Wireless Frequently Asked Questions and Troubleshooting Software Defined Access on Cisco DNA Center Version 1.1 and 1.2

Inhalt

Referenzdokumente veröffentlicht auf Cisco.com

- Leitfäden zur Wireless-Konfiguration für jede Version

- SD Wireless Deployment Guide

- Best Practice-Leitfaden für Wireless-Lösungen

- Technische Referenzdokumente für Wireless-Netzwerke

- Kompatibilitätsmatrix für SDA

- Benutzerhandbücher für Cisco DNA Center für jede Version

Befehlsreferenz für Fabric on Control Node, Edge Node, Wireless LAN Controller (WLC) und Access Point (AP)

Steuerungsknoten

- show lisp instance-id <L2 ap instance id> Ethernet-Server **MAC-Endgerätezuordnung (EID)**
- show lisp instance-id <L3 ap instance id> ipv4 server **IP to EID Mapping**
- show lisp instance-id 8188 Ethernet-Server address-Resolution **MAC to IP Mapping für eine bestimmte Instanz-ID**
- show lisp site
Edge-Knoten
- show lisp instance-id <L2 ap instance id> ethernet database wlc
- show lisp instance-id <L2 client instance id> ethernet database wlc
- Übersicht über Access-Tunnel anzeigen
WLC
- FabricMap-Übersicht anzeigen
- Fabric-Übersicht anzeigen
- FabricMap-Serverübersicht anzeigen
Access Point
- show ip tunnel fabric

AireOS WLC-Konfig.-Push vom Cisco DNA Center nach Bereitstellung (Hinweis: Verwenden der Referenz als 3504 WLC)

show radius summary after WLC Provisioning

```
(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
Name/RadiusRegionString
---  ----  ---------------  ------  --------  ----  --------  -------  ------------------------
------------------------------
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
```

Der WLAN-Konfigurationspush von wird unter "show wlan summary" angezeigt.

```
(sdawlc3504) >show wlan summary

Number of WLANs..... 7

WLAN ID  WLAN Profile Name / SSID                                                    Status
Interface Name        PMIPv6 Mobility
-------  ------------------------------------------------------------------------  --------  ----
---------------  --------------
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-Konfig.-Push vom Cisco DNA Center nach dem Hinzufügen von WLC zur Fabric

Wie kann überprüft werden, ob Map Server erreichbar ist?

Fabric Map-Server-Zusammenfassung nach dem Hinzufügen von WLC zur Fabric anzeigen

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

MS-IP     Connection status

--------------------------------

192.168.4.45    UP

192.168.4.66    UP
```

Debuggen der Fabric Map-Server-Verbindung

Die Konnektivität der Kontrollebene (Control Plane, CP) kann aus verschiedenen Gründen ausfallen oder ausfallen.

1. Wenn CP ausgefallen ist. (was in diesem Fall nicht der Fall ist)

2. Zwischenknoten, die nach unten gehen und WLC mit CP verbinden, z. B. Fusion-Router.

3. Wenn die CP-Verbindung zum WLC aufgrund einer unterbrochenen Verbindung ausfällt. Dabei kann es sich um WLC zum unmittelbaren Nachbarn oder CP zum unmittelbaren Nachbarn zum WLC handeln.

show Fabric Map-Server im Detail

show Fabric TCP create history <Map-Server IP>

Debugger, die weitere Informationen bereitstellen können

debuggen Fabric lisp map-server tcp enable

Wie kann überprüft werden, ob Fabric aktiviert ist, und welche Ausgabe sollte erwartet werden?

Fabric-Zusammenfassung nach dem Hinzufügen von WLC zur Fabric anzeigen

```
(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 reguested ...................... 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
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
```

Der WLAN-Konfigurationspush aus dem Cisco DNA Center wird unter "show Fabric WLAN summary" angezeigt, nachdem WLC der Fabric hinzugefügt und der Client-IP-Pool dem Fabric Wireless LAN (WLAN) unter Provivision > Fabric > Host Onboarding zugewiesen wurde.

Fabric-WLAN-Zusammenfassung nach Fabric-Bereitstellung anzeigen

```
(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
```

Prozess für den Austausch von WLCs, während Hochverfügbarkeit (HA) über das Cisco DNA Center konfiguriert wird

Führen Sie die Aktivität im Wartungsfenster aus. Die Konfiguration eines neuen WLC in einem HA-Paar über das Cisco DNA Center kann heute nicht ohne Entfernung des primären WLC aus der Fabric erreicht werden.

1. Stellen Sie sicher, dass sich der zu ersetzende WLC im Standby-Modus befindet. Falls nicht, führen Sie einen manuellen Switchover durch, und stellen Sie ihn in den Standby-Modus.
2. Deaktivieren der HA-Funktion im Cisco DNA Center von der Bereitstellungsseite
3. Wenn die HA-Funktion deaktiviert ist, wird der WLC automatisch aus dem Bestand entfernt.
4. Tauschen Sie den WLC physisch aus, und konfigurieren Sie grundlegende Voraussetzungen für den neuen WLC manuell.
5. Entdecken Sie den neuen WLC im Cisco DNA Center
6. Entfernen Sie den primären WLC aus der Fabric, die sich bereits im Cisco DNA Center befand. (Ohne diesen Schritt wird die Konfiguration der HA-Funktion mit einem neuen WLC fehlerhaft und fällt über das Cisco DNA Center aus.)
7. Konfigurieren Sie HA erneut mithilfe der neuen WLC- und Redundanzmanagement-IPs. [Beide WLCs werden neu geladen]
8. Führen Sie eine manuelle Re-Synchronisierung vom Bestand auf dem primären WLC durch, oder warten Sie auf den nächsten Re-Synchronisierungszyklus, um die Informationen im Cisco DNA Center zu aktualisieren. Nach Abschluss dieses Vorgangs wird der neu hinzugefügte WLC aus dem Bestand verschwinden und unter Hohe Verfügbarkeit als Standby angezeigt.
9. WLC wieder zu Fabric hinzufügen

KAFFEATEN

CSCvn24661 Cisco DNA-Center: WLC HA kann nicht gepaart werden, wenn einer der WLC bereits Teil einer Fabric ist

Problemumgehung:

1. Manuelle Konfiguration von WLC HA über CLI. Die Leistung wird nicht beeinträchtigt.

[HINWEIS: Kann HA nicht mehr über Cisco DNA Center konfigurieren oder deaktivieren]

2. Deaktivieren Sie Fabric über das Cisco DNA Center, wie in den oben beschriebenen Schritten empfohlen. [HINWEIS: Dies führt zu doppelt so hohen Ausfallzeiten, einmal während der Deaktivierung von Fabric und zweitens während der HA-Konfiguration]

Debuggen von Wireless-Problemen

Debuggen von AP-Join/Access Tunnel-Formation

1. Überprüfen Sie, ob der Access Point eine IP-Adresse erhält.

   show ip dhcp snooping-Bindung → Am Fabric Edge

   Wenn keine IP-Adresse für angeschlossene AP-Schnittstelle angezeigt wird, aktivieren Sie die folgenden Debugging-Funktionen auf dem Switch, und überprüfen Sie, ob der Access Point IP erhält oder nicht.

      debug ip dhcp snooping paket

      debug ip dhcp snooping event

   Beispiel für eine Protokolldatei im Anhang unten →

   Beispiel:

   Floor_Edge-6#sh ip dhcp Snooping-Bindung
   VLAN-Schnittstelle vom Typ MacAddress IPAddress Lease(sec)-Typ
   — — — — — — — —
   0C:75:BD:0D:46:60 182.10.50.7 670544 DHCP-Snooping 1021 GigabitEthernet1/0/7 → ***AP-Schnittstelle sollte über eine IP-Schnittstelle verfügen***

2. Überprüfen Sie, ob AP dem WLC beitritt.

   show ap summary → Auf WLC

   show ap join stat summary → Auf WLC anzeigen

   Wenn der Access Point noch nie dem WLC beigetreten ist, aktivieren Sie das folgende Debugging auf dem WLC.

      Debug-CAWAP-Ereignisse aktivieren

      Debug Capwap-Fehler aktivieren

3. Wenn AP CAPWAP bildet, aber keine Zugriffstunnel zwischen AP und Switch gebildet werden, führen Sie bitte die folgenden Prüfungen durch

Schritt 1: Verfügen APs in WLC über RLOC-IPs oder nicht. Wenn nicht, überprüfen Sie Buchstabe a unten.

   a) Um die Ausfallsicherheit des Fabric-Kontrollebenenprotokolls zu erhöhen, ist es

wichtig, dass **in der globalen Routing-Tabelle jedes Fabric-Knotens eine bestimmte Route zum WLC vorhanden ist**. Die Route zur IP-Adresse des WLC sollte entweder in das untergeordnete IGP-Protokoll an der Grenze umverteilt oder an jedem Knoten statisch konfiguriert werden. Das heißt, der WLC sollte nicht über die Standardroute erreichbar sein.

Schritt 2: Wenn die Access Points im WLC die richtigen RLOCs anzeigen und unter "Übersicht anzeigen" die RLOC-Anfrage mit RLOC vollständig erhalten ist, überprüfen Sie die folgenden Schritte.

b) Check on Control Plane Node, *"show lisp instance-id <L2 ap instance id> ethernet server"* → Dieser sollte Base Radio MAC for AP enthalten.

Überprüfen Sie den Fabric Edge-Knoten *"show lisp instance-id <L2 ap instance id> ethernet database wlc"* → Dieser sollte Base Radio MAC für AP und nicht die Ethernet-MAC des AP enthalten.

Wenn über 2 Befehle nicht die MAC-Adresse des APs mit Basisfunk anzeigen und die Zugriffstunnel nicht gebildet sind. Aktivieren Sie "debug lisp control plane all" auf Kontrollebene, und suchen Sie bei der Protokollierung nach Base Radio MAC. [**HINWEIS: "debug lisp control plane all" auf Kontrollebene ist wirklich chatty, deaktivieren Sie bitte die Konsolenprotokollierung, bevor Sie die Debug-Ebene aktivieren.]**

Wenn wie unten ein Authentifizierungsfehler auftritt, überprüfen Sie den Authentifizierungsschlüssel zwischen dem WLC- und CP-Knoten.

7. Dez. 17:42:01.655: LISP-0: MS Site EID IID 8188 prefix any-mac SVC_VLAN_IAF_MAC site_uci, fehlgeschlagene Authentifizierung für spezifischere 2c0b.e9c6.ec80/48

7. Dez. 17:42:01.659: LISP-0: Erstellung einer zuverlässigen Registrierungsmeldung, die für die IID 8188 EID 2c0b.e9c6.ec80/48 zurückgewiesen wurde, Ablehnungscode: Authentifizierungsfehler/2.

Überprüfung des Authentifizierungsschlüssels in der Fabric-Konfiguration zwischen WLC und CP.

Auf WLC, bitte unter Controller auf GUI prüfen → Fabric Configuration → Control Plane → (Pre Shared Key)

Aktivieren Sie auf dem CP den Switch mithilfe von sh running-config. | b Map-Server-Sitzung

CP#sh running-config | b Map-Server-Sitzung
map-server session passive-open WLC
Website_uci
description map-server konfiguriert von apic-em
authentication-key uci (Stellen Sie sicher, dass der Pre-shared Key auf WLC mit diesem Authentifizierungsschlüssel auf dem CP übereinstimmt) [HINWEIS: Im Allgemeinen wird dieser Schlüssel vom Cisco DNA Center weitergegeben. Ändern Sie ihn daher nur, wenn Sie ihn benötigen und wissen Sie, was auf CP/WLC konfiguriert ist.]

4. Allgemeine Prüfungen und Anzeigen von Befehlen für Access-Tunnel.

a) Zugriffstunnel-Zusammenfassung anzeigen

```
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) show platform software fed switch active ifm interfaces access-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#
```

Wenn die Access-Tunnel unter Befehl b) höher sind als a), ist dies ein Problem. In diesem Fall wurden die Fed-Einträge vom Fabric Edge nicht korrekt gelöscht. Daher gibt es im Vergleich zu IOS mehrere Access-Tunnel-Einträge auf der Fed. Vergleichen Sie Dest IP nach Ausführung von Befehl c). Wenn mehrere Access-Tunnel dieselbe Ziel-IP gemeinsam nutzen, liegt das Problem bei der Programmierung.

c) show platform-software-fed switch active ifm if-id <each AP IF-ID> [HINWEIS: Jede IF-ID kann vom vorherigen Befehl abgerufen werden.]

```
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) show platform software access-tunnel switch active R0

```
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
```

show platform software access-tunnel switch active R0 statistics

```
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) show platform software access-tunnel switch active 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
```

show platform software access-tunnel switch active F0 statistics

```
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) show platform software object-manager switch active f0 statistics

```
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) show platform software object-manager switch active f0 ausstehend-update

show platform software object-manager switch active f0 ausstehend-ack-update

show platform software object-manager switch active f0 error-object

5. Ablaufverfolgungen und Debugs, die gesammelt werden müssen.

a) Archivprotokolle sammeln, bevor Ablaufverfolgungen/Debuggen aktiviert werden

Request Platform Software Trace Archiv Ziel-Flash:<Dateiname>

```
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) Erhöhung des Protokollierungspuffers und Deaktivierung der Konsole

```
Floor_Edge-6(config)#logging buffered 214748364
Floor_Edge-6(config)#no logging console
```

c) Ablaufverfolgungen festlegen

set plattform software trace forward switch active R0 access-tunnel verbose
set plattform software trace forward switch active F0 access-tunnel verbose
set plattform software trace feed switch active ifm_main debug
Festlegen der Plattform-Software Trace Feed Switch active access_tunnel verbose

set platform software trace forward-manager switch active F0 aom verbose

d) Debugger aktivieren

debug l2lisp all
debug lisp control plane all

e) Port der "shutdown"-Schnittstelle, an dem der Access Point angeschlossen ist

f) Archiv-Protokolle wie Schritt a mit einem anderen Dateinamen sammeln

g) Umleiten der Protokolldatei in Flash

Floor_Edge-6#Show-Protokollierung | Flash umleiten:<Dateiname>

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

Clientdebuggen

Das Debuggen von Wireless-Clients auf SDA FEW kann kompliziert werden.

Bitte befolgen Sie den unten stehenden Workflow, um ein Gerät nach dem anderen zu entfernen.

1. WLC

2. Fabric-Edge

3. Access Point (beim Debuggen auf Fabric Edge-Punkten zum AP)

4. Knoten "Zwischengeschalteter Knoten/Border". (Bei Datenpfadproblemen)

5. Knoten "Kontrollebene". (Bei Problemen mit dem Steuerungspfad)

WLC-Debuggen

Bei Problemen mit der Client-Konnektivität beginnen Sie mit dem Debuggen, indem Sie Informationen über WLC sammeln, die Show-Befehle und Debugger enthalten.

AireOS WLC-Anzeigebefehle

show run-config

Showtechnik

show wlan summary

show wlan <id> —> Erfassen Sie diese Ausgabe für alle SSIDs, mindestens 1 für funktionierende und nicht funktionierende SSIDs

Fabric-Zusammenfassung anzeigen

Übersicht über Fabric Map Server anzeigen

Kundenzusammenfassung anzeigen

show client detail <mac_id>

AireOS WLC-Debug-Befehle

debug client <mac1> —> Client assoc, Roaming, debugs.

Debug Fabric Client detail enable —> Dadurch werden Informationen Fabric-Registrierungsnachrichten bereitgestellt.

Fabric Edge-Debuggen

Nach dem Debuggen auf dem WLC und der Feststellung, dass für den Client keine Probleme mit dem Control-Plane-Pfad vorliegen. Der Client wechselt von Assoc, Authentifizierung und Ausführungsstatus mit korrektem SGT-Tagging oder AAA-Parametern, fahren Sie mit diesem Schritt fort, um das Problem weiter zu isolieren.

Eine weitere zu überprüfende Sache ist, dass die Access-Tunnel-Programmierung korrekt ist, wie im Abschnitt zum Debuggen von AP beschrieben.

Befehle zur Überprüfung anzeigen

Finden Sie die L2-lisp-Instanz-ID von (zeigen Sie Client-Details <mac_id> von oben an)

show lisp instance-id <L2_LISP> ethernet database wlc —> Diese listet alle mit dem WLC verbundenen Clients für die spezifische L2-lisp-Instanz-ID auf. Die Anzahl der Quellen muss mit der Anzahl der Kontrollebenen-Knoten im Netzwerk übereinstimmen.

show lisp instance-id <L2_LISP> ethernet database wlc <client mac in h.h.h> —> Hier werden Details für den jeweiligen Client angezeigt.

Geräteverfolgungsdatenbank anzeigen | i Vl —> Spezifische SVI suchen, in der der Client verbunden ist und vorhanden sein muss.

Geräteverfolgungsdatenbank anzeigen | i <mac> —> Suchen Sie nach dem Clienteintrag, wobei das richtige VLAN, die richtige Schnittstelle, der richtige Status und das richtige Alter zu berücksichtigen sind.

show mac address table dynamic vlan <VLAN-ID> —> Der Eintrag für die MAC-Adresstabelle sollte mit der Datenbank für die Geräteverfolgung übereinstimmen. Falls ja, überprüfen Sie die MAC-Adresseingabe in der FED.

show ip dhcp snooping binding vlan <vlan_where_client_is_connected>

show ip arp vrf <VN>

show mac address table vlan <vlan_where_client_is_connected>

show platform software fed switch active matm macTable vlan <vlan_where_client_is_connected> —> Wenn dies korrekt ist, erfolgt die Programmierung für den Wireless-Client auf dem lokalen Switch ordnungsgemäß.

show platform software matm switch active F0 mac <mac_id>

Debug-Befehle im Fabric Edge

Erfassung von Fed-Traces bei Problemen bei der Programmierung des Client-Eintrags im Fabric Edge Es gibt zwei Möglichkeiten, das Gleiche zu tun, nachdem unten Debugger aktiviert wurde.

Debuggt und legt Befehle fest, die unabhängig von der Methode aktiviert werden müssen.

Set Platform Software Trace Feed Switch Aktive All-Module Emergency
Festlegen der Plattform-Software Trace-Feed-Switch active l2_fib_entry Ausführliches
Festlegen der Plattform-Software Trace-Feed Switch active l2_fib_adj verbose
set plattform software trace feed switch active inject verbots
set plattform software trace feed switch active matm verbose

debuggen (Deaktivieren Sie die Konsolenprotokollierung, und erhöhen Sie den Protokollierungspuffer)

Nachverfolgung von Debuggeräten

debug lisp control plane all

Debug-Plattform für alle

Debug-Match

Methode 1: Sammeln Sie aktive Ablaufverfolgungsprotokolle für einen bestimmten Client, nachdem Sie das Debuggen aktiviert haben [Hinweis, wenn das DHCP-Problem auftritt, verwenden Sie diese Methode nicht]

Warten Sie, bis das Problem reproduziert wurde.

debug plattform condition mac <mac-id> control plane
Start der Debug-Plattform
Stopp der Debug-Plattform
request plat soft trace filter binary wireless context mac <mac-id>

Leiten Sie die Konsolenprotokolle nach der Reproduktion des Problems zu blinken um.

Methode 2: Erfassen von Archiv-Ablaufverfolgungsprotokollen nach Aktivieren von Debuggen

Warten Sie, bis das Problem reproduziert wurde.

Anforderungsplattform Software Trace Archiv

Erfassen Sie die Datei decodieren die Protokolle und analysieren Sie eingespeist, iOS, Dateiprotokolle für das Client-Mac.

Leiten Sie die Konsolenprotokolle nach der Reproduktion des Problems zu blinken um.

Debuggen von Access Points

Debuggen auf 2800/3800/1562 AP-Modellen

Bei Problemen mit APs sollten Sie alle Anzeigebefehle und Protokolle des WLC sammeln, bevor Sie AP-seitige Protokolle sammeln und an SR anhängen.

Führen Sie die folgenden Schritte aus, um datenbezogene Probleme auf Clientseite zu debuggen.

1. AP-Anzeigebefehle sammeln: (2-3 Mal vor und nach Abschluss der Tests)

Schauuhr

term len 0

Zitronen

Showtechnik

Anzeigeprotokollierung

show controller ns stats show controller nstatus

show ip tunnel Fabric

Bei CWA-Problemen sammeln Sie zusätzlich zu den Top-Befehlen auch die folgenden Protokolle. Die folgenden Befehle müssen vor und nach Abschluss des Tests einmal gesammelt werden.

show client access-listen pre-auth all <client mac>

show client access-lists - post-auth all <client mac>

show ip access-lists

show controller d [0/1] Client

show capwap cli detail rcb

show tech support

2. AP-Debug (Filter pro MAC-Adresse)

Clientdatapath-Probleme:

debug dot11 client datapath eapol addr <mac>

debug dot11 client datapath dhcp addr <mac>

debug dot11 client datapath arp addr <mac>

Client-AP-Ablaufverfolgungen:

config ap client-trace-Adresse hinzufügen <mac>
config ap client-trace output console-log enable

config ap client-trace filter alle aktivieren

config ap client-trace filterprobe deaktivieren

config ap client-trace start

Zitronen

exec-timeout 0 0 0

CWA-Probleme:

debugccapwap client avc all

debugccapwap client acl

debugclient <client mac>

info address <mac> auf Client-Ebene debug dot11

debug dot11 client level events address <mac>

Debug Flexconnect pmk

Problem mit dem Client-DHCP-Debuggen

Einige Probleme, die mit den folgenden Debuggen gedebuggt werden können

1. DHCP-Erkennungsmeldungen auf dem Switch werden nicht angezeigt.

2. Wireless-Client erhält kein DHCP-Angebot zurück. DHCP Discover wird unter "debug ip dhcp snooping packet" protokolliert

3. Sammeln Sie die Paketerfassung an dem mit dem AP verbundenen Port, dem Uplink-Port und dem Port, der mit dem DHCP-Server auf der Fusionsseite verbunden ist.

Debugger/Anzeigen von Befehlen, die

1. Überprüfen Sie das Cisco DNA Center, ob die SSID dem IP-Pool zugewiesen ist.

2. Überprüfen Sie, ob WLAN auf dem WLC aktiviert ist.

3. Überprüfen Sie, ob Funkmodule aktiviert sind und sowohl 802.11a- als auch 802.11b-Netzwerke aktiviert sind.

AP-Integration

Traditionelle Methoden/Schritte: (Im Hinblick auf AP-VLAN-Bereich weist Option 43 oder Option 60 auf WLC hin)

1. Wählen Sie Authentifizierung als "Keine Authentifizierung" aus.

2. Konfigurieren Sie Infra_VN mit dem AP-IP-Pool und Default_VN mit dem Wireless-Client-IP-Pool.

3. Konfigurieren von Edge-Schnittstellenports, an denen APs mit Infra_VN verbunden sind

4. Sobald der Access Point die IP erhält und dem WLC beitritt, wird er im Gerätebestand erkannt.

5. Wählen Sie den Access Point aus, weisen Sie ihn einem bestimmten Standort zu, und stellen Sie den Access Point bereit.

6. Nach der Bereitstellung wird der Access Point der AP-Gruppe zugewiesen, die beim Hinzufügen von WLC zu Fabric erstellt wurde.

Plug-and-Play-/Zero-Touch-AP-Bereitstellung (Option 43 verweist auf das Cisco DNA Center, wenn der AP-VLAN-Bereich berücksichtigt wird)

AP-Debugger

DHCP-Debugger

Fabric-Edge-Seite:

Zu aktivierende Debugger:

debug ip dhcp snooping paket

debug ip dhcp snooping event

Beispiel für eine Protokolldatei im Anhang unten.