Understand Access Tunnel Creation in SD-Access

Contents

Introduction

This document describes what an access tunnel is in SD-Access, its purpose, and how you can triage the formation of the access tunnel.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Locator ID Separation Protocol (LISP)
- Wireless

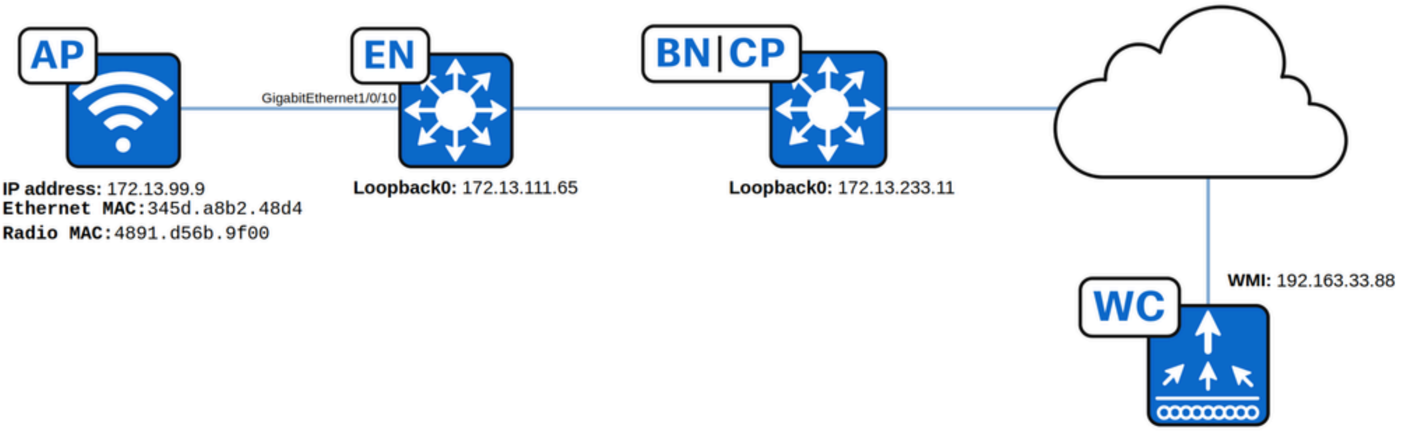
Components Used

The information in this document is based on these software and hardware versions:

- Cisco Wireless LAN Controller (WLC) - C9800-CL, Cisco IOS® XE 17.12.04
- SDA Edge Node - C9300-48P, Cisco IOS® XE 17.12.05
- SDA Border Node/Control Plane - C9500-48P, Cisco IOS® XE 17.12.05
- Cisco Access Point - C9130AXI-A, version 17.9.5.47

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Topology



Topology used in this article

Overview

An access-tunnel in Cisco SD-Access is a Virtual Extensible LAN (VXLAN) tunnel established between fabric edge nodes and Access Points (APs). This tunnel encapsulates client traffic in VXLAN, enabling seamless communication within the SD-Access fabric. The access-tunnel serves as a data plane overlay that carries traffic from wireless clients connected to the access point to the fabric edge, ensuring consistent policy enforcement and segmentation across the network.

Access-tunnel Formation Process

1. AP is plugged in and powers up via Power over Ethernet (PoE).
2. AP gets an IP address via DHCP in the overlay. During this process the AP also receives the option 43 from the DHCP server for the Wireless LAN Controller.
3. Fabric edge registers AP's IP address and Ethernet MAC and updates the LISP Control Plane.
4. WLC queries the LISP CP to know if the AP is connected to a fabric device .
5. LISP Control plane replies to the WLC with locator (Loopback 0 IP) of the fabric device which has the AP connected. If there is an answer it means the AP is attached to Fabric and is marked as Fabric enabled.
6. WLC does a L2 LISP registration for the AP Radio MAC in the LISP Control plane along with metada information from the WLC to the FE.
7. LISP Control plane notifies fabric edge and sends the metadata received from WLC. This metadata contains a flag that indicates that it is an AP and the AP IP address.
8. Fabric edge processes the informatio. It learns it is an AP and creates a VXLAN tunnel also known as Access tunnel between the AP and the fabric edge.

Read through these steps to ensure successful access-tunnel formation for AP onboarding within SD-Access. Any failure in these checks can prevent tunnel creation. If a step does not produce the expected results, focus troubleshooting efforts on the component related to that step.

Verify the Process

Verify if the AP Obtains an IP Address

To verify that the AP is receives an IP address, run this command on the edge node:

<#root>

```
Edge#show device-tracking database interface gigabitEthernet 1/0/10


...
     Network Layer Address   Link Layer Address  Interface  vlan prlvl age state     Time left
DH4

172.13.99.9



345d.a8b2.48d4

      Gi1/0/10

99

   0024  15s REACHABLE 237 s try 0(47302 s)
```

From the previous output, it can be confirmed that the AP connected to interface GigabitEthernet 1/0/10 has the IP address 172.13.99.9 on VLAN 99, with Ethernet MAC address 345d.a8b2.48d4.
If the output is empty, the AP has either failed to obtain an IP address or Power over ethernet (PoE) is not functioning. To confirm that PoE is operational, verify that the access point's MAC address is displayed in the MAC address table by running this command:

<#root>

```
Edge#show mac address-table interface gigabitEthernet 1/0/10


Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----

99



345d.a8b2.48d4

 DYNAMIC

Gi1/0/10
```

To confirm that inline power for PoE is operational, run this command:

<#root>

```
Edge#show power inline gigabitEthernet 1/0/10


Interface  Admin

Oper

   Power   Device      Class  Max
                         (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/10    auto

on
```

```
    30.0   C9130AXI-A   4    30.0
```

PoE is operational and working at 30.0 watts.

Note: After obtaining an IP address, the access point attempts to join the Wireless LAN Controller (WLC), similar to traditional networking. If the AP is not listed when running the show ap summary command, troubleshoot AP join.

Verify AP’s IP and Ethernet MAC Registration on LISP Control Plane

To identify the control plane, also known as the map server, for the fabric edge, run the command:

<#root>

```
Edge#show lisp session


Sessions for VRF default, total: 1, established: 1
Peer State Up/Down In/Out Users
```

```
172.13.233.11

:4342 Up 1d02h 326/324 12
```

Control plane is 172.13.233.11 which would be the loopback0 for that device.

Another way to identify the control plane for the fabric site is to run this command:

<#root>

```
Edge#show running-config | section map-server


etr map-server

172.13.233.11

 key 7 050F020C734848514D514117595853732F
etr map-server

172.13.233.11

 proxy-reply
etr map-server

172.13.233.11

 key 7 050F020C734848514D514117595853732F
etr map-server

172.13.233.11

 proxy-reply
```

On the WLC, you can also verify that the LISP session with the control plane is in the UP state:

<#root>

```
WLC#show wireless fabric summary


Fabric Status :

Enabled



Control-plane:
Name                    IP-address       Key                 Status
--------------------------------------------------------------------------------------------
default-control-plane

172.13.233.11

    ddc2df8446e2479d

Up
```

Use this command to find the AP's IP registered on the control plane:

<#root>

```
Border#show lisp instance-id 4097 ipv4 server 172.13.99.9


LISP Site Registration Information
...

EID-prefix: 172.13.99.9/32 instance-id 4097


First registered: 22:14:34
Last registered: 22:14:34
Routing table tag: 0
Origin: Dynamic, more specific of 172.13.99.0/24
...
TTL: 1d00h

State: complete


Extranet IID: Unspecified
Registration errors:

Authentication failures: 0


Allowed locators mismatch: 0

ETR 172.13.111.65:21839, last registered 22:14:34, proxy-reply, map-notify <-- Last registration


     TTL 1d00h, no merge, hash-function sha1
     state complete, no security-capability
    ...
     Domain-ID 1559520338
     Multihoming-ID unspecified
     sourced by reliable transport

Locator

       Local State Pri/Wgt Scope

172.13.111.65

 yes   up    10/10   IPv4 none
```

Note: APs always use the INFRA_VN for Layer 3, and this INFRA_VN is always mapped to instance ID 4097.

The registration is complete for the AP with IP address 172.13.99.9. There are no authentication failures, and it is connected to the edge node 172.13.111.65 (Locator).

To verify if the MAC address is registered on the control plane, first, identify the Layer 2 instance ID for the VLAN to which the AP is connected. Use these commands:

<#root>

```
Edge#show vlan id 99


VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------

99

 AP_VLAN active

L2LI0:8188
```

```
, Gi1/0/10, Ac0
...
```

VLAN **99** is mapped to instance ID 8188. Using this instance ID, run this command to confirm if the Ethernet MAC address is registered on the control plane:

<#root>

```
Border#show lisp instance-id 8188 ethernet server 345d.a8b2.48d4


LISP Site Registration Information
...

EID-prefix: 345d.a8b2.48d4/48 instance-id 8188


First registered: 22:57:39
Last registered: 22:57:39
Routing table tag: 0
Origin: Dynamic, more specific of any-mac
...

State: complete


Extranet IID: Unspecified
Registration errors:

Authentication failures: 0


Allowed locators mismatch: 0

ETR 172.13.111.65:21839, last registered 22:57:39, proxy-reply, map-notify


   TTL 1d00h, no merge, hash-function sha1
   state complete, no security-capability
   ...
   Domain-ID 1559520338
   Multihoming-ID unspecified
   sourced by reliable transport

Locator

      Local State Pri/Wgt Scope

172.13.111.65

 yes   up    10/10   IPv4 none
```

The registration for AP's ethernet MAC 345d.a8b2.48d4 is complete without any authentication failures and is connected on edge node 172.13.111.65 (Locator).

Verify That the WLC Is Marking the Device As Fabric-Enabled

<#root>

```
WLC#show fabric ap summary
```

```
Number of Fabric AP : 1

AP Name           Slots  AP Model

Ethernet MAC



Radio MAC

        Location Country

IP Address

  State
---------------------------------------------------------------------------------------------------------
AP345D.A8B2.48D4  3      C9130AXI-A

345d.a8b2.48d4



4891.d56b.9f00

   default location MX

172.13.99.9

 Registered
```

The AP with IP address 172.13.99.9 is correctly marked as a Fabric AP. If the AP is not listed, it indicates that the WLC failed to receive a response from the LISP control plane. In this output, the radio MAC address for the AP is 4891.d56b.9f00.

Note: If the AP is registered on the control plane but is not marked as Fabric-enabled, ensure that no firewall is blocking LISP traffic on UDP port 4342.

Verify the Radio MAC registration on LISP control plane

Use the same command that was used to verify the registration of the Ethernet MAC address, but replace the Ethernet MAC address with the radio MAC address:

<#root>

```
Border#show lisp instance-id 8188 ethernet server 4891.d56b.9f00


LISP Site Registration Information
...

EID-prefix: 4891.d56b.9f00/48 instance-id 8188


First registered: 22:49:43
Last registered: 22:49:43
Routing table tag: 0
```

```
Origin: Dynamic, more specific of any-mac
...
State: complete
Extranet IID: Unspecified
Registration errors:

Authentication failures: 0


Allowed locators mismatch: 0
ETR 192.163.33.88:59019, last registered 22:49:43, no proxy-reply, no map-notify
   TTL 1d00h, no merge, hash-function sha2
   state complete, no security-capability
   ...
   sourced by reliable transport
   Affinity-id: 0 , 0


WLC AP bit: Set



Locator

       Local State Pri/Wgt Scope

172.13.111.65

 yes   up    0/0     IPv4 none
```

The radio MAC address is fully registered without any authentication failures and is connected to edge node 172.13.111.65 (Locator). The output also shows WLC AP bit: Set, a flag used by the LISP control plane to indicate to the edge node that this registration belongs to an AP on its RLOC 172.13.111.65.

Verify the Access Tunnel Creation

The final step is to verify the creation of the access tunnel on the fabric edge. As stated earlier, this is the ultimate goal of AP onboarding in SD-Access. To verify the creation of the access tunnel, run this command:

<#root>

```
Edge#show access-tunnel summary


Access Tunnels General Statistics:
Number of AccessTunnel Data Tunnels = 1
Name   RLOC IP(Source)   AP IP(Destination) VRF ID Source Port Destination Port
------ --------------- ------------------ ------ ----------- ----------------

Ac0



172.13.111.65



172.13.99.9

       0      N/A         4789
```

```
Name IfId Uptime
------ ---------- --------------------

Ac0 0x00000058 0 day, 00:00:51
```

Access tunnel 0 connects AP 172.13.99.9 to edge node locator 172.13.111.65 and has been up for 51 seconds. The timer is set to 0 after every reset.

You can also confirm that the tunnel is programmed at the Forwarding Engine Driver (FED) abstraction layer, which interfaces directly with the switch hardware:

<#root>

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


Interface    IF_ID        State
----------------------------------------------------------------------

Ac0

0x00000058

  READY
```

Using the IF_ID, you can find more information about this tunnel:

<#root>

```
Edge#show platform software fed switch active ifm if-id 0x00000058


Interface IF_ID : 0x0000000000000058
Interface Name : Ac0
Interface Block Pointer : 0x73d6c83dc6f8

Interface Block State : READY


Interface State : Enabled


...

Interface Type : ACCESS_TUNNEL


...
Tunnel Type : L2Lisp
Encap Type : VxLan
...
```

This is a L2 lisp tunnel using VXLAN encapsulation and the interface type is access-tunnel.

Note: It is important that the number of access tunnels matches in the output of both the **show access-tunnel summary** command and the FED command. A mismatch can indicate a misprogramming.

On the AP, you can verify the creation for the access tunnel with this command:

<#root>

```
AP#show ip tunnel fabric


Fabric GWs Information:
Tunnel-Id GW-IP         GW-MAC            Adj-Status Encap-Type Packet-In
  Bytes-In Packet-Out Bytes-out
        1

172.13.111.65
```

```
00:00:0C:9F:F2:80

 Forward

VXLAN

      121
   17096    239       35041
AP APP Fabric Information:
GW_ADDR ENCAP_TYPE VNID SGT FEATURE_FLAG GW_SRC_MAC GW_DST_MAC
```

The AP has an access tunnel pointing to the edge node's locator 172.13.111.65. The MAC address 00:00:0C:9F:F2:80 belongs to Switch virtual interface (SVI) 99, which is the VLAN where the AP is connected. The encapsulation type is VXLAN.

Tip: The tunnel appears on the AP only when an active client is connected. Otherwise, the command returns an empty output.

Debugs and Traces

For more advanced debugging of access tunnel creation, enable these traces on the fabric edge:

```
set platformsoftware trace forwarding-manager switch active R0 access-tunnel debug
set platform software trace forwarding-manager switch active F0 access-tunnel debug
set platform software trace forwarding-manager switch active access-tunnel noise
request plat sof trace rotate all
show pla sof trace message forwarding-manager switch active R0 reverse
show pla sof trace message forwarding-manager switch active F0 reverse
show pla sof trace message fed sw active reverse
```

Catalyst 9000 access-tunnel platform-dependent commands to verify access-tunnel programming on fabric edge:

```
show platform software fed switch active ifm interfaces access-tunnel
show platform software access-tunnel switch active R0
show platform software access-tunnel switch active R0 statistics
show platform software access-tunnel switch active F0
show platform software access-tunnel switch active F0 statistics
show platform software fed switch active ifm if-id <if-id>
```

For debugging the process for the access tunnel on the WLC, enable these commands:

```
set platform software trace wncd chassis active r0 lisp-agent-api
set platform software trace wncd chassis active r0 lisp-agent-db
set platform software trace wncd chassis active r0 lisp-agent-fsm
set platform software trace wncd chassis active r0 lisp-agent-ha
set platform software trace wncd chassis active r0 lisp-agent-internal g
set platform software trace wncd chassis active r0 lisp-agent-lib
set platform software trace wncd chassis active r0 lisp-agent-lispmsg
set platform software trace wncd chassis active r0 lisp-agent-shim
set platform software trace wncd chassis active r0 lisp-agent-transport
```

Debugs for Registration Process. These commands can be run on the edge node to verify if it is attempting to register the AP's IP address and Ethernet MAC, and on the control plane to confirm if registration is occurring successfully.

```
debug lisp filter eid <mac-or-ip>
debug lisp control-plane all
```

Summary

- Access-tunnels in SD-Access are VXLAN tunnels between fabric edge nodes and access points that carry client traffic within the fabric encapsulated in VXLAN.

- They enable unified wireless data planes and consistent policy enforcement because the security group tag (SGT) is tagged at access point level for wireless endpoints.
- Verification and triage involve checking registration on fabric control plane, confirm creation on fabric edge nodes, and verify fabric status for the AP on the WLC using specific show commands.
- Troubleshooting focuses on ensuring tunnels are correctly created and remain stable after configuration changes.
- Access tunnel is the final goal when onboarding a new AP to SD-Access.