

Draadloze vaak gestelde vragen en probleemoplossing - softwaregedefinieerde toegang tot Cisco DNA Center release 1.1 en 1.2

Inhoud

[Referentiedocumenten gepubliceerd op Cisco.com](#)

[Opdrachtcontrole voor fabric op Control Node, Edge Node, Wireless LAN Controller \(WLC\) en access point \(AP\)](#)

[AireOS WLC Config vanuit Cisco DNA-centrum na provisioning \(opmerking: Referentie gebruiken als 3504 \(WLC\)\)](#)

[Straalsamenvatting tonen na provisioning van WLC](#)

[WLAN Config Push van BG wordt onder "Show WLAN summary" weergegeven](#)

[WLC Config - druk van Cisco DNA-centrum na toevoeging van WLC aan fabric](#)

[Hoe te controleren of Map Server bereikbaar is?](#)

[Verbindingen van fabric Map-server fouilleren](#)

[Hoe is Fabric ingeschakeld of niet en wat is de verwachte uitvoer?](#)

[WLAN Config Push van Cisco DNA Center wordt gezien onder "show fabric wlan samenvatting" na toevoeging van WLC aan Fabric en toewijzing van client-IP Pool aan Fabric Wireless LAN \(WLAN\) onder Voorziening > Fabric > Host Onboarding](#)

[Procesvoering voor actieve WLC-vervanging terwijl Hoge beschikbaarheid \(HA\) is ingesteld via Cisco DNA Center](#)

[Draadloze problemen oplossen](#)

[Afluisteren van IP-telefoons/toegang tot tunnelformatie](#)

[Clientfiltering](#)

[AP online](#)

[Traditionele methode/stappen: \(Rekening houdend met AP VLAN bereik heeft optie 43 of optie 60 gericht op WLC\)](#)

[Plug and Play/Zero Touch AP Provisioning \(rekening houdend met AP VLAN-bereik heeft optie 43, gericht op Cisco DNA-centrum\)](#)

Referentiedocumenten gepubliceerd op Cisco.com

- [Draadloze configuratie handleidingen voor elke release](#)
- [SD draadloze implementatiegids](#)
- [Handleiding voor draadloze beste praktijken](#)
- [Technische referentiedocumenten voor draadloos](#)
- [Compatibiliteitsmatrix voor SDA](#)
- [Cisco DNA Center-gebruikershandleidingen voor elke release](#)

Opdrachtcontrole voor fabric op Control Node, Edge Node, Wireless LAN Controller (WLC) en access point (AP)

Control-knooppunt

- toont client-id <L2 ap-instantie id> Ethernet-server **MAC to Endpoint Identification (EID) Toewijzing**
 - toont client-case-id <L3 ap-exemplaar id> ipv4 server- **IP aan EID-toewijzing**
 - Toon voorbeeld-id 8188 Ethernet server adresresolutie van de lijst **MAC aan IP Toewijzing voor een specifiek geval-ID**
 - de lissabonsite tonen
- Edge-knooppunt
- toont lisp instantie-id <L2 ap instantie-id> Ethernet-database wlc
 - toont lisp instantie-id <L2 client-instantie id> Ethernet-database wlc
 - samenvatting van de toegangstunnel
- WLC
- Samenvatting van wasgoed tonen
 - Samenvatting van het weefsel tonen
 - Samenvatting van fabric-kaart-server tonen
- Access point
- ip-tunnelstof tonen

AireOS WLC Config vanuit Cisco DNA-centrum na provisioning (opmerking: Referentie gebruiken als 3504 (WLC))

Straalsamenvatting tonen na provisioning van WLC

```
(sdawlc3504) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Accounting Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
Keywrap..... Disabled
Fallback Test:
  Test Mode..... Passive
  Probe User Name..... cisco-probe
  Interval (in seconds)..... 300
MAC Delimiter for Authentication Messages..... hyphen
MAC Delimiter for Accounting Messages..... hyphen
RADIUS Authentication Framed-MTU..... 1300 Bytes
```

Authentication Servers

Idx	Type	Server Address	Port	State	Tout	MgmtTout	RFC3576	IPSec	state/Profile
1	* NM	192.168.2.193	1812	Enabled	2	5	Enabled	Disabled	- /none
2	M	172.27.121.193	1812	Enabled	2	5	Enabled	Disabled	- /none

WLAN Config Push van BG wordt onder "Show WLAN summary" weergegeven

```
(sdawlc3504) >show wlan summary
```

```
Number of WLANs..... 7
```

WLAN ID	WLAN Profile Name / SSID	Status
1	Test / Test	Enabled
management	none	

17	dnac_guest_F_global_5dfbd_17 / dnac_guest_206	Disabled
management	none	
18	dnac_psk_2_F_global_5dfbd_18 / dnac_psk_206	Disabled
management	none	
19	dnac_wpa2__F_global_5dfbd_19 / dnac_wpa2_206	Enabled
management	none	
20	dnac_open__F_global_5dfbd_20 / dnac_open_206	Enabled
management	none	
21	Test!23_F_global_5dfbd_21 / Test!23	Disabled
management	none	

WLC Config - druk van Cisco DNA-centrum na toevoeging van WLC aan fabric

Hoe te controleren of Map Server bereikbaar is?

Samenvatting van fabric-kaart-server weergeven na toevoeging van WLC aan Fabric

```
(sdawlc3504) >show fabric map-server summary
```

```
MS-IP      Connection status
```

```
-----
```

```
192.168.4.45    UP
```

```
192.168.4.66    UP
```

Verbindingen van fabric Map-server fouilleren

De connectiviteit van het besturingsplane (CP) kan om verschillende redenen omlaag gaan of naar beneden blijven.

1. Als de CP daalde. (wat in dit geval niet het geval is)
2. Middenknooppunten die omlaag gaan en die WLC met CP verbinden, bijvoorbeeld fusierouter.
3. Als de CP-verbinding met de WLC is verbroken door de koppeling naar beneden. Dit kan WLC zijn naar de directe buurman of CP naar de directe buur van WLC.

gedetailleerde netwerkserver tonen

Toon de creatie van TCP-weefsel met de geschiedenis van <Map-Server IP>

Debugs die nadere informatie kunnen verstrekken

debug van tcp van fabric lisp-map-server

Hoe is Fabric ingeschakeld of niet en wat is de verwachte uitvoer?

samenvatting van het weefsel weergeven na toevoeging van WLC aan Fabric

```
(sdawlc3504) >show fabric summary
```

Fabric Support..... enabled

Enterprise Control Plane MS config

Primary Active MAP Server

IP Address..... 192.168.4.45

Secondary Active MAP Server

IP Address..... 192.168.4.66

Guest Control Plane MS config

Fabric TCP keep alive config

Fabric MS TCP retry count configured 3
Fabric MS TCP timeout configured 10
Fabric MS TCP keep alive interval configured 10
Fabric Interface name configured management

Fabric Clients registered 0

Fabric wlans enabled 3

Fabric APs total Registration sent 30

Fabric APs total DeRegistration sent 9

Fabric AP RLOC requested 15

Fabric AP RLOC response received 30

Fabric AP RLOC send to standby 0

Fabric APs registered by WLC 6

VNID Mappings configured: 4

Name	L2-Vnid	L3-Vnid	IP Address/Subnet
182_10_50_0-INFRA_VN	8188	4097	182.10.50.0 / 255.255.255.128
10_10_10_0-Guest_Area	8190	0	0.0.0.0 / 0.0.0.0
182_10_100_0-DEFAULT_VN	8191	0	0.0.0.0 / 0.0.0.0
182_11_0_0-DEFAULT_VN	8189	0	0.0.0.0 / 0.0.0.0

Fabric Flex-Acl-tables	Status
DNAC_FABRIC_FLEX_ACL_TEMPLATE	Applied

Fabric Enabled Wlan summary

WLAN ID	SSID	Type	L2 Vnid	SGT	RLOC IP	Clients
19	dnac_wpa2_206	WLAN	8189	0	0.0.0.0	0
182_11_0_0-DEFAULT_VN						
20	dnac_open_206	WLAN	8189	0	0.0.0.0	0
182_11_0_0-DEFAULT_VN						

WLAN Config Push van Cisco DNA Center wordt gezien onder "show fabric wlan samenvatting" na toevoeging van WLC aan Fabric en toewijzing van client-IP Pool aan Fabric Wireless LAN (WLAN) onder Voorziening > Fabric > Host Onboarding

Bekijk de samenvatting van het wasprogramma na Fabric-provisioning

```
(sdawlc3504) >show fabric wlan summary
```

WLAN ID	SSID	Type	L2 Vnid	SGT	RLOC IP	Clients
VNID	Name					
19	dnac_wpa2_206	WLAN	8189	0	0.0.0.0	0
182_11_0_0-DEFAULT_VN						
20	dnac_open_206	WLAN	8189	0	0.0.0.0	0
182_11_0_0-DEFAULT_VN						

Procesvoering voor actieve WLC-vervanging terwijl Hoge beschikbaarheid (HA) is ingesteld via Cisco DNA Center

Voer de activiteit uit in **Onderhoudsvenster**. Het opnieuw configureren van een WLC in HA-paar door Cisco DNA Center kan niet worden bereikt zonder Primaire WLC uit Fabric te verwijderen.

1. Zorg ervoor dat de WLC die moet worden vervangen in de stand-by modus staat. Als dit niet het geval is, voert u een handmatige omschakeling uit en laat deze stand-by staan
2. HA uit Cisco DNA Center uit Provisioning page
3. Zodra HA is uitgeschakeld, zal WLC automatisch uit de inventaris worden verwijderd.
4. Plaats de WLC fysiek en handmatig in te stellen basisvereisten op nieuwe WLC
5. Ontdek nieuwe WLC in Cisco DNA Center
6. Verwijder primaire WLC van fabric die al in Cisco DNA Center was. (Zonder deze stap zal het configureren van een nieuwe WLC een fout maken en falen via Cisco DNA Center)
7. Configureer de HA opnieuw met de nieuwe WLC en de redundantiebeheer IP's. [Beide WLC's worden opnieuw geladen]
8. Voer handmatig opnieuw synchroniseren uit van inventaris op Primaire WLC of wacht op de volgende hersynchronisatiecyclus om informatie in Cisco DNA Center bij te werken. Als het eenmaal is uitgevoerd, zal nieuwe WLC uit de inventaris verdwijnen en als standby onder Hoge beschikbaarheid worden weergegeven.
9. WLC terug naar fabric toevoegen

VOORBEELD

[CSCvn2461](#) Cisco DNA-centrum: Kan geen WLC HA koppelen als een van de WLC al deel uitmaakt van een stof

Werken:

1. Stel de WLC HA handmatig in via CLI. Er zal geen impact op de prestaties zijn. [OPMERKING: Kan HA niet langer configureren of uitschakelen via Cisco DNA Center]
2. Fabric via Cisco DNA Center uitschakelen zoals in bovenstaande stappen is beschreven. [LET OP: Dit zal leiden tot twee keer de downtime, één keer tijdens het uitschakelen van Fabric en een tweede keer tijdens het vormen van HA]

Draadloze problemen oplossen

Afluisteren van IP-telefoons/toegang tot tunnelformatie

1. Controleer of AP IP-adres heeft

IP-communicatie-bindend → weergeven op Fabric Edge

Als het geen IP voor de aangesloten AP interface toont, laat u hieronder details op de schakelaar toe en controleer of AP IP krijgt of niet

IP-pakketten voor snuffelen

debug van IP-communicatie

Monster logbestand bijgevoegd onder →

Voorbeeld:

```
Floor_Edge-6#sh ip-cp snuffelband
```

```
MacAddress IPAddress Lease (sec) type VLAN-interface
```

```
-----
```

```
0C:75:BD:0D:46:60 182.10.50.7 67054 dhcp-snooping 1021 Gigabit Ethernet1/0/7 →  
Ethernet-interface moet beschikken over een IP
```

2. Controleer of AP zich bij WLC aansluit

Samenvatting tonen → op WLC

toont overzicht van oproepen → Op WLC

Als AP nog nooit bij WLC is aangesloten, schakelt u onderstaande beelden op WLC in

debug-gebeurtenissen in

kapelfouten debug

3. Als AP-formulieren CAPWAP vormen, maar er geen toegang-tunnels worden gevormd tussen AP en Switch, dient u onderstaande controles uit te voeren

Stap 1: Heeft APs in WLC RLOC IPs of niet, als niet te controleren punt a) hieronder.

a) Om het Fabric Control plane protocol veerkrachtiger te maken, is het belangrijk dat **een specifieke route naar de WLC aanwezig is in de globale routingtabel van elk weefsel**. De route naar het IP-adres van WLC moet bij elk knooppunt opnieuw worden gedistribueerd in het IGP-onderliggend protocol aan de grens of statisch worden geconfigureerd. Met andere woorden, de WLC zou niet bereikbaar moeten zijn door de standaardroute.

Stap 2: Als AP's in WLC de juiste RLOC's tonen en onder "show fabric summary" de Samenvatting van RLOC tonen waar RLOC om gevraagd werd, gelieve dan onderstaande stappen te controleren

b) Controleer op het knooppunt van het besturingsplane, "*laat de client-id <L2 ap-instantie-id> Ethernet-server*" → het basisradio MAC voor AP bevatten

Controleer op Fabric Edge-knooppunt, "*laat de optie-id <L2 ap-instantie id> Ethernet-database wlc*" → Het moet Base Radio MAC voor AP bevatten en niet de Ethernet MAC

van AP.

Als boven 2 opdrachten geen Base Radio MAC van AP tonen en de toegang-tunnels niet vormen. Schakel "debug lisp control-plane all" in op het besturingsplane en zoek naar basisradio MAC in logging. [OPMERKING: "alle bedieningspaneel van de lissabonstrategie debug" in het besturingsplane is echt handig, schakelt u de houtkap uit voordat u de bugs aanzet]

Als we authenticatiefout zien zoals hieronder, controleer dan de verificatiesleutel tussen WLC en CP-knooppunt.

7 dec. 17:42:01.65 uur: LISP-0: MS Site EID IID 8188 prefix voor een willekeurige-mac SVC_VLAN_IAF_MAC site_uci, geen registratie voor meer specifieke 2c0b.e9c6.ec80/48

7 dec. 42:01.659: LISP-0: Gebouw van betrouwbare registratieformulierregistratie-afgewezen voor IID 8188 EID 2c0b.e9c6.ec80/48 , Afwijzingscode: Echtheidsfout/2.

Hoe controleert u de verificatiesleutel op de fabricconfiguratie tussen WLC en CP.

Controleer op WLC of GUI onder controller → Fabric Configuration → Control Plane → (Vooraf gedeelde sleutel) staat

Op CP, controleer dan op schakelaar met behulp van sh-run-fig | b-sessie over landkaarten

CP#sh-run-configuratie | b-sessie over landkaarten

passieve open WLC-sessie voor kaartserver

site_uci

beschrijving mapserver geconfigureerd vanuit apic-em

Verificatiesleutel uci (Controleer of een gedeelde sleutel op WLC overeenkomt met deze verificatiesleutel op CP) [LET OP: Over het algemeen houdt Cisco DNA Center op deze toets zodat deze niet wordt gewijzigd, tenzij dit nodig is en weet wat er op CP/WLC] wordt ingesteld

4. Algemene controles en displays voor toegangstunnels.

a) samenvatting van de toegangstunnel tonen

```
Floor_Edge-6#sh access-tunnel summary
```

```
Access Tunnels General Statistics:
```

```
Number of AccessTunnel Data Tunnels = 5
```

```
Name SrcIP SrcPort DestIP DstPort VrfId
```

```
-----  
Ac4 192.168.4.68 N/A 182.10.50.6 4789 0  
Ac24 192.168.4.68 N/A 182.10.50.5 4789 0  
Ac19 192.168.4.68 N/A 182.10.50.8 4789 0  
Ac15 192.168.4.68 N/A 182.10.50.7 4789 0  
Ac14 192.168.4.68 N/A 182.10.50.2 4789 0
```

```
Name IfId Uptime
```

```
-----
```

```

Ac4 0x00000037 2 days, 20:35:29
Ac24 0x0000004C 1 days, 21:23:16
Ac19 0x00000047 1 days, 21:20:08
Ac15 0x00000043 1 days, 21:09:53
Ac14 0x00000042 1 days, 21:03:20

```

b) met platformsoftware gevoede switch actieve ifm interfaces toegang-tunnel

```

Floor_Edge-6#show platform software fed switch active ifm interfaces access-tunnel
Interface                IF_ID                State
-----
Ac4                       0x00000037          READY
Ac14                      0x00000042          READY
Ac15                      0x00000043          READY
Ac19                      0x00000047          READY
Ac24                      0x0000004c          READY

```

Floor_Edge-6#

Als de toegangstunnels onder commando b) hoger zijn dan a) is dat een probleem. Hier zijn de Fed-items niet correct geklaard door Fabric Edge en dus zijn er meerdere access-tunnelitems op Fed in vergelijking met IOS. Vergelijk Dest IP na uitvoering van opdracht c). Als meerdere toegangstunnel dezelfde Destination IP delen is dat het probleem met programmering.

c) tonen platformsoftware gevoede switch actieve ifm indien-id <Elke AP IF-ID> [OPMERKING: Elke IF-ID kan uit vorige opdracht worden opgehaald]

```

Floor_Edge-6#show platform software fed switch active ifm if-id 0x00000037
Interface IF_ID          : 0x0000000000000037
Interface Name           : Ac4
Interface Block Pointer  : 0xffc0b04c58
Interface State          : READY
Interface Status         : ADD
Interface Ref-Cnt        : 2
Interface Type           : ACCESS_TUNNEL
    Tunnel Type          : L2Lisp
    Encap Type           : VxLan
    IF_ID                : 0x37

Port Information
Handle ..... [0x2e000094]
Type ..... [Access-tunnel]
Identifier ..... [0x37]
Unit ..... [55]
Access tunnel Port Logical Subblock
    Access Tunnel id    : 0x37
    Switch Num          : 1
    Asic Num            : 0
    PORT LE handle      : 0xffc0b03c58
    L3IF LE handle      : 0xffc0e24608
    DI handle           : 0xffc02cdf48
    RCP service id      : 0x0
    HTM handle decap    : 0xffc0e26428
    RI handle decap     : 0xffc0afb1f8
    SI handle decap     : 0xffc0e26aa8
    RCP opq info        : 0x1
    L2 Brdcast RI handle : 0xffc0e26808
    GPN                 : 3201
    Encap type          : VXLAN

```



```

L3 protocol      : 17
Src IP           : 192.168.4.68
Dest IP          : 182.10.50.6
Dest Port        : 4789
Underlay VRF     : 0
XID cpp handle   : 0xffc03038f8
Port L2 Subblock
Enabled          [No]
Allow dot1q      [No]
Allow native     [No]
Default VLAN     [0]
Allow priority tag ... [No]
Allow unknown unicast [No]
Allow unknown multicast [No]
Allow unknown broadcast [No]
Allow unknown multicast [Enabled]
Allow unknown unicast [Enabled]
IPv4 ARP snoop   [No]
IPv6 ARP snoop   [No]
Jumbo MTU        [0]
Learning Mode    [0]
Port QoS Subblock
Trust Type       [0x7]
Default Value    [0]
Ingress Table Map [0x0]
Egress Table Map [0x0]
Queue Map        [0x0]
Port Netflow Subblock
Port CTS Subblock
Disable SGACL    [0x0]
Trust            [0x0]
Propagate        [0x1]
%Port SGT        [-180754391]
Ref Count : 2 (feature Ref Counts + 1)
IFM Feature Ref Counts
FID : 91, Ref Count : 1
No Sub Blocks Present

```

d) actieve R0-tunnelschakelaar voor de platformsoftware tonen

```

Floor_Edge-6#show platform software access-tunnel switch active R0
Name      SrcIp      DstIp      DstPort  VrfId     Iif_id
-----
Ac4       192.168.4.68  182.10.50.6  0x12b5  0x0000  0x000037
Ac14      192.168.4.68  182.10.50.2  0x12b5  0x0000  0x000042
Ac15      192.168.4.68  182.10.50.7  0x12b5  0x0000  0x000043
Ac19      192.168.4.68  182.10.50.8  0x12b5  0x0000  0x000047
Ac24      192.168.4.68  182.10.50.5  0x12b5  0x0000  0x00004c

```

actieve R0-statistieken van de platformsoftware toegang-tunnelschakelaar

```

Floor_Edge-6#show platform software access-tunnel switch active R0 statistics
Access Tunnel Counters (Success/Failure)
-----
Create                6/0
Create Obj Download   6/0
Delete                3/0
Delete Obj Download   3/0
NACK                  0/0

```

e) tonen de platformsoftware toegang-tunnelschakelaar actief F0

```
Floor_Edge-6#show platform software access-tunnel switch active F0
```

Name	SrcIp	DstIp	DstPort	VrfId	Iif_id	Obj_id	Status
Ac4	192.168.4.68	182.10.50.6	0x12b5	0x000	0x000037	0x00d270	Done
Ac14	192.168.4.68	182.10.50.2	0x12b5	0x000	0x000042	0x03cbca	Done
Ac15	192.168.4.68	182.10.50.7	0x12b5	0x000	0x000043	0x03cb9b	Done
Ac19	192.168.4.68	182.10.50.8	0x12b5	0x000	0x000047	0x03cb6b	Done
Ac24	192.168.4.68	182.10.50.5	0x12b5	0x000	0x00004c	0x03caf4	Done

actieve F0-statistieken van de platformsoftware toegang-tunnelschakelaar

```
Floor_Edge-6#show platform software access-tunnel switch active F0 statistics
```

```
Access Tunnel Counters (Success/Failure)
```

```
-----  
Create          0/0  
Delete          3/0  
HW Create       6/0  
HW Delete       3/0  
Create Ack      6/0  
Delete Ack      3/0  
NACK Notify     0/0
```

f) actieve f0 statistieken van platform software object-Manager tonen

```
Floor_Edge-6#show platform software object-manager switch active f0 statistics
```

```
Forwarding Manager Asynchronous Object Manager Statistics
```

```
Object update: Pending-issue: 0, Pending-acknowledgement: 0  
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0  
Batch end:     Pending-issue: 0, Pending-acknowledgement: 0  
Command:      Pending-acknowledgement: 0  
Total-objects: 987  
Stale-objects: 0  
Resolve-objects: 3  
Error-objects: 1  
Paused-types: 0
```

g) de actieve f0 hangende-kwestie-update van de platformsoftware van-manager tonen

show platform software object-Manager-schakelaar actief f0 hangend-ack-update

de actieve f0 fout-object-manager-schakelaar van de platformsoftware tonen

5. Traces en debugs die moeten worden ingezameld.

a) Gebiedsbestanden verzamelen voordat sporen/uitwerpingen zijn toegestaan

Firewall van het platform zoeken archiefdoel flitser:<Filename>

```
Floor_Edge-6#request platform software trace archive target flash:Floor_Edge-6_12_14_18
```

```
Waiting for trace files to get rotated.
```

```
Creating archive file [flash:Floor_Edge-6_12_14_18.tar.gz]
```

```
Done with creation of the archive file: [flash:Floor_Edge-6_12_14_18.tar.gz]
```

b) Opslagbuffer verhogen en console uitschakelen

```
Floor_Edge-6(config)#logging buffered 214748364
```

```
Floor_Edge-6(config)#no logging console
```

c) Traces instellen

de actieve R0-toegangstunnelbreedtebreedtebreedten van de software voor het instellen van het platform

Hiermee stelt u de actieve F0-toegangstunnelbreedtebreedtebreedte in de software van het platform sporen van de schakelaar actief ifm_main debug software voor platform overtrekken van schakelaar actieve toegang_tunnelbreedten

Hiermee stelt u de actieve F0 aom-omloop van de software in

d) Debugs inschakelen

l2lisp debug

helemaal met lissingscontrolevlak reinigen

e) kop/geen kop interface-poort waar AP is aangesloten

f) Verzamel archiefbestanden op dezelfde manier als stap a) met een andere bestandsnaam

g) Logbestand omleiden naar flitser

Floor_Edge-6#show logging | flitser omleiden:<bestandsnaam>

```
Floor_Edge-6#show logging | redirect flash:console_logs_Floor_Edge-6_12_14_18
```

Clientfiltering

Het af luisteren van draadloze klanten die zich afvragen op SDA FEW kan lastig worden.

Volg onderstaande werkschema om één apparaat tegelijk te elimineren.

1. WLC
2. Fabric Edge
3. Access point (indien debuggen op fabric Edge punten bij AP)
4. Intermediair/grens-knooppunt. (Bij uitgifte van gegevenspad)
5. Knooppunt van besturingsplane. (Bij probleem beheerpad)

WLC-filtering

Voor problemen met clientconnectiviteit moet u beginnen met het fouilleren door informatie over WLC te verzamelen, die ook toonaangevende opdrachten en uiteinden omvat.

Opdrachten voor AireOS WLC-show

toonaangevend

toontechniek

samenvatting van het WLAN

tonen WLAN <id> —> Verzamel deze uitvoer voor alle SSID's, ten minste 1 voor het werken

en het niet werken

samenvatting van het weefsel

Samenvatting van fabric-kaart tonen

samenvatting van client

clientdetails tonen <mac_id>

Debug opdrachten van AireOS-WLC

<mac1> —> Clientassoc, roaming, debugs.

Schakel de detailinformatie van een wasmachine uit —> Dit biedt informatie over wasregistratieberichten

Debugging van fabricrand

Na het debuggen op WLC en waargenomen zijn er geen problemen met betrekking tot snijpad voor de client. Clientstappen van ASSOC, Verificatie en run status met juiste SGT-markering of AAA-parameters en gaan naar deze stap om de kwestie verder te isoleren.

Een ander ding om te verifiëren is de toegang-tunnel programmering is correct zoals beschreven in bovenstaande AP het zuiveren sectie.

tonen opdrachten om te verifiëren

Vind L2 lisp instantie-id van (toon clientdetails <mac_id> van boven)

Geeft een Cisco-instantie-id <L2_LISP> Ethernet-database WLC —> Dit geeft een lijst van alle WLC-geassocieerde clients voor die specifieke L2 lisp instantie-ID. Het aantal bronnen moet overeenkomen met het aantal besturingsplaneknooppunten in het netwerk

Geeft een client-id <L2_LISP> Ethernet-database WLC <client-mac in h.h> —> Dit geeft details voor de specifieke client weer

bestand voor het opsporen van apparatuur weergeven | i VI —> Specifieke SVI zoeken waar de cliënt verbonden is en aanwezig moet zijn.

bestand voor het opsporen van apparatuur weergeven | i <mac> —>Vind de client-ingang, dient tegen correct VLAN, interface, status en leeftijd te zijn.

toon mac adres-table dynamisch VLAN <VLAN-ID> -> De ingang voor de mac zou machine-tracking database moeten vergelijken, als het Mac-adres op FED wordt gecontroleerd

ip-dhcp-snooping-bindend vlan <vlan_waarbij_client_is_connected> tonen

IP-arp vrf <VN> tonen

toon mac adres-tafel vlan <vlan_waar_client_is_connected>

tonen de software van het platform gevoede switch actieve matm macTable vlan <vlan_Where_client_is_connected> —> Als dit correct is, wordt het programmeren voor draadloze client correct bij lokale switch uitgevoerd.

tonen platform software matm-schakelaar actief F0 mac <mac_id>

Debug-opdrachten in Fabric Edge

Noodzaak om sporen van Fed te verzamelen als er een probleem is in het programmeren van de client op Fabric Edge. Er zijn 2 manieren om hetzelfde te doen nadat je onder de afvoerbuisjes hebt geplaatst.

Debugs en set opdrachten die ongeacht de methode ingeschakeld moeten worden.

*software voor het instellen van de efro-schakelaar voor actieve all-modules
software van het platform overtrekken van de gebruikte schakelaar actieve l2_fib_entry breedband
software van het platform overtrek actieve l2_fib_adj breedband
software van het platform , met behulp van de schakelaar gevoede actieve injectiebreedten instellen
software voor het instellen van een actieve matm-breedband met de meegeleverde schakelaar*

debug (uitschakelen van console loggen en vergroten logbuffer)

apparaat-tracking debug

helemaal met lissingscontrolevlak reinigen

platform van alle debug

mat zuiveren

Methode 1: Verzamel radiofrequente overtrekbestanden voor specifieke client nadat u debugs hebt ingeschakeld [Opmerking als DHCP-probleem is, gebruik deze methode dan niet]

Wacht tot het probleem opnieuw wordt geproduceerd

platform conditioneren met een <mac-id> besturingsplane debug
start van platform debug
debug van perron
aanvraag voor platform van zachte sporen filter-binaire draadloze context mac-id>

Richt de logbestanden van de console opnieuw naar flitser nadat kwestie is gereproduceerd.

Methode 2: Verzamel archieflogbestanden nadat u uitwerpselen hebt ingeschakeld

Wacht tot het probleem opnieuw wordt geproduceerd

software-sporenarchief van het zoekplatform

Verzamel het bestand van de stammen en analyseer het gevoede, ios, fman logt voor client mac.

Richt de logbestanden van de console opnieuw naar flitser nadat kwestie is gereproduceerd.

Afluisteren van access point

Debugs op 2800/3800/1562 AP-modellen

Zorg er bij een AP-zijkwestie voor dat u alle WLC-show opdrachten en logbestanden verzamelt voordat u AP-zijlogbestanden verzamelt en aan SR hecht.

Volg onderstaande stappen om problemen met betrekking tot gegevens aan clientzijde te debug.

1. Verzamel AP tonen opdrachten: (2-3 maal, vóór en na afloop van de tests)

toonklok

term len 0

term mon

toontechiek

demonstreren

tonen controllers nss status

zie ip - tunnelmateriaal

Indien CWA-probleem zich voordoet, verzamelt u naast de opdrachten voor het bovenste gedeelte ook de onderstaande blogs. Hieronder vindt u opdrachten die één keer voor en na het uitvoeren van de test moeten worden verzameld.

vanaf de client toegangslijsten laten zien van alle <client-mac>

vanaf de auteur alle <client-mac> tonen met toegangslijsten

ip-toegangslijsten tonen

controller d [0/1]-client tonen

capwap-cli

technische ondersteuning tonen

2. AP-debug (filter per MAC-adres)

Clientdatapath-problemen:

debug dot11 client datapath eapol addr <mac>

debug dot11 client datapath dhcp-adres <mac>

debug dot11 client datapath arp addr <mac>

ClientAP-sporen:

*vanaf een client-overtrekken adres toevoegen <mac>
configuratie van ap client-Tracker uitvoerconsole-log*

vanaf een client-overtrekken filter insluiten

configuratie van ap client-overtrekken filtertest

vanaf client-overtrekken

term mon

vrijstelling 0 0

CWA-kwesties:

filmpje van kapWAP client avc all debug

debug capwap client

client <client-mac>

adres <mac> van info op klantniveau debug dot11

debug van dot11-gebeurtenissen op clientniveau, adres <mac>

debug van flexverbinding pmk

Sommige problemen die kunnen worden gezuiverd door gebruik onder debugs

1. DHCP-detectieberichten op switch niet zien
2. Draadloze client die DHCP-aanbiedingen niet terugkrijgt. DHCP-ontdekking wordt waargenomen bij "debug IP-snooping Packet"-logs
3. Verzamel de pakketvastlegging op de poort die is aangesloten op de AP, de uplink poort en de poort die is aangesloten op de DHCP-server aan de fusiekant.

Debugs/Show opdrachten die mogelijk zijn

1. Controleer op Cisco DNA Center of SSID's is toegewezen aan IP-pool
2. Controleer of WLAN is ingeschakeld op WLC
3. Controleer of radio's zijn ingeschakeld en zowel 802.11a- als 802.11b-netwerken zijn ingeschakeld

AP online

Traditionele methode/stappen: (Rekening houdend met AP VLAN bereik heeft optie 43 of optie 60 gericht op WLC)

1. Selecteer Verificatie als "Geen verificatie"
2. Configureer Infra_VN met AP IP-pool en Default_VN met draadloze client-IP-pool
3. Edge-interfacepoorten configureren waar APs zijn aangesloten op Infra_VN
4. Zodra AP de IP krijgt en zich bij WLC voegt, zal het in de inventaris van het apparaat worden ontdekt.
5. Selecteer AP en wijs aan specifieke plaats en voorziening AP toe.
6. Zodra voorziening is ingesteld, wordt AP toegewezen aan AP-groep die is gemaakt tijdens het toevoegen van WLC aan Fabric.

Plug and Play/Zero Touch AP Provisioning (rekening houdend met AP VLAN-bereik heeft optie 43, gericht op Cisco DNA-centrum)

AP Debugs

DHCP-debugs

Fabric Edge-zijde:

Debugs in te schakelen:

IP-pakketten voor snuffelen

debug van IP-communicatie

Monster logbestand bijgevoegd hieronder.