通過DNA實施軟體定義的無線接入

目錄

簡介

本檔案介紹如何為與支援光纖的WLC和存取Cisco DNA上的LAP相關的無線技術實作SDA.

必要條件

需求

思科建議您瞭解以下主題：

- 9800無線LAN控制器(WLC)組態
- 輕量型存取點(LAP)
- 思科DNA

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 9800-CL WLC Cisco IOS® XE版本17.9.3
- 思科存取器：9130AX、3802E、1832I
- Cisco DNA版本2.3.3.7

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

軟體定義存取

軟體定義訪問通過網路建立並自動實施安全策略，包括動態規則和自動分段，允許終端使用者控制和配置使用者連線到其網路的方式。SD-Access與連線的每個終端建立初始信任級別，並持續監控該終端以重新驗證其信任級別。如果端點行為不正常或檢測到處理，終端使用者可以立即對其進行控制並在發生違規之前採取行動，從而降低業務風險並保護它的資源。完全整合的解決方案，易於在新網路和已部署網路上部署和配置。

SD-Access是思科的一項技術，是傳統園區網路的演變，它通過使用軟體定義網路(SDN)元件提供基於意圖的網路(IBN)和中央策略控制。

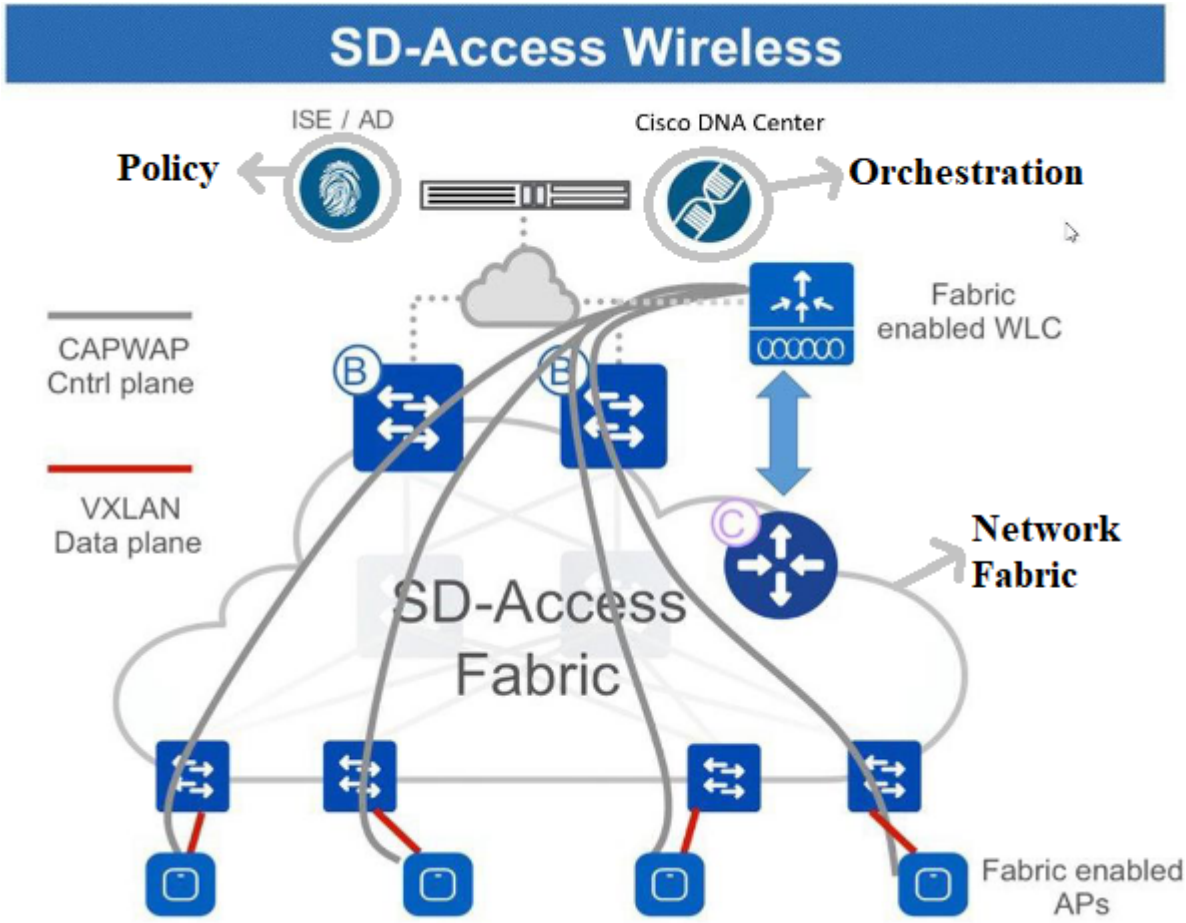
SD-Access的三個以網路為中心的支柱：

1. 網路交換矩陣：支援可程式設計重疊和虛擬化的網路本身抽象化。網路交換矩陣支援有線和無線訪問，允許它託管多個邏輯網路，這些網路彼此分割並根據業務意圖定義。
2. 協調：Cisco DNA是SDA的協調器引擎。Cisco DNA的功能與SDN控制器類似。它在交換矩陣中實施策略和配置更改。還整合了支援網路設計並通過DNA保證支援即時網路遙測操作和效能分析的工具。Cisco DNA的作用是協調網路交換矩陣，以提供策略更改和網路意圖，以實現安全性、服務品質(QoS)和微分段。
3. 原則：身份服務引擎(ISE)是定義網路策略的工具。ISE組織如何將裝置和節點分割為虛擬網路。ISE還定義可伸縮組標籤(SGT)，訪問裝置在進入交換矩陣時使用該標籤對使用者流量進行分段。SGR負責實施ISE定義的微分段策略。

SDA建立在集中協調的基礎上。思科DNA作為可程式設計協調引擎、ISE作為策略引擎以及新一代可程式設計交換機的組合使其成為比以往任何產品都更靈活、更易於管理的交換矩陣系統。

附註：本檔案專門介紹SD-Access無線。

網路交換矩陣由以下元素組成：

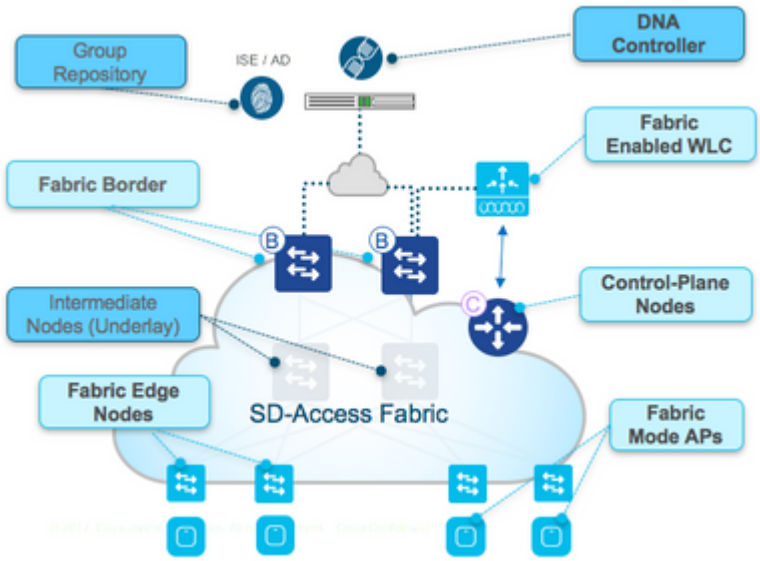


網路交換矩陣的元素

與交換矩陣的無線整合為無線網路帶來多項優勢，例如：解決簡化問題、跨物理位置擴展子網實現移動性；以及採用在有線和無線域上一致的集中策略進行微分段。它還可以使控制器在繼續充當無線網路的集中服務和控制平面的同時，擺脫資料平面轉發職責。因此，無線控制器可擴充性實際上得到了提高，因為它不再需要像FlexConnect模型那樣處理資料平面流量。

SD-Access無線架構

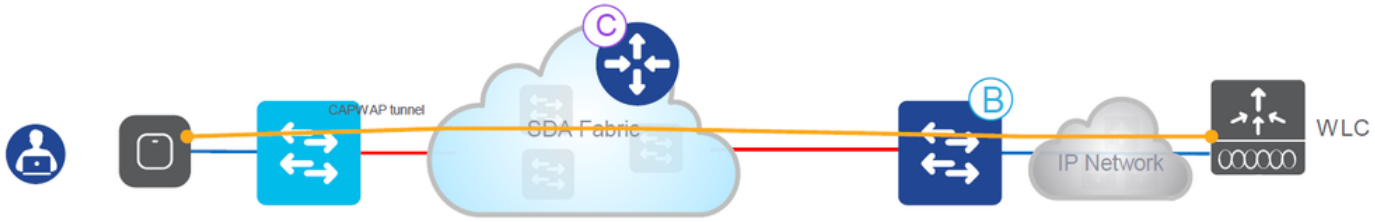
概觀



SDA概述

有兩種主要的SDA支援的無線部署模式：

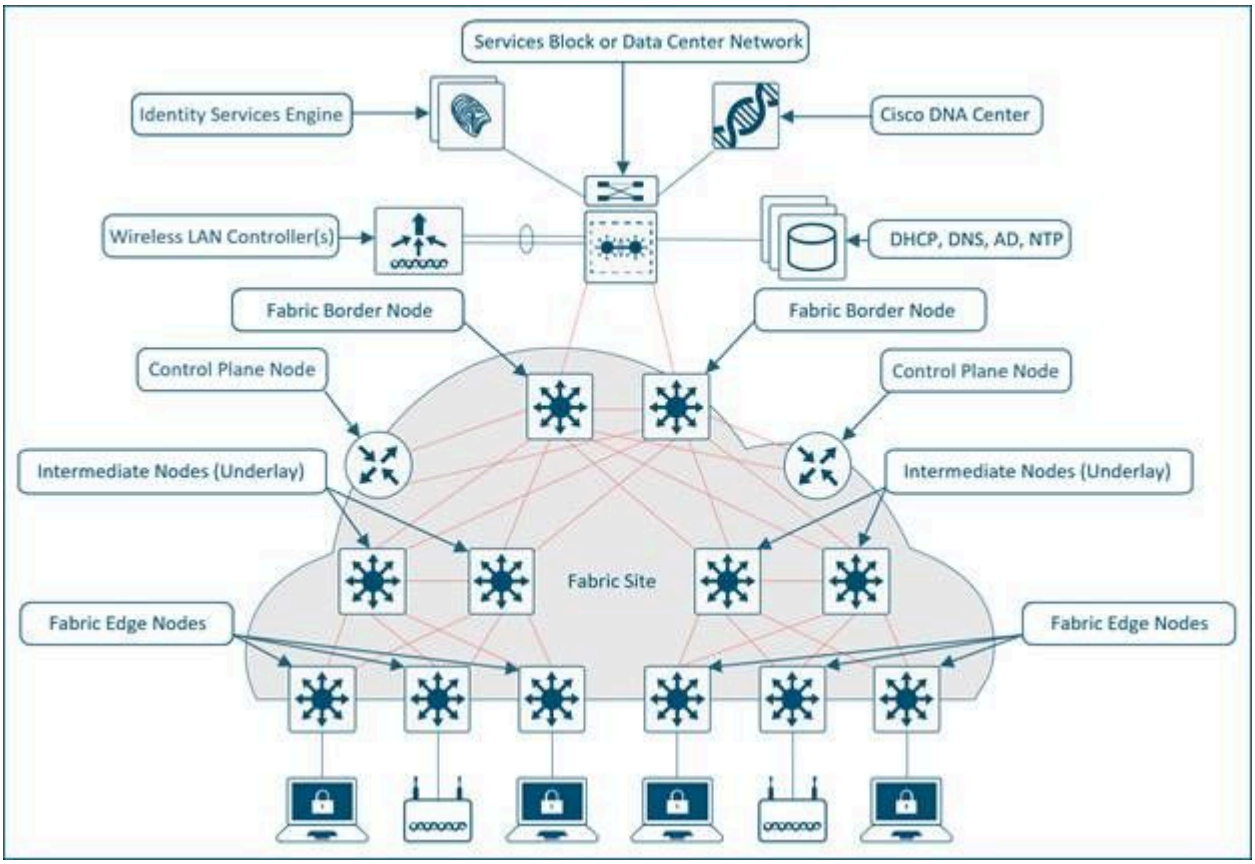
一種是機頂盒(OTT)方法，即連線交換矩陣有線網路頂部的傳統CAPWAP部署。SDA交換矩陣將CAPWAP控制和資料平面流量傳輸到無線控制器：



Over-The-Top方法

在此部署模型中，SDA交換矩陣是無線流量的傳輸網路（通常在遷移中部署）。 AP的工作方式與經典本地模式非常相似：capwap控制平面和資料平面都終止於控制器上，這意味著控制器不會直接參與交換矩陣。當有線交換機首次遷移到SDA交換矩陣，但無線網路尚未準備好進行完全交換矩陣重疊整合時，通常使用此模式。

其他部署模式為完全整合的SDA模式。無線網路完全整合到交換矩陣並參與重疊，它允許不同的WLAN成為不同虛擬網絡(VN)的一部分。 無線控制器僅管理CAPWAP控制平面（用於管理AP），而CAPWAP資料平面不會進入控制器：



完全整合的SDA模型

無線資料平面的處理方式與有線交換機類似 — 每個AP將資料封裝在VXLAN中，並將其傳送到交換矩陣邊緣節點，然後通過該交換矩陣將其傳送到另一個邊緣節點。無線控制器必須配置為交換矩陣控制器，這是對其正常操作的修改。

支援交換矩陣的控制器與交換矩陣控制平面通訊，它註冊第2層客戶端MAC地址和第2層虛擬網路識別符號(VNI)資訊。AP負責與無線端點進行通訊，並通過封裝和解除封裝流量來協助VXLAN資料平面。

SDA角色和術語

網路交換矩陣由以下元素組成：

- 控制平面節點：這是位置對映系統（主機資料庫），是位置分隔符協定(LISP)控制平面的一部分，用於管理終端標識(EID)到位置關係（或裝置關係）。 控制平面可以是提供控制平面功能的專用路由器，也可以與其他交換矩陣網路元素共存。

- 交換矩陣邊界節點：通常是在外部網路和SDA交換矩陣之間的邊界起作用的路由器，為交換矩陣中的虛擬網路提供路由服務。它將外部第3層網路連線到SDA交換矩陣。

- 交換矩陣邊緣節點：交換矩陣內將非交換矩陣裝置（例如交換機、AP和路由器）連線到SDA交換矩陣的裝置。這些節點使用虛擬可擴展LAN(VXLAN)建立虛擬重疊隧道和VN，並將SGT強加於交換矩陣繫結的流量。交換矩陣邊緣兩端的網路都位於SDA網路內部。它們將有線終端連線到SD-Access交換矩陣。

- 中間節點：這些節點位於SDA交換矩陣的核心內，連線到邊緣或邊界節點。中間節點只需將

SDA流量作為IP資料包轉發，而不知道涉及多個虛擬網路。

- 交換矩陣WLC:已啟用交換矩陣且參與SDA控制平面但不處理CAPWAP資料平面的無線控制器。
- 交換矩陣模式AP:支援交換矩陣的接入點。無線流量在AP上採用VXLAN封裝，這允許通過邊緣節點將其傳送到交換矩陣。
- Cisco DNA(DNAC):適用於軟體定義存取(SDA)網狀架構重疊網路的企業SDN控制器，負責自動化和保證任務。它還可以用於構成底層網路裝置的某些自動化和相關任務（即與SDA無關）。
- ISE：身分識別服務引擎(ISE)是一個增強型策略平台，可以服務於各種角色和功能，尤其是身份驗證、授權和記帳(AAA)伺服器的角色和功能。ISE通常與Active Directory(AD)進行互動，但使用者可以在本地配置，也可以在ISE本身進行較小部署配置。

附註：控制平面是SDA架構的關鍵基礎設施部分，因此建議採用彈性方式部署。

底層網路和重疊網路

SDA架構利用光纖技術，支援在實體網路（底層網路）上執行的可程式化虛擬網路（重疊網路）。

交換矩陣是重疊。

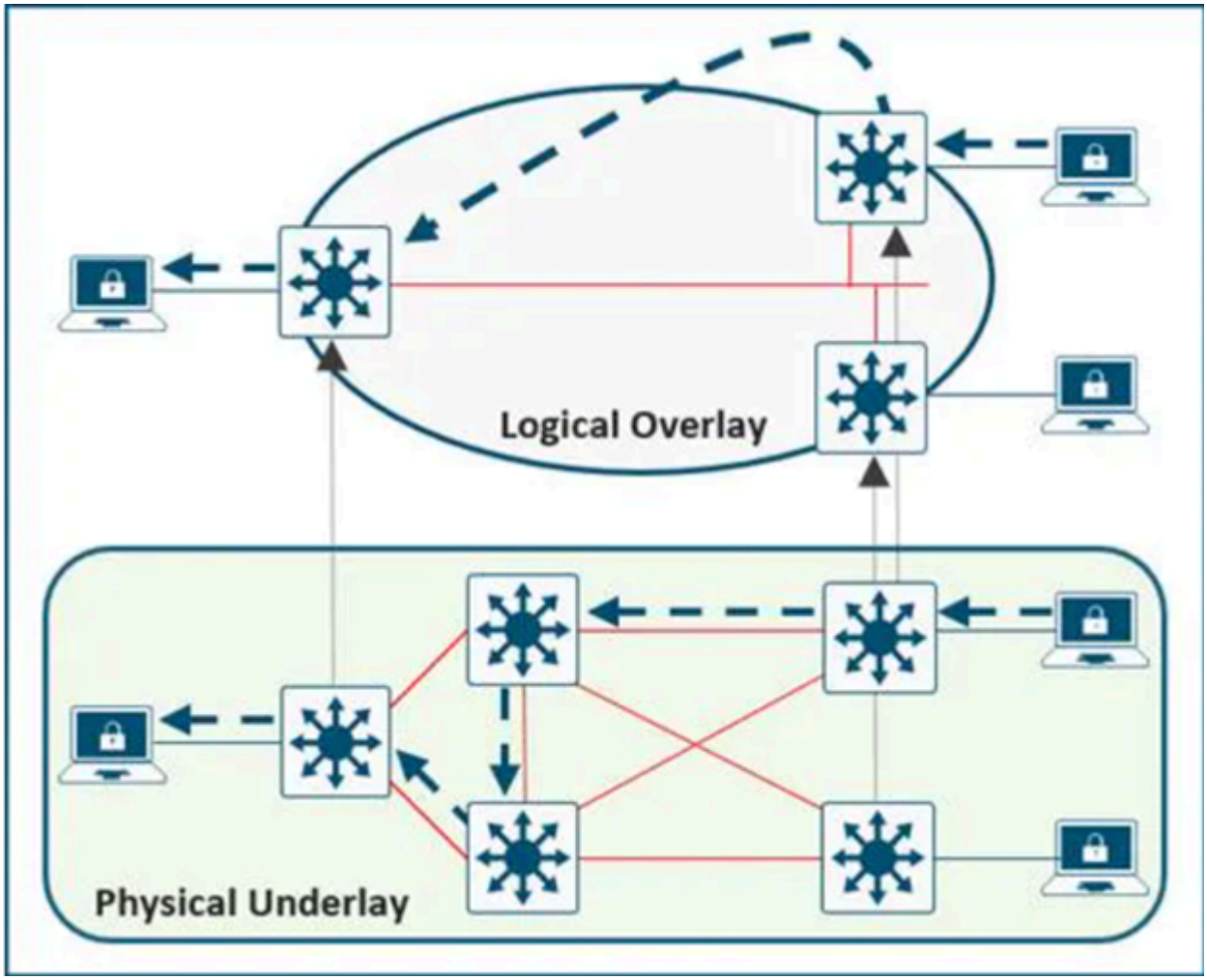
重疊網路是一種邏輯拓撲，用於虛擬連線裝置，構建於任意物理底層拓撲之上。它使用備用轉發屬性來提供底層未提供的其他服務。它在底層上建立，用於建立一個或多個虛擬化和分段網路。由於重疊由軟體定義，因此可以非常靈活的方式連線它們而不受物理連線的限制。這是一種實施安全策略的簡單方法，因為重疊可以可程式設計為具有單個物理出口點（交換矩陣邊界節點），並且可以使用一個防火牆來保護其後的網路（無論這些網路是否可以定位）。 重疊使用VXLAN封裝流量。VXLAN封裝整個第2層訊框，以便透過底層傳輸，其中每個重疊網路均由VXLAN網路識別碼(VNI)識別。 重疊結構往往比較複雜，在部署的新虛擬網路或實施安全策略時需要大量的管理員開銷。

網路重疊示例：

- GRE、mGRE
- MPLS、VPLS
- IPSec、DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI

底層網路由用於部署SDA網路的物理節點（如交換機、路由器和無線AP）定義。底層的所有網路元素都必須使用路由協定建立IP連線。雖然底層網路不太可能使用傳統的訪問、分佈及核心模式，但它必須使用設計完善的第3層基礎，該層基礎可提供強大的效能、可擴充性和高可用性。

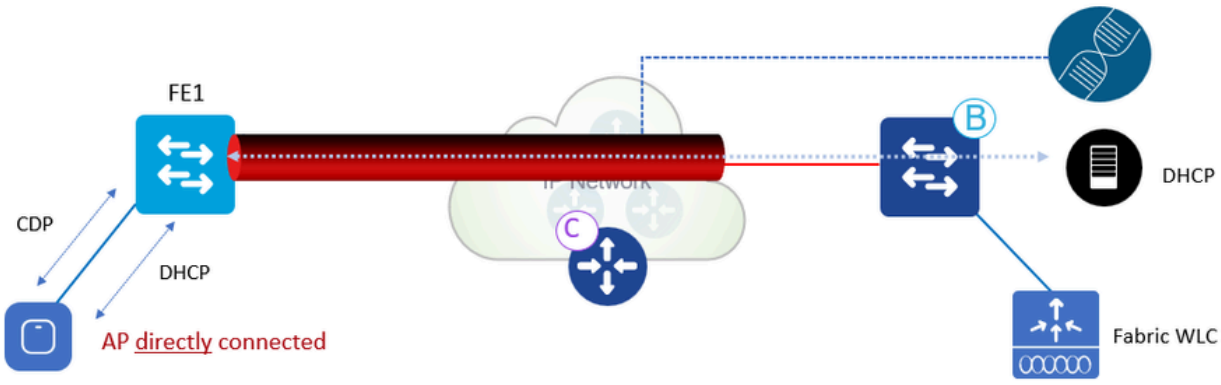
附註：SDA在底層網路中支援IPv4，在重疊網路中支援IPv4和/或IPv6。



底層網路和重疊網路

基本工作流程

AP加入



AP加入工作流

AP加入工作流：

1.管理員在INFRA_VN的DNAC中配置AP池。思科DNA在所有交換矩陣邊緣節點上預調配配置到自動板載AP。

2. AP已插入並通電。Fabric Edge通過CDP發現它是AP，並應用宏將交換機埠分配到正確的VLAN（或介面模板）。

3. AP通過重疊中的DHCP獲取IP地址。

4.交換矩陣邊緣註冊AP IP地址和MAC(EID)並更新控制平面(CP)。

5. AP使用傳統方法學習WLC的IP。交換矩陣AP作為本地模式AP加入。

6. WLC檢查其是否支援交換矩陣（第2波或第1波AP）。

7.如果Fabric支援AP，WLC會查詢CP以瞭解AP是否連線到Fabric。

8.控制平面(CP)使用RLOC回覆WLC。這意味著AP已連線到交換矩陣，並且顯示為「Fabric enabled」。

9. WLC為CP中的AP執行L2 LISP註冊（即AP「特殊」安全客戶端註冊）。 這用於將重要的後設資料資訊從WLC傳遞到交換矩陣邊緣。

10.響應此代理註冊，控制平面(CP)通知Fabric Edge並傳遞從WLC接收的後設資料（表示它是AP和AP IP地址的標誌）。

11. Fabric Edge處理該資訊，它瞭解其是AP並建立到指定IP的VXLAN隧道介面(最佳化：交換器端已準備好使用者端加入)。

debug/show命令可用於驗證和驗證AP加入工作流。

控制平面

debug lisp control-plane all

show lisp instance-id <L3例項id> ipv4服務器（必須顯示由連線AP的邊緣交換機註冊的AP IP地址。）

show lisp instance-id <L2 instance id> ethernet server（必須顯示AP無線電以及ethernet mac-address、由WLC註冊的AP無線電以及由AP連線的邊緣交換機的ethernet mac。）

邊緣交換機

debug access-tunnel all

debug lisp control-plane all

顯示存取通道摘要

show lisp instance < L2例項id>乙太網資料庫wlc接入點(必須在此處顯示AP無線電mac。)

WLC

show fabric ap summary

WLC LISP調試

set platform software trace wncd chassis active r0 lisp-agent-api debug

set platform software trace wncd chassis active r0 lisp-agent-db debug

set platform software trace wncd chassis active r0 lisp-agent-fsm debug

set platform software trace wncd chassis active r0 lisp-agent-internal debug

set platform software trace wncd chassis active r0 lisp-agent-lib debug

set platform software trace wncd chassis active r0 lisp-agent-lispmsg debug

set platform software trace wncd chassis active r0 lisp-agent-shim debug

set platform software trace wncd chassis active r0 lisp-agent-transport debug

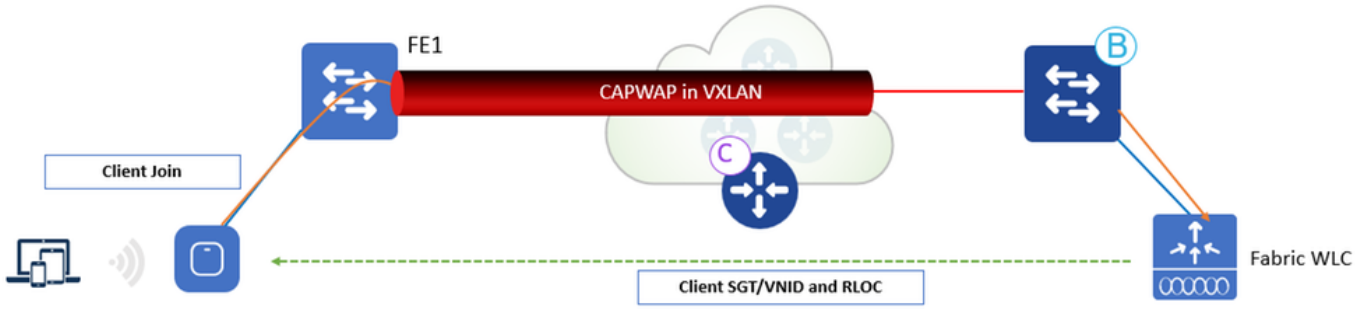
set platform software trace wncd chassis active r0 lisp-agent-ha debug

set platform software trace wncd chassis active r0 ewlc-infra-evq debug

存取點

show ip tunnel fabric

客戶端板載



客戶端板載工作流

客戶端板載工作流：

1.客戶端對啟用交換矩陣的WLAN進行身份驗證。WLC從ISE獲取SGT，使用客戶端L2VNID更新AP，並使用RLOC IP更新SGT。WLC知道來自內部資料庫的AP的RLOC。

2. WLC代理在CP中註冊客戶端L2資訊；這是LISP修改的消息，用於傳遞其他資訊，如客戶端SGT。

3.交換矩陣邊緣由CP通知，並將第2層中的客戶端MAC新增到轉發表，然後根據客戶端SGT從ISE獲取策略。

4.客戶端發起DHCP請求。

5. AP使用L2 VNI資訊將其封裝在VXLAN中。

6.交換矩陣邊緣將第2層VNID對映到VLAN介面並在重疊中轉發DHCP（與有線交換矩陣客戶端相同）。

7.客戶端從DHCP接收IP地址。

8. DHCP監聽（和/或靜態的ARP）會觸發交換矩陣邊緣將客戶端EID註冊到CP。

debug/show命令可用於驗證和驗證客戶端板載工作流。

控制平面

debug lisp control-plane all

邊緣交換機

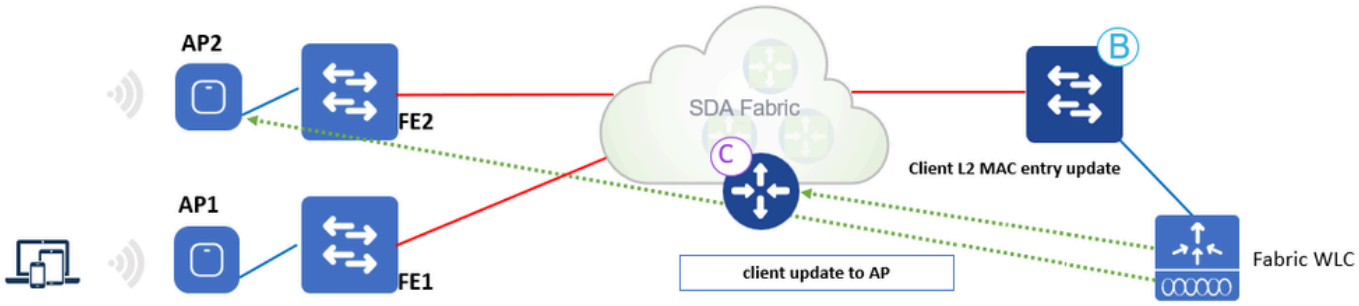
debug lisp control-plane all

debug ip dhcp snooping packet/event

WLC

對於LISP通訊，調試與AP加入相同。

客戶端漫遊



客戶端漫遊工作流

客戶端漫遊工作流：

1.客戶端在FE2上漫遊到AP2（交換機間漫遊）。AP通知WLC。

2. WLC使用客戶端資訊(SGT、RLOC)更新AP上的轉發表。

3. WLC使用新的RLOC交換矩陣邊緣2更新CP中的第2層MAC條目。

4. CP然後通知：

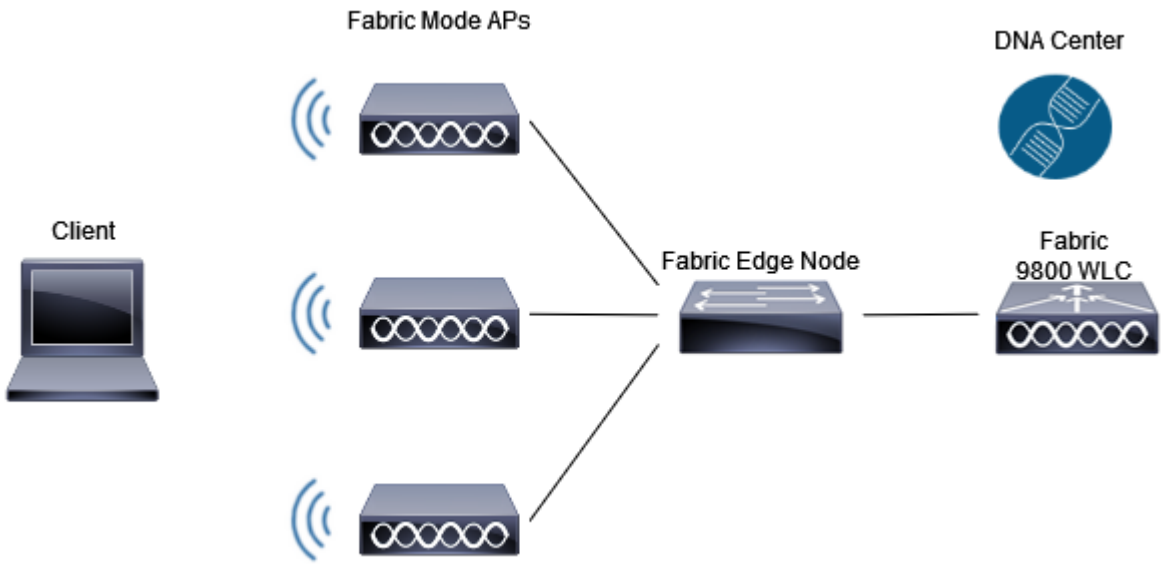
- 交換矩陣邊緣FE2（漫遊到交換機）將客戶端MAC新增到指向VXLAN隧道的轉發表中。
- 交換矩陣邊緣FE1（從交換機漫遊）為無線客戶端進行清理。

5. Fabric Edge在收到流量後更新CP資料庫中的L3條目(IP)。

6.漫遊是第2層，因為交換矩陣邊緣2具有相同的VLAN介面（任播GW）。

設定

網路圖表



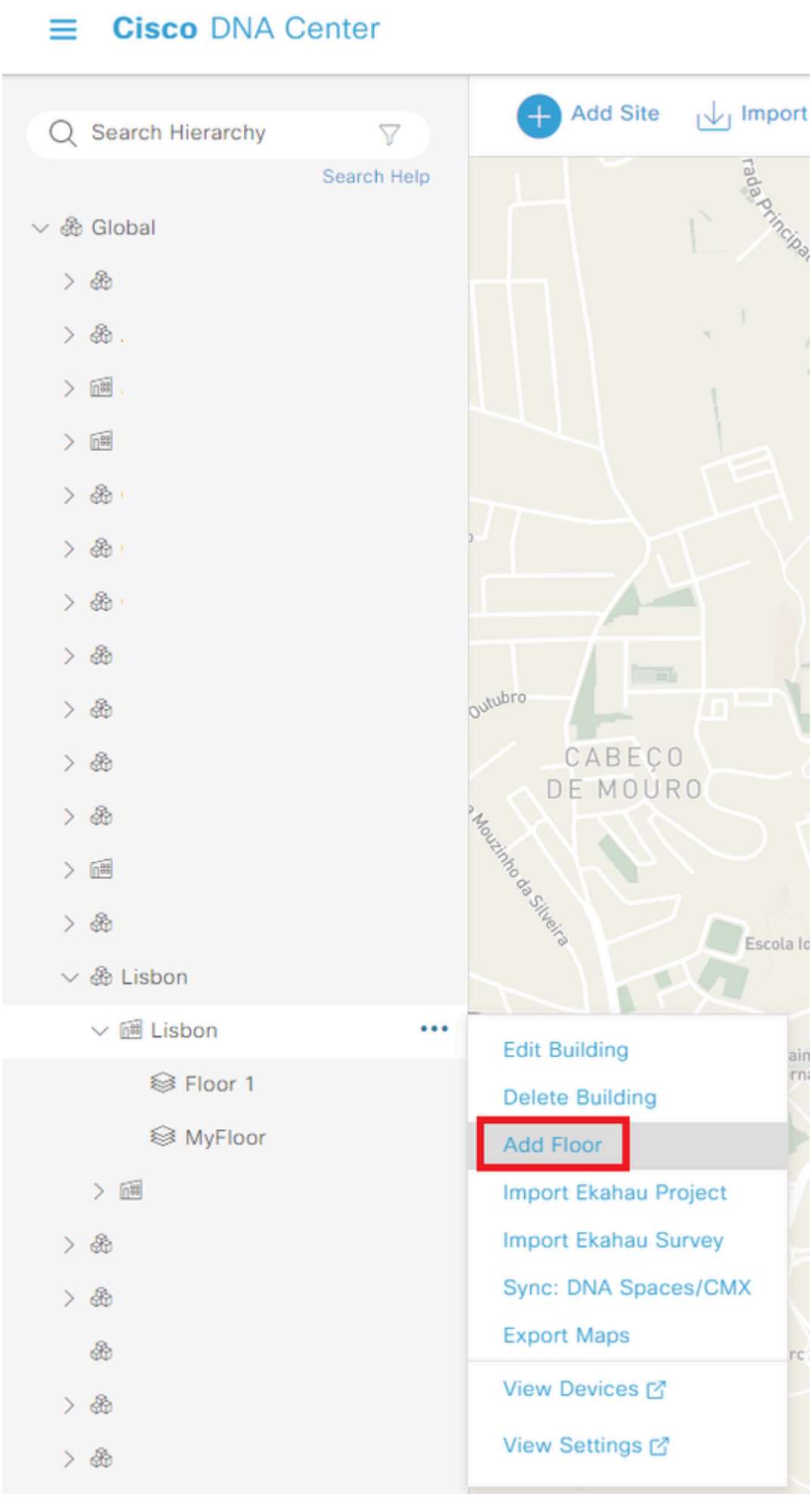
網路圖表

Cisco DNA中的WLC發現和布建

新增WLC

步驟1。導覽至要新增WLC的位置。您可以新增新的建築/樓層。

導覽至Design > Network Hierarchy，然後輸入building/floor，或者您可以建立新樓層，如下圖所示：

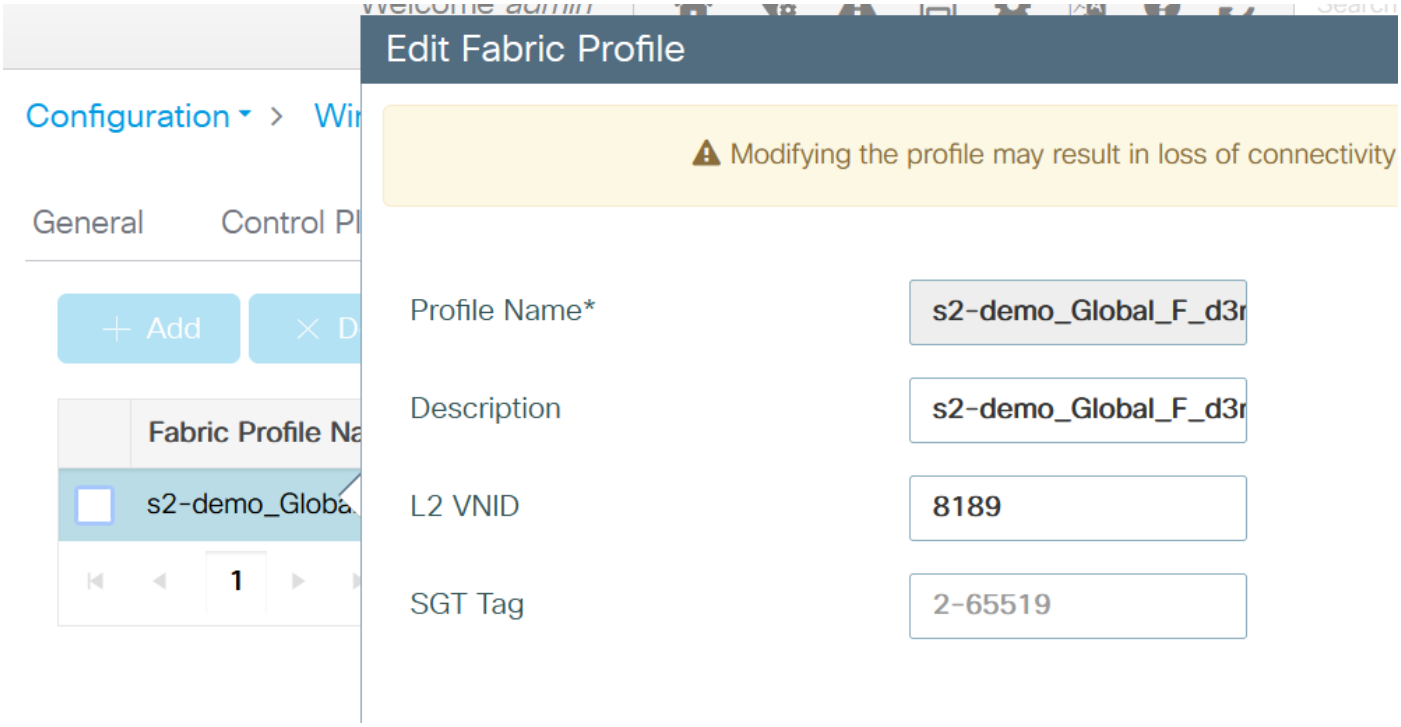


建立新樓層

步驟3.增加樓層。您也可以上傳地板上的平面的影象。

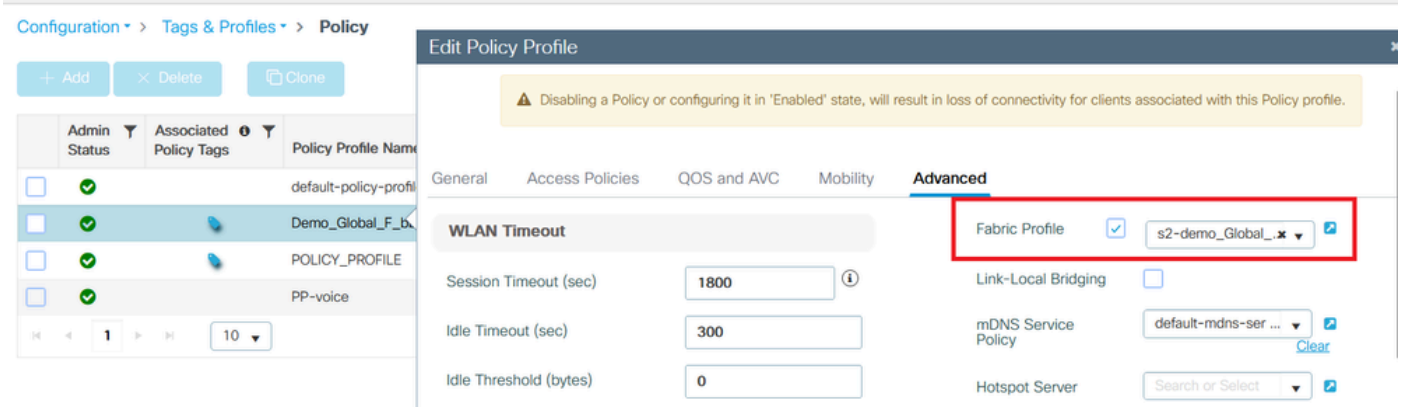
的交換矩陣配置檔案新增到所選池，並將策略配置檔案對映到交換矩陣配置檔案，為交換矩陣啟用該配置檔案。

在WLC GUI側，導覽至Configuration > Wireless > Fabric > Profiles。



交換矩陣配置檔案

步驟6.導覽至Configuration > Tags & Profiles > Policy。驗證對映到策略配置檔案的交換矩陣配置檔案：



策略上配置的交換矩陣配置檔案

驗證

驗證WLC和Cisco DNA上的光纖組態

在WLC CLI上：

WLC1# show tech

WLC1# show tech wireless

控制平面配置：

router lisp

 locator-table default

 locator-set WLC

  172.16.201.202

  exit-locator-set

  !

 map-server session passive-open WLC

 站點site_uci

  說明從Cisco DNA-Center配置的對映伺服器

  authentication-key 7 <Key>

CB1-S1#sh lisp會話

VRF預設會話總數：9，已建立：5

對等狀態開啟/關閉輸入/輸出

172.16.201.202:4342向上3d07h 14/14

WLC組態：

無線交換矩陣

wireless fabric control-plane default-control-plane

ip address 172.16.2.2 key 0 47aa5a

WLC1# show fabric map-server summary

MS-IP連線狀態

172.16.1.2up

WLC1# show wireless fabric summary

交換矩陣狀態：已啟用

控制平面：

名稱IP地址金鑰狀態

---

default-control-plane 172.16.2.2 47aa5a Up

在WLC GUI上，導覽至Configuration > Wireless > Fabric，然後確認交換矩陣狀態是否為Enabled。

導覽至Configuration > Wireless > Access Points。從清單中選擇一個AP。驗證交換矩陣狀態是否為「Enabled（啟用）」。

在Cisco DNA上，導覽至Provision > Fabric Sites，確認您是否有交換矩陣站點。在該交換矩陣站點上，導航到交換矩陣基礎架構>交換矩陣，並驗證WLC是否已作為交換矩陣啟用。

疑難排解

客戶端未獲取IP地址

步驟1.檢驗SSID是否為交換矩陣。在WLC GUI上，導覽至Configuration > Tags & Profiles > Policy。選擇策略並導航到高級。驗證是否啟用了Fabric Profile。

步驟2.檢查客戶端是否停滯在IP learn狀態。在WLC GUI上，導覽至Monitoring > Wireless > Clients。驗證客戶端狀態。

步驟3.驗證策略是否需要DHCP。

步驟4.如果流量在AP — 邊緣節點之間本地交換，請收集客戶端連線的AP日誌（客戶端跟蹤）。檢驗DHCP發現是否已轉發。如果沒有DHCP提供到達，則邊緣節點上發生錯誤。如果未轉發DHCP，則AP上出現了問題。

步驟5.您可以收集邊緣節點埠上的EPC以檢視DHCP發現資料包。如果您沒有看到DHCP發現資料包，則問題出在AP上。

未廣播SSID

步驟1.檢驗AP無線電是否關閉。

步驟2.檢查WLAN是否處於開啟狀態並啟用廣播SSID。

步驟3.驗證AP是否啟用了交換矩陣。導覽至Configuration > Wireless > Access Points，選擇一個AP，然後在General索引標籤上可以看到已啟用交換矩陣狀態和RLOC資訊。

步驟4.導覽至Configuration > Wireless > Fabric > Control Plane。驗證是否已配置控制平面（使用IP地址）。

步驟5.導覽至Configuration > Tags & Profiles > Policy。選擇策略並導航到高級。驗證是否啟用了

Fabric Profile。

步驟6.導覽至Cisco DNA，然後重複執行Create SSID和Provision WLC中的步驟。Cisco DNA必須再次將SSID推送到WLC。

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。