

Implementierung von Software-Defined Access für Wireless-Netzwerke mit DNA

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[SD-Access](#)

[SD-Access Wireless-Architektur](#)

[Überblick](#)

[SDA-Rollen und -Terminologie](#)

[Underlay- und Overlay-Netzwerke](#)

[Grundlegende Workflows](#)

[AP-Beitritt](#)

[Client integriert](#)

[Client-Roaming](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[WLC-Erkennung und -Bereitstellung in Cisco DNA](#)

[WLC hinzufügen](#)

[Access Points hinzufügen](#)

[SSID erstellen](#)

[WLC bereitstellen](#)

[Access Points bereitstellen](#)

[Fabric-Standort erstellen](#)

[WLC zur Fabric hinzufügen](#)

[AP-Beitritt](#)

[Client integriert](#)

[Überprüfung](#)

[Überprüfen der Fabric-Konfiguration auf WLC und Cisco DNA](#)

[Fehlerbehebung](#)

[Client erhält keine IP-Adresse](#)

[SSID wird nicht übertragen](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Implementierung von SDA für Wireless-Technologie im Zusammenhang mit Fabric-fähigem WLC und der Zugriff auf LAP über Cisco DNA beschrieben..

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der 9800 Wireless LAN Controller (WLC)
- Lightweight Access Points (LAP)
- Cisco DNA

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 9800-CL WLC Cisco IOS® XE, Version 17.9.3
- Cisco Access Points: 9130AX, 3802E, 1832I
- Cisco DNA Version 2.3.3.7

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

SD-Access

Mit Software-Defined Access werden Sicherheitsrichtlinien im gesamten Netzwerk mit dynamischen Regeln und automatisierter Segmentierung eingerichtet und automatisch durchgesetzt. Endbenutzer können so steuern und konfigurieren, wie die Benutzer eine Verbindung mit ihrem Netzwerk herstellen. SD-Access stellt für alle verbundenen Endgeräte eine anfängliche Vertrauensstufe her und überwacht diese kontinuierlich, um die Vertrauensstufe erneut zu überprüfen. Wenn sich ein Endgerät nicht normal verhält oder eine Bedrohung erkannt wird, kann der Endbenutzer sofort eindämmen und Maßnahmen ergreifen, bevor eine Sicherheitsverletzung stattfindet, das Geschäftsrisiko verringert und die Ressourcen schützt. Vollständig integrierte Lösung, einfache Bereitstellung und Konfiguration in neuen und bereitgestellten Netzwerken

SD-Access ist eine Technologie von Cisco, die eine Weiterentwicklung des traditionellen Campus-Netzwerks darstellt und absichtsbasierte Netzwerkfunktionen (IBN) sowie eine zentrale Richtlinienkontrolle unter Verwendung von SDN-Komponenten (Software-Defined Networking) bietet.

Die drei netzwerkzentrierten Grundpfeiler von SD-Access:

1. Eine Netzwerkstruktur: Es ist eine Abstraktion des Netzwerks, die programmierbare

Overlays und Virtualisierung unterstützt. Die Netzwerk-Fabric unterstützt sowohl kabelgebundenen als auch Wireless-Zugriff und ermöglicht das Hosting mehrerer logischer Netzwerke, die voneinander segmentiert und nach Geschäftszweck definiert sind.

2. Orchestrierung: Cisco DNA ist die Orchestrierungs-Engine von SDA. Cisco DNA funktioniert wie ein SDN Controller. Sie implementiert Richtlinien und Konfigurationsänderungen in der Fabric. Darüber hinaus enthält es ein Tool, das das Netzwerkdesign unterstützt und über DNA Assurance Netzwerkelektrometrie- und Leistungsanalysen in Echtzeit ermöglicht. Die Rolle der Cisco DNA besteht in der Orchestrierung der Netzwerk-Fabric zur Bereitstellung von Richtlinienänderungen und Netzwerkintenz für Sicherheit, Quality of Service (QoS) und Mikrosegmentierung.
3. Richtlinie: Identity Services Engine (ISE) ist das Tool, das Netzwerkrichtlinien definiert. Die ISE organisiert, wie Geräte und Knoten in virtuelle Netzwerke segmentiert werden. Die ISE definiert außerdem skalierbare Group Tags (SGTs), die von Zugriffsgeräten zur Segmentierung des Benutzerdatenverkehrs beim Eintritt in die Fabric verwendet werden. Die SGRs müssen die von der ISE definierte Mikrosegmentierungsrichtlinie durchsetzen.

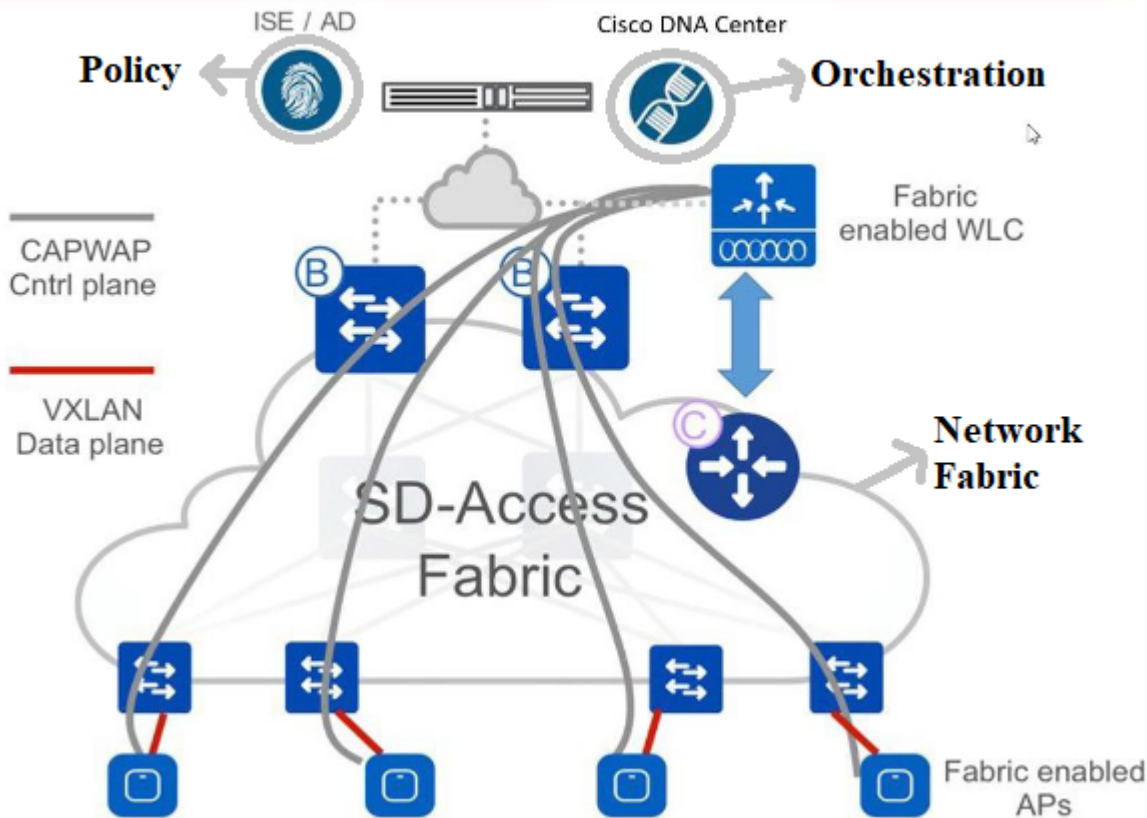
SDA basiert auf zentraler Orchestrierung. Die Kombination aus Cisco DNA als programmierbare Orchestrierungs-Engine, ISE als Richtlinien-Engine und einer neuen Generation programmierbarer Switches macht das Fabric-System weitaus flexibler und verwaltbarer als alles andere.



Anmerkung: Dieses Dokument behandelt speziell SD-Access Wireless.

Die Netzwerk-Fabric besteht aus folgenden Elementen:

SD-Access Wireless

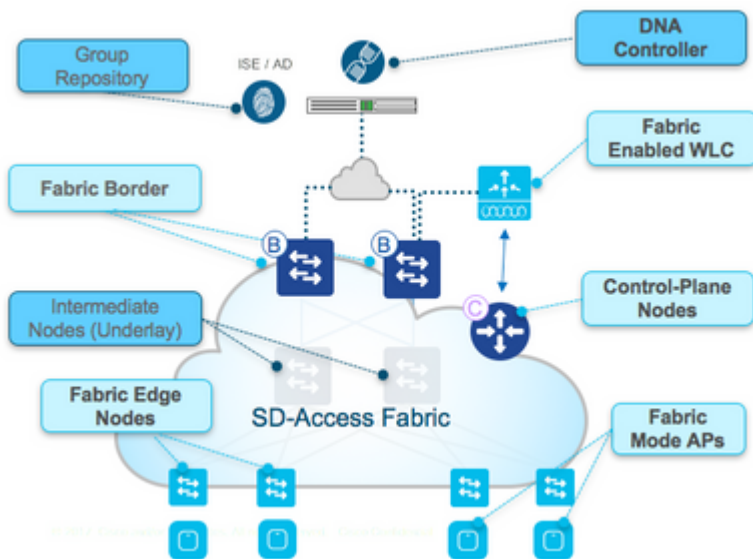


Elemente der Netzwerkstruktur

Die Wireless-Integration in die Fabric bietet u. a. folgende Vorteile für das Wireless-Netzwerk: Berücksichtigung von Vereinfachungen und Mobilität mit ausgedehnten Subnetzen über physische Standorte hinweg; und Mikrosegmentierung mit zentralisierten Richtlinien, die in der gesamten kabelgebundenen und Wireless-Domäne konsistent sind. Darüber hinaus kann der Controller Aufgaben auf der Datenebene weiterleiten, während er weiterhin als zentrale Services- und Kontrollebene für das Wireless-Netzwerk fungiert. Dadurch wird die Skalierbarkeit der Wireless-Controller sogar erhöht, da diese ähnlich wie beim FlexConnect-Modell keinen Datenverkehr auf Datenebene mehr verarbeiten müssen.

SD-Access Wireless-Architektur

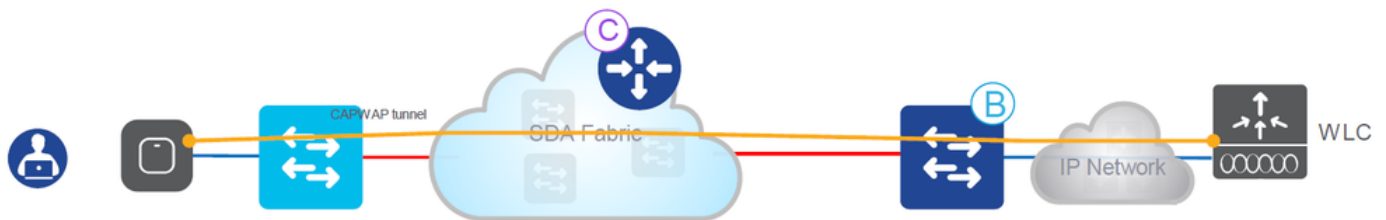
Überblick



SDA - Überblick

Es gibt zwei primäre SDA-unterstützte Wireless-Bereitstellungsmodelle:

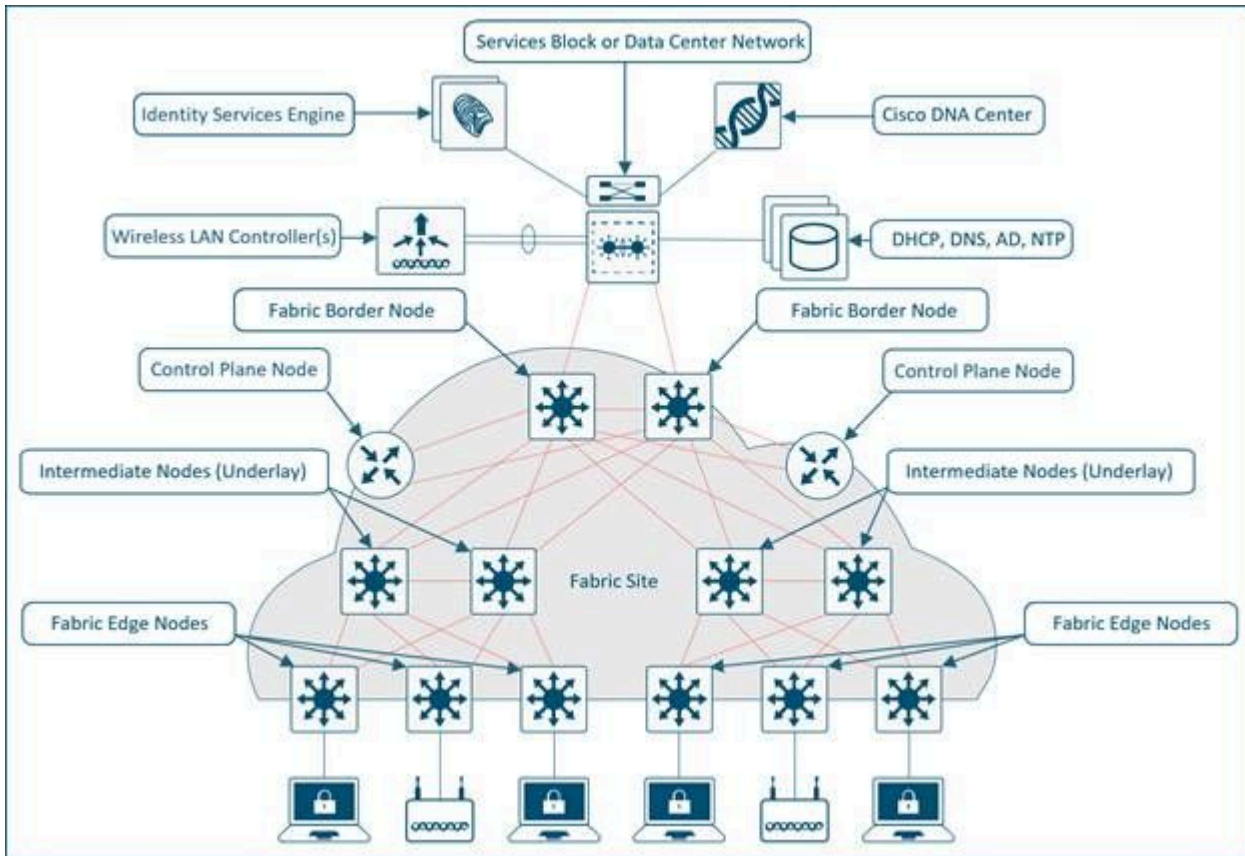
Bei der einen handelt es sich um eine OTT-Methode (Over-the-Top), eine herkömmliche CAPWAP-Bereitstellung, die mit einem kabelgebundenen Fabric-Netzwerk verbunden ist. Die SDA-Fabric transportiert den CAPWAP-Kontroll- und Datenebenenverkehr an den Wireless Controller:



Over-the-Top-Methode

Bei diesem Bereitstellungsmodell ist die SDA-Fabric ein Transportnetzwerk für Wireless-Datenverkehr (ein Modell, das häufig bei Migrationen eingesetzt wird). Der Access Point arbeitet sehr ähnlich wie der klassische lokale Modus: Sowohl die CAPWAP-Kontroll- als auch die Datenebene enden auf dem Controller, d. h. der Controller ist nicht direkt Teil der Fabric. Dieses Modell wird häufig verwendet, wenn kabelgebundene Switches zum ersten Mal in die SDA-Fabric migriert werden, das Wireless-Netzwerk jedoch noch nicht für eine vollständige Fabric-Overlay-Integration bereit ist.

Die anderen Bereitstellungsmodelle sind vollständig integrierte SDA-Modelle. Das Wireless-Netzwerk ist vollständig in die Fabric integriert und nimmt an Overlays teil. So können verschiedene WLANs Teil verschiedener virtueller Netzwerke (VNs) sein. Der Wireless Controller verwaltet nur die CAPWAP-Kontrollebene (zur Verwaltung der APs), und die CAPWAP-Datenebene kommt nicht zum Controller:



Vollständig integriertes SDA-Modell

Die Wireless-Datenebene wird ähnlich behandelt wie kabelgebundene Switches: Jeder WAP kapselt Daten in VXLAN und sendet sie an einen Fabric-Edge-Knoten, wo sie dann über das Fabric an einen anderen Edge-Knoten gesendet werden. Die Wireless-Controller müssen als Fabric-Controller konfiguriert werden, was eine Änderung gegenüber dem normalen Betrieb darstellt.

Fabric-fähige Controller kommunizieren mit der Fabric-Steuerungsebene, registrieren Layer-2-Client-MAC-Adressen und Layer-2-VNI-Informationen (Virtual Network Identifier). Die APs sind für die Kommunikation mit Wireless-Endgeräten zuständig und unterstützen die VXLAN-Datenebene durch Kapselung und Entkapselung des Datenverkehrs.

SDA-Rollen und -Terminologie

Die Netzwerk-Fabric besteht aus folgenden Elementen:

- **Knoten der Kontrollebene:** Hierbei handelt es sich um das Standortzuordnungssystem (Host-Datenbank), das Teil der LISP-Kontrollebene (Location Separator Protocol) ist und die EID-Beziehungen (Endpoint Identity) zu Standorten (oder Gerätebeziehungen) verwaltet. Die Kontrollebene kann entweder ein dedizierter Router sein, der Funktionen der Kontrollebene bereitstellt, oder sie kann mit anderen Elementen des Fabric-Netzwerks koexistieren.
- **Fabric-Randknoten:** In der Regel ein Router, der an der Grenze zwischen externen Netzwerken und der SDA-Struktur arbeitet und Routing-Services für die virtuellen Netzwerke in der Struktur bereitstellt. Sie verbindet externe Layer-3-Netzwerke mit der SDA-Fabric.

- Fabric-Edge-Knoten: Gerät innerhalb der Fabric, das Nicht-Fabric-Geräte wie Switches, APs und Router mit der SDA-Fabric verbindet. Dabei handelt es sich um die Knoten, die die virtuellen Overlay-Tunnel und VNs mit Virtual eXtensible LAN (VXLAN) erstellen und die SGTs dem Fabric-gebundenen Datenverkehr auferlegen. Die Netzwerke auf beiden Seiten des Fabric-Edge befinden sich im SDA-Netzwerk. Sie verbinden kabelgebundene Endgeräte mit der SD-Access-Fabric.
- Zwischenknoten: Diese Knoten befinden sich im Kern der SDA-Fabric und sind mit Edge- oder Border-Knoten verbunden. Die zwischengeschalteten Knoten leiten den SDA-Datenverkehr lediglich als IP-Pakete weiter, ohne zu wissen, dass mehrere virtuelle Netzwerke involviert sind.
- Fabric-WLC: Wireless Controller, der Fabric-fähig ist und an der SDA-Kontrollebene beteiligt ist, die CAPWAP-Datenebene jedoch nicht verarbeitet.
- Fabric-Modus-APs: Fabric-fähige Access Points. Der Wireless-Datenverkehr wird am WAP VXLAN-gekapselt, sodass er über einen Edge-Knoten in die Fabric gesendet werden kann.
- Cisco DNA (DNAC): Der SDN-Controller der Enterprise-Klasse für das SDA-Fabric-Overlay-Netzwerk (Software Defined Access) ist für Automatisierungs- und Sicherheitsaufgaben zuständig. Es kann auch für einige Automatisierungs- und ähnliche Aufgaben für die Netzwerkgeräte genutzt werden, die das Underlay bilden (d. h. nicht SDA-bezogen).
- ISE: Die Identity Services Engine (ISE) ist eine erweiterte Richtlinienplattform, die eine Vielzahl von Rollen und Funktionen bereitstellen kann, nicht zuletzt die des AAA-Servers (Authentication, Authorization and Accounting). Die ISE interagiert in der Regel mit Active Directory (AD), Benutzer können jedoch für kleinere Bereitstellungen lokal sowie auf der ISE selbst konfiguriert werden.



Anmerkung: Die Kontrollebene ist ein wichtiger Infrastrukturbestandteil der SDA-Architektur. Daher wird empfohlen, sie ausfallsicher bereitzustellen.

Underlay- und Overlay-Netzwerke

Die SDA-Architektur nutzt Fabric-Technologie, die programmierbare virtuelle Netzwerke (Overlay-Netzwerke) unterstützt, die in einem physischen Netzwerk (einem Underlay-Netzwerk) ausgeführt werden.

Ein Stoff ist ein Overlay.

Ein Overlay-Netzwerk ist eine logische Topologie zur virtuellen Verbindung von Geräten, die auf einer beliebigen physischen Underlay-Topologie aufbaut. Er verwendet alternative Weiterleitungsattribute, um zusätzliche Services bereitzustellen, die nicht vom Underlay bereitgestellt werden. Sie wird auf der Basis erstellt, um ein oder mehrere virtualisierte und segmentierte Netzwerke zu erstellen. Aufgrund des softwaredefinierten Charakters von Overlays

ist es möglich, diese auf sehr flexible Weise und ohne Einschränkungen der physischen Konnektivität zu verbinden. Dies ist eine einfache Möglichkeit zur Durchsetzung von Sicherheitsrichtlinien, da das Overlay so programmiert werden kann, dass es einen einzigen physischen Austrittspunkt (den Fabric Border Node) hat, und eine Firewall verwendet werden kann, um die Netzwerke dahinter zu schützen (unabhängig davon, ob sie sich befinden). Das Overlay kapselt den Datenverkehr mithilfe von VXLAN. VXLAN kapselt vollständige Layer-2-Frames für den Transport über das Underlay, wobei jedes Overlay-Netzwerk durch einen VXLAN Network Identifier (VNI) identifiziert wird. Overlay-Fabrics sind in der Regel komplex und erfordern einen hohen Administrator-Overhead bei der Bereitstellung neuer virtueller Netzwerke oder bei der Implementierung von Sicherheitsrichtlinien.

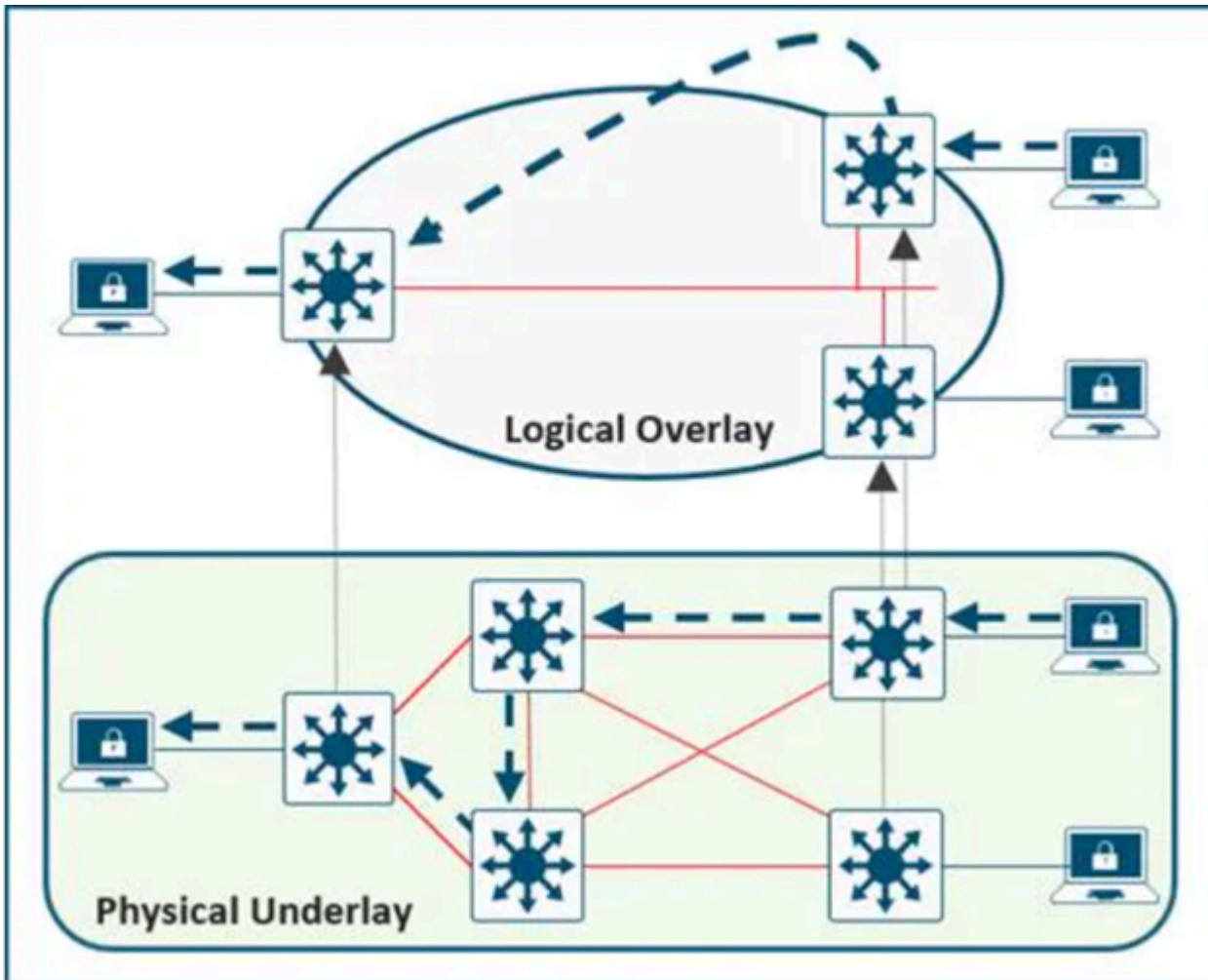
Beispiele für Netzwerk-Overlays:

- GRE, mGRE
- MPLS, VPLS
- IPSec, DMVPN
- CAPWAP
- LISTE
- OTV
- DFA
- ACI

Ein Underlay-Netzwerk wird durch die physischen Knoten wie Switches, Router und Wireless-APs definiert, die für die Bereitstellung des SDA-Netzwerks verwendet werden. Alle Netzwerkelemente des Underlays müssen über ein Routing-Protokoll eine IP-Konnektivität herstellen. Auch wenn das Underlay-Netzwerk wahrscheinlich nicht das herkömmliche Access-, Distribution- und Core-Modell verwendet, muss es eine gut konzipierte Layer-3-Grundlage verwenden, die robuste Leistung, Skalierbarkeit und hohe Verfügbarkeit bietet.



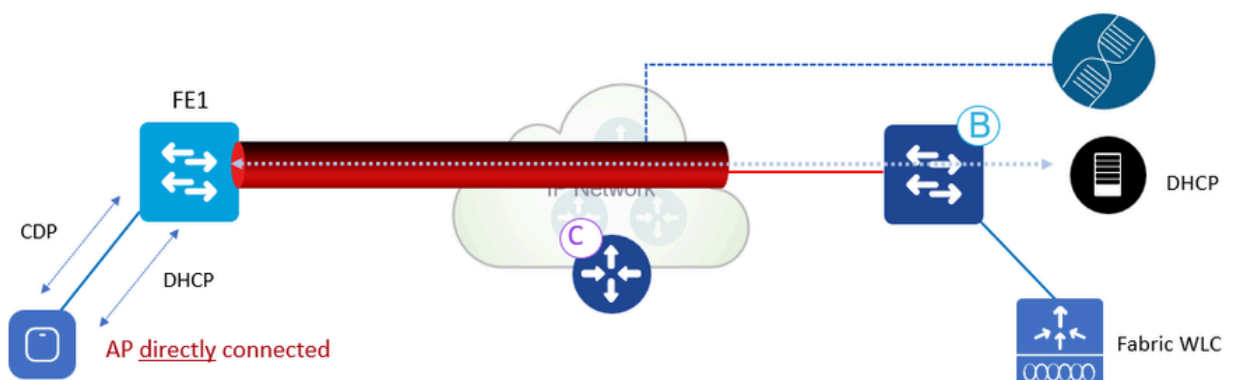
Anmerkung: SDA unterstützt IPv4 im Underlay-Netzwerk und IPv4 und/oder IPv6 in Overlay-Netzwerken.



Underlay- und Overlay-Netzwerke

Grundlegende Workflows

AP-Beitritt



AP-Join-Workflow

AP-Join-Workflow:

1. Admin konfiguriert den AP-Pool in DNAC in INFRA_VN. Cisco DNA stellt auf allen Fabric Edge-

Knoten eine Konfiguration bereit, um APs automatisch zu integrieren.

2. Der Access Point ist angeschlossen und hochgefahren. Fabric Edge erkennt, dass es sich um einen Access Point via CDP handelt, und wendet das Makro an, um dem Switch-Port das richtige VLAN zuzuweisen (oder die Schnittstellenvorlage anzuwenden).

3. AP bekommt eine IP-Adresse via DHCP im Overlay.

4. Fabric Edge registriert die IP-Adresse und MAC (EID) der APs und aktualisiert die Kontrollebene (CP).

5. AP lernt WLCs IP mit traditionellen Methoden. Der Fabric-AP wird als Zugangspunkt im lokalen Modus hinzugefügt.

6. WLC prüft, ob er Fabric-fähig ist (Wave 2- oder Wave 1-APs).

7. Wenn AP für Fabric unterstützt wird, fragt WLC den CP ab, um zu erfahren, ob AP mit Fabric verbunden ist.

8. Control Plane (CP) antwortet auf WLC mit RLOC. Das bedeutet, dass der Access Point mit dem Fabric verbunden ist und als "Fabric-fähig" angezeigt wird.

9. WLC führt eine L2-LISP-Registrierung für AP im CP durch (d. h. die AP-"spezielle" sichere Client-Registrierung). Hiermit werden wichtige Metadateninformationen vom WLC an den Fabric Edge übergeben.

10. Als Reaktion auf diese Proxy-Registrierung benachrichtigt Control Plane (CP) Fabric Edge und übergibt die vom WLC empfangenen Metadaten (Flag, das angibt, dass es sich um einen Access Point und die IP-Adresse des Access Points handelt).

11. Fabric Edge verarbeitet die Informationen, erkennt, dass es sich um einen AP handelt und erstellt eine VXLAN-Tunnelschnittstelle zur angegebenen IP (Optimierung: Switch-Seite ist bereit für den Beitritt von Clients).

Mit den Befehlen debug/show kann der AP-Join-Workflow überprüft und validiert werden.

Steuern Sie Fläche

```
debug lisp control-plane all
```

show lisp instance-id <L3 instance id> ipv4 server (Muss die vom Edge-Switch registrierte AP-IP-Adresse anzeigen, mit der der AP verbunden ist.)

show lisp instance-id <L2 instance id> Ethernet-Server (Muss die AP-Funk- sowie Ethernet-MAC-Adresse, die vom WLC registrierte AP-Funk und die Ethernet-MAC-Adresse des Edge-Switches anzeigen, mit dem der AP verbunden ist.)

Edge-Switch

```
debug access-tunnel all
```

debug lisp control-plane all

Übersicht über den Zugriffstunnel anzeigen

show lisp instance < L2 instance id> ethernet database wlc access-points (Muss den AP-Funk hier anzeigen.)

WLC

Fabric AP-Zusammenfassung anzeigen

WLC LISP-Debugging

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

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 debugging

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

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

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

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

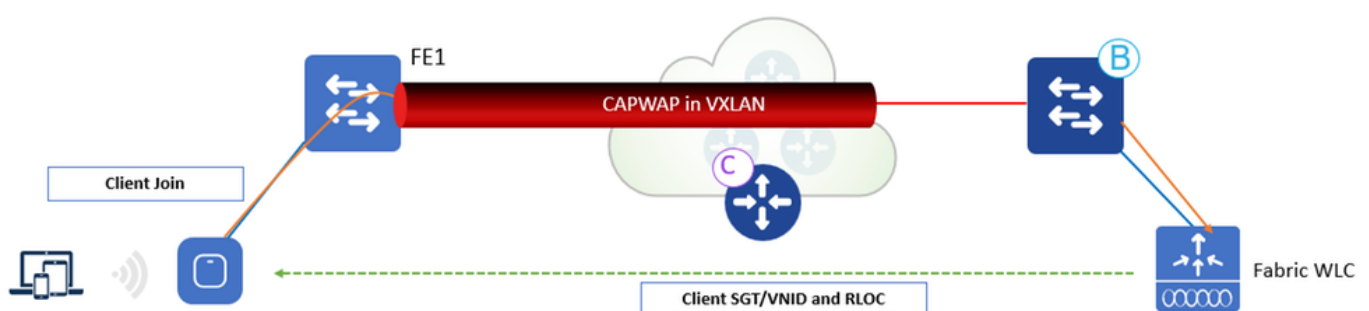
set platform software trace wncd chassis active r0 lisp-agent-ha debug

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

Access Point

IP-Tunnelstruktur anzeigen

Client integriert



Integrierter Client-Workflow

Client-Onboard-Workflow:

1. Der Client authentifiziert sich bei einem Fabric-fähigen WLAN. WLC erhält SGT von der ISE, aktualisiert AP mit dem Client L2VNID und SGT zusammen mit RLOC IP. WLC kennt den RLOC des AP aus der internen Datenbank.
2. WLC-Proxy registriert Client-L2-Info in CP; Diese Nachricht wurde von LISP modifiziert, um zusätzliche Informationen wie das Client-SGT weiterzugeben.
3. Fabric Edge wird vom CP benachrichtigt und fügt der Weiterleitungstabelle Client-MAC in L2 hinzu. Anschließend wird die Richtlinie basierend auf dem Client-SGT von der ISE abgerufen.
4. Der Client initiiert eine DHCP-Anforderung.
5. AP kapselt es in VXLAN mit L2 VNI-Informationen.
6. Fabric Edge weist L2-VNID der VLAN-Schnittstelle zu und leitet DHCP im Overlay weiter (wie bei einem kabelgebundenen Fabric-Client).
7. Der Client erhält eine IP-Adresse von DHCP.
8. DHCP-Snooping (und/oder ARP für statische) löst die EID-Registrierung des Clients durch den Fabric Edge beim CP aus.

Mit den Befehlen debug/show kann der integrierte Client-Workflow überprüft und validiert werden.

Steuern Sie Fläche

```
debug lisp control-plane all
```

Edge-Switch

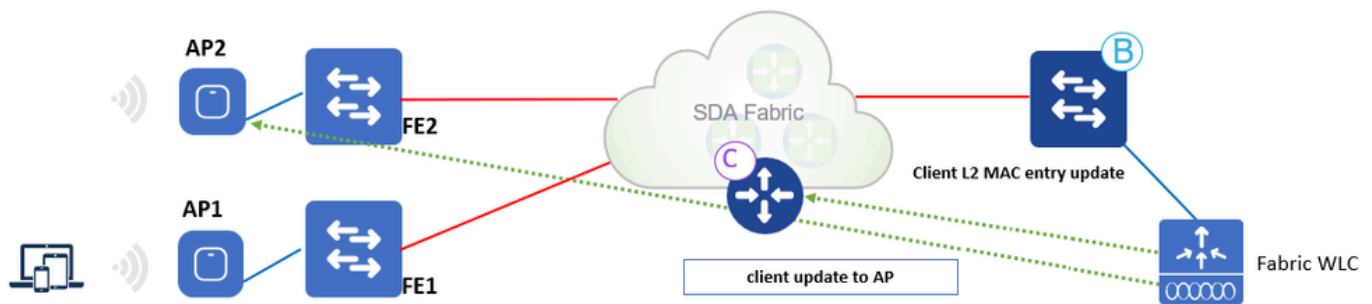
```
debug lisp control-plane all
```

```
debug ip dhcp snooping paket/event
```

WLC

Für die LISP-Kommunikation werden die gleichen Debugging-Anweisungen wie für den AP-Join verwendet.

Client-Roaming



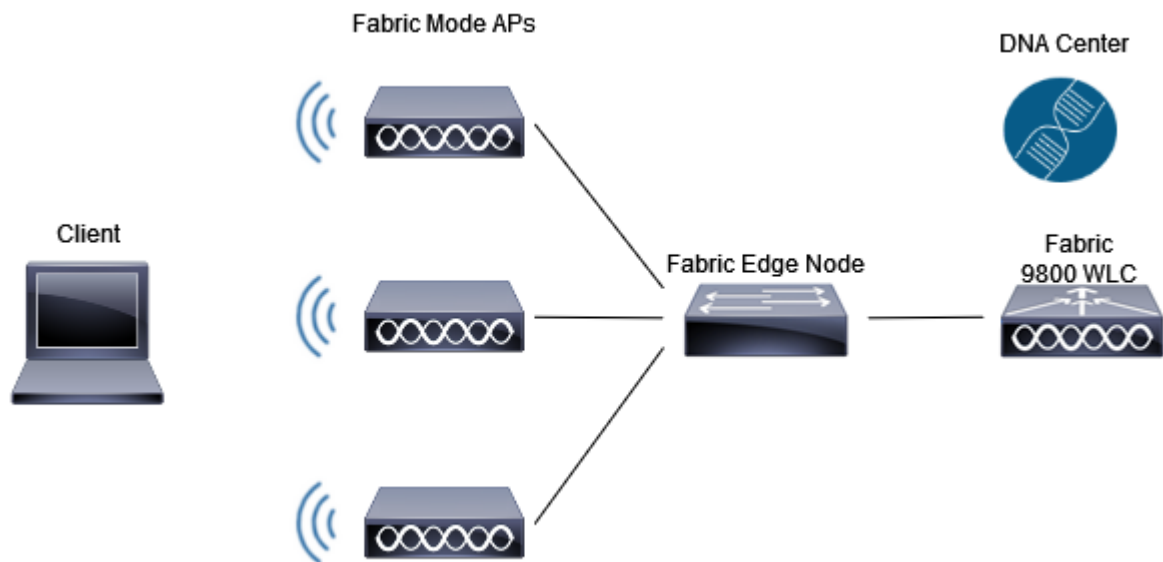
Client-Roaming-Workflow

Client-Roaming-Workflow:

1. Client wechselt auf FE2 zu AP2 (Inter-Switch-Roaming). WLC wird vom AP benachrichtigt.
2. WLC aktualisiert die Weiterleitungstabelle auf dem Access Point mit Client-Informationen (SGT, RLOC).
3. WLC aktualisiert den L2-MAC-Eintrag in CP mit dem neuen RLOC Fabric Edge 2.
4. CP teilt dann mit:
 - Fabric Edge FE2 (Roam-to-Switch), um die Client-MAC zur Weiterleitungstabelle hinzuzufügen, die auf den VXLAN-Tunnel verweist.
 - Fabric Edge FE1 (Roam-from-Switch) zur Bereinigung für den Wireless-Client.
5. Fabric Edge aktualisiert den L3-Eintrag (IP) in der CP-Datenbank, sobald Datenverkehr empfangen wird.
6. Roaming ist Layer 2, da Fabric Edge 2 über dieselbe VLAN-Schnittstelle (Anycast GW) verfügt.

Konfigurieren

Netzwerkdiagramm



Netzwerkdigramm

WLC-Erkennung und -Bereitstellung in Cisco DNA

WLC hinzufügen

Schritt 1: Navigieren Sie zu dem Ort, an dem Sie den WLC hinzufügen möchten. Sie können ein neues Gebäude/Stockwerk hinzufügen.

Navigieren Sie zu Design > Network Hierarchy, und geben Sie das Gebäude/Stockwerk ein. Sie können auch ein neues Stockwerk erstellen, wie in der Abbildung dargestellt:

Search Hierarchy

Search Help

Global

>

>

>

>

>

>

>

>

>

>

>

>

>

>

Lisbon

Lisbon

Floor 1

MyFloor

>

>


>

>

>

+ Add Site

↓ Import



Edit Building

Delete Building

Add Floor

Import Ekahau Project

Import Ekahau Survey

Sync: DNA Spaces/CMX

Export Maps

View Devices

View Settings

Neue Ebene erstellen

Schritt 2: Fügen Sie Ebene hinzu. Sie können auch ein Bild der Anlage des Bodens hochladen.

und überprüfen Sie die konfigurierte Zeichenfolge. Sie müssen den richtigen SNMP Community String hinzufügen, wenn Sie den WLC zur Cisco DNA hinzufügen, und sicherstellen, dass netconf-yang auf dem 9800 WLC mit den Befehlen show netconf-yang status aktiviert ist. Klicken Sie am Ende auf Hinzufügen:

[Administration](#) > [Management](#) > [SNMP](#)

SNMP Mode ENABLED

[General](#) [SNMP Views](#) **[Community Strings](#)** [V3 User Groups](#) [V3 Users](#) [Hosts](#) [Wireless Traps](#)

[+ Add](#) [× Delete](#)

	Community Name	Access Mode
<input type="checkbox"/>	private	Read/Write
<input type="checkbox"/>	public	Read Only

1 10 1 - 2 of 2 items

SNMP-Konfiguration

Schritt 5: Fügen Sie die WLC-IP-Adresse, die CLI-Anmeldeinformationen (die von der Cisco DNA für die Anmeldung am WLC verwendet werden und auf dem WLC konfiguriert werden müssen, bevor sie zur Cisco DNA hinzugefügt werden), den SNMP-String hinzu, und überprüfen Sie, ob der NETCONF-Port auf Port 830 konfiguriert ist:

Add Device

1 Device Controllability is **Enabled**. Configuration changes will be made on network devices during discovery/inventory or when device is associated to a site. Firepower Management Center devices are not supported. [Learn more](#) | [Disable](#)

Type*

Network Device

Device IP / DNS Name*

10.48.39.186

Credentials

[Validate](#)

Note: CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.

^ CLI *

☐ Select global credential ☒ Add device specific credential

Username*

admin

Password*

Enable Password

WARNING: Do not use 'admin' as the username for your device CLI credentials, if you are using Cisco ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

^ SNMP *

☒ Select global credential ☐ Add device specific credential

Version*

V2C

Credential*

private | Write

SNMP RETRIES AND TIMEOUT *

HTTP(S)

^ NETCONF

Port

830

[Hint](#)

Netconf with user privilege 15 is mandatory for enabling Wireless Services on Wireless capable devices such as C9800 Switches/Controllers. The NETCONF credentials are required to connect to eWLC devices. Majority of data collection is done using NETCONF for eWLC.

[Cancel](#)

[Add](#)

WLC hinzufügen

Der WLC wird als NA angezeigt, da die Cisco DNA noch synchronisiert ist:

<input type="checkbox"/>		NA	10.48.39.186	Reachable	Not Available	Managed Syncing...	N/A	NA	Assign
--------------------------	--	----	--------------	------------------------	---------------	------------------------------------	-----	----	------------------------

WLC im Synchronisierungsprozess

Wenn der Synchronisierungsvorgang abgeschlossen ist, werden der WLC-Name, die IP-Adresse, sowie die verwaltete und die Softwareversion angezeigt, sofern diese erreichbar ist:

<input type="checkbox"/>		9800-17-9-RMI-RP-HA.dns-ams.cisco.com	10.48.39.186	Wireless Controller	Reachable	Not Available	Managed	N/A	No Health	Assign	17.9.3
--------------------------	--	---------------------------------------	--------------	---------------------	------------------------	---------------	----------------------	-----	-----------	------------------------	--------

WLC synchronisiert

Schritt 6: Zuweisen des WLC zu einem Standort Klicken Sie in der Geräteliste auf Zuweisen, und wählen Sie einen Standort aus:

Assign Device to Site

Serial Number
9

Devices
9800-17-9-RMI-RP-HA.dns-ams.cisco

 Choose a site

Gerät dem Standort zuweisen

Sie können den Standort jetzt oder zu einem späteren Zeitpunkt zuweisen:

Assign Device to Site

☒ Now ☐ Later

☐ Generate configuration preview

Creates preview which can be later used to deploy on selected devices. View status in [Work Items](#)

Task Name*

Assign 1 Device(s) to Site

Gerät jetzt oder zu einem späteren Zeitpunkt dem Standort zuweisen

Access Points hinzufügen

Schritt 1: Sobald der WLC hinzugefügt wurde und erreichbar ist, navigieren Sie zu Provision > Inventory > Global > Unassigned Devices (Bereitstellung > Bestand > Global > Nicht zugewiesene Geräte) und suchen Sie nach den APs, die Sie Ihrem WLC hinzugefügt haben:

Global

Unassigned Devices

<

Access Points hinzufügen

Schritt 2: Wählen Sie die Option Zuordnen. Zuweisen der APs zu einem Standort Aktivieren Sie das Kontrollkästchen Auf alle anwenden, um die Konfiguration für mehrere Geräte gleichzeitig vorzunehmen.

Assign Device to Site

Serial Number F	Devices 3800E-I	Choose a floor
		<input checked="" type="checkbox"/> Apply to All
K	DO_NOT_MOVE.Static_AP1	Choose a floor
K	AP0C75	Choose a floor

Zuweisen von APs zum Standort

Navigieren Sie zu Ihrem Stockwerk, und Sie können alle ihm zugewiesenen Geräte sehen - WLC und APs:

Lisbon / Lisbon / Floor 1

DEVICES (4)
FOCUS: Inventory

Filter | Add Device Tag Actions | Take a Tour

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site	Image Version
3800E-I	10.14.19.173	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1	17.9.3.50
9800-17-9-RMI-RP-HA.dns-ams.cisco.com	10.48.39.186	Wireless Controller	Reachable	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1	17.9.3
AP0C75	10.14.19.190	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1	17.9.3.50
DO_NOT_MOVE.Static_AP1	10.14.19.78	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1	17.9.3.50

Dem Standort zugewiesene Geräte

SSID erstellen

Schritt 1: Navigieren Sie zu Design > Network Settings > Wireless > Global, und fügen Sie eine SSID hinzu:

Network Device Credentials IP Address Pools SP Profiles **Wireless** Telemetry

Find Hierarchy Search help

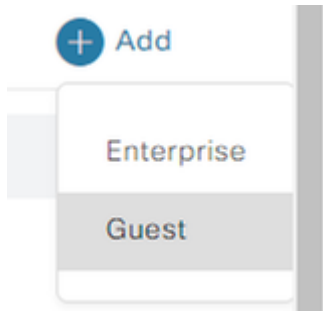
Global 1-Licensing

SSID (26)

Search Table


SSID erstellen

Sie können eine Unternehmens-SSID oder eine Gast-SSID erstellen. In dieser Demo wird eine Gast-SSID erstellt:



Unternehmens- oder Gast-SSID

Schritt 2: Wählen Sie die Einstellung für die SSID aus. In diesem Fall wird eine offene SSID erstellt. Admin-Status und Broadcast-SSID müssen aktiviert sein:

 Cisco DNA Center

Basic Settings

Fill the information like name, wireless options, state and network to complete the basic setup of SSID

Wireless Network Name (SSID)*
Demo

Wireless Option ⓘ
☒ Multi band operation (2.4GHz, 5GHz, 6GHz) ☐ Multi band operation with Band Select ☐ 5GHz only ☐ 2.4GHz only ☐ 6GHz Only

Primary Traffic Type
Best Effort (Silver) ▼ ⓘ

SSID STATE

☒ Admin Status

☒ Broadcast SSID

SSID-Grundeinstellungen

Security Settings

Configure the security level and authentication, authorization, & accounting for SSID

SSID Name: Demo (Guest)

Level of Security

L2 SECURITY

☐ Enterprise ☐ Personal ☐ Open Secured ☒ Open

Least Secure :

Any user can associate to the network.

L3 SECURITY

☐ Web Policy ☒ Open

Least Secure :

Any user can associate to the network.

Authentication, Authorization, and Accounting Configuration



Please associate one or more AAA servers using Configure AAA link to ensure right configuration is pushed for the selected security setting.



[Configure AAA](#)

☒ Mac Filtering

☐ Fast Lane [?](#)

☐ Deny RCM Clients [?](#)

SSID-Sicherheitseinstellungen



Vorsicht: Vergessen Sie nicht, einen AAA-Server für die SSID zu konfigurieren und zuzuordnen. Die Liste der Standardmethoden wird zugeordnet, wenn keine AAA-Server konfiguriert sind.

Wenn Sie auf Weiter klicken, werden die erweiterten Einstellungen für Ihre SSID angezeigt:

Configure the advanced fields to complete SSID setup.


Erweiterte SSID-Einstellungen

Associate SSID to Profile

SSID Name: Demo (Guest)

Profil hinzufügen

Schritt 4: Geben Sie dem Profil einen Namen, wählen Sie Fabric aus, und klicken Sie am Ende auf Associate Profile:

 Associate Profile

Cancel

Profile Name

DemoProfile

Fabric

☒ Yes ☐ No

Profil zuordnen

Es wird eine Zusammenfassung der SSID und des Profils angezeigt, die Sie erstellt haben:

Summary

Review all changes

▼ Basic Settings [Edit](#)

SSID Name	Demo
Primary Traffic Type	Best Effort (Silver) ⓘ
Admin Status	Yes
Broadcast SSID	Yes

▼ Security Settings [Edit](#)

L2 Security	open
L3 Security	open
AAA Servers	
Mac Filtering	Yes
Fast Lane	No
Deny RCM Clients	No
Enable Posture	No
ACL Name	

▼ Advanced Settings [Edit](#)

Fast Transition (802.11r)	Disable
Over the DS	No
MFP Client Protection	Optional
Session Timeout	1800
Client Exclusion	180
Radius Client Profiling	No
NAS-ID	

▼ Network Profile Settings [Edit](#)

DemoProfile	Fabric (Associated)
-------------	---------------------

Sie konfigurieren möchten. In dieser Demo wurden die Standardeinstellungen konfiguriert. Klicken Sie auf Speichern:

Wireless / Create RF Profile

This RF-Profile will be provisioned on the wireless lan controller during Access Point (AP) Network Provision or Access Point Plug and Play Onboarding. It will also be pushed during WLC network provisioning when the RF profile is associated to a network profile configured under advanced settings for AireOS controllers.

Create Wireless Radio Frequency Profile

Profile Name: DemoRFProfile

PROFILE TYPE

2.4 GHz

Parent Profile

High Medium (Typical) Low Custom

DCA Channel

Select All

1 6 11

Advanced Options

Select All

Show Advanced

Supported Data Rate

Enable 802.11n data rates

1 2 5.5 6 9 11 12 18 24 36 48 54

Mandatory Data Rates

1 2 5.5 6 9 11 12 18 24 36 48 54

TX Power Configuration

Power Level

7 30

Site IDP

Medium

Cancel Save

Einfaches RF-Profil hinzufügen

Access Points bereitstellen

Schritt 1: Navigieren Sie zu Ihrem Gebäude/Stockwerk. Wählen Sie APs und Aktionen > Bereitstellung > Gerät bereitstellen aus:

DEVICES (4)
FOCUS: Inventory

Filter Add Device Tag Actions ⓘ Take a Tour 3 Selected

Device Name	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site
3800E-I	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1
9800-17-9-RMI-RP-HA.dns			Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1
AP0C75			Not Scanned	Managed	N/A	6	.../Lisbon/Floor 1
DO_NOT_MOVE.Static_AP1			Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1

Inventory

Software Image

Provision

Telemetry

Device Replacement

Others

Compliance

Assign Device to Site

Provision Device

LAN Automation

LAN Automation Status

Learn Device Config

Configure WLC HA

Configure WLC Mobility

Manage LED Flash Status

APs bereitstellen

Schritt 2: Überprüfen Sie, ob der zugewiesene Standort korrekt ist, und wählen Sie Auf alle anwenden aus:

Inventory / Provision Devices

1 Assign Site **2** Configuration **3** Summary

Serial Number F	Devices 3800E-I	Global/Lisbon/Lisbon/Floor 1 × Apply to All ⓘ
K	AP0C75	Global/Lisbon/Lisbon/Floor 1 ×
K	DO_NOT_MOVE.Static_AP1	Global/Lisbon/Lisbon/Floor 1 ×

Zuweisen von Standorten zu APs

Schritt 3: Wählen Sie aus der Dropdown-Liste ein RF-Profil aus, und vergewissern Sie sich, dass die SSID die richtige ist:

Inventory / Provision Devices

1 Assign Site **2** Configuration **3** Summary

⚠ Zones and SSIDs are listed from Provisioned Wireless profile(s) for each Access point. For newly added Zones and SSIDs, Please provision Controller prior to Access point provision.

9130AXE Access points with 17.6 version and higher, support advanced configurations to configure Radio Antenna profiles on Antenna slot.

Advanced Configuration

Serial Number	Device Name	AP Zone Name	RF Profile	SSIDs
F	3800E-I	Not Applicable	DemoRFProfile	Demo
Apply to All ⓘ				
K	AP0C75	Not Applicable	DemoRFProfile	Demo
K	DO_NOT_MOVE.Static_AP1	Not Applicable	DemoRFProfile	Demo

RF-Profil auswählen

Schritt 4: Überprüfen der Einstellungen der Access Points Wenn alles in Ordnung ist, wählen Sie Bereitstellen:

Inventory / Provision Devices

1 Assign Site

2 Configuration

3 Summary

3800E-1

APOC75

DO_NOT_MOVE.Static_AP1

Device Details

Device Name: 3800E-1

Serial Number: F

Mac Address: 78

Device Location: Global/Lisbon/Lisbon/Floor 1

AP Zone Details

AP Zone Name: default-zone

RF Profile Details

RF Profile Name: DemoRFProfile

Radio Type	2.4GHz	5GHz	60GHz
Parent Profile	HIGH	LOW	CUSTOM
Status	Enabled	Enabled	Enabled
DCA Channels	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64	37, 41, 45, 49, 53, 57, 61, 65
Ignored DCA Channels ⓘ	N/A	149,153,157,161	149,153,157,161
Channel Width	20 MHz	20 MHz	Best
Supported Data Rates (in Mbps)	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54
Mandatory Data Rates (in Mbps)	9	6	6
Tx Power Level (in dBm)	7/30	-10/30	-10/30
TPC Power Threshold (in dBm)	-70	-60	-70
Rx SOP	MEDIUM	LOW	AUTO
Max Client	200	200	200

Cancel

Apply

Bereitstellung der APs

Schritt 5: Die Gerätebereitstellung kann zu einem bestimmten Zeitpunkt oder zu einem späteren Zeitpunkt erfolgen. Wählen Sie am Ende Apply (Anwenden):

Provision Device

☒ Now

☐ Later

☐ Generate configuration preview

Creates preview which can be later used to deploy on selected devices. If Site assignment is invoked during configuration preview, Device controllability configuration will be pushed to corresponding device(s). View status in [Work Items](#)

Task Name*

Provision Device

Cancel

Apply

APs jetzt oder zu einem späteren Zeitpunkt bereitstellen



Vorsicht: Bei der Bereitstellung müssen die APs, die bereits Teil der konfigurierten Ebene für das ausgewählte HF-Profil sind, verarbeitet und neu gestartet werden.

Die APs werden jetzt bereitgestellt.

Schritt 6: Navigieren Sie auf der WLC-Seite zu Configuration > Wireless > Access Points. Überprüfen Sie, ob die AP-Tags von der Cisco DNA entfernt wurden:

Configuration > Wireless > Access Points

▼ All Access Points

Total APs : 3

Misconfigured APs
Tag : 0 Country Code : 0 LSC Fallback : 0 Select an Action ▼

tion	Country Code	LSC Fallback	Policy Tag	Site Tag	RF Tag	Location	Country
Misconfigured	Misconfigured	Misconfigured					
No	No	No	PT_Lisbo_Lisbo_Flo or1_45ce7	ST_Lisbo_Lisbon_3 e5f5_0	DemoRFProfile	default location	PT
No	No	No	PT_Lisbo_Lisbo_Flo or1_45ce7	ST_Lisbo_Lisbon_3 e5f5_0	DemoRFProfile	default location	PT
No	No	No	PT_Lisbo_Lisbo_Flo or1_45ce7	ST_Lisbo_Lisbon_3 e5f5_0	DemoRFProfile	default location	PT

1 10

1 - 3 of 3 access points

Tags auf APs

Schritt 7: Navigieren Sie zu Configuration > Tags & Profiles > WLANs, und vergewissern Sie sich, dass die SSID von Cisco DNA weitergeleitet wurde:

Configuration > Tags & Profiles > WLANs

+ Add × Delete 📄 Clone Enable WLAN Disable WLAN WLAN Wizard

Selected WLANs : 0

<input type="checkbox"/>	Status	Name	ID	SSID	Security
<input type="checkbox"/>		Demo_Global_NF_986e8d08	17	Demo	[open],MAC Filtering

1 10

1 - 1 of 1 items

WLAN

Fabric-Standort erstellen

Schritt 1: Navigieren Sie zu Bereitstellung > Fabric-Standorte. Erstellen Sie eine Fabric-Site:

Virtual Networks

Fabric Sites

Transits

Q Search Table


+ Create Fabric Sites and Fabric Zones


Fabric-Standorte erstellen


Schritt 2. Wählen Sie das Gebäude/Stockwerk für Ihre Fabric-Website:


Fabric Site Location


A Fabric Site begins at the selected level of hierarchy. All levels below the selected level are included as part of the Fabric Site.


Q Search  [Search Help](#)


▼ ○  Global


> ○ 


> ○ 


> ○ 


> ○ 


> ○ 


> ○ 


> ○ 


> ○ 


> ○ 


> ○ 

> ○ 

> ○ 

▼ ○  Lisbon

▼ ○  Lisbon

●  Floor 1

Fabric-Standort auswählen

Schritt 3: Wählen Sie eine Authentifizierungsvorlage aus. In dieser Demo wurde keine angewendet:

Authentication Template

Select a Template for the Fabric Site. The Template will apply a port-based network access control configuration to all access ports on Edge Nodes and Extended Nodes.

- ☐ Closed Authentication ⓘ [Edit](#)
- ☐ Open Authentication ⓘ [Edit](#)
- ☐ Low Impact ⓘ [Edit](#)
- ☒ None ⓘ

Authentifizierungsvorlage

Schritt 3. Sie können wählen, ob Sie die Fabric-Zone jetzt oder später einrichten möchten:

Fabric Zones

Fabric Zones are optional. They reside within a Fabric Site and can only contain Edge Nodes and Extended Nodes. If Fabric Zones are used, only select Virtual Networks and Anycast Gateways (IP address pools) are provisioned to the Edge Nodes in each Fabric Zone.

If Fabric Zones are not used, all Virtual Networks and Anycast Gateways are provisioned to all Edge Nodes in the Fabric Site.

Setup Fabric Zones Later

All IP address pools and Virtual Networks are provisioned to all fabric Edge Nodes.

Setup Fabric Zones Now

Specific IP address pools and Virtual Networks can be assigned to fabric Edge Nodes in one or more Fabric Zones.


Select one or more areas, buildings, or floors to enable as a fabric zone


A Fabric Zone begins at the selected level of hierarchy. All levels below the selected level are included as part of the Fabric Zone.

LEGEND  Fabric Site

Search Hierarchy

Search Help

☐  Floor 1



Fabric-Zonen einrichten

Schritt 4: Überprüfen der Einstellungen der Fabric-Zone Wenn alles in Ordnung ist, wählen Sie Bereitstellen:

Summary

Review the Fabric Site and Fabric Zone settings before deploying.

Fabric Site Location Edit	
Site Name	Global/Lisbon/Lisbon/Floor 1
Wired Endpoint Data Collection Edit	
Monitor wired clients	Enable
Authentication Template Edit	
Authentication Template	No Authentication
Fabric Zones Edit	
Enable fabric zones?	No

Changes saved

[Review](#)

[Back](#)

[Deploy](#)

Fabric-Standort bereitstellen

Sie haben einen Fabric-Standort erstellt:

Success! You created a Fabric Site.

Your Fabric Site, Global/Lisbon/Lisbon/Floor_1, was created successfully.



Erstellung des Fabric-Standorts

WLC zur Fabric hinzufügen

Navigieren Sie zu Bereitstellung > Fabric-Standorte, und wählen Sie Ihre Fabric-Website aus. Klicken Sie auf den oberen Rand Ihres WLC, und navigieren Sie zur Registerkarte Fabric. Aktivieren Sie Fabric für den WLC, und wählen Sie Hinzufügen:

The screenshot shows the Cisco Fabric Sites configuration interface. On the left, under 'Fabric Sites', 'Floor 1' is selected. The main panel displays details for a specific Fabric Site: '9800-17-9-RMI-RP-HA.dns-ams.cisco.com (10.48.39.186)'. The 'Fabric' tab is active, and the 'Fabric' toggle switch is turned on. A red box highlights the 'Fabric' tab and the toggle switch.

WLC zur Fabric hinzufügen

AP-Beitritt

Schritt 1: Navigieren Sie zu Design > Network Settings > IP Address Pools. Erstellen Sie einen IP-

Adresspool.

IP-Adresspool

Schritt 2: Navigieren Sie zu Bereitstellung > Fabric-Standorte, und wählen Sie Ihre Fabric-Website aus. Navigieren Sie zu Host Onboarding > Virtual Networks.

INFRA_VN wird eingeführt, um APs einfach zu integrieren. APs befinden sich im Fabric-Overlay, aber INFRA_VN ist der globalen Routing-Tabelle zugeordnet. Nur APs und erweiterte Knoten können zu INFRA_VN gehören. Die Layer-2-Erweiterung wird automatisch aktiviert, und der L2-LISP-Service wird aktiviert.

Wählen Sie INFRA_VN > Hinzufügen aus:

Virtuelles Netzwerk bearbeiten

Schritt 3: Fügen Sie einen IP-Adresspool mit dem Pool-Typ als AP hinzu:

Edit Virtual Network: INFRA_VN

< Back

Virtuelles Netzwerk S1-INFRA bearbeiten

Schritt 4: Überprüfen, ob die Layer-2-Erweiterung aktiviert ist

Filter | Delete | Enable/Disable Supplicant-Based Extended Node Onboarding

Reset Export Add

Find

VLAN Name	Pool Type	Supplicant-Based Extended Node	IP Address Pool	VLAN	Layer-2 Flooding	Layer-2 Extension
VLAN0039	AP	Disabled	S1-INFRA 172.16.0.0/24	39	Disabled	Enabled

Virtuelles Netzwerk bearbeiten

Mit Pool Type = AP und Layer-2-Erweiterung zu ON stellt die Cisco DNA eine Verbindung zum WLC her und setzt die Fabric-Schnittstelle für das AP-Subnetz für L2 und L3 VN_IDs auf VN_ID-Zuordnung.

Schritt 5: Navigieren Sie auf der WLC-GUI zu Configuration > Wireless > Fabric > General (Konfiguration > Wireless > Fabric > Allgemein). Fügen Sie einen neuen Client und eine AP VN_ID hinzu:

Configuration > Wireless

General Control Plane

Fabric Status

Fabric VNID Mapping

+ Add -x Del

Name

S2-INFRA

1

Configure Multicast and IGMP

Edit Add Client and AP VNID

Name* S2-INFRA

L2 VNID* 8188

Control Plane Name default-control-pl ...

L3 VNID 4097

IP Address 172.16.0.0

Netmask 255.255.255.0

Cancel Update & Apply to Device

Neuen Client und AP VN_ID hinzufügen

Schritt 6: Navigieren Sie zu Konfiguration > Wireless > Access Points. Wählen Sie einen Access Point aus der Liste aus. Überprüfen Sie, ob der Fabric-Status aktiviert ist, die IP-Adresse der Kontrollebene und der Name der Kontrollebene:

Edit AP			
AP Mode	Local	Primary Software Version	17.9.3.50
Operation Status	Registered	Predownloaded Status	N/A
Fabric Status	Enabled	Predownloaded Version	N/A
CleanAir NSL Key		Next Retry Time	N/A
AP Name	RLOC IP	Boot Version	1.1.2.4
AP0C75-BDB	10.XX.XX.XX	IOS Version	17.9.3.50
3800E-I	Control Plane Name	Mini IOS Version	0.0.0.0
	default-control-plane		

AP-Fabric-Status überprüfen

Client integriert

Schritt 1: Fügen Sie den Pool dem virtuellen Netzwerk hinzu, und überprüfen Sie, ob der Umschalter für die Layer-2-Erweiterung ON ist, um die L2-LISP- und Layer-2-Subnetzerweiterung im Client-Pool/Subnetz zu aktivieren. In Cisco DNA 1.3.x ist eine Deaktivierung nicht möglich.

☐ Layer 2 Only ⓘ
 ☐ Layer 3 Only ⓘ

IP Address Pool
 S1_CLIENT-IP (10.0.0.0/24)

VLAN
 39

VLAN Name
 VLAN0039

☐ Auto generate VLAN name

Security Group
 Traffic
 Data

☐ IP-directed broadcast ⓘ

☐ Layer-2 Flooding ⓘ
☐ Critical Pool ⓘ
☒ Wireless Pool

☐ Bridge-Network Virtual Machine ⚠

IP-Adresspool hinzufügen

Schritt 2: Überprüfen, ob die Layer-2-Erweiterung und der Wireless-Pool aktiviert sind

Filter		Actions								
<input type="checkbox"/>	VLAN Name	IP Address Pool	VLAN	Traffic Type	Security Group	Layer-2 Flooding	Wireless Pool	Bridge-Network Virtual Machine	Layer-2 Extension	
<input type="checkbox"/>	VLAN0039	S1- CLIENT-IP 10.0.0.0/24	39	Data	-	Disabled	Enabled	Disabled	Enabled	

Showing 1 of 1

Virtuelles Netzwerk bearbeiten

Schritt 3: Navigieren Sie auf der WLC-GUI-Seite zu Configuration > Wireless > Fabric > General (Konfiguration > Wireless > Fabric > Allgemein). Fügen Sie einen neuen Client und AP VN_ID hinzu.

Wenn der Pool dem virtuellen Netzwerk zugewiesen wird, wird die entsprechende Fabric-Schnittstelle zur VNID-Zuordnung an den Controller weitergeleitet. Dies sind alle L2-VNIDs.

Configuration > Wireless > Fabric

General Control Plane Profiles

Fabric Status

ENABLED 

 Apply

Fabric VNID Mapping

+ Add

× Delete

	Name	L2 VNID	L3 VNID	IP Address	Netmask
<input type="checkbox"/>	S2-INFRA	8188	4097	172.16.0.0	255.255.255.0
<input type="checkbox"/>	10_1_0_0-S2_CORP_VN	8189	0	0.0.0.0	0.0.0.0

1 - 2 of 2 items

Neuen Client und AP VN_ID hinzufügen

Schritt 4: SSIDs werden dem Pool in den jeweiligen virtuellen Netzwerken zugeordnet:

Floor 1

Fabric Infrastructure Host Onboarding

Authentication Template Virtual Networks Wireless SSIDs

Wireless SSID's

☐ Enable Wireless Multicast

Reset

Save

Find

SSID Name	Type	Security	Traffic Type	Address Pool	Scalable Group
-----------	------	----------	--------------	--------------	----------------

Demo

Enterprise

WPA2
PersonalVoice +
Data

Choose Pool

10_1_0_0-S2_CORP_VN

Assign SGT

Zugeordnete SSIDs

Schritt 5: Ein Fabric-Profil mit der L2-VNID wird zum ausgewählten Pool hinzugefügt, und das Richtlinienprofil wird dem Fabric-Profil zugeordnet. Es wird für Fabric aktiviert.

Navigieren Sie auf der WLC-GUI-Seite zu Configuration > Wireless > Fabric > Profiles.

Configuration > Wireless > Fabric > Profiles

General Control Plane

+ Add × Delete

Fabric Profile Name

s2-demo_Global_F_d3r

1

Edit Fabric Profile

⚠ Modifying the profile may result in loss of connectivity

Profile Name*

s2-demo_Global_F_d3r

Description

s2-demo_Global_F_d3r

L2 VNID

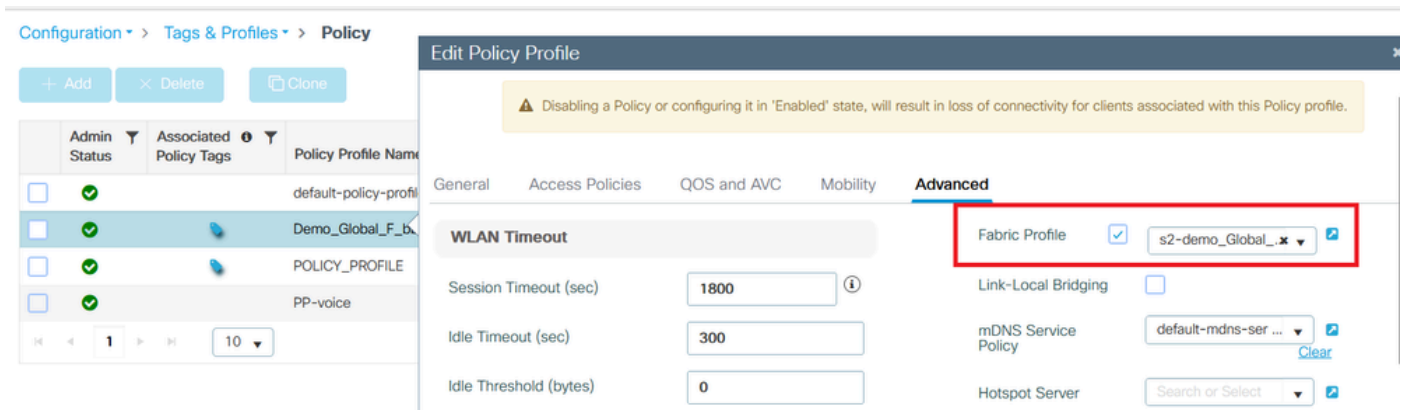
8189

SGT Tag

2-65519

Fabric-Profil

Schritt 6: Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie. Überprüfen Sie das dem Richtlinienprofil zugeordnete Fabric-Profil:



Auf der Richtlinie konfiguriertes Fabric-Profil

Überprüfung

Überprüfen der Fabric-Konfiguration auf WLC und Cisco DNA

In der WLC-CLI:

WLC1# show tech

WLC1# show tech wireless

Konfiguration der Kontrollebene:

Router-Schnittstelle

Locator-Table-Standard

Locator-Set WLC

172.16.201.202

Exit-Locator-Set

!

map-server session passive-open WLC

Site site_uci

description map-server configured from Cisco DNA-Center

authentication-key 7 <Schlüssel>

CB1-S1#sh lisp-Sitzung

Sitzungen für VRF-Standard, gesamt: 9, eingerichtet: 5

Peer-Status aktiv/inaktiv ein-/ausgehend

172.16.201.2012:4342 Bis 3d07h 14/14

WLC-Konfiguration:

Wireless-Fabric

Wireless Fabric-Kontrollebene Standard-Kontrollebene

ip address 172.16.2.2 key 0 47aa5a

WLC1# Fabric Map-Server-Zusammenfassung anzeigen

Status der MS-IP-Verbindung

172.16.1.2 UP

WLC1# Zusammenfassung der Wireless-Fabric anzeigen

Fabric-Status: Aktiviert

Kontrollebene:

Name IP-Adresse Schlüsselstatus

default-control-plane 172.16.2.2 47aa5a Up

Navigieren Sie auf der WLC-GUI zu Configuration > Wireless > Fabric, und überprüfen Sie, ob der Fabric-Status aktiviert ist.

Navigieren Sie zu Konfiguration > Wireless > Access Points. Wählen Sie einen Access Point aus der Liste aus. Überprüfen Sie, ob der Fabric-Status aktiviert ist.

Navigieren Sie auf der Cisco DNA zu Provisioning > Fabric Sites, und überprüfen Sie, ob Sie eine Fabric Site verwenden. Navigieren Sie an diesem Fabric-Standort zu Fabric Infrastructure > Fabric, und überprüfen Sie, ob der WLC als Fabric aktiviert ist.

Fehlerbehebung

Client erhält keine IP-Adresse

Schritt 1: Überprüfen der Fabric der SSID Navigieren Sie in der WLC-GUI zu Configuration > Tags & Profiles > Policy. Wählen Sie die Richtlinie aus, und navigieren Sie zu Advanced (Erweitert). Überprüfen Sie, ob das Fabric-Profil aktiviert ist.

Schritt 2: Überprüfen Sie, ob der Client im IP-Lernstatus feststeckt. Navigieren Sie auf der WLC-GUI zu Monitoring > Wireless > Clients. Überprüfen Sie den Client-Status.

Schritt 3: Überprüfen Sie, ob die Richtlinie DHCP erforderlich ist.

Schritt 4: Wenn der Datenverkehr lokal zwischen dem AP-Edge-Knoten umgeschaltet wird, sammeln Sie AP-Protokolle (client-trace) für die Client-Verbindung. Überprüfen Sie, ob die DHCP-Erkennung weitergeleitet wird. Wenn kein DHCP-Angebot eingeht, ist am Edge-Knoten etwas falsch. Wenn der DHCP-Server nicht weitergeleitet wird, liegt am Access Point ein Fehler vor.

Schritt 5: Sie können einen EPC am Edge-Knoten-Port erfassen, um die DHCP-Ermittlungspakete anzuzeigen. Wenn die DHCP-Ermittlungspakete nicht angezeigt werden, liegt das Problem am Access Point.

SSID wird nicht übertragen

Schritt 1: Überprüfen Sie, ob die AP-Funkmodule ausgefallen sind.

Schritt 2: Überprüfen Sie, ob das WLAN den Status hat und die SSID für Broadcast aktiviert ist.

Schritt 3: Überprüfen der AP-Konfiguration, wenn AP Fabric-fähig ist Navigieren Sie zu Configuration > Wireless > Access Points, wählen Sie einen Access Point aus, und auf der Registerkarte General (Allgemein) werden Fabric Status Enabled (Fabric-Status aktiviert) und die RLOC-Informationen angezeigt.

Schritt 4: Navigieren Sie zu Konfiguration > Wireless > Fabric > Kontrollebene. Überprüfen Sie, ob die Kontrollebene konfiguriert ist (mit der IP-Adresse).

Schritt 5: Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie. Wählen Sie die Richtlinie aus, und navigieren Sie zu Advanced (Erweitert). Überprüfen Sie, ob das Fabric-Profil aktiviert ist.

Schritt 6: Navigieren Sie zur Cisco DNA, und wiederholen Sie die Schritte unter "[SSID erstellen](#) und [WLC bereitstellen](#)". Die Cisco DNA muss die SSID erneut an den WLC senden.

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.