Connecting to Digital
Connect & Secure 2019

Deepdive SD-Access

Jesse Schmidt
Systems Engineer Enterprise Networks

14 maart 2019
Cisco DNA Architecture

Intent-based networking

Cisco DNA Center™

Cisco DNA Automation

Cisco DNA Security

Cisco DNA Assurance

Traditional Cisco and third-party networks

Cisco DNA-ready networks

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Fabric
Underlay – Overlay
What exactly is a Fabric?

A Fabric is an Overlay

• An Overlay network is a logical topology used to virtually connect devices, built on top of some arbitrary physical Underlay topology.

• An Overlay network often uses alternate forwarding attributes to provide additional services, not provided by the Underlay.

Examples of Network Overlays

- GRE or mGRE
- MPLS or VPLS
- IPSec or DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI
SD-Access Underlay / Overlay

Overlay Network

Overlay Control Plane

Encapsulation

Edge Device

Underlay Network

Underlay Control Plane

Hosts
(End-Points)

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
**SD-Access Underlay**

**Manual vs. Automated**

### Manual Underlay

You can reuse your existing IP network as the Fabric Underlay!

- **Key Requirements**
  - IP reach from Edge to Edge/Border/CP
  - Can be L2 or L3 – We recommend L3
  - Can be any IGP – We recommend ISIS

- **Key Considerations**
  - MTU (Fabric Header adds 50B)
  - Latency (RTT of ≤/≥ 100ms)

### Automated Underlay

Prescriptive fully automated Global and IP Underlay Provisioning!

- **Key Requirements**
  - Leverages standard PNP for Bootstrap
  - Assumes New / Erased Configuration
  - Uses a Global “Underlay” Address Pool

- **Key Considerations**
  - PNP pre-setup is required
  - 100% Prescriptive (No Custom)
Fabric Roles & Terminology

- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – External Data Collector(s) are leveraged to analyze Endpoint to App flows and monitor fabric status
- **Control Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access Fabric
- **Fabric Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access Fabric
- **Fabric Wireless Controller** – A Fabric device (WLC) that connects Wireless Endpoints to the SD-Access Fabric
Virtual Network maintains a separate Routing & Switching instance for the devices within it.
SD-Access Scalable Group

Scalable Group is a logical ID object to “group” Users and/or Devices.
SD-Access Host Pool

Host Pool provides basic IP functions necessary for attached Endpoints
Anycast GW provides a single L3 Default Gateway for IP capable endpoints.
SD-Access Stretched Subnets

**Stretched Subnets** allow an IP subnet to be “stretched” via the overlay.
Layer2 Overlays allows Non-IP hosts to connect Broadcast & Multicast
SD-Access Key Components
Key Components of SD-Access

1. Control Plane based on LISP
2. Data-Plane based on VXLAN
3. Policy-Plane based on TrustSec

Key Differences

- L2 + L3 Overlay vs L2 or L3 Only
- Host Mobility with Anycast Gateway
- Adds VRF + SGT into Data-Plane
- Virtual Tunnel Endpoints (No Static)
- No Topology Limitations (Basic IP)
SD-Access Key Component – LISP

1. Control Plane based on LISP

Routing Protocols = Big Tables & More CPU with Local L3 Gateway

BEFORE

IP Address = Location + Identity

LISP DB + Cache = Small Tables & Less CPU with Anycast L3 Gateway

AFTER

Separate Identity from Location

Routing Protocols = Big Tables & More CPU

Endpoint Routes are Consolidated to LISP DB

Topology Routes + Endpoint Routes

Only Local Routes

Top Mobility
Locator / ID Separation Protocol
LISP Mapping System

LISP “Mapping System” is analogous to a DNS lookup

- DNS resolves **IP Addresses** for queried **Name**
  - Answers the “WHO IS” question

  ![Diagram of DNS resolution](image)
  
  **Host**
  
  **DNS Server**
  
  [Who is `lisp.cisco.com`?]

  - Address is `153.16.5.29, 2610:D0:110C:1::3`

  ![DNS URL Resolution](image)

- LISP resolves **Locators** for queried **Identities**
  - Answers the “WHERE IS” question

  ![Diagram of LISP resolution](image)
  
  **LISP Router**
  
  **LISP Map System**
  
  [Where is `2610:D0:110C:1::3`?]

  - Locator is `128.107.81.169, 128.107.81.170`
SD-Access Key Components – VXLAN

1. Control Plane based on LISP
2. Data-Plane based on VXLAN

- Supports L2 Overlay
- Supports L3 Overlay
SD-Access Key Components – TrustSec

1. Control Plane based on LISP
2. Data-Plane based on VXLAN
3. Policy-Plane based on TrustSec
SD-Access Wireless Integration
Wireless Integration
Where to connect APs and WLC?

Access Points
• AP is directly connected to FE
• AP is part of Fabric overlay
• AP belongs to the INFRA_VRF which is mapped to the global routing table (new in DNAC 1.1)
• AP joins the WLC in Local mode

WLC
• WLC is connected outside Fabric (optionally directly to Border)
• WLC needs to reside in global routing table
• No need for inter-VRF leaking for AP to join the WLC
• WLC can only belong to one FD. WLC talks to one CP (two for HA)

Design Notes:
1) Fabric AP is in local mode, need < 20ms latency between AP & WLC
2) If WLC is used also for non-Fabric (mixed mode), considered MAC and ARP table scale of the directly-connected Border device
Key takeaways

• Plan your personal demo: https://cs.co/sdademo
• Contact your Cisco AM to schedule a design session
• Pick up your SD-Access book