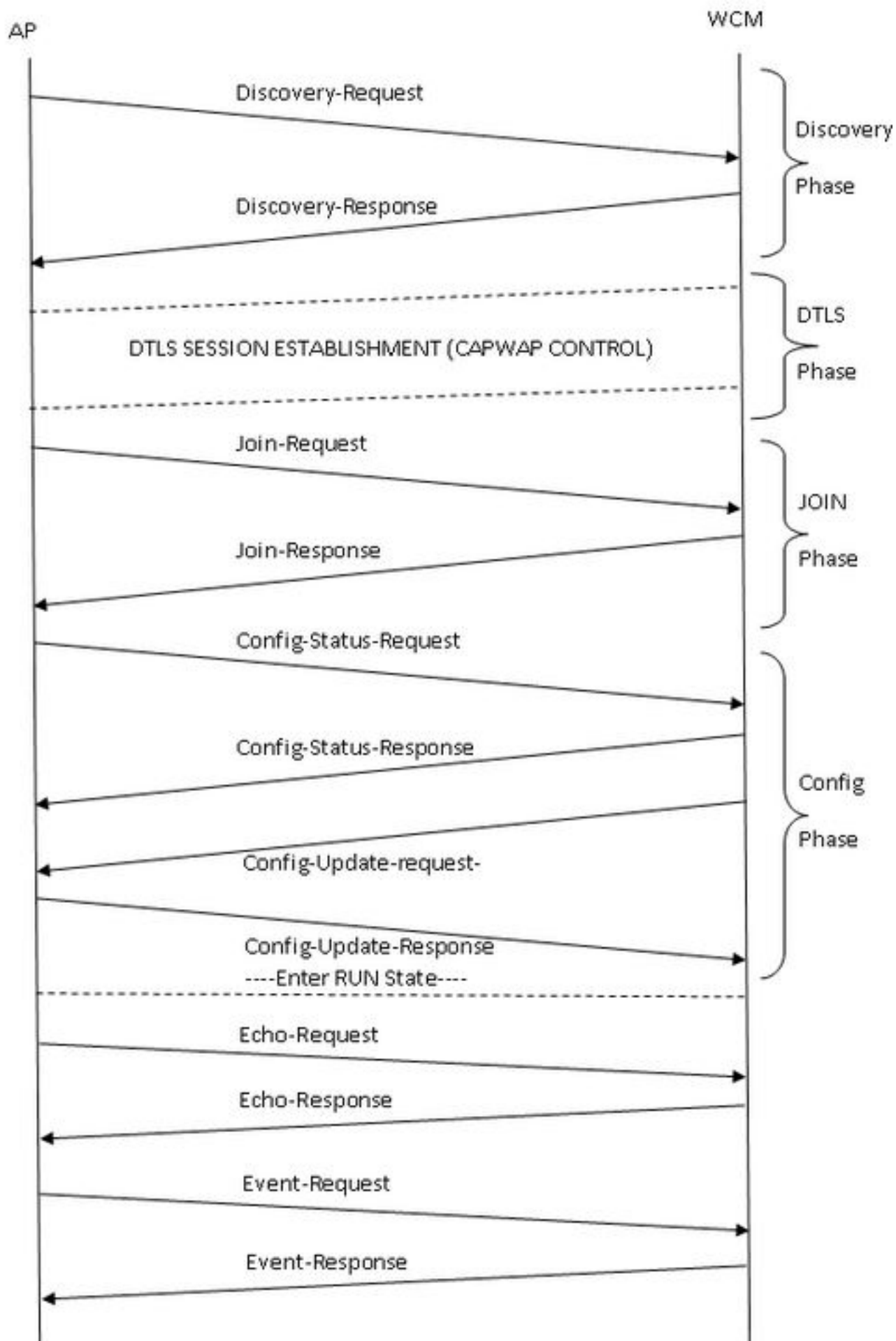
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Produits connexes

Ce document s'applique à tous les contrôleurs convergés d'accès.

- Contrôleurs de radio de gamme Cisco 5760
- Commutateurs de la gamme Cisco Catalyst 3560
- Commutateurs de gamme Cisco Catalyst 3850

## **AP joignent l'ordre**



# Dépannez

## Étapes de base

Afin de dépanner AP joignez la question sur les contrôleurs convergés d'accès, se terminent ces étapes :

1. Confirmez qu'AP peut tirer une adresse IP. Du commutateur où AP est branché, entrez :  
`#show cdp neighbor <port_id> detail`  
Remarque: Pour la gamme Catalyst 3850 commutez, AP doit être directement connecté à la gamme Catalyst 3850 commutent et la configuration switchport devrait être :

<>de yole d'interface

Switchport mode access

Le switchport access vlan X >> où x est le VLAN Sans fil X d'interface de gestion configuré sur la gamme Catalyst 3850 commutent.

2. Assurez-vous que le WLC peut cingler l'adresse IP et vice versa.
3. Vérifiez qu'un contrôleur de mobilité sans fil (MC) est configuré sur le réseau. Si vous êtes enregistré dans un agent de mobilité, assurez-vous que le contrôleur de mobilité de tunnel est en activité.  
`#show wireless mobility summary`

4. Assurez-vous que le permis AP est activé sur MC :  
`#show license right-to-use summary`

5. Confirmez que code de pays approprié est activé :  
`#show wireless country configured`

## Suivis de contrôleur

Une fois que la configuration correcte est en place, si AP échoue, des commandes trace peuvent être accrues pour davantage de diagnostic. Ces commandes trace sont disponibles sur le contrôleur afin de dépanner CAPWAP et AP se joignent :

- **capwap de suivi de #Set**
- **capwap AP de suivi de #Set**
- **suivi groupe-AP de #Set**

Basé sur l'examen des informations de suivi, les suivis groupe-AP la sortie que plus appropriée fournie pour AP se joignent dépannent. Par conséquent, ce suivi (non filtré) est discuté en détail dans ce document. Référez-vous à la section générale de conseils de tech de ce document pour plus d'informations sur des options et des limites de filtrage sur ceci suivi.

Remarque: La sortie témoin (filtrée et non filtrée) pour le capwap et le capwap AP est incluse pour la référence.

- Afin de visualiser les valeurs par défaut du suivi, entrez :

```
#show trace settings group-ap
```

```
Buffer Properties:
```

```
Feature-Name
```

```
Size          Level
```

```
-----  
-----  
capwap/ap/event
```

```
0          warning
```

```
dtls/ap/event
```

```
0          warning
```

```
iosd-wireless/capwap
```

```
0          warning
```

```
Feature-Name: capwap/ap/event
```

```
Filters: None
```

```
Feature-Name: dtls/ap/event
```

```
Filters: None
```

```
Feature-Name: iosd-wireless/capwap
```

```
Filters: None
```

Remarque: Par défaut, il n'y a aucun filtre réglé sur les suivis l'uns des.

- Afin d'effacer le suivi mettez en mémoire tampon qui correspond au suivi groupe-AP, entrent `#set trace control group-ap clear`

- Afin de placer le niveau de suivi pour le suivi groupe-AP, entrez :

```
#set trace group-ap level ?
```

```
debug      Debug-level messages (7)
```

```
default    Unset Trace Level Value
```

```
err        Error conditions (3)
```

```
info       Informational (6)
```

```
warning    Warning conditions (4)
```

Utilisez le niveau du suivi groupe-AP de `#set` mettent au point mettent au point tandis que vous dépannez.

- Afin de vérifier le niveau de suivi, entrez :

```
# show trace settings group-ap
```

```
Buffer Properties:
```

```
Feature-Name
```

```
Size          Level
```

```
-----  
-----  
capwap/ap/event
```

```
0          debug
```

```
dtls/ap/event
```

```
0          debug
```

```
iosd-wireless/capwap
```

```
0          debug
```

```
Feature-Name: capwap/ap/event
```

```
Filters: None
```

```
Feature-Name: dtls/ap/event
```

```
Filters: None
```

```
Feature-Name: iosd-wireless/capwap
```

```
Filters: None
```

- Afin de visualiser les informations de suivi, entrez :

```
# show trace messages group-ap
```

## Discovery-Request/Response

[11/14/13 14:50:17.484 UTC 702f4a 8528] f84f.57ca.3860 **Discovery Request** from 10.201.234.24:18759

[11/14/13 14:50:17.484 UTC 702f4b 8528] f84f.57ca.3860 Discovery apType = 0, apModel = AIR-CAP2602I-A-K9, Discovery supportedRadios = 0, incomingRadJoinPriority = 1, Discovery versionNum = 167863296

[11/14/13 14:50:17.484 UTC 702f4c 8528] f84f.57ca.3860 Join Priority Processing status =0, Incoming Ap's Priority 1, MaxLrads = 50, joined Aps =0

[11/14/13 14:50:17.484 UTC 702f4d 8528] f84f.57ca.3860 Validated Discovery request with dest ip : 255.255.255.255 from AP 10.201.234.24. Response to be sent using ip : 10.201.234.4

[11/14/13 14:50:17.484 UTC 702f4e 8528] Encode static AP manager 10.201.234.4, AP count 0

[11/14/13 14:50:17.484 UTC 702f4f 8528] acEncodeMwarTypePayload encode mwarType = 0 in capwapMwarTypePayload.

[11/14/13 14:50:17.484 UTC 702f50 8528] f84f.57ca.3860 **Discovery Response** sent to 10.201.234.24:18759

[11/14/13 14:50:27.484 UTC 57 8528] Connection not found in hash table - Table empty.

## DTLS-prise de contact

**Remarque: C'est du point de vue AP, ainsi seulement des messages envoyés par AP sont vus.**

[11/14/13 14:50:27.484 UTC 702f51 8528] DTLS connection not found, creating new connection for 10:201:234:24 (18759) 10:201:234:4 (5246)

[11/14/13 14:50:27.484 UTC 702f52 8528] acDtlsCallback: entering...

[11/14/13 14:50:27.484 UTC 702f53 8528] acDtlsCallback: cb->code 10

[11/14/13 14:50:27.484 UTC 58 8528] Certificate installed for PKI based authentication.

[11/14/13 14:50:27.484 UTC 59 8528] Incremented concurrent handshaking count 1

[11/14/13 14:50:27.484 UTC 5a 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=0

[11/14/13 14:50:27.484 UTC 5b 8528] f84f.57ca.3860 **msg=ClientHello** len=44 seq=0 frag\_off=0 frag\_len=44

[11/14/13 14:50:27.485 UTC 5c 8528] f84f.57ca.3860 Handshake in progress...

[11/14/13 14:50:27.489 UTC 5d 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=1

[11/14/13 14:50:27.489 UTC 5e 8528] f84f.57ca.3860 **msg=ClientHello** len=76 seq=1 frag\_off=0 frag\_len=76 (**with cookie**)

[11/14/13 14:50:27.490 UTC 5f 8528] f84f.57ca.3860 Handshake in progress...

[11/14/13 14:50:27.670 UTC 60 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=2

[11/14/13 14:50:27.670 UTC 61 8528] f84f.57ca.3860 **msg=Certificate** len=1146  
seq=2 frag\_off=0 frag\_len=519

[11/14/13 14:50:27.670 UTC 62 8528] f84f.57ca.3860 Handshake in progress...

[11/14/13 14:50:27.670 UTC 63 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=3

[11/14/13 14:50:27.670 UTC 64 8528] f84f.57ca.3860 **msg=Certificate** len=1146  
seq=2 frag\_off=519 frag\_len=519

[11/14/13 14:50:27.670 UTC 65 8528] f84f.57ca.3860 Handshake in progress...

[11/14/13 14:50:27.670 UTC 66 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=4

[11/14/13 14:50:27.670 UTC 67 8528] f84f.57ca.3860 **msg=Certificate** len=1146  
seq=2 frag\_off=1038 frag\_len=108

[11/14/13 14:50:27.671 UTC 702f54 8528] acDtlsCallback: entering...

[11/14/13 14:50:27.671 UTC 702f55 8528] acDtlsCallback: cb->code 3

[11/14/13 14:50:27.672 UTC 68 8528] Verify X.509 certificate from wtp  
7c69.f604.9460

[11/14/13 14:50:27.673 UTC 702f56 8528] acDtlsCallback Cert validation PENDING

[11/14/13 14:50:27.673 UTC 69 8528] f84f.57ca.3860 Certificate verification -  
pending...

[11/14/13 14:50:27.673 UTC 6a 8528] f84f.57ca.3860 Handshake in process..  
awaiting certificate verification result..

[11/14/13 14:50:27.673 UTC 6b 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=5

[11/14/13 14:50:27.673 UTC 6c 8528] f84f.57ca.3860 **msg=ClientKeyExchange**  
len=130 seq=3 frag\_off=0 frag\_len=130

[11/14/13 14:50:27.673 UTC 702f57 8528] acDtlsCallback: entering...

[11/14/13 14:50:27.673 UTC 702f58 8528] acDtlsCallback: cb->code 3

[11/14/13 14:50:27.674 UTC 6d 8528] Verify X.509 certificate from wtp  
7c69.f604.9460

[11/14/13 14:50:27.675 UTC 702f59 8528] acDtlsCallback Cert validation PENDING

[11/14/13 14:50:27.675 UTC 6e 8528] f84f.57ca.3860 Certificate verification -  
pending...

[11/14/13 14:50:27.675 UTC 6f 8528] f84f.57ca.3860 Handshake in process..  
awaiting certificate verification result..

[11/14/13 14:50:27.675 UTC 70 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=6

[11/14/13 14:50:27.675 UTC 71 8528] f84f.57ca.3860 **msg=CertificateVerify**  
len=258 seq=4 frag\_off=0 frag\_len=258

[11/14/13 14:50:27.675 UTC 702f5a 8528] acDtlsCallback: entering...

[11/14/13 14:50:27.675 UTC 702f5b 8528] acDtlsCallback: cb->code 3

[11/14/13 14:50:27.676 UTC 72 8528] Verify X.509 certificate from wtp 7c69.f604.9460

[11/14/13 14:50:27.676 UTC 702f5c 8528] acDtlsCallback Cert validation PENDING

[11/14/13 14:50:27.676 UTC 73 8528] f84f.57ca.3860 Certificate verification - pending...

[11/14/13 14:50:27.676 UTC 74 8528] f84f.57ca.3860 Handshake in process.. awaiting certificate verification result..

[11/14/13 14:50:27.677 UTC 75 8528] f84f.57ca.3860 **record=ChangeCiphersSpec** epoch=0 seq=7

[11/14/13 14:50:27.677 UTC 702f5d 8528] acDtlsCallback: entering...

[11/14/13 14:50:27.677 UTC 702f5e 8528] acDtlsCallback: cb->code 3

[11/14/13 14:50:27.677 UTC 76 8528] Verify X.509 certificate from wtp 7c69.f604.9460

[11/14/13 14:50:27.678 UTC 702f5f 8528] acDtlsCallback Cert validation PENDING

[11/14/13 14:50:27.678 UTC 77 8528] f84f.57ca.3860 Certificate verification - pending...

[11/14/13 14:50:27.678 UTC 78 8528] f84f.57ca.3860 Handshake in process.. awaiting certificate verification result..

[11/14/13 14:50:27.678 UTC 79 8528] f84f.57ca.3860 record=Handshake epoch=1 seq=0

[11/14/13 14:50:27.678 UTC 7a 8528] f84f.57ca.3860 **msg=Unknown or Encrypted**

[11/14/13 14:50:27.679 UTC 702f60 8528] acDtlsCallback: entering...

[11/14/13 14:50:27.679 UTC 702f61 8528] acDtlsCallback: cb->code 3

[11/14/13 14:50:27.679 UTC 7b 8528] Verify X.509 certificate from wtp 7c69.f604.9460

[11/14/13 14:50:27.680 UTC 702f62 8528] acDtlsCallback Cert validation PENDING

[11/14/13 14:50:27.680 UTC 7c 8528] f84f.57ca.3860 Certificate verification - pending...

[11/14/13 14:50:27.680 UTC 7d 8528] f84f.57ca.3860 Handshake in process.. awaiting certificate verification result..

[11/14/13 14:50:27.681 UTC 7e 8528] Tickling the connection: 10.201.234.4:5246 <-> 10.201.234.24:18759.

[11/14/13 14:50:27.681 UTC 702f63 8528] acDtlsCallback: entering...

[11/14/13 14:50:27.681 UTC 702f64 8528] acDtlsCallback: cb->code 3

[11/14/13 14:50:27.682 UTC 7f 8528] **Verify X.509 certificate from wtp 7c69.f604.9460 >> AP Ethernet mac**

[11/14/13 14:50:27.683 UTC 702f65 8528] acDtlsCallback Cert validation SUCCESS.

[11/14/13 14:50:27.683 UTC 80 8528] f84f.57ca.3860 **Certificate verification - passed!**

[11/14/13 14:50:27.706 UTC 81 8528] f84f.57ca.3860 **Connection established!**

[11/14/13 14:50:27.706 UTC 702f66 8528] acDtlsCallback: entering...

[11/14/13 14:50:27.706 UTC 702f67 8528] acDtlsCallback: cb->code 0

[11/14/13 14:50:27.706 UTC 82 8528] f84f.57ca.3860 **DTLS Connection 0x5789a5e0**



established on local port 5246

[11/14/13 14:50:27.706 UTC 83 8528] f84f.57ca.3860 Setting DTLS MTU for link to peer 10.201.234.24:18759

[11/14/13 14:50:27.706 UTC 84 8528] Load Balancer: Platform Not supported, Exiting from ctrl\_tunnel\_lb

[11/14/13 14:50:27.706 UTC 85 8528] Capwap Control DTLS key plumbing: Get SA resources from LB for AP IP 10.201.234.24, rc = 4

[11/14/13 14:50:27.706 UTC 86 8528] Plumbing DTLS keys for local 10.201.234.4:5246 and peer 10.201.234.24:18759, anc\_sw\_id 0, anc\_asic\_id 0, res\_sw\_id 0, res\_asic\_id 0

[11/14/13 14:50:27.706 UTC 87 8528] Created CAPWAP control DTLS engine session 10.201.234.4:5246 <-> 10.201.234.24:18759.

[11/14/13 14:50:27.706 UTC 88 8528] f84f.57ca.3860 Sending Finished using epoch 1

[11/14/13 14:50:27.706 UTC 702f68 8528] DTLS Session established server (10.201.234.4:5246), client (10.201.234.24:18759)

[11/14/13 14:50:27.706 UTC 702f69 8528] Starting wait join timer for AP: 10.201.234.24:18759

[11/14/13 14:50:27.707 UTC 30e2 267] %DTLS: entering dtls\_add\_dtls\_session\_db\_entry

[11/14/13 14:50:27.707 UTC 30e3 267] %DTLS: sip = 0xac9ea04 dip = 0xac9ea18 sport =5246 dport=18759

[11/14/13 14:50:27.707 UTC 30e4 267] %DTLS: dtls\_add\_dtls\_session\_db\_entry: anchor\_port iifd : 1088ec00000003b : capwap\_iifd : 0 : session type : 0 : sw\_num : 0 : asic : 0

[11/14/13 14:50:27.707 UTC 30e5 267] %DTLS: bk\_sw\_num : 0 bk\_asic : 0

[11/14/13 14:50:27.710 UTC 89 8528] Received DTLS engine action feedback for CAPWAP connection

[11/14/13 14:50:27.711 UTC 8a 8528] DTLS Engine Add Success received for connection 10.201.234.4:5246 / 10.201.234.24:18759

[11/14/13 14:50:27.711 UTC 8b 8528] Key plumb succeeded

[11/14/13 14:50:27.711 UTC 8c 8528] Decrement concurrent handshaking count 0

[11/14/13 14:50:27.711 UTC 8d 8528] Updating state for wtp f84f.57ca.3860 ip 10.201.234.24

[11/14/13 14:50:27.711 UTC 8e 8528] CAPWAP WTP entry not yet created.

[11/14/13 14:50:27.712 UTC 702f6a 8528] Unable to find the First RCB index. Return Value: 2

## Joignez la Demande-réponse

[11/14/13 14:50:27.712 UTC 702f6b 8528] f84f.57ca.3860 **Join Request** from 10.201.234.24:18759

[11/14/13 14:50:27.712 UTC 702f6c 8528] f84f.57ca.3860 For phy port iif id 0x01088ec00000003b, control session - anc sw id 0, anc asic id 0, res sw id 0, res asic id 0 in RCB for AP 10.201.234.24

[11/14/13 14:50:27.712 UTC 8f 8528] Creating WTP 0x3823a0f0 for AP f84f.57ca.3860 with hardware encryption flag = TRUE

[11/14/13 14:50:27.712 UTC 702f6d 8528] f84f.57ca.3860 Deleting AP entry 10.201.234.24:18759 from temporary database.

[11/14/13 14:50:27.712 UTC 702f6e 8528] CAPWAP Interface-Name CAPWAP WCM Client f84f57ca3860 used for IIF ID allocation

[11/14/13 14:50:27.712 UTC 702f6f 8528] **CAPWAP IIF ID Allocation Successful! ID:0x00d2a98000000796** for AP 10.201.234.24, AP hash 1 **[This indicates generation of a capwapx interface seen in show ip interface brief]**

[11/14/13 14:50:27.712 UTC 702f70 8528] Adding Node to AVL Tree with IIF Id:0xd2a98000000796

[11/14/13 14:50:27.712 UTC 702f71 8528] WTP IIF ID Type: 0

[11/14/13 14:50:27.712 UTC 702f72 8528] Timer created successfully for WTP IIF ID: 0xd2a98000000796

[11/14/13 14:50:27.712 UTC 702f73 8528] Added IIF ID to AVL Tree Database 0xd2a98000000796

[11/14/13 14:50:27.712 UTC 702f74 8528] f84f.57ca.3860 Join Version: = 167863296

[11/14/13 14:50:27.712 UTC 702f75 8528] Encode static AP manager 10.201.234.4, AP count 0

[11/14/13 14:50:27.712 UTC 702f76 8528] f84f.57ca.3860 Join resp: CAPWAP Maximum Msg element len = 87

[11/14/13 14:50:27.712 UTC 702f77 8528] f84f.57ca.3860 **Join Response sent** to 10.201.234.24:18759

[11/14/13 14:50:27.712 UTC 702f78 8528] f84f.57ca.3860 **CAPWAP State: Join**

[11/14/13 14:50:27.712 UTC 702f79 8528] f84f.57ca.3860 capwap\_ac\_platform.c:767 - Operation State 0 ==> 4

[11/14/13 14:50:27.713 UTC 702f7a 8528] f84f.57ca.3860 Register LWAPP event for AP f84f.57ca.3860 slot 0

[11/14/13 14:50:27.713 UTC 702f7b 8528] capwap\_iif\_client\_action\_func: myid = 1, myid\_len=1

[11/14/13 14:50:27.713 UTC 702f7c 8528] CAPWAP Interface ID Acked Id-0x00d2a98000000796 by IIF - IIF status = 0x1001, for AP 10.201.234.24, rcb->ap\_registered = 1

[11/14/13 14:50:27.713 UTC 702f7d 8528] f84f.57ca.3860 Not ready to send Config Status Response to AP 10.201.234.24 as SPI ACK is not received

[11/14/13 14:50:27.713 UTC 702f7e 8528] Unable to find entry for PhyIifId: 0x1088ec000000003b from AVL Tree

[11/14/13 14:50:27.713 UTC 702f7f 8528] Adding Node to Physical Iif Id AVL Tree with PhyIifId:0x1088ec000000003b

[11/14/13 14:50:27.713 UTC 702f80 8528] Unable to find entry for PhyIifId: 0x1088ec000000003b from AVL Tree

[11/14/13 14:50:27.713 UTC 702f81 8528] f84f.57ca.3860 Register LWAPP event for

AP f84f.57ca.3860 slot 1

[11/14/13 14:50:27.713 UTC 702f82 8528] Added PhyIifId: 0x1088ec00000003b to AVL Tree Database

[11/14/13 14:50:27.714 UTC 702f83 8528] Get the Interface name from the Phy-Port-IIF-ID:0x1088ec00000003b

[11/14/13 14:50:27.714 UTC 702f84 8528]

---Phy-IIF-ID = 0x1088ec00000003b-----

[11/14/13 14:50:27.714 UTC 702f85 8528] f84f.57ca.3860 Not ready to send Config Status Response to AP 10.201.234.24 as SPI ACK is not received

[11/14/13 14:50:27.714 UTC 702f86 8528] CSM-SPAM:Input monitor name after copying from vapcb to vap data is wireless-avc-basic

[11/14/13 14:50:27.714 UTC 702f87 8528] CSM-SPAM:Output monitor name after copying from vapcb to vapdata is wireless-avc-basic

[11/14/13 14:50:27.714 UTC 702f88 8528] CSM-SPAM:Input monitor name after copying from vapcb to vap data is wireless-avc-basic

[11/14/13 14:50:27.714 UTC 702f89 8528] CSM-SPAM:Output monitor name after copying from vapcb to vapdata is wireless-avc-basic

[11/14/13 14:50:27.714 UTC 702f8a 8528] RSN Capabilities: (26)

[11/14/13 14:50:27.714 UTC 702f8b 8528] [0000] 30 18 01 00 00 0f ac 02 02 00 00 0f ac 02 00 0f

[11/14/13 14:50:27.714 UTC 702f8c 8528] [0016] ac 04 01 00 00 0f ac 02 28 00

[11/14/13 14:50:27.714 UTC 702f8d 8528] WARP IEs: (12)

[11/14/13 14:50:27.714 UTC 702f8e 8528] [0000] dd 0a 00 c0 b9 01 00 00 00 08 01 01

[11/14/13 14:50:27.714 UTC 702f8f 8528] f84f.57ca.3860 Not ready to send Config Status Response to AP 10.201.234.24 as SPI ACK is not received

[11/14/13 14:50:27.715 UTC 702f90 8528] Physical interface Info: IIF-ID = 0x1088ec00000003b, Message Code = 0x802, Interface Name ->gigabitethernet1/0/24, Interface Type = 0x92, Client N<truncated>

[11/14/13 14:50:27.715 UTC 702f91 8528] Updated AVL entry for phyIifid: 0x1088ec00000003b macAddr:f84f.57ca.3860, phyIfName: gigabitethernet1/0/24 Number of APs on this Phy <truncated>

[11/14/13 14:50:27.725 UTC 702f92 8528] capwap opaque data f84f.57ca.3860 length = 0

[11/14/13 14:50:27.725 UTC 702f93 8528] No update; will insert f84f.57ca.3860

## Demande-réponse d'état de configuration/Demande-réponse de mise à jour

[11/14/13 14:50:27.869 UTC 702f94 8528] f84f.57ca.3860 **Configuration Status from** 10.201.234.24:18759

[11/14/13 14:50:27.870 UTC 702f95 8528] f84f.57ca.3860 **CAPWAP State: Configure**

[11/14/13 14:50:27.870 UTC 702f96 8528] f84f.57ca.3860 New unsupported Payload

254 in message from AP f84f.57ca.3860, Return SUCCESS

[11/14/13 14:50:27.870 UTC 702f97 8528] f84f.57ca.3860 Decoding new unsupported Payload 254 in message from AP f84f.57ca.3860, Return SUCCESS

[11/14/13 14:50:27.870 UTC 702f98 8528] Invalid channel 11 spacificied for the AP AP2602I-1, slotId = 0

[11/14/13 14:50:27.870 UTC 702f99 8528] Invalid channel 56 spacificied for the AP AP2602I-1, slotId = 1

[11/14/13 14:50:27.870 UTC 702f9a 8528] f84f.57ca.3860 Updating IP info for AP f84f.57ca.3860 -- static 0, 10.201.234.24/255.255.255.224, gtw 10.201.234.2

[11/14/13 14:50:27.870 UTC 702f9b 8528] f84f.57ca.3860 Updating IP 10.201.234.24 ==> 10.201.234.24 for AP f84f.57ca.3860

|

[11/14/13 14:50:27.870 UTC 702fab 8528] f84f.57ca.3860 LWAPP message validation failed for SPAM Vendor Specific Payload(104) in message of len=7 from AP f84f.57ca.3860

[11/14/13 14:50:27.870 UTC 702fac 8528] f84f.57ca.3860 Failed to validate vendor specific message element

[11/14/13 14:50:27.871 UTC 702fad 8528] f84f.57ca.3860 **Setting MTU to 1485**

[11/14/13 14:50:27.871 UTC 702fae 8528] f84f.57ca.3860 Platform not Supported, exiting Load Balancer function

[11/14/13 14:50:27.871 UTC 702faf 8528] load balancer rc=4 for AP 10.201.234.24, IIF ID:0x00d2a98000000796

[11/14/13 14:50:27.871 UTC 702fb0 8528] opaque data size 0 with capwap interface create f84f.57ca.3860

[11/14/13 14:50:27.871 UTC 702fb1 8528] spiCapwapParams-> data\_tunnel.opaque\_data.opaque\_data\_len: 0

[11/14/13 14:50:27.871 UTC 702fb2 8528] f84f.57ca.3860 Data Tunnel Create timer started for 240 seconds timeout

[11/14/13 14:50:27.871 UTC 702fb3 8528] f84f.57ca.3860 **Data Tunnel created - tunnel type NON\_CRYPTO**, load balancer support Not supported, tunnel mtu 1449,

anc\_sw\_id 0, anc\_asic\_id 0, res\_sw\_id 0, res\_asic\_id 0

anc\_wp\_iif\_id 0x0000000000000000, res\_wp\_iif\_id 0x0000000000000000

[11/14/13 14:50:27.871 UTC 702fb4 8528] f84f.57ca.3860 Not ready to send Config Status Response to AP 10.201.234.24 as SPI ACK is not received

[11/14/13 14:50:27.871 UTC 702fb5 8528] f84f.57ca.3860 AP f84f.57ca.3860 associated. Last AP failure was due to Configuration changes,reason: controller reboot command

[11/14/13 14:50:27.871 UTC 30e6 260] [CAPWAP]: CAPWAP data tunnel create message.

[11/14/13 14:50:27.871 UTC 30e7 260] [CAPWAP]: capwap\_data\_tunnel\_create called

[11/14/13 14:50:27.871 UTC 30e8 260] [CAPWAP]: Data tunnel id = 0xd2a98000000796

[11/14/13 14:50:27.871 UTC 30e9 260] [CAPWAP]: Tunnel Entry not found for AP

(10.201.234.24, 18759)

[11/14/13 14:50:27.873 UTC 30ea 260] [CAPWAP]: CAPWAP IDB init complete

[11/14/13 14:50:27.882 UTC 30eb 260] [CAPWAP]: capwap\_interface\_status\_update:  
tunnel 0xd2a98000000796 status 0

[11/14/13 14:50:27.882 UTC 30ec 260] [CAPWAP]: csb pd flag 0 opaque\_data\_len 0  
attr opaque\_data 0x00000000

[11/14/13 14:50:27.882 UTC 30ed 260] [CAPWAP]: Send capwap\_data\_tunnel\_status\_update  
0 Slot-Unit 1 Unit 1 for iif\_id 0xd2a98000000796 to WCM.

[11/14/13 14:50:27.882 UTC 30ee 260] [CAPWAP]: (capwap\_process\_fed\_results) CAPWAP  
FED result (0) for IIF ID: 0xd2a98000000796

[11/14/13 14:50:27.882 UTC 702fb6 8528

Received CAPWAP Tunnel SPI update opaque size 0

[11/14/13 14:50:27.882 UTC 702fb7 8528] opaque data len 0 with capwap server update

[11/14/13 14:50:27.883 UTC 702fb8 8528] f84f.57ca.3860 SPI ACK : Capwap Data  
Tunnel create successful for iifid:0x00d2a98000000796 AP:10.201.234.24

[11/14/13 14:50:27.883 UTC 702fb9 8528]

Received CAPWAP interface update opaque len 0

[11/14/13 14:50:27.883 UTC 702fba 8528] **SPI IifId ACK: Capwap Data Tunnel Created  
Successfully for IifId: 0x00d2a98000000796 AP: 10.201.234.24**

[11/14/13 14:50:27.883 UTC 702fbb 8528] f84f.57ca.3860 **OK to send Config Status  
Response to AP 10.201.234.24**

[11/14/13 14:50:27.888 UTC 30ef 260] [CAPWAP]: Notify PM (done).

[11/14/13 14:50:27.888 UTC 30f0 260] [CAPWAP]: SNMP Register: Cal HWIDB 32f44570

[11/14/13 14:50:27.888 UTC 30f1 260] [CAPWAP]: capwap\_port\_hashitem added: slot 1  
slotunit 24 vlan 1104

[11/14/13 14:50:27.888 UTC 30f2 260] [CAPWAP]: 7c69.f604.9460 is AP's mac addr

[11/14/13 14:50:27.932 UTC 702fbc 8528] Sending multicast payload to ap AP2602I-1,  
mcast\_mode 0, mcast group 0.0.0.0

[11/14/13 14:50:27.933 UTC 702fbd 8528] f84f.57ca.3860 Config status response sent  
to 10.201.234.24:18759

[11/14/13 14:50:27.933 UTC 702fbe 8528] f84f.57ca.3860 Configuration Status  
Response sent to 10:201:234:24

[11/14/13 14:50:27.933 UTC 702fbf 8528] f84f.57ca.3860 Configuration update  
request for Band Select Cfg sent to 10.201.234.24:18759

[11/14/13 14:50:27.933 UTC 702fc0 8528] f84f.57ca.3860 Configuration update  
request for HaConfig message sent to 10.201.234.24:18759

[11/14/13 14:50:27.934 UTC 702fc1 8528] f84f.57ca.3860 Configuration update  
request for AP NGWC Qos sent to 10.201.234.24:18759

[11/14/13 14:50:28.121 UTC 702fc2 8528] f84f.57ca.3860 Change State Event  
Request from 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fc3 8528] f84f.57ca.3860 Received LWAPP Up event for AP f84f.57ca.3860 slot 0!

[11/14/13 14:50:28.122 UTC 702fc4 8528] f84f.57ca.3860 Radio state change for slot: 0 state: 2 cause: 0 detail cause: 0

[11/14/13 14:50:28.122 UTC 702fc5 8528] f84f.57ca.3860 Change State Event Response sent to 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fc6 8528] f84f.57ca.3860 CAPWAP State: Run

[11/14/13 14:50:28.122 UTC 702fc7 8528] f84f.57ca.3860 Sending the remaining config to AP 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fc8 8528] f84f.57ca.3860 AP Going to RUN 10.201.234.24: ConcurrentJoins: 0

[11/14/13 14:50:28.122 UTC 702fc9 8528] f84f.57ca.3860 **Configuration update request** for Init VAP-DATA for slot 1 sent to 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fca 8528] f84f.57ca.3860 Configuration update request for configuring association limit params sent to 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fcb 8528] f84f.57ca.3860 Configuration update request for Band Select Cfg sent to 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fcc 8528] f84f.57ca.3860 Configuration update request for HaConfig message sent to 10.201.234.24:18759

[11/14/13 14:50:28.123 UTC 702fcd 8528] CAPWAP: No update, will insert f84f.57ca.3860

[11/14/13 14:50:28.123 UTC 702fce 8528] capwap opaque data f84f.57ca.3860 length = 0

[11/14/13 14:50:28.124 UTC 702fcf 8528] CAPWAP HA insert f84f.57ca.3860

[11/14/13 14:50:28.124 UTC 702fd0 8528] CAPWAP HA insert f84f.57ca.3860

[11/14/13 14:50:28.124 UTC 702fd1 8528] f84f.57ca.3860 Configuration update request for PHY payload sent to 10:201:234:24

[11/14/13 14:50:28.126 UTC 702fd2 8528] f84f.57ca.3860 **Configuration Update Response** from 10.201.234.24:18759

[11/14/13 14:50:28.126 UTC 702fd3 8528] f84f.57ca.3860 Configuration update request for RrmInterferenceCtrl payload sent to 10:201:234:24

[11/14/13 14:50:28.126 UTC 702fd4 8528] f84f.57ca.3860 Configuration update request for RrmNeighbourCtrl payload sent to 10.201.234.24

[11/14/13 14:50:28.126 UTC 702fd5 8528] f84f.57ca.3860 Configuration update request for RrmReceiveCtrl payload sent to 10:201:234:24

[11/14/13 14:50:28.126 UTC 702fd6 8528] f84f.57ca.3860 Configuration update request for CcxRmMeas payload sent to 10.201.234.24

[11/14/13 14:50:28.132 UTC 702fd7 8528] f84f.57ca.3860 Change State Event Request from 10.201.234.24:18759

[11/14/13 14:50:28.132 UTC 702fd8 8528] f84f.57ca.3860 Radio state change for slot: 1 state: 2 cause: 0 detail cause: 0

[11/14/13 14:50:28.132 UTC 702fd9 8528] f84f.57ca.3860 Change State Event  
Response sent to 10.201.234.24:18759

[11/14/13 14:50:28.132 UTC 702fda 8528] f84f.57ca.3860 CAPWAP State: Run

[11/14/13 14:50:28.132 UTC 702fdb 8528] f84f.57ca.3860 Sending the remaining  
config to AP 10.201.234.24:18759

[11/14/13 14:50:28.133 UTC 702fdc 8528] f84f.57ca.3860 Configuration update  
request for qos pm payload payload sent to 10.201.234.24:18759

[11/14/13 14:50:28.133 UTC 702fdd 8528] f84f.57ca.3860 Received LWAPP Up  
event for AP f84f.57ca.3860 slot 1!

[11/14/13 14:50:28.133 UTC 702fde 8528] f84f.57ca.3860 Configuration update  
request for PHY payload sent to 10:201:234:24

[11/14/13 14:50:28.133 UTC 702fdf 8528] f84f.57ca.3860 Configuration update  
request for RrmInterferenceCtrl payload sent to 10:201:234:24

[11/14/13 14:50:28.133 UTC 702fe0 8528] f84f.57ca.3860 Configuration update  
request for RrmNeighbourCtrl payload sent to 10.201.234.24

[11/14/13 14:50:28.134 UTC 702fe1 8528] f84f.57ca.3860 Configuration update  
request for RrmReceiveCtrl payload sent to 10:201:234:24

[11/14/13 14:50:28.134 UTC 702fe2 8528] f84f.57ca.3860 Configuration update  
request for CcxRmMeas payload sent to 10.201.234.24

[11/14/13 14:50:28.188 UTC 702fe3 8528] f84f.57ca.3860 Configuration Update  
Response from 10.201.234.24:18759

[11/14/13 14:50:28.188 UTC 702fe4 8528] f84f.57ca.3860 Change State Event  
Request from 10.201.234.24:18759

[11/14/13 14:50:28.188 UTC 702fe5 8528] f84f.57ca.3860 Change State Event  
Response sent to 10.201.234.24:18759

[11/14/13 14:50:28.188 UTC 702fe6 8528] f84f.57ca.3860 CAPWAP State: Run

[11/14/13 14:50:28.188 UTC 702fe7 8528] f84f.57ca.3860 Sending the remaining  
config to AP 10.201.234.24:18759

[11/14/13 14:50:28.194 UTC 702fe8 8528] f84f.57ca.3860 Configuration Update  
Response from 10.201.234.24:18759

[11/14/13 14:50:28.194 UTC 702fe9 8528] f84f.57ca.3860 **WTP Event Request**  
from 10.201.234.24:18759

[11/14/13 14:50:28.194 UTC 702fea 8528] f84f.57ca.3860 **WTP Event Response**  
sent to 10.201.234.24:18759

## Les raisons communes pour AP joignent la panne

Cette section décrit des causes classiques d'AP joignent la panne.

**Problème 1 : AP sur le commutateur de gamme Catalyst 3850 n'est pas dans le VLAN de gestion Sans fil.**

## interface gig1/0/22 de passage de #show

```
interface GigabitEthernet1/0/22
description AP
switchport access vlan 25
switchport mode access
```

## passage de #show | radio inc.

```
wireless mobility controller
wireless management interface Vlan1104
```

## log de #show

```

*%CAPWAP-3-DISC_WIRELESS_INTERFACE_ERR: 1 wcm: Unable to process discovery
request from AP 0019.0737.f630 , VLAN (25) scrIp (10.10.25.13) dstIp
(255.255.255.255), could not get wireless interface belonging to this network
AP est dans VLAN 25, et il n'y a aucune configuration Sans fil d'interface de gestion pour VLAN
25.
```

## Problème 2 : Le modèle AP est sans support.

Voici un test d'AP1131.

## log de #show

```

*%CAPWAP-3-JOIN_UNSUPP_AP: 1 wcm: Received a join request from an unsupported AP
0019.0737.f630 AP8-1131AG-eb:66 (model AIR-AP1131AG-A-K9)
```

## Problème 3 : Le permis de compte AP n'est pas activé sur le contrôleur.

## résumé de droit-à-utilisation de permis de #show

License Name	Type	Count	Period left
ipservices	permanent	N/A	Lifetime
apcount	base	0	Lifetime
apcount	adder	0	Lifetime

License Level In Use: ipservices

License Level on Reboot: ipservices

Evaluation AP-Count: Disabled

Total AP Count Licenses: 0

AP Count Licenses In-use: 0

AP Count Licenses Remaining: 0

## log de #show

```

*%LWAPP-3-AP_LICENSE_REQUEST_ERR: 1 wcm: License request failed for AP
```



0c:68:03:eb:9b:20 - Check for Controller Licenses

\*%CAPWAP-3-AP\_DB\_ALLOC: 1 wcm: Unable to alloc AP entry in database for 10.201.234.xx:29817

## **Problème 4 : Le domaine réglementaire est mal adapté.**

### **pays Sans fil de #show configuré**

Configured Country.....: BE - Belgium

Configured Country Codes

BE - Belgium : 802.11a Indoor,Outdoor/ 802.11b / 802.11g

### **log de #show**

\*%LWAPP-3-RD\_ERR8: 1 wcm: Country code (US ) not configured for AP 0c:68:03:eb:9b:20

\*%LWAPP-3-RD\_ERR4: 1 wcm: Invalid regulatory domain 802.11bg:-E 802.11a:-E for AP 0c:68:03:eb:9b:20

## **Problème 5 : Le contrôleur de mobilité sans fil n'est pas défini.**

### **résumé de mobilité sans fil de #show**

Mobility Agent Summary:

Mobility Role	:	Mobility Agent
Mobility Protocol Port	:	16666
Mobility Switch Peer Group Name	:	
Multicast IP Address	:	0.0.0.0
DTLS Mode	:	Enabled
Mobility Domain ID for 802.11r	:	0xac34
Mobility Keepalive Interval	:	10
Mobility Keepalive Count	:	3
Mobility Control Message DSCP Value	:	0
Switch Peer Group Members Configured	:	0

Link Status is Control Link Status : Data Link Status

The status of Mobility Controller:

IP	Public IP	Link Status
0.0.0.0	0.0.0.0	- : -

### **log de #show**

\*%LWAPP-3-AP\_LICENSE\_REQUEST\_ERR: 1 wcm: License request failed for AP 0c:68:03:eb:9b:20 - AP License Request timedout, ensure MC link is up, Resettting AP

## **Problème 6 : AP a le code de maille là-dessus.**

\*%CAPWAP-3-SPI\_TUNNEL\_CREATE\_ACK\_NOT\_REC: 1 wcm: Dropping discovery request from AP 0c68.03eb.9b20 - SPI Tunnel Create Ack not received[...It occurred 3 times/sec!..]

Ce message est tout à fait générique et non indicatif de la question actuelle. Afin de diagnostiquer plus loin jusqu'à ce que se connecter supplémentaire soit ajouté pour cette problématique spécifique, examinez le log de console AP.

## **Problème 7 : L'AP3700 est connecté à une gamme Catalyst 3850 commute que les passages 3.3.0SE.**

log de #show

```
*%CAPWAP-3-DISC_UNSUPPORTED_AP: 1 wcm: Rejecting discovery request from unsupported AP
08cc.68b4.4780 [...It occurred 2 times/sec!..]
```

## **Problème 8 : Le temps de contrôleur est en dehors de l'intervalle de validité de certificat AP.**

horloge de #show

```
*00:14:59.459 GMT0:0 Thu Jan 1 1970
```

log de #show

```
*Jan 1 00:05:51.338: %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Certificate chain
validation has failed. The certificate (SN: 17978AAD00000036823E) is not yet valid
Validity period starts on 04:25:46 GMT0:0 Jun 8 2013
```

```
*Jan 1 00:05:51.344: *%DTLS-4-BAD_CERT: 1 wcm: Certificate verification failed.
Peer IP: 10.201.234.21
```

```
*Jan 1 00:05:51.344: *%DTLS-3-HANDSHAKE_FAILURE: 1 wcm: Failed to complete DTLS handshake
with peer 10.201.234.21 Reason: no certificate returned
```

## **Problème 9 : La liste d'autorisation AP est activée sur le WLC ; AP n'est pas dans la liste d'autorisation.**

authentique-liste du #show AP

```
Authorize MIC APs against AAA : Enabled
```

```
Authorize LSC APs against Auth-List : Disabled
```

APs Allowed to Join:

```
AP with Manufacturing Installed Certificate : Enabled
```

```
AP with Self-Signed Certificate : Disabled
```

```
AP with Locally Significant Certificate : Disabled
```

log de #show

```
*%LWAPP-3-RADIUS_ERR: 1 wcm: Could not send join reply, AP authorization failed;
AP:0c:68:03:eb:9b:20
```

```
*%CAPWAP-3-DATA_TUNNEL_DELETE_ERR2: 1 wcm: Failed to delete CAPWAP data tunnel
with interface id: 0x0 from internal database. Reason: AVL database entry not found
```

## **Problème 10 : La stratégie MIC AP est désactivée.**

authentique-liste du #show AP

```
Authorize MIC APs against AAA : Disabled
```

Autorisez LSC aps contre l'Authentique-liste : Handicapé

Aps permis pour se joindre :

AP avec Manufacturing Installed Certificate : Handicapé

AP avec le certificat Auto-signé : Handicapé

AP avec localement - le certificat significatif : Handicapé

log de #show

```
*%LOG-3-Q_IND: 1 wcm: Validation of SPAM Vendor Specific Payload failed - AP
f8:4f:57:3b:8c:d0
*%CAPWAP-3-ALREADY_IN_JOIN: 1 wcm: Dropping join request from AP f84f.573b.8cd0 -
AP is already in joined state
*%CAPWAP-3-DATA_TUNNEL_DELETE_ERR2: 1 wcm: Failed to delete CAPWAP data tunnel
with interface id: 0x0 from internal database. Reason: AVL database entry not found
```

Ce message n'aide pas à trouver la cause principale de la question. Cependant, le suivi affiche ce message.

messages groupe-AP de suivi de #show

|

```
MIC AP is not allowed to join by config
```

|

## Conseils généraux de tech

Cette section fournit quelques conseils utiles.

- Quand vous commencez le processus de dépannage, l'espace libre a précédemment collecté des suivis pour la caractéristique spécifique. Dans ce cas, capwap, groupe-AP, et tous les suivis filtrés.  
**# capwap de contrôle de set trace# contrôle groupe-AP de set trace**  
**# le système-filtrer-suivi de contrôle de set trace >>** ceci efface les suivis filtrés et ne peut pas être exécuté sur une base de par-caractéristique
- AP se joignent sur les contrôleurs convergés d'accès se sert de l'adresse MAC par radio d'AP. Ainsi, quand vous placez un filtre pour le suivi, servez-vous de l'adresse MAC de radio ou de base d'AP. Sélectionnez la commande de **show ap join stats summary** afin de trouver l'adresse MAC par radio.
- Des questions avec des Certificats ne sont traitées par IOSd et exigent l'utilisation de met au point, pas des suivis, pour davantage de diagnostic.  
**crypto PKI API de #debugcryptos rappels de PKI de #debugcrypto pki server de #debugcryptos transactions de PKI de #debugcryptos messages de PKI de #debug**