

Implementazione dell'accesso definito dal software per wireless con DNA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Accesso SD](#)

[Architettura wireless ad accesso SD](#)

[Panoramica](#)

[Ruoli e terminologia SDA](#)

[Reti Underlay e Overlay](#)

[Workflow di base](#)

[Join AP](#)

[Client integrato](#)

[Roam client](#)

[Configurazione](#)

[Esempio di rete](#)

[Rilevamento e provisioning WLC in Cisco DNA](#)

[Aggiungi WLC](#)

[Aggiungi Access Point](#)

[Crea SSID](#)

[Provisioning WLC](#)

[Provisioning dei punti di accesso](#)

[Crea sito fabric](#)

[Aggiungi WLC a fabric](#)

[Join AP](#)

[Client integrato](#)

[Verifica](#)

[Verifica della configurazione del fabric su WLC e Cisco DNA](#)

[Risoluzione dei problemi](#)

[Il client non ottiene l'indirizzo IP](#)

[SSID non trasmesso](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come implementare SDA per la tecnologia wireless relativa ai WLC abilitati per fabric e accedere ai LAP su Cisco DNA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione dei Wireless LAN Controller (WLC) 9800
- LAP (Lightweight Access Point)
- Cisco DNA

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Accesso SD

L'accesso definito dal software stabilisce e applica automaticamente i criteri di sicurezza in tutta la rete, con regole dinamiche e segmentazione automatizzata, e consente all'utente finale di controllare e configurare il modo in cui gli utenti si connettono alla rete. SD-Access stabilisce un livello iniziale di attendibilità per ogni endpoint connesso e lo controlla continuamente per verificarne nuovamente il livello di attendibilità. Se un endpoint non si comporta normalmente o viene rilevata una minaccia, l'utente finale può contenerlo immediatamente e intervenire prima che si verifichi la violazione, riducendo i rischi aziendali e proteggendo le risorse. Soluzione completamente integrata e facile da installare e configurare su reti nuove e distribuite.

SD-Access è una tecnologia Cisco che rappresenta un'evoluzione della tradizionale rete di campus che offre una rete basata su intent (IBN) e il controllo centralizzato delle policy con l'utilizzo di componenti Software-Defined Networking (SDN).

Tre pilastri di accesso SD incentrati sulla rete:

1. Un fabric di rete: Si tratta di un'astrazione della rete stessa che supporta sovrapposizioni programmabili e virtualizzazione. La struttura di rete supporta sia l'accesso cablato che wireless e consente di ospitare più reti logiche segmentate tra loro e definite in base alle finalità aziendali.

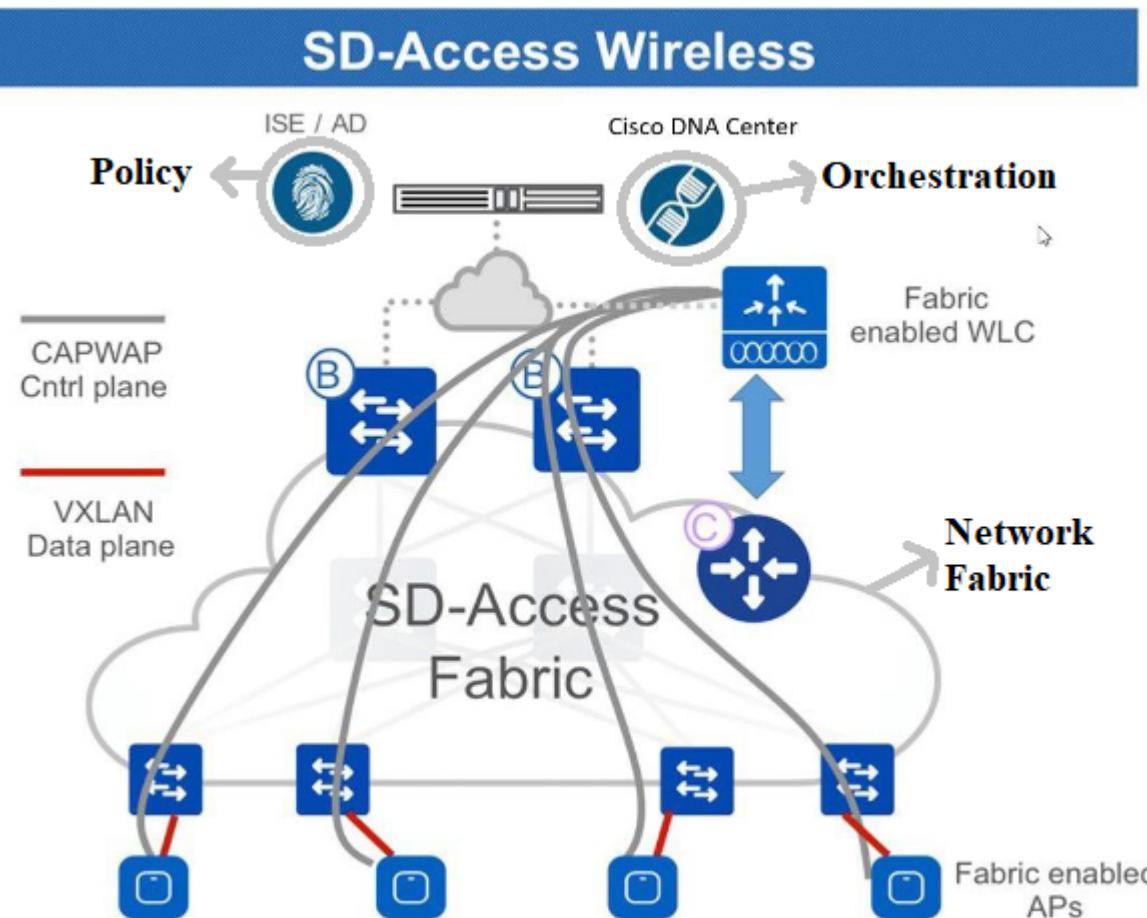
2. Orchestrazione: Cisco DNA è il motore di orchestrazione di SDA. Cisco DNA funziona come un controller SDN. Implementa policy e modifiche alla configurazione nel fabric. Incorpora inoltre uno strumento che supporta la progettazione della rete e le operazioni di telemetria di rete in tempo reale e l'analisi delle prestazioni tramite DNA Assurance. Il ruolo di Cisco DNA è quello di orchestrare il fabric di rete per apportare modifiche alle policy e all'intento della rete per la sicurezza, la qualità del servizio (QoS) e la microsegmentazione.
3. Policy: Identity Services Engine (ISE) è lo strumento che definisce i criteri di rete. ISE organizza la segmentazione di dispositivi e nodi in reti virtuali. ISE definisce anche i SGT (Scalable Group Tag) utilizzati dai dispositivi di accesso per segmentare il traffico degli utenti quando entrano nella struttura. Le SGR sono responsabili di implementare la policy di microsegmentazione definita da ISE.

L'architettura SDA è basata su un'orchestrazione centralizzata. Le combinazioni di Cisco DNA come motore di orchestrazione programmabile, ISE come motore delle regole e una nuova generazione di switch programmabili lo rendono un sistema fabric molto più flessibile e gestibile di qualsiasi cosa sia venuta prima.



Nota: Questo documento tratta in modo specifico di SD-Access Wireless.

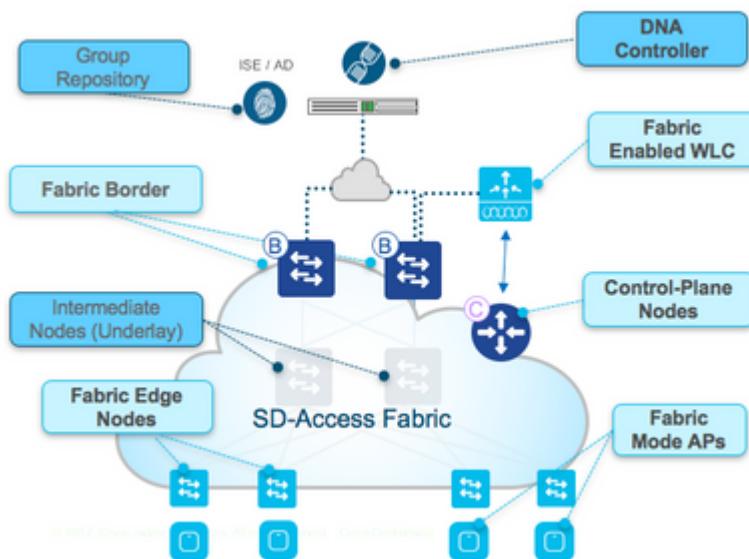
Il fabric di rete è composto dai seguenti elementi:



L'integrazione wireless con il fabric comporta diversi vantaggi per la rete wireless, ad esempio: la semplificazione, la mobilità con subnet allungate tra siti fisici; e la microsegmentazione con regole centralizzate che siano coerenti su entrambi i domini cablati e wireless. Consente inoltre al controllore di scartare il data plane per inoltrare i compiti mentre continua a funzionare come servizio centralizzato e control plane per la rete wireless. Di conseguenza, la scalabilità del controller wireless è in realtà aumentata perché non è più necessario elaborare il traffico del data plane, come avviene per il modello FlexConnect.

Architettura wireless ad accesso SD

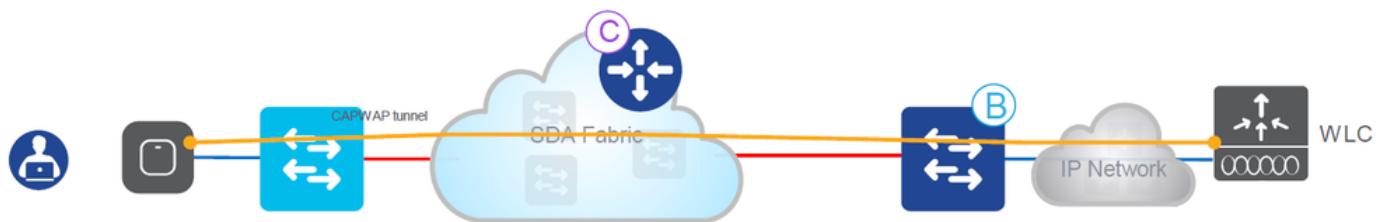
Panoramica



Panoramica su SDA

Esistono due modelli di distribuzione wireless principali supportati da SDA:

La prima è un metodo OTT (over-the-top), un'implementazione CAPWAP tradizionale connessa su una rete cablata fabric. Il fabric SDA trasporta il controllo CAPWAP e il traffico del data plane al controller wireless:

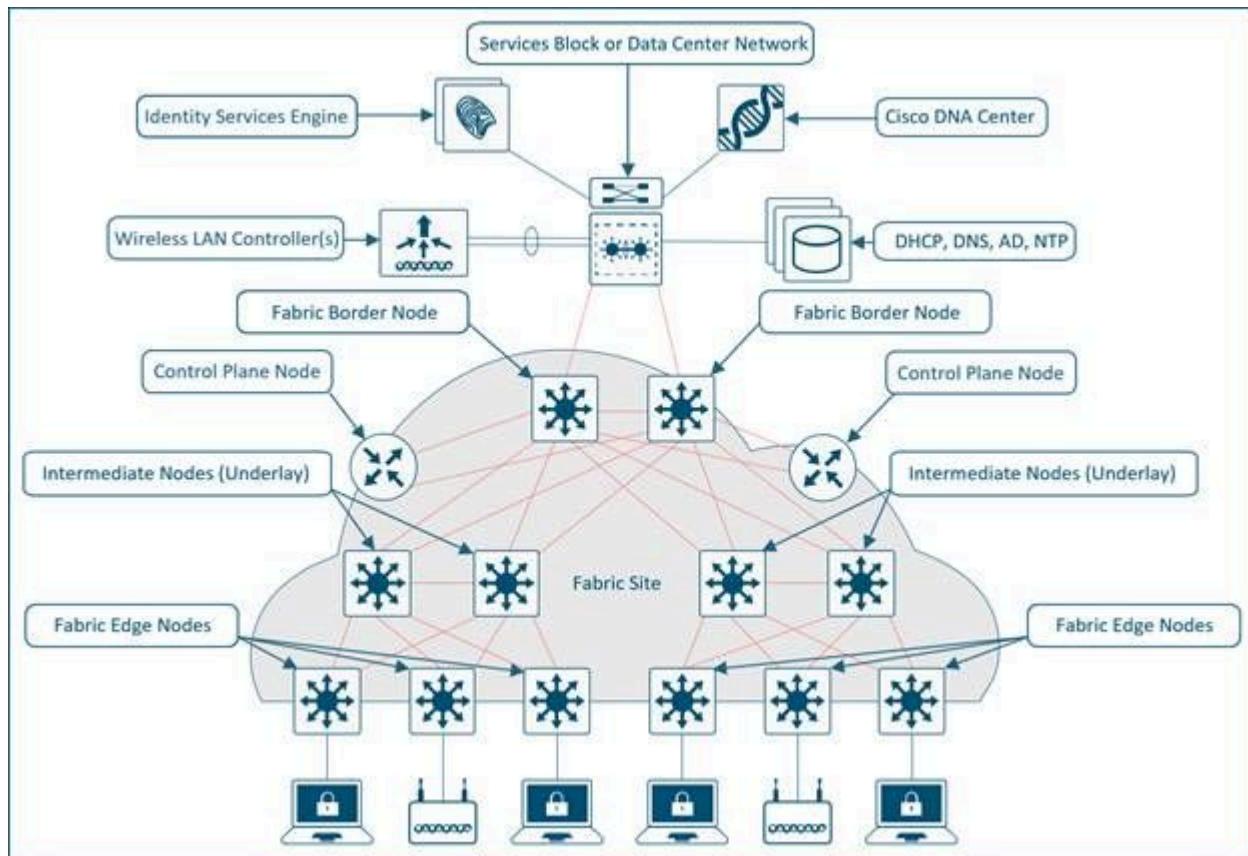


Metodo Over-The-Top

In questo modello di distribuzione, il fabric SDA è una rete di trasporto per il traffico wireless (un modello spesso implementato nelle migrazioni). L'access point funziona in modo molto simile alla modalità locale classica: sia il controllo CAPWAP che i piani dati terminano sul controller, il che significa che il controller non partecipa direttamente al fabric. Questo modello viene spesso

utilizzato quando viene eseguita la migrazione degli switch cablati al fabric SDA, ma la rete wireless non è ancora pronta per l'integrazione completa della sovrapposizione del fabric.

Gli altri modelli di distribuzione sono il modello SDA completamente integrato. La rete wireless è completamente integrata nel fabric e partecipa agli overlay; consente a diverse WLAN di far parte di diverse reti virtuali (VN). Il controller wireless gestisce solo il control plane CAPWAP (per gestire i punti di accesso) e il data plane CAPWAP non viene recapitato al controller:



Modello SDA completamente integrato

Il piano dati wireless viene gestito in modo simile agli switch cablati: ogni punto di accesso incapsula i dati nella VXLAN e li invia a un nodo periferico della struttura, dove vengono quindi inviati a un altro nodo periferico della struttura. I controller wireless devono essere configurati come controller fabric, il che rappresenta una modifica rispetto al loro normale funzionamento.

I controller abilitati all'infrastruttura comunicano con il control plane dell'infrastruttura, registrano gli indirizzi MAC dei client di layer 2 e le informazioni VNI (Virtual Network Identifier) di layer 2. Gli access point sono responsabili della comunicazione con gli endpoint wireless e assistono il data plane VXLAN dall'incapsulamento e dal traffico di deincapsulamento.

Ruoli e terminologia SDA

Il fabric di rete è composto dai seguenti elementi:

- **Nodo Control-Plane:** Si tratta del sistema di mappatura della posizione (database host) che fa parte del piano di controllo del protocollo LISP (Location Separator Protocol), che gestisce l'identità dell'endpoint (EID) alle relazioni di posizione (o alle relazioni tra dispositivi).

control plane può essere un router dedicato che fornisce le funzioni del control plane oppure può coesistere con altri elementi della rete fabric.

- Nodi del bordo dell'infrastruttura: In genere un router che funziona al confine tra le reti esterne e il fabric SDA, che fornisce servizi di routing alle reti virtuali nel fabric. Collega le reti esterne di layer 3 al fabric SDA.
- Nodi Fabric Edge: Dispositivo all'interno della struttura che connette dispositivi non di struttura, ad esempio switch, AP e router alla struttura SDA. Si tratta dei nodi che creano le sovrapposizioni virtuali dei tunnel e delle VN con la VXLAN (Virtual eXtensible LAN) e impongono le SGT al traffico associato alla struttura. Le reti su entrambi i lati del lato del fabric si trovano all'interno della rete SDA. Collegano gli endpoint cablati al fabric SD-Access.
- Nodi intermedi: Questi nodi si trovano all'interno del nucleo del fabric SDA e si connettono a nodi di bordo o di bordo. I nodi intermedi si limitano a inoltrare il traffico SDA come pacchetti IP, ignari del fatto che vi siano più reti virtuali coinvolte.
- WLC fabric: Controller wireless abilitato per il fabric che partecipa al control plane SDA ma non elabora il data plane CAPWAP.
- AP modalità fabric: Punti di accesso abilitati per l'infrastruttura. Il traffico wireless è incapsulato tramite VXLAN sull'access point, che consente di inviarlo al fabric tramite un nodo edge.
- Cisco DNA (DNAC): Enterprise SDN Controller per la rete di sovrapposizione del fabric SDA (Software Defined Access) ed è responsabile sia delle attività di automazione che delle attività di verifica. Può anche essere utilizzato per alcune attività di automazione e correlate per i dispositivi di rete che costituiscono l'underlay (che non è correlato a SDA).
- ISE: Identity Services Engine (ISE) è una piattaforma di policy avanzata in grado di supportare una vasta gamma di ruoli e funzioni, non ultima quella del server di autenticazione, autorizzazione e accounting (AAA). ISE interagisce in genere con Active Directory (AD), ma è possibile configurare gli utenti sia localmente che sulla stessa ISE per installazioni di dimensioni inferiori.



Nota: Il control plane è un componente dell'infrastruttura critica dell'architettura SDA, pertanto si consiglia di implementarlo in modo resiliente.

Reti Underlay e Overlay

L'architettura SDA utilizza la tecnologia fabric che supporta le reti virtuali programmabili (overlay networks) che vengono eseguite su una rete fisica (underlay network).

Un tessuto è un Overlay.

Una rete di overlay è una topologia logica utilizzata per connettere virtualmente i dispositivi, costruita su una topologia di underlay fisica arbitraria. Vengono utilizzati attributi di inoltro alternativi per fornire servizi aggiuntivi non forniti dall'applicazione sottostante. Viene creato sulla parte superiore della base per creare una o più reti virtualizzate e segmentate. Grazie alla natura software delle sovrapposizioni, è possibile collegarle in modo molto flessibile senza i vincoli della connettività fisica. È un modo semplice per applicare i criteri di sicurezza, poiché la sovrapposizione può essere programmabile per avere un singolo punto di uscita fisico (il nodo del bordo dell'infrastruttura) e un firewall può essere utilizzato per proteggere le reti dietro di esso (se possono essere individuate). L'overlay incapsula il traffico con l'uso della VXLAN. VXLAN incapsula frame completi di layer 2 per il trasporto attraverso la struttura sottostante con ciascuna rete di sovrapposizione identificata da un VXLAN Network Identifier (VNI). Le strutture sovrapposte tendono ad essere complesse e richiedono un notevole sovraccarico da parte degli amministratori sulle nuove reti virtuali installate o per implementare i criteri di sicurezza.

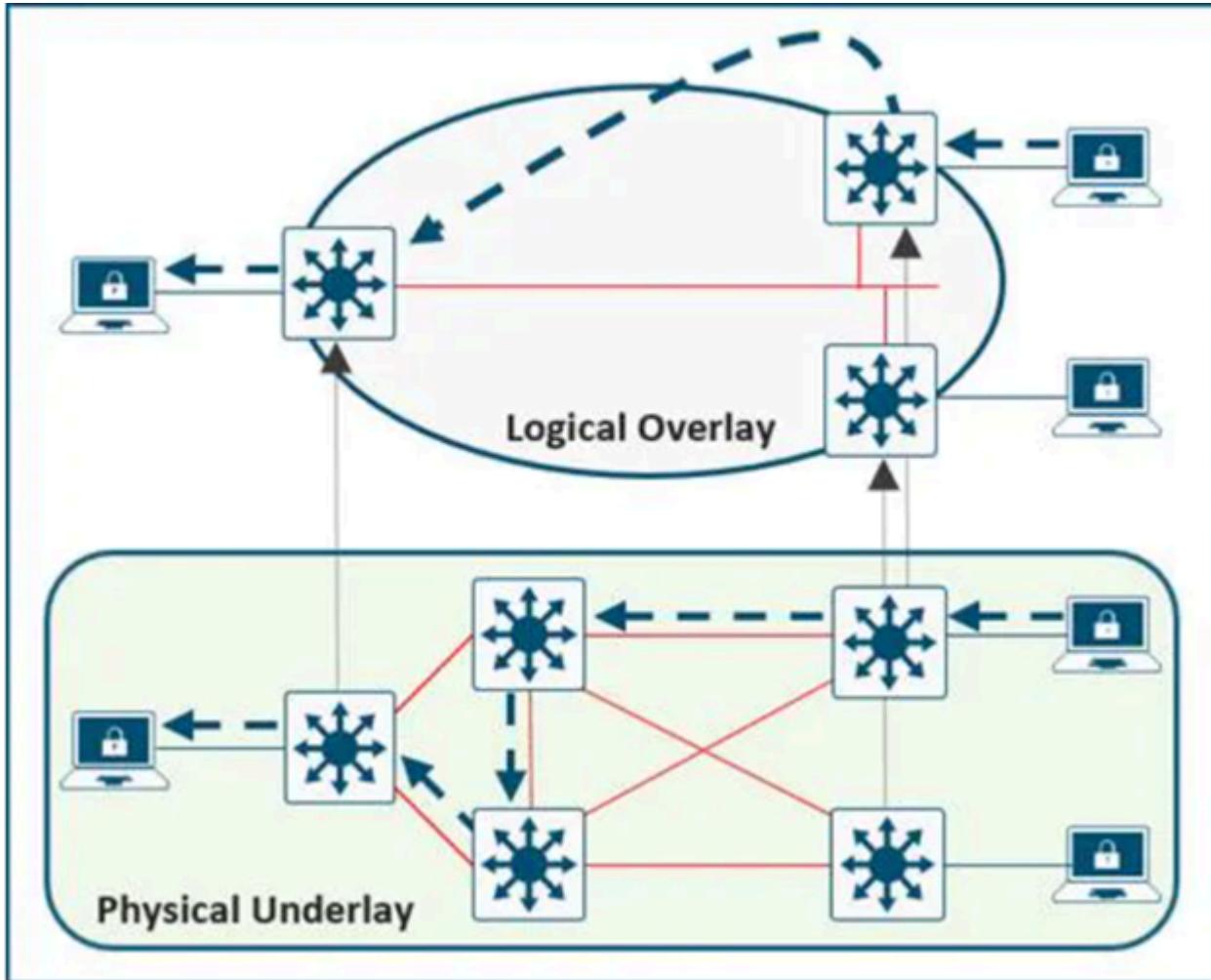
Esempi di sovrapposizioni di rete:

- GRE, mGRE
- MPLS, VPLS
- IPsec, DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI

Una rete Underlay è definita dai nodi fisici, quali switch, router e punti di accesso wireless, utilizzati per distribuire la rete SDA. Tutti gli elementi di rete dell'alloggiamento devono stabilire la connettività IP tramite l'uso di un protocollo di routing. Anche se è improbabile che la rete sottostante utilizzi il tradizionale modello di accesso, distribuzione e core, deve utilizzare una base Layer 3 ben progettata che offra prestazioni affidabili, scalabilità ed elevata disponibilità.



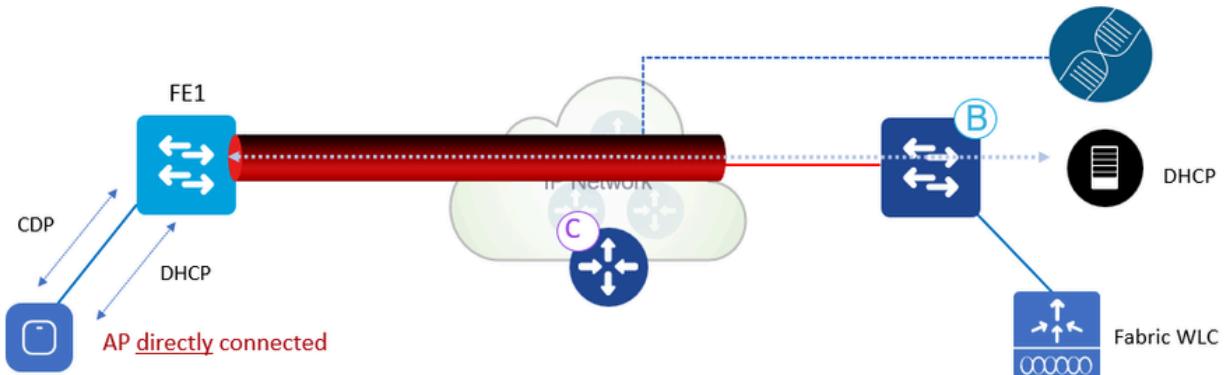
Nota: SDA supporta IPv4 nella rete sottostante e IPv4 e/o IPv6 nelle reti sovrapposte.



Reti Underlay e Overlay

Workflow di base

Join AP



Flusso di lavoro di aggiunta AP

Flusso di lavoro di aggiunta AP:

1. L'amministratore configura il pool AP in DNAC in INFRA_VN. Cisco DNA esegue il pre-

provisioning di una configurazione su tutti i nodi Fabric Edge per l'integrazione automatica dei punti di accesso.

2. L'access point è collegato alla rete elettrica e si accende. Fabric Edge scopre di essere un access point tramite CDP e applica la macro per assegnare (o il modello di interfaccia) alla porta dello switch la VLAN corretta.
3. AP ottiene un indirizzo IP tramite DHCP nella sovrapposizione.
4. Fabric Edge registra l'indirizzo IP e l'indirizzo MAC (EID) degli access point e aggiorna il Control Plane (CP).
5. AP apprende l'IP del WLC con i metodi tradizionali. L'access point fabric viene aggiunto come access point in modalità locale.
6. Il WLC verifica se è compatibile con la struttura (access point Wave 2 o Wave 1).
7. Se l'access point è supportato per l'infrastruttura, WLC chiede all'access point se è connesso all'infrastruttura.
8. Il Control Plane (CP) risponde al WLC con RLOC. Questo significa che il punto di accesso è collegato al fabric e viene visualizzato come "Fabric enabled".
9. WLC esegue una registrazione LISP L2 per AP in CP (ossia una registrazione client sicura "speciale" AP). Viene utilizzato per passare importanti informazioni sui metadati dal WLC al Fabric Edge.
10. In risposta a questa registrazione proxy, Control Plane (CP) notifica Fabric Edge e passa i metadati ricevuti dal WLC (flag che indica che si tratta di un access point e l'indirizzo IP dell'access point).
11. Fabric Edge elabora le informazioni, apprende di essere un access point e crea un'interfaccia tunnel VXLAN per l'IP specificato (ottimizzazione: il lato switch è pronto per l'aggiunta dei client).

I comandi debug/show possono essere utilizzati per verificare e convalidare il flusso di lavoro del join AP.

Piano di controllo

debug lisp control-plane all

show lisp instance-id <ID istanza L3> server ipv4 (deve mostrare l'indirizzo IP dell'access point registrato dallo switch periferico a cui è connesso l'access point).

show lisp instance-id <L2 instance id> server ethernet (deve mostrare la radio AP, nonché l'indirizzo MAC ethernet, la radio AP registrata dal WLC e la mac ethernet dallo switch periferico a cui è connesso l'access point).

Edge switch

```
debug access-tunnel all
```

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

```
show access-tunnel summary
```

```
show lisp instance < L2 instance id> ethernet database wlc access-points (visualizzare qui la radio mac del punto di accesso).
```

WLC

mostra riepilogo ap infrastruttura

Debug LISP WLC

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

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

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

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

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

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

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

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

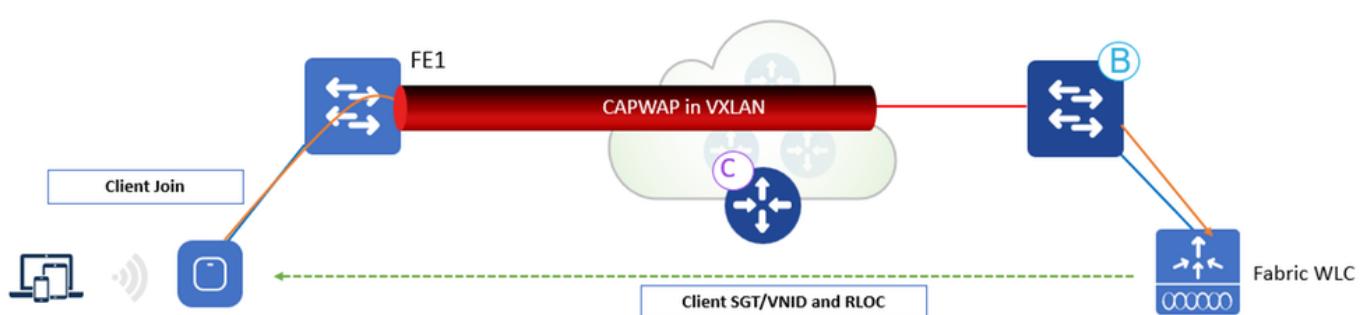
```
set platform software trace wncl chassis active r0 lisp-agent-ha debug
```

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

Access Point

```
show ip tunnel fabric
```

Client integrato



Flusso di lavoro integrato client

Flusso di lavoro integrato nel client:

1. Il client esegue l'autenticazione su una WLAN abilitata per Fabric. WLC ottiene SGT da ISE, aggiorna l'access point con il client L2VNID e SGT insieme all'IP RLOC. Il WLC conosce il RLOC dell'access point dal database interno.
2. Il proxy WLC registra le informazioni L2 del client in CP; Questo è il messaggio LISP modificato per passare informazioni aggiuntive, come il client SGT.
3. Fabric Edge riceve la notifica da CP e aggiunge l'indirizzo MAC client in L2 alla tabella di inoltro e va a recuperare la policy da ISE basata sul SGT client.
4. Il client avvia la richiesta DHCP.
5. AP incapsula il pacchetto nella VXLAN con le informazioni VNI L2.
6. Fabric Edge mappa il VNID L2 all'interfaccia VLAN e inoltra il DHCP nella sovrapposizione (come per un client Fabric cablato).
7. Il client riceve un indirizzo IP da DHCP.
8. Lo snooping DHCP (e/o ARP per statico) attiva la registrazione dell'EID del client da parte del perimetro della struttura al PC.

I comandi debug/show possono essere usati per verificare e convalidare il flusso di lavoro onboard del client.

Piano di controllo

debug lisp control-plane all

Edge switch

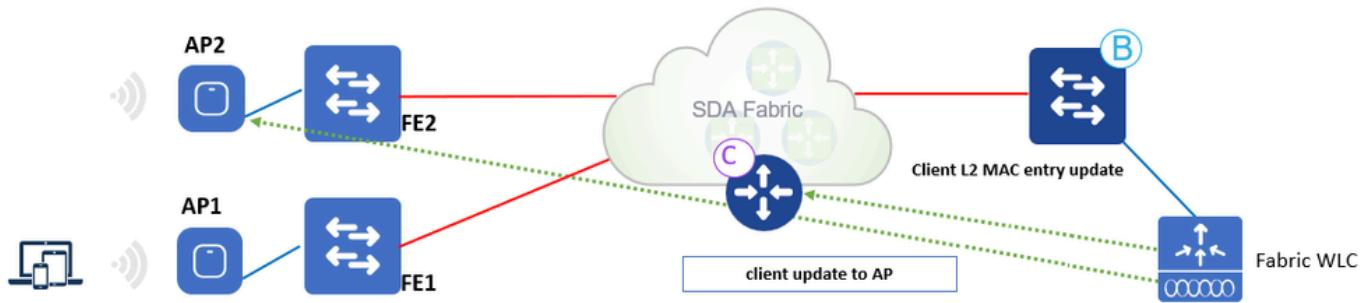
debug lisp control-plane all

pacchetto/evento di snooping ip dhcp di debug

WLC

Per la comunicazione LISP, sono presenti gli stessi debug di AP join.

Roam client



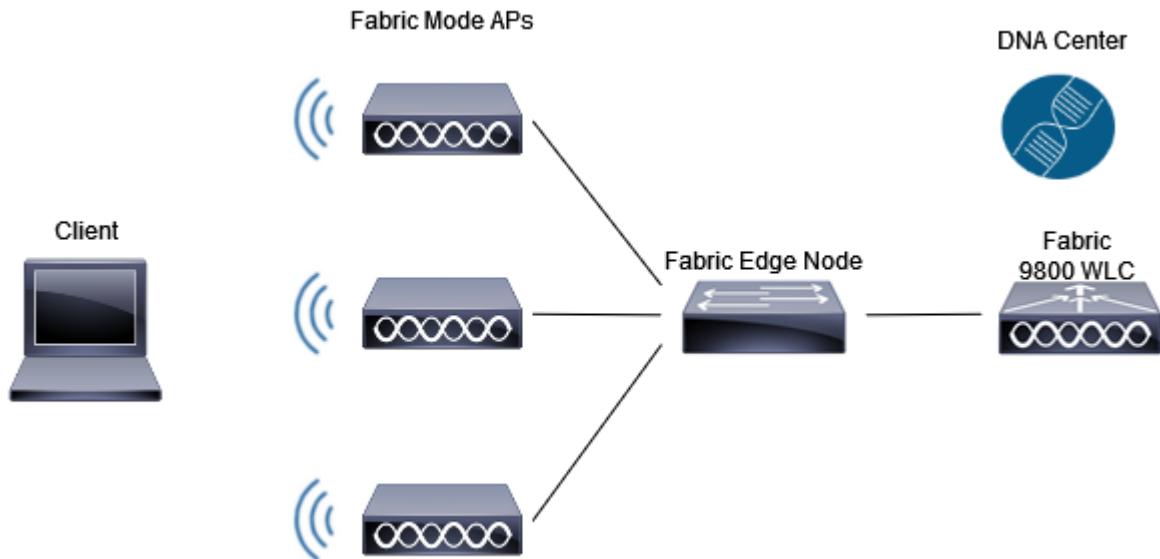
Flusso di lavoro roaming client

Flusso di lavoro roaming client:

1. Il client esegue il roaming verso AP2 su FE2 (roaming inter-switch). Il WLC riceve una notifica dall'access point.
2. WLC aggiorna la tabella di inoltro sull'access point con le informazioni sul client (SGT, RLOC).
3. WLC aggiorna la voce MAC L2 in CP con il nuovo RLOC Fabric Edge 2.
4. CP comunica quindi:
 - Fabric Edge FE2 (roaming verso lo switch) per aggiungere l'indirizzo MAC del client alla tabella di inoltro che punta al tunnel VXLAN.
 - Fabric Edge FE1 (switch da roaming) per eseguire la pulizia del client wireless.
5. Fabric Edge aggiorna la voce L3 (IP) nel database CP in base al traffico ricevuto.
6. Il roaming è sul layer 2, poiché il fabric Edge 2 ha la stessa interfaccia VLAN (Anycast GW).

Configurazione

Esempio di rete



Esempio di rete

Rilevamento e provisioning WLC in Cisco DNA

Aggiungi WLC

Passaggio 1. Passare alla posizione in cui si desidera aggiungere il WLC. È possibile aggiungere un nuovo edificio/piano.

Passare a Progettazione > Gerarchia di rete e inserire l'edificio/piano, oppure è possibile creare un nuovo piano, come mostrato nell'immagine:

 Cisco DNA Center

The screenshot shows the SiteWise software interface. On the left, there is a search bar labeled "Search Hierarchy" and a "Search Help" button. Below this is a tree view of the hierarchy:

- Global
 - Building 1
 - Building 2
 - Building 3
 - Building 4
 - Building 5
 - Building 6
 - Building 7
 - Building 8
 - Building 9
 - Building 10
- Lisbon
 - Lisbon
 - Floor 1
 - MyFloor
 - Building 11
 - Building 12
 - Building 13
 - Building 14
 - Building 15
 - Building 16
 - Building 17
 - Building 18
 - Building 19

On the right, a map of the area around CABEÇO DE MOURO is displayed. A context menu is open over a building, with the following options:

- Edit Building
- Delete Building
- Add Floor
- Import Ekahau Project
- Import Ekahau Survey
- Sync: DNA Spaces/CMX
- Export Maps
- View Devices
- View Settings

The "Add Floor" option is highlighted with a red box.

Crea nuovo piano

Ricaccia 2. Aggiungere il

(Amministrazione > Gestione > SNMP > Stringhe della community), quindi verificare la stringa configurata. Quando si aggiunge il WLC sul Cisco DNA, è necessario aggiungere la stringa della community SNMP corretta e verificare che netconf-yang sia abilitato sul WLC 9800 con i comandi show netconf-yang status. Alla fine, fare clic su Add (Aggiungi):

The screenshot shows the 'Community Strings' tab selected in the top navigation bar. Below the table, it says '1 - 2 of 2 items'. The table has columns for 'Community Name' and 'Access Mode'. It lists two entries: 'private' with 'Read/Write' access and 'public' with 'Read Only' access.

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

Configurazione SNMP

Passaggio 5. Aggiungere l'indirizzo IP del WLC, le credenziali CLI (le credenziali che Cisco DNA utilizza per accedere al WLC e che devono essere configurate sul WLC prima di aggiungerle a Cisco DNA), la stringa SNMP e verificare se la porta NETCONF è configurata sulla porta 830:

Add Device

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**

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**

Aggiungi WLC

Il WLC si mostra come NA perché Cisco DNA è ancora in processo di sincronizzazione:

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

WLC in processo di sincronizzazione

Al termine del processo di sincronizzazione, è possibile visualizzare il nome del WLC, l'indirizzo IP, se raggiungibile, gestito e la versione del software:

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

WLC sincronizzato

Passaggio 6. Assegnare il WLC a un sito. Nell'elenco dei dispositivi, fare clic su Assegna, quindi scegliere un sito:

Assign Device to Site

Serial Number
9

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

 Choose a site

Assegna dispositivo al sito

È possibile decidere di assegnare il sito subito o in un secondo momento:

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

Assegna dispositivo al sito ora o in seguito

Aggiungi Access Point

Passaggio 1. Dopo aver aggiunto il WLC e averlo raggiunto, selezionare Provisioning > Inventory > Globale > Dispositivi non assegnati e cercare gli AP aggiunti al WLC:

DEVICES (12) FOCUS: Inventory										
	Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site	
<input checked="" type="checkbox"/>	3800E-I	10.14.19.173	Unified AP	Reachable	Not Scanned	Managed	N/A	10	Assign	1
<input checked="" type="checkbox"/>	AP0C75	10.14.19.190	Unified AP	Reachable	Not Scanned	Managed	N/A	10	Assign	1
<input type="checkbox"/>			Unified AP	Reachable	Not Scanned	Managed	N/A	7	Assign	1
<input type="checkbox"/>			Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	8
<input type="checkbox"/>			Unified AP	Unreachable	Not Scanned	Managed	N/A	NA	Assign	8
<input type="checkbox"/>			Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	1
<input type="checkbox"/>			Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	1
<input type="checkbox"/>			Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	1
<input type="checkbox"/>			Unified AP	Reachable	Not Scanned	Managed	N/A	NA	Assign	1
<input checked="" type="checkbox"/>	DO_NOT_MOVE_Static_AP1	10.14.19.78	Unified AP	Reachable	Not Scanned	Managed	N/A	10	Assign	1
<input type="checkbox"/>			Unified AP	Reachable	Not Scanned	Managed	N/A	6	Assign	1
<input type="checkbox"/>			Unified AP	Reachable	Not Scanned	Managed	N/A	10	Assign	1
<input type="checkbox"/>			Wireless Controller	Reachable	Not Scanned	Managed	CLI Authentica...	Non-Compliant	No Health	Assign

Aggiungi Access Point

Passaggio 2. Selezionare l'opzione Assegna. Assegnare gli access point a un sito. Selezionare la casella Applica a tutte per eseguire la configurazione per più dispositivi contemporaneamente.

Assign Device to Site

Serial Number	Devices	Action
F	3800E-I	Choose a floor
K	DO_NOT_MOVE.Static_AP1	Choose a floor
K	AP0C75	Choose a floor

Assegna access point al sito

Spostarsi sul pavimento e visualizzare tutti i dispositivi assegnati - WLC e AP:

DEVICES (4)										
FOCUS: Inventory										
	Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site	Image Version
<input type="checkbox"/>	3800E-I	10.14.19.173	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1	17.9.3.50
<input type="checkbox"/>	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
<input type="checkbox"/>	AP0C75	10.14.19.190	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1	17.9.3.50
<input type="checkbox"/>	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

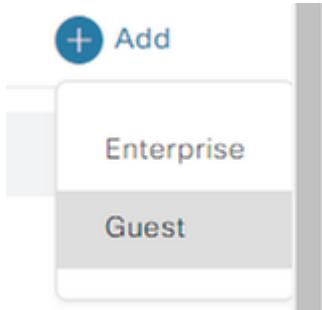
Dispositivi assegnati al sito

Crea SSID

Passaggio 1. Passare a Progettazione > Impostazioni di rete > Wireless > Globale e aggiungere un SSID:

Crea SSID

È possibile creare un SSID Enterprise o un SSID Guest. In questa demo viene creato un SSID guest:



SSID aziendale o guest

Passaggio 2. Scegliere l'impostazione desiderata per l'SSID. In questo caso, viene creato un SSID aperto. Lo stato di amministrazione e Broadcast SSID devono essere abilitati:



Basic Settings

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

Wireless Network Name (SSID)*

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

Impostazioni di base SSID

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 [\(i\)](#)

Deny RCM Clients [\(i\)](#)

Impostazioni di sicurezza SSID



Attenzione: Non dimenticare di configurare e associare il server AAA per l'SSID. Se non è configurato alcun server AAA, viene eseguito il mapping dell'elenco di metodi predefinito.

Quando si fa clic su avanti, è possibile visualizzare le impostazioni avanzate per il proprio SSID:

Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: Demo (Guest)

Fast Transition (802.11r)

Adaptive Enable Disable

Over the DS

11k

Neighbor List

MFP Client Protection ⓘ

Optional Required Disabled

Session Timeout ⓘ

in (secs)*
1800

Client Exclusion ⓘ

in (secs)*
180

11v BSS Transition Support

BSS Max Idle Service

Client User Idle Timeout

Client User Idle Timeout(Default: 300 secs)*
300

Directed Multicast Service

Radius Client Profiling ⓘ

NAS-ID ⓘ

NAS-ID Opt. 1

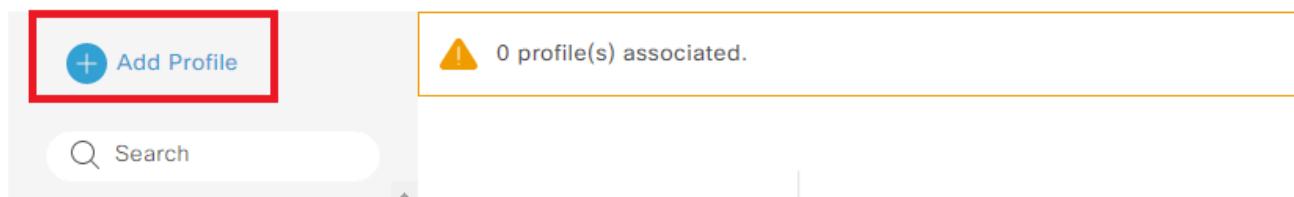
Impostazioni avanzate SSID

Passaggio 3. Dopo la creazione dell'SSID, è necessario associarlo a un profilo. Fare clic su Aggiungi profilo:

Associate SSID to Profile

Select a Profile on the left or Add Profile and click 'Associate' to associate the SSID to Profile.

SSID Name: Demo (Guest)



Aggiungi profilo

Passaggio 4. Assegnare un nome al profilo, selezionare Fabric e fare clic su Associa profilo:

 Associate Profile

Cancel

Profile Name

DemoProfile

Fabric

Yes

No

Associa profilo

Viene visualizzato un riepilogo del SSID e del profilo creati:

Summary

Review all changes

Basic Settings [Edit](#)

SSID Name	Demo
Primary Traffic Type	Best Effort (Silver) i
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)
-------------	---------------------

Riepilogo SSID

Design > Network Settings > Wireless > Global (Progettazione > Impostazioni di rete > Wireless > Globale) e aggiungere il nuovo profilo RF:

Aggiungi profilo RF

Passaggio 8. (Facoltativo) Assegnare un nome al profilo RF e selezionare le impostazioni che si desidera configurare. In questa demo sono state configurate le impostazioni predefinite. Fare clic su Salva:

Aggiungi profilo RF di base

Provisioning dei punti di accesso

Passaggio 1. Passare all'edificio/piano. Selezionare i punti di accesso e Azioni > Provisioning > Provisioning dispositivo:

DEVICES (4)
FOCUS: Inventory ▾

Filter | Add Device Tag Actions ▾ | Take a Tour | 3 Selected

Device Name	Inventory	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site
3800E-I	Software Image >	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1
9800-17-9-RMI-RP-HA.dns	Provision >	Assign Device to Site	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1	
AP0C75	Telemetry >	Provision Device	Not Scanned	Managed	N/A	6	.../Lisbon/Floor 1	
DO_NOT_MOVE.Static_AP1	Device Replacement >	LAN Automation	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1	
	Others >	LAN Automation Status	Not Scanned	Managed	N/A	10	.../Lisbon/Floor 1	
	Compliance >	Learn Device Config						
		Configure WLC HA						
		Configure WLC Mobility						
		Manage LED Flash Status						

Provisioning dei punti di accesso

Passaggio 2. Verificare che il sito assegnato sia corretto e selezionare Applica a tutte:

Cisco DNA Center Network Devices / Inventory / Provision Devices

Inventory / Provision Devices

1 Assign Site 2 Configuration 3 Summary

Serial Number F	Devices 3800E-I	<input checked="" type="checkbox"/> Apply to All
K	AP0C75	<input checked="" type="checkbox"/> Global/Lisbon/Lisbon/Floor 1
K	DO_NOT_MOVE.Static_AP1	<input checked="" type="checkbox"/> Global/Lisbon/Lisbon/Floor 1

Assegna sito ai punti di accesso

Passaggio 3. Selezionare un profilo RF dall'elenco a discesa e verificare che il SSID sia corretto:

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 F	Device Name 3800E-I	AP Zone Name Not Applicable	RF Profile DemoRFProfile	SSIDs Demo
K	AP0C75	Not Applicable	DemoRFProfile	Demo
K	DO_NOT_MOVE.Static_AP1	Not Applicable	DemoRFProfile	Demo

Seleziona profilo RF

Passaggio 4. Verificare le impostazioni sui punti di accesso. Se tutto è corretto, selezionare Distribuisci:

Inventory / Provision Devices

1 Assign Site 2 Configuration 3 Summary

3800E-I AP0C75 DO_NOT_MOVE_Static_AP1	<p>Device Details</p> <p>Device Name: 3800E-I Serial Number: F Mac Address: 7B Device Location: Global/Lisbon/Lisbon/Floor 1</p> <p>AP Zone Details</p> <p>AP Zone Name: default-zone</p> <p>RF Profile Details</p> <table border="1"><tr><td>RF Profile Name: DemoRFProfile</td><td>Radio Type: 2.4GHz</td><td>5GHz</td><td>6GHz</td></tr><tr><td>Parent Profile: HIGH</td><td>LOW</td><td>CUSTOM</td><td></td></tr><tr><td>Status: Enabled</td><td>Enabled</td><td>Enabled</td><td></td></tr><tr><td>DCA Channels: 1, 6, 11</td><td>36, 40, 44, 48, 52, 56, 60, 64</td><td>37, 41, 45, 49, 53, 57, 61, 65</td><td></td></tr><tr><td>Ignored DCA Channels: N/A</td><td>149,153,157,161</td><td>149,153,157,161</td><td></td></tr><tr><td>Channel Width: 20 MHz</td><td>20 MHz</td><td>Best</td><td></td></tr><tr><td>Supported Data Rates (in Mbps): 9,12,18,24,36,48,54</td><td>6,9,12,18,24,36,48,54</td><td>6,9,12,18,24,36,48,54</td><td></td></tr><tr><td>Mandatory Data Rates (in Mbps): 9</td><td>6</td><td>6</td><td></td></tr><tr><td>Tx Power Level (in dBm): 7/30</td><td>-10/30</td><td>-10/30</td><td></td></tr><tr><td>TPC Power Threshold (in dBm): -70</td><td>-60</td><td>-70</td><td></td></tr><tr><td>Rx SQR: MEDIUM</td><td>LOW</td><td>AUTO</td><td></td></tr><tr><td>Max Client: 200</td><td>200</td><td>200</td><td></td></tr></table>	RF Profile Name: DemoRFProfile	Radio Type: 2.4GHz	5GHz	6GHz	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 SQR: MEDIUM	LOW	AUTO		Max Client: 200	200	200	
RF Profile Name: DemoRFProfile	Radio Type: 2.4GHz	5GHz	6GHz																																														
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 SQR: MEDIUM	LOW	AUTO																																															
Max Client: 200	200	200																																															

Cancel Deploy

Distribuisci provisioning AP

Passaggio 5. Il provisioning del dispositivo può essere implementato al momento o in un secondo momento. Alla fine, selezionare Applica:

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

Esegui provisioning dei punti di accesso ora o in seguito



Attenzione: Quando si esegue il provisioning, gli access point, che fanno già parte della base configurata per il profilo RF selezionato, devono essere elaborati e riavviati.

Provisioning degli access point completato.

Passaggio 6. Sul lato WLC, selezionare Configurazione > Wireless > Access Point. Verificare che i tag AP siano stati spinti da Cisco DNA:

Configuration > Wireless > Access Points

▼ All Access Points

Misconfigured APs			Select an Action		
Total APs : 3	Tag : 0	Country Code : 0	LSC Fallback : 0		
tion	Country Code Misconfigured	LSC Fallback Misconfigured	Policy Tag	Site Tag	RF Tag
No	No	PT_Lisbo_Lisbo_Flo or1_45ce7	ST_Lisbo_Lisbon_3 e5f5_0	DemoRFProfile	default location PT
No	No	PT_Lisbo_Lisbo_Flo or1_45ce7	ST_Lisbo_Lisbon_3 e5f5_0	DemoRFProfile	default location PT
No	No	PT_Lisbo_Lisbo_Flo or1_45ce7	ST_Lisbo_Lisbon_3 e5f5_0	DemoRFProfile	default location PT

Tag su access point

Passaggio 7. Passare a Configurazione > Tag e profili > WLAN e verificare che l'SSID sia stato inviato da Cisco DNA:

Configuration > Tags & Profiles > WLANs

+ Add	X Delete	Clone	Enable WLAN	Disable WLAN	WLAN Wizard
Selected WLANs : 0					
<input type="checkbox"/>	Status	Name	ID	SSID	Security
<input checked="" type="checkbox"/>	Demo	Demo_Global_NF_986e8d08	17	Demo	[open],MAC Filtering
1 - 1 of 1 items					

WLAN

Crea sito fabric

Passaggio 1. Passare a Provisioning > Siti fabric. Creare un sito infrastruttura:

Cisco DNA Center

Virtual Networks

Fabric Sites

Transits

Search Table

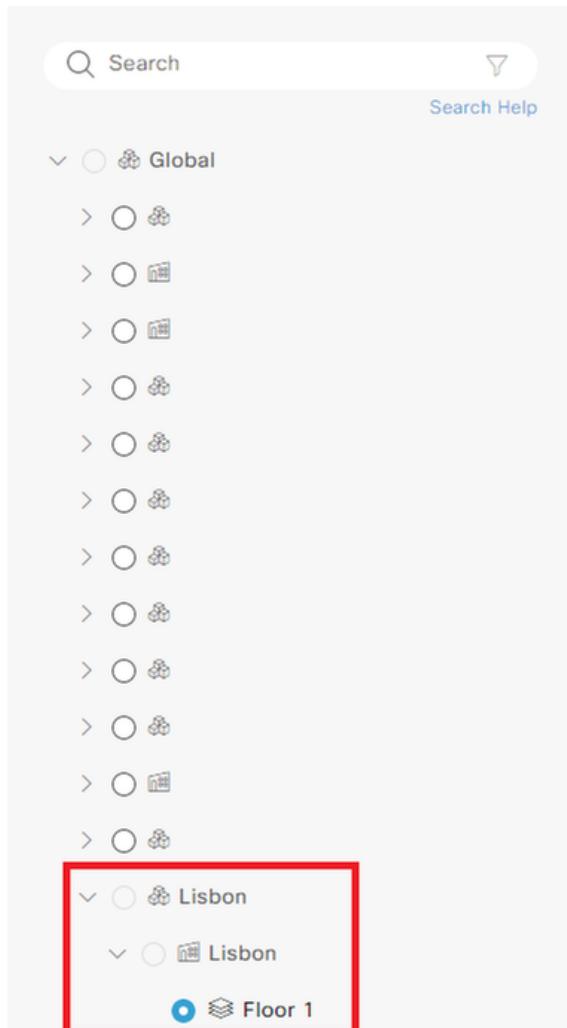
+ Create Fabric Sites and Fabric Zones

Crea siti fabric

Passaggio 2. Selezionare l'edificio/piano per la sede del fabric:

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.



Seleziona sito fabric

Passaggio 3. Selezionare un modello di autenticazione. In questa demo, Nessuno è stato applicato:

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

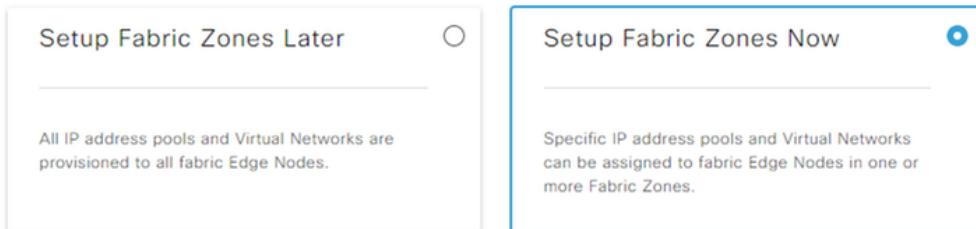
Modello di autenticazione

Passaggio 3. È possibile scegliere se impostare la zona struttura subito o in un secondo momento:

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.



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

A screenshot of a search interface. At the top, there is a search bar with the placeholder 'Search Hierarchy' and a dropdown arrow icon. Below the search bar, the text 'Search Help' is visible. A list item 'Floor 1' is shown with a checkbox to its left. At the bottom left of the interface is a blue circular button with a downward-pointing triangle icon.

Imposta zone fabric

Passaggio 4. Verificare le impostazioni dell'area di infrastruttura. Se tutto è corretto, selezionare Distribuisci:

Summary

Review the Fabric Site and Fabric Zone settings before deploying.

The screenshot shows the 'Fabric Site Location' configuration page. A red box highlights the 'Site Name' field set to 'Global/Lisbon/Lisbon/Floor_1'. Other sections like 'Wired Endpoint Data Collection' and 'Authentication Template' are also visible. At the bottom right, there are 'Review', 'Back', and a blue 'Deploy' button, with the 'Deploy' button being highlighted by a red box.

Distribuisci sito fabric

È stato creato un sito fabric:

Success! You created a Fabric Site.

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

Creazione sito fabric

Aggiungi WLC a fabric

Passare a Provisioning > Siti fabric e selezionare il sito fabric. Fare clic nella parte superiore del WLC e selezionare la scheda Fabric. Abilitare l'infrastruttura al WLC e selezionare Add:

The screenshot shows the 'Fabric Sites' page. A red box highlights 'Floor 1' under 'Fabric Infrastructure'. On the right, a detailed view of 'Floor 1' is shown with tabs for 'Details' (highlighted with a red box) and 'Fabric' (also highlighted with a red box). The 'Fabric' tab shows a 'Wireless LAN Controller' entry with a blue 'On' switch, which is also highlighted with a red box.

Aggiungi WLC a fabric

Join AP

Passaggio 1. Passare a Progettazione > Impostazioni di rete > Pool di indirizzi IP. Creare un pool di indirizzi IP.

The screenshot shows the 'IP Address Pools' section of a network management interface. It lists three existing pools: 'S1-INFRA', 'S2-INFRA', and 'S3-INFRA'. A modal window titled 'Add IP Pool' is open, prompting for a 'Pool Name' (set to 'S1-INFRA'), 'Pool Type' (set to 'AP'), and 'IP Address Space' (set to '172.16.0.0/24'). Below these fields are options for 'Gateway IP Address', 'DHCP Server(s)', and 'DNS Server(s)'. The 'Pool Type' field is highlighted with a red box.

Pool di indirizzi IP

Passaggio 2. Passare a Provisioning > Siti fabric e selezionare il sito fabric. Passare a Host Onboarding > Virtual Networks (Caricamento host > Reti virtuali).

INFRA_VN è stato introdotto per semplificare i punti di accesso integrati. I punti di accesso sono sovrapposti alla struttura, ma INFRA_VN è mappato alla tabella di routing globale. Solo i punti di accesso e i nodi estesi possono appartenere a INFRA_VN. L'estensione di livello 2 viene attivata automaticamente e il servizio LISP L2 viene attivato.

Selezionare INFRA_VN > Aggiungi:

The screenshot shows the 'Fabric Infrastructure' section with the 'Virtual Networks' tab selected. A list of virtual networks is displayed, including 'DEFAULT_VN' and 'INFRA_VN', with 'INFRA_VN' highlighted by a red box. To the right, a detailed view of 'Edit Virtual Network: INFRA_VN' is shown, featuring tabs for 'General', 'Advanced', and 'Host Onboarding'. The 'General' tab is active, showing the VLAN name 'VLAN 39' and the IP address pool 'S1-INFRA (172.16.0.0/24)'. The 'Host Onboarding' tab is also visible.

Modifica rete virtuale

Passaggio 3. Aggiungere un pool di indirizzi IP con il tipo di pool AP:

Edit Virtual Network: INFRA_VN

< Back

The screenshot shows the 'Edit Virtual Network: INFRA_VN' configuration page. The 'General' tab is selected. Key settings include:

- IP Address Pool:** S1-INFRA (172.16.0.0/24)
- Pool Type:** AP
- VLAN:** 39
- VLAN Name:** VLAN0039
- Auto generate VLAN name:**

Modifica S1-INFRA rete virtuale

Passaggio 4. Verificare se l'estensione di livello 2 è abilitata.

						Reset	Export	Add
Filter		Delete Enable/Disable Suplicant-Based Extended Node Onboarding						
<input type="checkbox"/>	VLAN Name ▾	Pool Type	Suplicant-Based Extended Node	IP Address Pool	VLAN	Layer-2 Flooding	Layer-2 Extension	⋮
<input type="checkbox"/>	VLAN0039	AP	Disabled	S1-INFRA 172.16.0.0/24	39	Disabled	Enabled	

Modifica rete virtuale

Con il tipo di pool = AP e l'estensione di livello 2 impostata su ON, Cisco DNA si connette al WLC e imposta l'interfaccia di fabric sul mapping VN_ID per la subnet AP per entrambi i VN_ID L2 e L3.

Passaggio 5. Sul lato GUI del WLC, selezionare Configuration > Wireless > Fabric > General (Configurazione > Wireless > Fabric > Generale). Aggiungere un nuovo client e un VN_ID AP:

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

Aggiungi nuovo client e AP VN_ID

Passaggio 6. Passare a Configurazione > Wireless > Access Point. Selezionare un punto di accesso dall'elenco. Verificare che lo stato dell'infrastruttura sia Abilitato, che l'indirizzo IP del control plane e il nome del control plane:

Edit AP			
Configuration	AP Mode	Local	Primary Software Version
All Access Points	Operation Status	Registered	Predownloaded Status
Total APs : 3	Fabric Status	Enabled	Predownloaded Version
AP Name	CleanAir NSI Key		Next Retry Time
AP0C75-BDB	RLOC IP	10.XX.XX.XX	Boot Version
3800E-I	Control Plane Name	default-control-plane	IOS Version
			Mini IOS Version

Verifica dello stato dell'infrastruttura AP

Client integrato

Passaggio 1. Aggiungere il pool alla rete virtuale e verificare che l'opzione Estensione di livello 2 sia attivata per abilitare l'estensione LISP L2 e l'estensione subnet di livello 2 nel pool/subnet client. In Cisco DNA 1.3.x non è possibile disabilitarlo.

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 (checked)

Bridge-Network Virtual Machine ⚠

Aggiungi pool di indirizzi IP

Passaggio 2. Verificare se l'estensione di livello 2 e il pool wireless sono abilitati.

Edit Virtual Network: S1_Corp_VN

Filter	Actions							
VLAN Name		VLAN	Traffic Type	Security Group	Layer-2 Flooding	Wireless Pool	Bridge-Network Virtual Machine	Layer-2 Extension
VLAN0039	S1-CLIENT-IP 10.0.0.0/24	39	Data	-	Disabled	Enabled	Disabled	Enabled

Showing 1 of 1

Modifica rete virtuale

Passaggio 3. Sul lato GUI del WLC, selezionare Configuration > Wireless > Fabric > General (Configurazione > Wireless > Fabric > Generale). Aggiungere un nuovo client e un AP VN_ID.

Quando il pool viene assegnato alla rete virtuale, l'interfaccia dell'infrastruttura corrispondente al mapping VNID viene inviata al controller. Si tratta di VNID L2.

Configuration > Wireless > Fabric

General Control Plane Profiles

Fabric Status

ENABLED

Apply

Fabric VNID Mapping

+ Add X 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

Aggiungi nuovo client e AP VN_ID

Passaggio 4. Gli SSID vengono mappati al pool nelle rispettive reti virtuali:

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 Personal	Voice + Data	Choose Pool 10_1_0_0-S2_Corp_VN	Assign SGT

SSID mappati

Passaggio 5. Un profilo di infrastruttura con VNID L2 viene aggiunto al pool scelto e il profilo dei criteri viene mappato al profilo di infrastruttura, è abilitato per Fabric.

Dal lato GUI del WLC, selezionare Configuration > Wireless > Fabric > Profiles (Configurazione > Wireless > Fabric > Profili).

Edit Fabric Profile

Configuration > Wireless > Fabric > Profiles

⚠️ Modifying the profile may result in loss of connectivity

General	Control Plane				
+ Add	X D				
<table border="1"> <thead> <tr> <th>Fabric Profile Name</th> </tr> </thead> <tbody> <tr> <td>s2-demo_Global_F_d3r</td> </tr> </tbody> </table>		Fabric Profile Name	s2-demo_Global_F_d3r		
Fabric Profile Name					
s2-demo_Global_F_d3r					
<table border="1"> <thead> <tr> <th>L2 VNID</th> <th>SGT Tag</th> </tr> </thead> <tbody> <tr> <td>8189</td> <td>2-65519</td> </tr> </tbody> </table>		L2 VNID	SGT Tag	8189	2-65519
L2 VNID	SGT Tag				
8189	2-65519				

Profilo fabric

Passaggio 6. Passare a Configurazione > Tag e profili > Criterio. Verificare il profilo infrastruttura mappato al profilo criteri:

The screenshot shows the 'Edit Policy Profile' interface in Cisco DNA Center. The 'Advanced' tab is active. A warning message at the top states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.' The 'Fabric Profile' section is highlighted with a red box, showing 's2-demo_Global_F_b' selected. Other settings include WLAN Timeout (Session Timeout: 1800 sec, Idle Timeout: 300 sec, Idle Threshold: 0 bytes), Link-Local Bridging (unchecked), mDNS Service Policy (default-mdns-ser ...), and Hotspot Server (Search or Select).

Profilo infrastruttura configurato nel criterio

Verifica

Verifica della configurazione del fabric su WLC e Cisco DNA

Dalla CLI del WLC:

WLC1# show tech

WLC1# show tech wireless

Configurazione del control plane:

lisp router

tabella di localizzazione predefinita

WLC locator-set

172.16.201.202

exit-locator-set

!

sessione map-server WLC a apertura passiva

sito_uci

descrizione map-server configurato da Cisco DNA-Center

authentication-key 7 <Chiave>

Sessione lisp CB1-S1#sh

Sessioni per VRF predefinite, totale: 9, stabilito: 5

Stato Peer Attivo/Inattivo In/Out

172.16.201.202:4342 Su 3d07h 14/14

Configurazione WLC:

fabric wireless

wireless fabric control-plane default-control-plane

indirizzo ip 172.16.2.2, chiave 0 47aa5a

WLC1# show fabric map-server summary

Stato connessione MS-IP

—

172.16.1.2 SU

WLC1# show wireless fabric summary

Stato fabric: Attivato

Piano di comando:

Nome Indirizzo IP Stato chiave

—

default-control-plane 172.16.2.2 47aa5a Up

Dalla GUI del WLC, selezionare Configuration > Wireless > Fabric (Configurazione > Wireless > Fabric) e verificare se lo stato del fabric è Enabled (Abilitato).

Selezionare Configuration > Wireless > Access Point. Selezionare un punto di accesso dall'elenco. Verificare che lo stato dell'infrastruttura sia Abilitato.

Su Cisco DNA, passare a Provisioning > Siti fabric e verificare se si dispone di un sito fabric. Sul sito dell'infrastruttura, passare a Fabric Infrastructure > Fabric e verificare se il WLC è abilitato come infrastruttura.

Risoluzione dei problemi

Il client non ottiene l'indirizzo IP

Passaggio 1. Verificare se l'SSID è fabric. Dalla GUI del WLC, selezionare Configuration > Tag e profili > Criteri. Selezionare il criterio e passare a Avanzate. Verificare se il profilo dell'infrastruttura è abilitato.

Passaggio 2. Verificare se il client è bloccato nello stato di apprendimento IP. Dalla GUI del WLC, selezionare Monitoraggio > Wireless > Client. Verificare lo stato del client.

Passaggio 3. Verificare se il criterio è DHCP obbligatorio.

Passaggio 4. Se il traffico viene commutato localmente tra il nodo del punto di accesso e il nodo del bordo, raccogliere i log del punto di accesso (traccia del client) per la connessione del client. Verificare se il rilevamento DHCP è stato inoltrato. Se non viene ricevuta alcuna offerta DHCP, si verifica un errore nel nodo perimetrale. Se il protocollo DHCP non viene inoltrato, significa che si è verificato un errore nell'access point.

Passaggio 5. È possibile raccogliere un EPC sulla porta del nodo perimetrale per visualizzare i pacchetti DHCP discover. Se il comando DHCP discover packets non è visibile, il problema è nell'access point.

SSID non trasmesso

Passaggio 1. Verificare se le radio AP sono inattive.

Passaggio 2. Verificare che la WLAN sia nello stato attivo e che il SSID di trasmissione sia abilitato.

Passaggio 3. Verificare la configurazione del punto di accesso se il punto di accesso è abilitato per l'infrastruttura. Passare a Configurazione > Wireless > Access Point, selezionare un access point e nella scheda Generale è possibile visualizzare lo stato del fabric abilitato e le informazioni RLOC.

Passaggio 4. Passare a Configurazione > Wireless > Fabric > Control Plane. Verificare che il control plane sia configurato (con l'indirizzo IP).

Passaggio 5. Passare a Configurazione > Tag e profili > Criterio. Selezionare il criterio e passare a Avanzate. Verificare se il profilo dell'infrastruttura è abilitato.

Passaggio 6. Passare a Cisco DNA e ripetere la procedura su [Crea SSID](#) e [Esegui provisioning WLC](#). Il Cisco DNA deve spingere di nuovo il SSID sul WLC.

Informazioni correlate

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuracy di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).