Software Defined Access

Under The Hood

Shawn Wargo
Principal Engineer - Technical Marketing
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKCRS-2810
Software Defined Access
Cisco Live Barcelona - Session Map

Missed One? Sessions are available online @ CiscoLive.com

You Are Here

Tuesday (Jan 30)
08:00-11:00
11:00-13:00
13:00-15:00
15:00-18:00

BRKEWN-2021
SDA Setup

BRKEWN-2020
Wireless Overview

Hardware Overview

Wednesday (Jan 31)
08:00-11:00
11:00-13:00
13:00-15:00
15:00-18:00

BRKDCN-2489
DC Integration

BRKCRS-2814
Assurance

Design & Scale

Thursday (Feb 01)
08:00-11:00
11:00-13:00
13:00-15:00
15:00-18:00

BRKCRS-2811
External Connect

BRKCRS-2816
Routed Underlay

Migration

Friday (Feb 02)
08:00-11:00
11:00-13:00
13:00-15:00
15:00-18:00

LTRCRS-2810 (1)
Hands-On Lab

LTRCRS-2810 (2)
Hands-On Lab

LTRCRS-2810
Hands-On Lab
Session Agenda

1. **Key Benefits**
   Why do you care?

2. **Key Concepts**
   What is SD-Access?

3. **Fabric Fundamentals**
   How does it work?

4. **Controller Fundamentals**
   How does it work?

5. **Take Away**
   Where to get started?
Key Benefits

Why do you care?
New Requirements for the Digital Age

Insights & Actions
Automation & Assurance
Security & Compliance

Innovate FASTER
REDUCE Cost & Complexity
LOWER Risk

Cisco Digital Network Architecture (DNA)
Cisco’s Intent-based Networking

The Network. Intuitive.

Powered by Intent. Informed by Context.

DNA Center
- Policy
- Automation
- Analytics

Network Infrastructure
- Switching
- Routers
- Wireless

Learning

Intent

Context

Security
Software Defined Access
Networking at the speed of Software!

- **DNA Center**
  - Policy
  - Automation
  - Analytics

- **Identity-Based**
  - Policy & Segmentation
  - Decoupled security policy from VLAN and IP Address

- **Automated Network Fabric**
  - Single Fabric for Wired & Wireless
  - with workflow Automation

- **Insights & Telemetry**
  - Analytics and Insights into User and Application behavior

- **IoT Network**
- **Employee Network**
- **SDA Extension**
- **User Mobility**
  - Policy stays with user
Streamlined Design

“Create site hierarchy, build out wireless heat maps and formulate reusable network profiles for your device provisioning...”
Simplified Provisioning

“Deploy devices into your Network using “world class” prescriptive configurations with Minimal Clicks...”
Segmentation

“Virtual Networks and Micro-Segmentation made simple to more effectively secure boundaries between user and device groups...”
Policy Enforcement

“Assigned policy follows users and devices irrespective of location or place in network...”
Insights & Telemetry

“Proactive issue identification and resolution through analytics and insights into User and Application behavior...”

SD-Access Benefits
Key Concepts

What is Software Defined Access?
What is SD-Access?
What is SD-Access?

Campus Fabric + DNA Center (Automation & Assurance)

- **Campus Fabric**
  - **CLI or API approach** to build a LISP + VXLAN + CTS Fabric overlay for your enterprise Campus networks
    - CLI provides backwards compatibility but management is box-by-box.
    - API provides device automation via NETCONF/YANG
  - Separated management systems
What is SD-Access?
Campus Fabric + DNA Center (Automation & Assurance)

- **SD-Access**
  - GUI approach provides automation & assurance of all Fabric configuration, management and group-based policy
  - DNA Center integrates multiple systems, to orchestrate your LAN, Wireless LAN and WAN access

- **Campus Fabric**
  - CLI or API approach to build a LISP + VXLAN + CTS Fabric overlay for your enterprise Campus networks
  - CLI provides backwards compatibility but management is box-by-box. API provides device automation via NETCONF/YANG
  - Separated management systems
Roles & Terminology

What is Software Defined Access?

1. High-Level View
2. Roles & Platforms
3. Fabric Constructs
A Fabric is an Overlay

An *Overlay network* is a *logical topology* used to *virtually connect* devices, built *over* an 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, mGRE
- MPLS, VPLS
- IPSec, DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI
SD-Access
Fabric Terminology

Overlay Network
Overlay Control Plane
Encapsulation

Edge Device

Underlay Network
Underlay Control Plane
Hosts (End-Points)
Why Overlays?

**Flexible Virtual Services**
- Mobility - Map Endpoints to Edges
- Services - Deliver using Overlay
- Scalability - Reduce Protocol State
- Flexible and Programmable

**Simple Transport Forwarding**
- Redundant Devices and Paths
- Keep It Simple and Manageable
- Optimize Packet Handling
- Maximize Network Reliability (HA)

*SD-Access*

Separate the “Forwarding Plane” from the “Services Plane”
SD-Access
Fabric 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**
Fully automated prescriptive IP network Underlay Provisioning!

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

- **Key Considerations**
  - Seed Device pre-setup is required
  - 100% Prescriptive (No Custom)
Would you like to know more?
Routed Underlay

Check out the following session:

**BRKCRS-2816**
SD-Access - Building the Routed Underlay

This session covers:
- More details about Fabric Underlay
- How to automate Underlay setup
- Underlay best practices and tips
Would you like to know more?
Routed Underlay

Check out the following session:

**BRKCRS-2812**
SD-Access - Integrating with Existing Network

This session covers:
- More details about Fabric Underlay & Overlay
- How to migrate legacy networks to SD-Access
- Various SD-Access design approaches
DNA Center – Enterprise SDN Controller provides GUI management and abstraction via Apps that share context

Identity Services – NAC & ID Systems (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition

Analytics Engine – Data Collectors (e.g. NDP) 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 SDA Fabric

Fabric Edge Nodes – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric

Fabric Wireless Controller – A Fabric device (WLC) that connects APs and Wireless Endpoints to the SDA Fabric
Roles & Terminology

What is Software Defined Access?

1. High-Level View
2. Roles & Platforms
3. Fabric Constructs
**Control-Plane Node** runs a Host Tracking Database to map location information

- A simple Host Database that maps Endpoint IDs to a current Location, along with other attributes
- Host Database supports multiple types of Endpoint ID lookup types (IPv4, IPv6 or MAC)
- Receives Endpoint ID map registrations from Edge and/or Border Nodes for “known” IP prefixes
- Resolves lookup requests from Edge and/or Border Nodes, to locate destination Endpoint IDs
SD-Access Platforms
Control-Plane Nodes

**Catalyst 3K**
- Catalyst 3850
- 1/10G SFP
- 10/40G NM Cards
- IOS-XE 16.6.2+

**Catalyst 9K**
- Catalyst 9500
- 10/40G SFP/QSFP
- 10/40G NM Cards
- IOS-XE 16.6.2+

**Catalyst 6K**
- Catalyst 6800
- Sup2T/6T
- 6840/6880-X
- IOS 15.4.1SY4+

**ASR1K, ISR4K & CSRv**
- CSRv
- ASR 1000-X/HX
- ISR 4300/4400
- IOS-XE 16.6.2+

* Wired Only
SD-Access Fabric
Edge Nodes – A Closer Look

**Edge Node** provides first-hop services for Users / Devices connected to a Fabric

- Responsible for Identifying and Authenticating Endpoints (e.g. Static, 802.1X, Active Directory)
- Register specific Endpoint ID info (e.g. /32 or /128) with the Control-Plane Node(s)
- Provide an Anycast L3 Gateway for the connected Endpoints (same IP address on all Edge nodes)
- Performs encapsulation / de-encapsulation of data traffic to and from all connected Endpoints
SD-Access Platforms
Edge Nodes

**Catalyst 3K**
- Catalyst 3650/3850
- 1/MGIG RJ45
- 10/40G NM Cards
- IOS-XE 16.6.3+

**Catalyst 9K**
- Catalyst 9300
- 1/MGIG RJ45
- 10/40/mG NM Cards
- IOS-XE 16.6.3+

**Catalyst 4K**
- Catalyst 4500
- Sup8E/9E (Uplink)
- 4700 Cards
- IOS-XE 3.10.1+

**Catalyst 9400**
- Catalyst 9400
- Sup1E
- 9400 Cards
- IOS-XE 16.6.3+
SD-Access @ DNA Center

Edge Nodes

Select Devices  Host Onboarding

1. Select device to be added to the fabric
2. Select Control Plane Node
3. Select Border Node

Validation

Search Topology

Select Devices to add, remove or identify. Shift + Click to select multiple.
SD-Access Fabric

Border Nodes

**Border Node** is an Entry / Exit point for data traffic going In / Out of a Fabric

There are 2 Types of **Border Node**!

- **Internal Border**
  - Used for “Known” Routes inside your company

- **External Border (Default)**
  - Used for “Unknown” Routes outside your company
# SD-Access Platforms

**Border Nodes**

<table>
<thead>
<tr>
<th>Catalyst 3K</th>
<th>Catalyst 9K</th>
<th>Catalyst 6K</th>
<th>ASR1K &amp; ISR4K</th>
<th>Nexus 7K*</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.jpg" alt="Catalyst 3K Image" /></td>
<td><img src="image2.jpg" alt="Catalyst 9K Image" /></td>
<td><img src="image3.jpg" alt="Catalyst 6K Image" /></td>
<td><img src="image4.jpg" alt="ASR1K &amp; ISR4K Image" /></td>
<td><img src="image5.jpg" alt="Nexus 7K* Image" /></td>
</tr>
<tr>
<td><strong>Catalyst 3850</strong></td>
<td><strong>Catalyst 9500</strong></td>
<td><strong>Catalyst 6800</strong></td>
<td><strong>ASR 1000-X/HX</strong></td>
<td><strong>Nexus 7700</strong></td>
</tr>
<tr>
<td>1/10G SFP+</td>
<td>10/40G SFP/QSFP</td>
<td>Sup2T/6T</td>
<td>ISR 4430/4450</td>
<td>Sup2E</td>
</tr>
<tr>
<td>10/40G NM Cards</td>
<td>10/40G NM Cards</td>
<td>6840/6880-X</td>
<td>1/10G/40G</td>
<td>M3 Cards</td>
</tr>
<tr>
<td>IOS-XE 16.6.3+</td>
<td>IOS-XE 16.6.3+</td>
<td>IOS 15.4.1SY4+</td>
<td>IOS-XE 16.6.3+</td>
<td>NXOS 8.2.1+</td>
</tr>
</tbody>
</table>

* External Border Only
**Internal Border** advertises Endpoints to outside, and known Subnets to inside

- Connects to any “known” IP subnets available from the outside network (e.g. DC, WLC, FW, etc.)

- Exports all internal IP Pools to outside (as aggregate), using a traditional IP routing protocol(s).

- Imports and registers (known) IP subnets from outside, into the Control-Plane Map System

- Hand-off requires mapping the context (VRF & SGT) from one domain to another.
External Border is a “Gateway of Last Resort” for any unknown destinations

- Connects to any “unknown” IP subnets, outside of the network (e.g. Internet, Public Cloud)
- Exports all internal IP Pools outside (as aggregate) into traditional IP routing protocol(s).
- Does NOT import unknown routes. It is a “Default” Exit, if no entry is available in Control-Plane.
- Hand-off requires mapping the context (VRF & SGT) from one domain to another.
SD-Access @ DNA Center

External Borders

PHOENIX

Select Devices
Host Onboarding

1. Select device to be added to the fabric
2. Select Control Plane Node
3. Select Border Node

Validation

Search Topology

Select Devices to add, remove or identify. Shift + Click to select multiple.

Border to

- Rest of Company (internal)
- Outside World (External)
- Anywhere (Internal & External)

BGP

Local AS Number
65535

Border Handoff

- Layer 3

VRF-Lite

Border_Automation (192.168.111.0/24)

External Interface

Feedback
SD-Access - Border Deployment

Why? Internal Traffic with External Borders
SD-Access - Border Deployment
Why? Internal Traffic with Internal Borders
Would you like to know more?

External Connectivity

Check out the following session:

**BRKCRS-2811**

SD-Access - Connecting to External Networks

This session covers:

- More details about Fabric Border Nodes
- How Borders communicate to outside networks
- Various Fabric Border design approaches
Would you like to know more?
External Connectivity

Check out the following session:

**BRKCRS-2815**
SD-Access - Deploy a Fabric in Large Enterprise

This session covers:

- More details about Fabric Border Nodes
- How multiple Fabrics communicate
- Various Multi-Site design approaches
**Fabric Enabled WLC** is integrated into Fabric for SDA Wireless clients

- Connects to Fabric via Border (Underlay)
- Fabric Enabled APs connect to the WLC (CAPWAP) using a dedicated Host Pool (Overlay)
- Fabric Enabled APs connect to the Edge via VXLAN
- Wireless Clients (SSIDs) use regular Host Pools for data traffic and policy (same as Wired)
- Fabric Enabled WLC registers Clients with the Control-Plane (as located on local Edge + AP)
**SD-Access Platforms**

**Fabric Wireless**

<table>
<thead>
<tr>
<th>3504 WLC</th>
<th>5500 WLC</th>
<th>8500 WLC</th>
<th>Wave 2 APs</th>
<th>Wave 1 APs*</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="3504 WLC" /></td>
<td><img src="image2.png" alt="5500 WLC" /></td>
<td><img src="image3.png" alt="8500 WLC" /></td>
<td><img src="image4.png" alt="Wave 2 APs" /></td>
<td><img src="image5.png" alt="Wave 1 APs*" /></td>
</tr>
<tr>
<td><strong>AIR-CT3504</strong></td>
<td><strong>AIR-CT5520</strong></td>
<td><strong>AIR-CT8540</strong></td>
<td><strong>1800/2800/3800</strong></td>
<td><strong>1700/2700/3700</strong></td>
</tr>
<tr>
<td>150 APs</td>
<td>1500 APs</td>
<td>5000 APs</td>
<td>11ac Wave2 APs</td>
<td>11ac Wave1 APs</td>
</tr>
<tr>
<td>1G/mGig RJ45</td>
<td>1G/10G SFP+</td>
<td>1G/10G SFP+</td>
<td>1G/mGig RJ45</td>
<td>1G RJ45</td>
</tr>
<tr>
<td>AireOS 8.5.1+</td>
<td>AireOS 8.5.1+</td>
<td>AireOS 8.5.1+</td>
<td>AireOS 8.5.1+</td>
<td>AireOS 8.5.1+</td>
</tr>
</tbody>
</table>

* Some caveats with Wave1 APs.
Would you like to know more?

Fabric Wireless

Check out the following session:

BRKEWN-2020
SD-Access - Wireless Integration

This session covers:

• More details about Fabric Wireless
• How Fabric WLC and APs communicate
• Various Fabric Wireless approaches
Would you like to know more?

Fabric Wireless

Check out the following session:

**BRKEWN-2021**
SD-Access - How to setup Wireless

This session covers:
- More details about Fabric Wireless
- SD-Access Fabric Wireless Setup (LIVE)
- Fabric Wireless best practices and tips
Roles & Terminology
What is Software Defined Access?

1. High-Level View
2. Roles & Platforms
3. Fabric Constructs
**SD-Access Fabric**
Virtual Network—A Closer Look

**Virtual Network** maintains a separate Routing & Switching table for each instance

- Control-Plane uses Instance ID to maintain separate VRF topologies ("Default" VRF is Instance ID “4098”)
- Nodes add VNID to the Fabric encapsulation
- Endpoint ID prefixes (Host Pools) are routed and advertised within a Virtual Network
- Uses standard “vrf definition” configuration, along with RD & RT for remote advertisement (Border Node)
**Scalable Group** is a logical policy object to “group” Users and/or Devices

- Nodes use “Scalable Groups” to ID and assign a unique Scalable Group Tag (SGT) to Endpoints
- Nodes add SGT to the Fabric encapsulation
- SGTs are used to manage address-independent “Group-Based Policies”
- Edge or Border Nodes use SGT to enforce local Scalable Group ACLs (SGACLs)
SD-Access @ DNA Center
Virtual Networks and Scalable Groups

Create or Modify Virtual Network by selecting Available Scalable Groups.

Virtual Network Name*
DEFAULT_VN

Available Scalable Groups

Groups in the Virtual Network

Contractors
Developers
Employees
Guests

Auditors...
BYOD
Development_S...
Network_Servic... PCI_Servers
Point_of_Sale_S...
Product_...?
Producti...?
Quarantined_Sy... Test_Servers
TrustSe...?
Unknown
Host Pool provides basic IP functions necessary for attached Endpoints

- Edge Nodes use a Switch Virtual Interface (SVI), with IP Address /Mask, etc. per Host Pool
- Fabric uses Dynamic EID mapping to advertise each Host Pool (per Instance ID)
- Fabric Dynamic EID allows Host-specific (/32, /128, MAC) advertisement and mobility
- Host Pools can be assigned Dynamically (via Host Authentication) and/or Statically (per port)
Stretched Subnets allow an IP subnet to be “stretched” via the Overlay

- Host IP based traffic arrives on the local Fabric Edge SVI, and is then transferred by Fabric
- Fabric Dynamic EID mapping allows Host-specific (/32, /128, MAC) advertisement and mobility
- Host 1 connected to Edge A can now use the same IP subnet to communicate with Host 2 on Edge B
- No longer need a VLAN to connect Host 1 and 2 😊
Anycast GW provides a single L3 Default Gateway for IP capable endpoints

- Similar principle and behavior as HSRP / VRRP with a shared “Virtual” IP and MAC address
- The same Switch Virtual Interface (SVI) is present on EVERY Edge, with the same Virtual IP and MAC
- Control-Plane with Fabric Dynamic EID mapping creates a Host (Endpoint) to Edge relationship
- When a Host moves from Edge 1 to Edge 2, it does not need to change it’s Default Gateway 😊
Layer 2 Extension allows Non-IP endpoints to use Broadcast & L2 Multicast

- Similar principle and behavior as Virtual Private LAN Services (VPLS) P2MP Overlay
- Uses a pre-built Multicast Underlay to setup a P2MP tunnel between all Fabric Nodes.
- L2 Broadcast and Multicast traffic will be distributed to all connected Fabric Nodes.
- Can be enabled for specific Host Pools that require L2 services (use Stretched Subnets for L3)
SD-Access @ DNA Center
Host Pools & Layer-2 Extension

Edit Virtual Network: USERS

Filter

<table>
<thead>
<tr>
<th>IP Pool Name</th>
<th>Traffic Type</th>
<th>Address Pool</th>
<th>Layer-2 Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Border_Automation</td>
<td>Choose Traffic</td>
<td>192.168.111.0/24</td>
<td>Off</td>
</tr>
<tr>
<td>PHNX_AP</td>
<td>Choose Traffic</td>
<td>10.100.0.0/16</td>
<td>Off</td>
</tr>
<tr>
<td>PHNX_WIRED</td>
<td>Data</td>
<td>10.111.0.0/16</td>
<td>Off</td>
</tr>
<tr>
<td>PHNX_WIRELESS</td>
<td>Data</td>
<td>10.112.0.0/16</td>
<td>On</td>
</tr>
</tbody>
</table>

Show 10 entries
Showing 1 - 4 of 4

Cancel  Update
Fabric Fundamentals

What is Campus Fabric?

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

2. **Data-Plane** based on **VXLAN**

3. **Policy-Plane** based on **CTS**

**Key Differences**

- L2 + L3 Overlay -vs- L2 or L3 Only
- Host Mobility with Anycast Gateway
- Adds VRF + SGT into Data-Plane
- Virtual Tunnel Endpoints (Automatic)
- NO Topology Limitations (Basic IP)
1. **Control-Plane** based on **LISP**

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

BEFORE
IP Address = Location + Identity

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

AFTER
Separate Identity from Location

Endpoint Routes are Consolidated to LISP DB

Only Local Routes

Fabric Database
Fabric Operation
Control-Plane Roles & Responsibilities

Fabric Control Plane
- EID to Location Mappings
- Can be distributed across multiple nodes

Fabric Edge Node
- Edge Encap / Decap
- Ingress / Egress to EID

Fabric Border Node
- Connects between Fabric and non-Fabric domains
- Proxy Encap / Decap

EID = End-point Identifier
- Host Address or Subnet

RLOC = Routing Locator
- Local Router Address

EID = End-point Identifier
RLOC = Routing Locator

Fabric Control Plane

EID Space

EID
- a.a.a.0/24
- b.b.b.0/24
- c.c.c.0/24
- d.d.0.0/16

RLOC
- w.x.y.1
- x.y.w.2
- c.c.c.0/24
- d.d.0.0/16

Prefix
- w.x.y.1
- x.y.w.2
- c.c.c.0/24
- d.d.0.0/16

Next-hop
- e.f.g.h
- e.f.g.h
- e.f.g.h
- e.f.g.h
Fabric Operation
Control Plane Register & Resolution

Cache Entry (on Fabric Edge)
10.2.2.2/32 → (2.1.2.1)

Database Mapping Entry (on FE)
10.2.2.2/32 → (2.1.2.1)

10.2.2.3/16  10.2.2.2/16  10.2.2.5/16  10.2.2.4/16

Subnet 10.2.0.0 255.255.0.0 stretched across

Database Mapping Entry (on FE)
10.2.2.4/32 → (3.1.2.1)

Where is 10.2.2.2?
Fabric Operation
Fabric Internal Forwarding (Edge to Edge)

1. DNS Entry: D.abc.com A 10.2.2.2

2. 10.1.0.1 → 10.2.2.2

3. EID-prefix: 10.2.2.2/32
   Locator-set: 2.1.2.1, priority: 1, weight:100
   Path Preference Controlled by Destination Site

4. 1.1.1.1 → 2.1.2.1
   10.1.0.1 → 10.2.2.2

5. 10.1.0.1 → 10.2.2.2

IP Network

Branch
10.1.0.0/24

Fabric Edge

Non-Fabric

Non-Fabric

Fabric Borders

Mapping Entry

Fabric Edges

10.2.3/16
10.2.2/16
10.2.4/16
10.2.5/16

Subnet 10.2.0.0 255.255.0.0 stretched across

BRKCRS-2810 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Fabric Operation
Host Mobility – Dynamic EID Migration

Routing Table
10.2.1.0/24 – Local
10.2.1.10/32 – Local
10.2.1.10/32 – LISP0

Fabric Control Plane
10.10.0.0/16 – 12.0.0.1
10.2.1.10/32 – 12.1.1.1
10.2.1.10/32 – 12.2.2.1

Map Register
EID: 10.17.1.10/32
Node: 12.1.1.1

Subnet 10.2.0.0 255.255.0.0 stretched across

Campus Bldg 1
10.2.1.10

Fabric Edges

DC1

10.10.0.0/24

Fabric Borders

10.2.1.10/32 – Local
10.2.1.10/32 – Local
10.2.1.10/32 – LISP0

12.1.1.1
12.0.0.1
12.2.2.2

IP Network

10.2.1.10
10.2.1.10

Campus Bldg 2

Routing Table
10.2.1.0/24 – Local
10.2.1.10/32 – Local
# SD-Access Fabric

Unique Control-Plane Extensions compared to LISP

<table>
<thead>
<tr>
<th>Capability</th>
<th>Traditional LISP</th>
<th>SD-Access Fabric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Extension</td>
<td>Not Supported</td>
<td>Fabric Control Plane extended to support MAC to IP binding, and Layer 2 Overlays</td>
</tr>
<tr>
<td>Virtual Networks</td>
<td>Layer-3 (aka VRF) based VN only</td>
<td>Both Layer-3 (VRF) and Layer-2 VN support (using VXLAN)</td>
</tr>
<tr>
<td>Fast Roaming</td>
<td>Fast roaming not supported</td>
<td>Fabric Control Plane extended to support fast roaming in =/&lt; 50ms</td>
</tr>
<tr>
<td>Wireless Extensions</td>
<td>Not Supported</td>
<td>Fabric Control Plane supports wireless extensions for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AP Onboarding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Wireless Guest</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VXLAN functionality on AP</td>
</tr>
</tbody>
</table>
Fabric Fundamentals

What is Campus Fabric?

1. Control-Plane
2. Data-Plane
3. Policy-Plane
SD-Access Fabric

Key Components – VXLAN

1. **Control-Plane** based on LISP

2. **Data-Plane** based on VXLAN

---

**ORIGINAL PACKET**

- ETHERNET
- IP
- PAYLOAD

**PACKET IN LISP**

- ETHERNET
- IP
- UDP
- LISP
- IP
- PAYLOAD

**PACKET IN VXLAN**

- ETHERNET
- IP
- UDP
- VXLAN
- ETHERNET
- IP
- PAYLOAD

- Supports L3 Overlay Only
- Supports L2 & L3 Overlay
VXLAN-GPO Header
MAC-in-IP with VN ID & Group ID

- Outer MAC Header
- Outer IP Header
- UDP Header
- VXLAN Header
- Inner (Original) MAC Header
- Inner (Original) IP Header
- Original Payload
- VXLAN Flags RRRRIRRR
  - Group ID
  - VN ID
  - Reserved
- Next-Hop MAC Address
- Src VTEP MAC Address
- IP Header Misc. Data
- Protocol 0x11 (UDP)
- Header Checksum
- Source IP
- Dest. IP
- UDP 4789

- Allows 16M possible VRFs
- Allows 64K possible SGTs
Data-Plane Overview
Fabric Header Encapsulation

Fabric Data-Plane provides the following:
• Underlay address advertisement & mapping
• Automatic tunnel setup (Virtual Tunnel End-Points)
• Frame encapsulation between Fabric Nodes

Support for VXLAN header format
• Support for Layer 2 and Layer 3 Segmentation using VNI (VXLAN Network Identifier)
• VXLAN header carries MAC payload (MAC in IP)
• Support for Group Tags for Policy

Triggers Control Plane events
• Registration of Endpoints (Hosts)
• ARP or NDP Learning on L3 Gateways
• Map-Reply or Cache on Fabric Nodes
### SD-Access Fabric
Unique Data-Plane Extensions compared to LISP

<table>
<thead>
<tr>
<th>Capability</th>
<th>LISP Header</th>
<th>VXLAN Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>SGT Tag</td>
<td>No place to carry SGT</td>
<td>VXLAN-GPO uses Reserved field to carry SGT</td>
</tr>
<tr>
<td>Layer 3 Extension (VRF)</td>
<td>Yes</td>
<td>Yes, by mapping VRF-&gt;VNI</td>
</tr>
<tr>
<td>Layer 2 Extension</td>
<td>Not Supported</td>
<td>Fabric supports Layer 2 extension by mapping VLAN -&gt;VNI</td>
</tr>
<tr>
<td>Wireless</td>
<td>Not Supported</td>
<td>AP to Fabric Edge uses VXLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fabric Edge to Edge/Border uses VXLAN for both Wired and Wireless (same)</td>
</tr>
</tbody>
</table>
Fabric Fundamentals

What is Campus Fabric?

1. Control-Plane
2. Data-Plane
3. Policy-Plane
SD-Access Fabric
Key Components – Group Based Policy

1. **Control-Plane** based on LISP

2. **Data-Plane** based on VXLAN

3. **Policy-Plane** based on CTS

- **VRF + SGT**

VRF + SGT
SD-Access Policy
Two Level Hierarchy - Macro Level

Virtual Network (VN)
First level Segmentation ensures zero communication between forwarding domains. Ability to consolidate multiple networks into one management plane.

Building Management VN

Campus Users VN

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Second level Segmentation ensures role based access control between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.
SD-Access Policy

Policy Types

Access Control Policy
Who can access What?
Rules for Inter-Group Access: Permit / Deny Group to Group

Application Policy
How to treat Traffic?
QoS for Applications
Application Compression
Application Caching

Traffic Copy Policy
Need to Mirror Traffic?
Configures ERSPAN for specific endpoints and traffic (source and destination SGT)

Employee 1
Edge Switch
Finance Servers
1. App to User Contracts

App to User Contracts

provider ➔ consumer

2. User to User Contracts

User to User Contracts

consumer ➔ provider

Authored and Enforced in Campus/Branch
Group Assignment
Two ways to assign SGT

Dynamic Classification
- Campus Access
- Distribution
- Core
- WLC
- VLAN to SGT
- 802.1X
- MAB
- WebAuth

Static Classification
- L3 Interface (SVI) to SGT
- L2 Port to SGT
- DC Core
- DC Access
- Enterprise Backbone
- Firewall
- Hypervisor SW
- Subnet to SGT
- VM (Port Profile) to SGT
Group Propagation
VN & SGT in VXLAN-GPO Encapsulation

Classification
Static or Dynamic VN and SGT assignments

Propagation
Carry VN and Group context across the network

Enforcement
Group Based Policies ACLs, Firewall Rules

Encapsulation

Decapsulation

Edge Node 1

Edge Node 2

VXLAN

VXLAN

VN ID

VN ID

SGT ID

SGT ID
**Policy Enforcement**

**Ingress Classification with Egress Enforcement**

- **User Authenticated** = Classified as **Marketing (5)**
- **FIB Lookup** = Destination IP = SGT 20
- **Destination Classification**
  - CRM: SGT 20
  - Web: SGT 30

**Diagram Notes**:
- **SRC**: 10.1.10.220
- **DST**: 10.1.100.52
- **SGT**: 5
- **SRC**: 10.1.10.220
- **DST**: 10.1.200.100
- **SGT**: 30
- **ByOD (7)**
  - **Deny**
  - **Permit**
- **Marketing (5)**
  - **Permit**
  - **Deny**
- **Nexus 7000**
- **Nexus 5500**
- **Nexus 2248**
- **ISE**
- **Enterprise Backbone**

---

**Cisco Live!**

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
SD-Access @ DNA Center
Group-Based Access Control Policy

- Group-Based Access Control (Fabric)
- IP-Based Access Control (Non-Fabric)
- Application Policies
- Traffic Copy Policies

Last updated: 8:56 am
Add Policy

Policy Name
Status
Description

- Guests-Guests
DEPLOYED
Access Policy for ISE EgressMatrixCell [Guests-Guests]

Showing 1 - 1 of 1
SD-Access @ DNA Center
Group-Based Access Control Policy

Create Policy by selecting Source, Destination, and applying a Contract

Available Scalable Groups

Source
Scalable Groups

Destination
Scalable Groups
# SD-Access Fabric

Unique Data-Plane Extensions compared to LISP

<table>
<thead>
<tr>
<th>Capability</th>
<th>Traditional CTS</th>
<th>SD-Access Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>SGT Propagation</td>
<td>Enabled hop-by-hop, or by separate</td>
<td>Carried with the data traffic inside</td>
</tr>
<tr>
<td></td>
<td>Security-Group Exchange Protocol (SXP) sessions</td>
<td>VXLAN-GPO (overlay) end-to-end</td>
</tr>
<tr>
<td>VN Integration</td>
<td>Not Supported</td>
<td>VN + SGT-aware Firewalls</td>
</tr>
<tr>
<td>Access Control Policy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>QoS (App) Policy</td>
<td>Not Supported</td>
<td>App based QoS policy, to optimize</td>
</tr>
<tr>
<td></td>
<td></td>
<td>application traffic priority</td>
</tr>
<tr>
<td>Traffic Copy Policy</td>
<td>Not Supported</td>
<td>SRC/DST based Copy policy (using ERSPAN) to capture data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>traffic</td>
</tr>
</tbody>
</table>
Would you like to know more?
Fabric Wireless

Check out the following session:

**BRKCRS-3811**
SD-Access - Policy Driven Manageability

This session covers:
- More details about Group-Based Policy
- How VNs and SGTs are related
- Various Fabric Policy design approaches
Controller Fundamentals

What is DNA Center?

1. DNAC Architecture
2. DNAC User Interface
3. DNAC Workflows
**SD-Access DNA Center Appliance**

**DNA Center Platform**

**DN1-HW-APL**

**DNAC 1.1 Scale:** [Per Node](#)
- 5,000 Nodes (1K Devices + 4K APs)
- 25,000 Clients (Concurrent Hosts)

- **Fully Integrated Automation & Assurance**
  - Centralized Deployment - Cloud Tethered
  - Built-In Telemetry Collectors (FNF, SNMP, Syslog, etc)
  - Built-In Contextual Connectors (ISE/PxGrid, IPAM, etc)
  - Multi-Node High Availability (3 Node, Automation)
  - RBAC, Backup & Restore, Scheduler, APIs

- **1RU Server (Small form factor)**
  - UCS 220 M4: 64-bit x86
  - vCPU: 44 core (2.2GHz)
  - RAM: 256GB DDR4
  - Control Disks: 2 x 480GB SSD RAID1
  - System Disks: 6 x 1.9TB SSD M-RAID
  - Network: 2 x 10GE SFP+
  - Power: 2 x 770W AC PSU

**Single Appliance for DNAC (Automation + Assurance)**
SD-Access
DNA Center – Service Components

Cisco DNA Center 1.1
Design | Policy | Provision | Assurance

NCP 1.1
Network Control Platform

NDP 1.1
Network Data Platform

Cisco ISE 2.3
Identity Services Engine

SNS 9500 Series
ISE Appliance

Cisco Switches | Cisco Routers | Cisco Wireless

Campus Fabric

Cisco DNA Center Appliance

DN1-HW-APL
DNA Center Appliance

AAA
RADIUS
EAPoL

NETCONF
SNMP
SSH

HTTP
NetFlow
Syslogs
DNA Center Interaction
Automated Provisioning and Telemetry Enrichment

Telemetry Intent
Alerts
Violations

Inventory, Topology, Host, Group
Network State changes
Path Trace information

Network Control Platform
Configuration Push
Telemetry Configuration

Network Data Platform
Telemetry Data Collection
DNA Center and ISE integration
Identity and Policy Automation

Cisco Identity Services Engine
- Authentication Authorization Policies
- Groups and Policies

Campus Fabric

Fabric Management
Policy Authoring Workflows

Cisco DNA Center

PxGrid REST APIs
DNA Center and ISE integration

ISE node roles in SD-Access

ISE-PSN

Authorization Policy

<table>
<thead>
<tr>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>SGT-10</td>
</tr>
<tr>
<td>Contractor</td>
<td>SGT-20</td>
</tr>
<tr>
<td>Things</td>
<td>SGT-30</td>
</tr>
</tbody>
</table>

ISE-PAN

DNA-Center

Admin/Operate

pxGrid

ISE-MNT

ISE-PXG

Exchange Topics

- TrustSecMetaData
- SGT Name: Employee = SGT-10
- SGT Name: Contractor = SGT-20
- SessionDirectory*

Bob with Win10 on CorpSSID

* Future Plan
Controller Fundamentals

What is DNA Center?

1. DNAC Architecture
2. DNAC User Interface
3. DNAC Workflows
SD-Access
Campus Fabric + DNA Center (Automation & Assurance)

Campus Fabric

- SmartCLI Macros
- Simple User Inputs
- Customized Workflows
- Box-by-Box Management

SD Access

- Programmable APIs
- NETCONF / YANG
- Automated Workflows
- Box-by-Box Management

- DNA Center GUI
- Cross-App REST APIs
- Automated Workflows
- Centralized Management
DNA Center

4 Step Workflow

**Design**
- Global Settings
- Site Profiles
- DDI, SWIM, PNP
- User Access

**Policy**
- Virtual Networks
- ISE, AAA, Radius
- Endpoint Groups
- Group Policies

**Provision**
- Fabric Domains
- CP, Border, Edge
- FEW, OTT WLAN
- External Connect

**Assurance**
- Health Dashboard
- 360° Views
- FD, Node, Client
- Path Traces

Planning & Preparation

Installation & Integration
SDA - Design

DNA Center
Design, Automate and Assure your Network

Network Hierarchy
Network Settings
Image Management
Network Profiles
SDA - Provision

Device On-Boarding
Device Inventory
Fabric Administrator
Host On-Boarding
SDA - Assurance

Health Scores
Client 360
Device 360
Application 360
Click to Resolve
Would you like to know more?
Fabric Assurance

Check out the following session:

**BRKCRS-2814**
SD-Access - Fabric Assurance

This session covers:
- More details about Fabric Assurance
- How DNA Center uses NDP
- Fabric Assurance best practices & tips
SD-Access Resources
Would you like to known more?

cisco.com/go/sdaccess
• SD-Access At-A-Glance
• SD-Access Design Guide
• SD-Access FAQs
• SD-Access Migration Guide
• SD-Access Solution Data Sheet
• SD-Access Solution White Paper

cisco.com/go/cvd
• SD-Access Design Guide - Dec 2017
• SD-Access Deploy Guide - Jan 2018

cisco.com/go/dnacenter
• DNA Center At-A-Glance
• DNA Center "How To" Video Resources
• DNA Center Data Sheet
How about a **LIVE** Demo?
Take Away

Key Points
Session Summary

SD-Access = Campus Fabric + DNA Center
SD-Access Support
Fabric ready platforms for your digital ready network

**Switching**
- Catalyst 9400
- Catalyst 9300
- Catalyst 9500
- Catalyst 4500E
- Catalyst 6800
- Nexus 7700
- Catalyst 3650 and 3850

**Routing**
- ASR-1000-X
- ASR-1000-HX
- ISR 4430
- ISR 4450
- ISRv/CSRv

**Wireless**
- AIR-CT5520
- AIR-CT8540
- AIR-CT3504
- Wave 2 APs (1800,2800,3800)
- Wave 1 APs (1700,2700,3700)

**Extended**
- CDB
- 3560-CX
- IE (2K/3K/4K/5K)

* with Caveats
What to Do Next?

- **SD-Access Capable**
- **DNA Center**
- **Cisco Services**

**Refresh your Hardware & Software**
- Get SD-Access Capable Devices with DNA Advantage OS License

**Deploy the DNA Center**
- Get DNA Center Appliances with DNA Center Software

**Engage with Cisco Services**
- Cisco Services can help you to Test - Migrate - Deploy
SD-Access - Cisco on Cisco
Live SD-Access Deployment @ Cisco Systems

750 Wired & Wireless users

Fabric Border Control-Plane Nodes: 2
Fabric Edge Nodes: 7
Fabric Access Points: 98
Virtual Networks: 3
Scalable Groups: 16
Wireless SSIDs: 2
Address Pools: 8

Built and managed by the Cisco Engineering team, in conjunction with Cisco IT Services

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
The First Step...

#NewEra
#CiscoDNA
#NetworkIntuitive
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKCRS-2810
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Tech Circle
- Meet the Engineer 1:1 meetings
- Related sessions
Thank you