SD-Access Wireless Integration

Why and How integrating wireless in SDA

Simone Arena, Principal Engineer
BRKEWN-2020
Software Defined Access – Wireless Integration

Session Objective

Is your Campus Network facing some, or all, of these challenges?

• Host and IoT onboarding and Mobility (w/o stretching VLANs)
• Network Segmentation (w/o implementing MPLS)
• Role-based Access Control (w/o hop-by-hop TrustSec)
• Common Policy for Wired and Wireless (w/o using multiple tools)
• Consistency Across Campus, WAN and Branch (w/o using multiple tools)

The goal of this session is to explain the value of SD-Access Fabric and show you how with SD-Access Wireless you can overcome some of these challenges.
Agenda

• SD-Access: why would you care?
• SD-Access Wireless Architecture
• Demo: Let’s make it real!
• Under the hood
• SD-Access Wireless Design & Deploy
• Adoption/Migration scenarios
• Key takeaways

“…starting with a golden circle and the question "Why?"

Simon Sinek, TED talk, 2009
Cisco Webex Teams

Questions?
Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

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

Webex Teams will be moderated by the speaker until June 18, 2018.

cs.co/ciscolivebot#BRKEWN-2020
Software Defined Access
Cisco Live Orlando - Session Map

Missed One? Sessions are available online @ CiscoLive.com

Monday (June 11)  Tuesday (June 12)  Wednesday (June 13)  Thursday (June 14)

08:00-11:00  11:00-13:00  13:00-15:00  15:00-18:00  08:00-11:00  11:00-13:00  13:00-15:00  15:00-18:00  08:00-11:00  11:00-13:00  13:00-15:00  15:00-18:00

BRKEWN-2020 Wireless Deep dive  BRKCRS-2815 (1) Design & Scale  BRKCRS-2812 (2) Design & Scale  BRKCRS-2815 (2) Migration
BRKEWN-2021 From scratch  BRKCRS-2811 External Connect  BRKCRS-2812 (1) Migration  BRKCRS-2815 (2) Migration
BRKCRS-2810 Solution Overview  BRKCRS-2814 Assurance  BRKCRS-2816 Routed Underlay  BRKDCN-2489 DC Integration
BRKCRS-2811 External Connect  BRKCRS-2814 Assurance  BRKCRS-2816 Routed Underlay  BRKCRS-2817 Extension for IOT
BRKCRS-2810 (2) Hands-On Lab  LTRCRS-2810 (2) Hands-On Lab  LTRCRS-2816 Routed Underlay  LTRCRS-2816 Routed Underlay
BRKCRS-2812 (1) Migration  BRKCRS-2812 (1) Migration  BRKCRS-2815 (2) Migration  BRKCRS-2815 (2) Migration
Digital Transformation—Challenge for Enterprise IT

Data growth
Connected devices
Threat surface areas

Enterprise Trends driving Digital Transformation

- Mobility
  - 3.64
  - Devices per Person
- IoT
  - 7.5B
  - Things Connected
- Cloud

$60B
Spent of
Network
Operations

An evolved world needs a network evolved.
Key Challenges for Traditional Networks

Secure Onboarding
- More users and endpoints
- Policy based on VLANs
- Very hard to Segment

Complex to Manage
- Very little Automation
- Mostly all CLI driven
- Error prone

Slow Issue Resolution
- Separated user policies for wired and wireless networks
- Different policy definition and enforcement points

Traditional Networks Cannot Keep Up!
Introducing Software-Defined Access
Policy-Based Automation from Edge to Cloud

- Automation
  - Simple Policy Definition and Enforcement
  - Industry Best-Practices and Policy Compliance

- Secure Fabric
  - Virtual Networks and Groups Made Easy
  - Decouple Policy from Network Topology

- Assurance
  - Monitoring and Troubleshooting
  - Proactive Issue Identification and Resolution
Introducing Software-Defined Access
Policy-Based Automation from Edge to Cloud

Cisco ISE 2.3
Identity Services Engine

Cisco Switches | Cisco Routers | Cisco Wireless

Cisco DNA Centre 1.1

AAA
RADIUS
EAPoL

HTTPS
NetFlow
Syslogs

NETCONF
SNMP
SSH

API

DNA CENTER

Policy
Design
Provision
Assurance

SD-Access Fabric

Cisco DNA Centre Appliance

DN1-HW-APL

NCP
Network Controller Platform

NDP
Network Data Platform

API

Cisco Switches | Cisco Routers | Cisco Wireless

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
SD-Access Fabric: Why Would You Care?
What is the Problem?

User Group policy rollout - Today

- Three user Groups
- One single SSID
- Differentiated policies per Group
- Guest segmentation (wired and wireless)

Customer Policy requirements:

<table>
<thead>
<tr>
<th>Customer Policy requirements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production Serv.</td>
</tr>
<tr>
<td>Employee</td>
</tr>
</tbody>
</table>

Network Touch Points

Trunks

L3 Switch

L2 Switch

BYOD

Employee

Contractor

Production Servers

Developer Servers

LAN Core

AAA

DHCP

AD

WLC
What is the Problem?

User Group policy rollout - Today

1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets

What if You Need to Add Another Group & Policy?

1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets

5. Many different User Interfaces

Production Servers
Developer Servers
LAN Core
AAA
DHCP
AD
One SSID
BYOD
Employee
Contractor

Multiple Steps and Touch Points

What is the Problem?

User Group policy rollout - Today

1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets

What if You Need to Add Another Group & Policy?

1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets

5. Many different User Interfaces

Production Servers
Developer Servers
LAN Core
AAA
DHCP
AD
One SSID
BYOD
Employee
Contractor

Multiple Steps and Touch Points

What is the Problem?

User Group policy rollout - Today

1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets

What if You Need to Add Another Group & Policy?

1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets

5. Many different User Interfaces

Production Servers
Developer Servers
LAN Core
AAA
DHCP
AD
One SSID
BYOD
Employee
Contractor

Multiple Steps and Touch Points

What is the Problem?

User Group policy rollout - Today

1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets

What if You Need to Add Another Group & Policy?

1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets

5. Many different User Interfaces

Production Servers
Developer Servers
LAN Core
AAA
DHCP
AD
One SSID
BYOD
Employee
Contractor

Multiple Steps and Touch Points
What is the Problem?

Policy Model Today

Network Policy

- QoS
- Security
- Redirect/copy
- Traffic engineering
- etc.

Policy is based on “5 Tuple”

- Only Transitive information
- Survives end to end
What is the Problem?

Policy Model Today

Network Policy

- Locate you
- Identify you
- Drive “treatment”
- Constrain you

IP Addresses

IP Address “meaning” OVERLOAD

User/device info?

What is the Problem?
Policy Model Today

Network Policy

- Locate you
- Identify you
- Drive “treatment”
- Constrain you

IP Addresses

IP Address “meaning” OVERLOAD

User/device info?
But What If …

… we could make the IP address just be a LOCATOR for you, and provide other ways to group users / devices to apply POLICY?

Key Assertion

If we could “break the dependence” between IP addressing and policy, we could greatly simplify networks – and make networks much more functional.
You could **build and run your network** in a simpler way …

Apply **Policy irrespectively of network constructs** (VLAN, subnet, IP address)

Easily implement **Network Segmentation** (w/o implementing MPLS)

Provide **L2 and L3 flexibility** (w/o stretching VLANs)

---

**With a Fabric…**

… we could make the IP address just be a LOCATOR for you, and provide other ways to group users / devices to apply POLICY?

---

**Key Assertion**

If we could “break the dependence” between IP addressing and policy, we could **greatly simplify** networks – and make networks **much more functional**.
What exactly is a Fabric?

A Fabric provides an Overlay network

An Overlay 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
What exactly is a Fabric?

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)

Separation of the “Forwarding Plane” from the “Services Plane”

IT Challenge (Business): Network Uptime

IT Challenge (Employee): New Services

The Boss

YOU

The User
What is unique about SDA Fabric?

Key components

1. Control-Plane based on LISP
Locator / ID Separation Protocol
Location and Identity separation

Traditional Behavior - Location + ID are “Combined”

When the Device moves, it gets a new IPv4 or IPv6 Address for its new Identity and Location

Overlay Behavior - Location & ID are “Separated”

When the Device moves, it keeps the same IPv4 or IPv6 Address. It has the same Identity

Device IPv4 or IPv6 Address represents both Identity and Location

Device IPv4 or IPv6 Address represents Identity only

End Point ID (EID) space

Prefix                          RLOC
192.158.28.101                171.68.226.120
169.16.17.96                  171.68.226.121
172.16.19.90                  171.68.226.122
192.58.28.128                  171.68.226.123
172.16.19.90                  171.68.226.124
192.58.28.128                  171.68.226.125
189.16.17.89                  171.68.226.126

Prefix                          RLOC
192.158.28.101                171.68.226.120
169.16.17.96                  171.68.226.121
172.16.19.90                  171.68.226.122
192.58.28.128                  171.68.226.123
172.16.19.90                  171.68.226.124
192.58.28.128                  171.68.226.125
189.16.17.89                  171.68.226.126
What is unique about SDA Fabric?

Key components

1. **Control-Plane** based on LISP
2. **Data-Plane** based on VXLAN
3. **Policy-Plane** with Cisco TrustSec (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 (No Static)
- No Topology Limitations (Basic IP)

Cisco Hardware and Software innovations

UADP and QFP allow for Flexibility – Key to Supporting the Evolution to Network Fabrics
What is unique about SDA Fabric?

Key Components - VXLAN

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

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

![Diagram showing packet structure](image-url)
What is unique about SDA Fabric?
Key Components – Cisco TrustSec (CTS)

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

VRF + SGT

VRF = Virtual Routing & Forwarding  
SGT = Scalable Group Tagging
Cisco TrustSec

Traditional Access Control is Extremely Complex

**Limits of Traditional Segmentation**
- Security Policy based on Topology (Address)
- High cost and complex maintenance

```
#CLUS
BRKEWN-2020 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
```
Cisco TrustSec
Traditional Access Control is Extremely Complex

**Enforcement**
- Group Based Policies
- ACLs, Firewall Rules

**Propagation**
- Carry “Group” context through the network using only SGT

**Classification**
- Static or Dynamic SGT assignments

---

DC switch receives policy for only what is connected

Classification
- Static or Dynamic SGT assignments

Propagation
- Carry “Group” context through the network using only SGT

Enforcement
- Group Based Policies
- ACLs, Firewall Rules
What is Unique about SDA Fabric?

Fabric brings Policy Simplification

Fabric breaks dependency between IP and Policy. Separation of Forwarding and Services planes. In Fabric Polices are tied to User/Device Identity

DNA Centre – Automation and Assurance
- Single User Interface for Fabric Management & Orchestration
- Policies definition based on User, Device or App Group
- Design, Deploy and Monitoring and Troubleshooting

Fabric Overlay – Services plane
- Dynamically connects Users/Devices/Things
- IP is an ID not used for traffic forwarding
- End to End Policies and Segmentation

Fabric Underlay – Forwarding plane
- Connects the network elements to each other
- Optimized for traffic forwarding (scalability, performance)
- Networking constructs like IP, VLANs, live here
You Convinced me on Fabric...but still, Why Integrate Wireless?
Centralized Unified Wireless Network Strengths

- Simplified operations? Yes with WLC
- Network Overlay? CAPWAP
- L3 roaming across Campus? WLC as Mobility Anchor
- Simplified IP addressing? WLC as mobility Anchor
- Guest traffic segmentation? Foreign-Anchor
Wired Network Strengths

- Segmentation
  - VRF-Lite, MPLS
- Complex ACL capabilities
  - Scalable TCAMs
- Distributed Data Plane
  - Scalable and Reliable
- Distributed Feature Plane
  - AVC, NetFlow,
- Comprehensive QoS capable
  - 12-class, Queuing
SD-Access Wireless Bringing You the Best of Both Worlds
SD-Access Wireless Architecture
SD-Access Fabric Architecture

Roles and Terminology

- **DNA Controller** – Enterprise SDN Controller provides GUI management abstraction via multiple Service Apps, which share information.
- **Group Repository** – External ID Services (e.g., ISE) is leveraged for dynamic User or Device to Group mapping and policy definition.
- **Control-Plane (CP) Node** – Map System that manages Endpoint ID to Location relationships. Also known as Host Tracking DB (HTDB).
- **Border Nodes** – A Fabric device (e.g., Core) that connects External L3 network(s) to the SDA Fabric.
- **Edge Nodes** – A Fabric device (e.g., Access or Distribution) that connects wired endpoints to the SDA Fabric.
- **Fabric Wireless Controller** – Wireless Controller (WLC) fabric-enabled, participate in LISP control plane.
- **Fabric Mode APs** – Access Points that are fabric-enabled. Wireless traffic is VXLAN encapsulated at AP.
SD-Access Wireless Architecture

Bringing the best of both architectures by...

1. Simplifying the Control & Management Plane

2. Optimizing the Data Plane

3. Integrating Policy & Segmentation E2E
SD-Access Wireless Architecture
Simplifying the Control Plane

Automation
- DNAC simplifies the Fabric deployment,
  Including the wireless integration component

Centralized Wireless Control Plane
- WLC still provides client session management
- AP Mgmt, Mobility, RRM, etc.
- Same operational advantages of CUWN

LISP control plane Management
- WLC integrates with LISP control plane
- WLC updates the CP for wireless clients
- Mobility is integrated in Fabric thanks to LISP CP

Fabric enabled WLC:
WLC is part of LISP control plane
SD-Access Wireless Architecture

Control Plane Node – A Closer Look

Fabric Control-Plane Node is based on a LISP Map Server / Resolver

Runs the LISP Endpoint ID Database to provide overlay reachability information

- A simple Host Database, that tracks **Endpoint ID** to Edge Node bindings (**RLOCs**)
- Host Database supports **multiple types of Endpoint ID** (EID), such as IPv4 /32, IPv6 /128* or MAC/48
- Receives prefix registrations from Edge Nodes for wired clients, and from Fabric mode WLCs for wireless clients
- Resolves lookup requests from FE to locate Endpoints
- Updates Fabric Edge nodes, Border nodes with wireless client mobility and RLOC information

(*) coming after FCS
SD-Access Wireless Architecture
Control Plane Node – A Closer Look

Fabric Mode WLC integrates with the LISP Control Plane

Control Plane is centralized at the WLC for all Wireless functions

- WLC is still responsible for: AP image/config, Radio Resource Management (RRM) and client session management and roaming

- For Fabric integration:
  - For wireless, client MAC address is used as EID.
  - Interacts with the Host Tracking DB on Control-Plane node for Client MAC address registration with SGT and L2 VNI
  - The VN information is a Layer 2 VN (L2 VNID) information and it’s mapped to a VLAN on the FEs
  - Responsible for updating the Host Tracking DB with roaming information for wireless clients
  - Fabric enabled WLC needs to be co-located at the same site with APs (latency between AP and WLC needs to be < 20 ms)
SD-Access Wireless Architecture

Optimizing the Data Plane

Automation
- DNAC simplifies the Fabric deployment,
- Including the wireless integration component

Centralized Wireless Control Plane
- WLC still provides client session management
- AP Mgmt, Mobility, RRM, etc.
- Same operational advantages of CUWN

Optimized Distributed Data Plane
- Fabric overlay with Anycast GW + Stretched subnet
- VLAN extension with no complications
- All roaming is Layer 2

VXLAN from the AP
- Carrying hierarchical policy segmentation starting from the edge of the network

Fabric enabled WLC:
WLC is part of LISP control plane

Fabric enabled AP:
AP encapsulates Fabric SSID traffic in VXLAN

SD-Access Fabric
SD-Access Wireless Architecture
Optimizing the Data Plane: Fabric Edge – A Closer Look

Fabric Edge Node is based on a LISP Tunnel Router

Provides connectivity for Users and Devices connected to the Fabric

- Responsible for Identifying and Authenticating wired Endpoints
- Registers Endpoint ID (IP address) info with the Control-Plane Node(s)
- Provide VN services for Wireless Clients
- Onboard APs into fabric and form VXLAN tunnels with APs
- Provides Anycast L3 Gateway for connected Endpoints
SD-Access Wireless Architecture
Optimizing the Data Plane: Anycast Gateway – A Closer Look

Anycast GW provides a single L3 Default Gateway

Based on Virtual IP address (VIP)

- Similar principle and behavior as HSRP / VRRP with a shared Virtual IP and MAC address
- The same Switched Virtual Interface (SVI) is present on every Edge, with the same Virtual IP and MAC
- If (when) a Host moves from Edge A to Edge B, it does not need to change its (L3) Default Gateway!
SD-Access Wireless Architecture
Optimizing the Data Plane: Stretched subnets – A Closer Look

Stretched subnets allow an IP subnet to be “stretched” via the overlay

Based on a Anycast GW + LISP Dynamic EID + VXLAN overlay

- Host IP based traffic arrives on the local Fabric Edge SVI, and is then transferred by LISP
- LISP Dynamic EID allows Host-specific (/32, /128, MAC) advertisement and mobility
- **No longer need to stretch a VLAN** across access layer switches to connect Host 1 and 2 to get L2 adjacency
- Client 1 connected to Fabric Edge (FE) A can talk to client B as they are on the same IP subnet.
SD-Access Wireless Architecture

Optimizing the Data Plane: Stretched subnets – A Closer Look

**Fabric Mode AP integrates with the VXLAN Data Plane**

Wireless Data Plane is distributed across APs

- Fabric mode AP is a local mode AP and needs to be **directly connected** to FE
- CAPWAP control plane goes to the WLC using Fabric
- **Fabric is enabled per SSID:**
  - For Fabric enabled SSID, AP converts 802.11 traffic to 802.3 and encapsulates it into VXLAN encoding VNI and SGT info of the client
  - Forwards client traffic based on forwarding table as programmed by the WLC. Usually VXLAN DST is first hop switch.
- AP applies all wireless specific feature like SSID policies, AVC, QoS, etc.
SD-Access Wireless Architecture

Simplifying policy and Segmentation

1. AP removes the 802.11 header
2. AP adds the 802.3/VXLAN/underlay IP header
SD-Access Wireless Architecture

Simplifying policy and Segmentation

APs embed the Policy information in the VXLAN header and forwards it

The client VRF is represented by the Layer 2 Virtual Network (L2 VNID)

Hierarchical Segmentation:
1. Virtual Network (VN) == VRF - isolated routing Control Plane + Data Plane
2. Scalable Group Tag (SGT) – User Group identifier
SD-Access Wireless Architecture
Simplifying policy and Segmentation

FEA does a lookup to CP to locate client B

FE decapsulates the VXLAN header, looks at the L2 VNID and maps it to the VLAN and L2 LISP instance.
Then FE A does the lookup and rebuild the VXLAN encapsulates to the destination FE B
SD-Access Wireless Architecture
Simplifying policy and Segmentation

- Client A
- VXLAN (Data)
- FE A
- Client B

**FE** removes the outer IP header, looks at the VNID, maps it to the VLAN.

Also looks at the SGT and applies the policy before forwarding the packet.
SD-Access Wireless Benefits

User Group policy rollout

1. Define Groups in AD

2. Design and Deploy in DNA-C
   - Create Virtual Network for Corporate
   - Define Policies
     - Role/Group based
   - Apply Policies
     - SGT based

3. Upon user authentication, Policy is automatically applied and carried end to end
1. Define Groups in AD
2. Design and Deploy in DNA-C
   - Create Virtual Network for Corporate
   - Define Policies
     - Role/Group based
   - Apply Policies
     - SGT based

What can DNA Center do? Take a Tour.

Need to add functionality to DNA Center? Add applications
Want to learn more about DNA Center? Watch video

Design
Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.
- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

Provision
Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.
- Discover and provision switches to defined sites
- Provision RADIUS and AAA to defined sites
- Set up Campus Fabric across switches

Policy
Use policies to automate and simplify network management services.
- Segment your network or Virtual Networks
- Create scalable groups to describe your critical assets
- Define segregation policies to meet your policy goals
Benefits of SD-Access Wireless: another example
What is the Problem?
Workspace of the Future

You need a Distributed Data plane without the complications that normally comes along in terms of IP addressing, roaming, etc.

What about...
- Fully leveraging the speed of 802.11ac/ax?
- Mobility everywhere
- Handling east-west traffic from tools like Spark room? And Video, video and video...
- Onboarding Sensors and IoT devices securely
- Leveraging great innovation at the switch level
- etc...

What about IP addressing design?

Data Centre
AAA
AD
LDAP
DNS
DHCP
WLC

Campus
**SD-Access Wireless Benefits**

**Workspace of the future with SDA**

- Data Plane is distributed and optimized
- Subnet is everywhere so subnetting design is SIMPLE
- Mobility is integrated in the Fabric
- Layer 2 extension for IoT

*The advantages of distributed DP without the pain*

Data plane is optimized without the complication of distributing the traffic
SDA Wireless Value Proposition

Security - Policy Simplification
- E2E Segmentation based on SGT and VRF
- Topology agnostic Policy: any underlay network, abstracted from VLANs, ACLs, IP subnetting
- Consistent Policy for wired and wireless

Data Plane Optimization and Scale
- L2 Mobility everywhere with optimized data plane
- Optimized data plane: no more hair-pinning of traffic for Enterprise and Guest traffic. No VLAN spanning, no large broadcast domain, no SPT, simple subnetting
- Easy to scale, just add switches and APs to the Fabric

Operation Simplification
- DNAC Automation: reduce the management touch points
- DNAC Assurance: Proactive monitoring and troubleshooting of the E2E network
- Wireless centralized Control Plane – same simplified wireless operations as today
What Products Make This Architecture?
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
- W2 APs (1800, 2800, 3800, 4800)
- Wave 1 APs (1700, 2700, 3700)

Extended
- CDB
- 3560-CX
- IE 4K/5K

* with Caveats
SD-Access Wireless
Platform Support

<table>
<thead>
<tr>
<th>WLC Model</th>
<th>AIR-CT Model</th>
<th>Description</th>
<th>Wave 2 APs</th>
<th>Wave 1 APs</th>
</tr>
</thead>
<tbody>
<tr>
<td>3504 WLC</td>
<td>AIR-CT3504</td>
<td>1G/mGig AireOS 8.5</td>
<td>1800/2800/3800 11ac Wave2 APs 1G/MGIG RJ45</td>
<td>1700/2700/3700 11ac Wave1 APs 1G RJ45</td>
</tr>
<tr>
<td>5520 WLC</td>
<td>AIR-CT5520</td>
<td>No 5508 1G/10G SFP+ AireOS 8.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8540 WLC</td>
<td>AIR-CT8540</td>
<td>8510 supported 1G/10G SFP+ AireOS 8.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* 8.8 code
* with Caveats
### SD-Access Platforms

**Edge Nodes**

<table>
<thead>
<tr>
<th>Catalyst 3K</th>
<th>Catalyst 9300</th>
<th>Catalyst 4K</th>
<th>Catalyst 9400</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Catalyst 3K" /></td>
<td><img src="image" alt="Catalyst 9300" /></td>
<td><img src="image" alt="Catalyst 4K" /></td>
<td><img src="image" alt="Catalyst 9400" /></td>
</tr>
<tr>
<td>• Catalyst 3650/3850</td>
<td>• Catalyst 9300</td>
<td>• Catalyst 4500</td>
<td>• Catalyst 9400</td>
</tr>
<tr>
<td>• 1/10G RJ45, SFP</td>
<td>• 1/10G RJ45, SFP</td>
<td>• Sup8E/9E (Uplink)</td>
<td>• Sup1/XL</td>
</tr>
<tr>
<td>• 10/40G NM Cards</td>
<td>• 10/40/40G NM Cards</td>
<td>• 4700 Cards</td>
<td>• 9400 Cards</td>
</tr>
<tr>
<td>• IOS-XE 16.6.3+</td>
<td>• IOS-XE 16.6.3+</td>
<td>• IOS-XE 3.10.1E+</td>
<td>• IOS-XE 16.6.3+</td>
</tr>
</tbody>
</table>

For Your Reference
SD-Acccess Platforms
Control-Plane Nodes

Catalyst 3K
• Catalyst 3850
• 1/10G SFP
• 10/40G NM Cards
• IOS-XE 16.6.3+

Catalyst 9500
• Catalyst 9500
• 10/40G SFP/QSFP
• 10/40G NM Cards
• IOS-XE 16.6.3+

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

Catalyst 6K*
* Wired Only

Support for Wireless in DNAC 1.2 with IOS 15.5.1SY

ASR1K, ISR4K & CSRv
• CSRv
• ASR 1000-X/HX
• ISR 4300/4400
• IOS-XE 16.6.3+
SD-Access Platforms

Border Nodes

### Catalyst 3K
- Catalyst 3850
- 1/10G SFP+
- 10/40G NM Cards
- IOS-XE 16.6.3+

### Catalyst 9K
- Catalyst 9500
- 10/40G SFP/QSFP
- 10/40G NM Cards
- IOS-XE 16.6.3+

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

### Nexus 7K*
- Nexus 7700
- Sup2E
- M3 Cards
- NXOS 8.2.1+

* External Border Only

### ASR1K & ISR4K
- ASR 1000-X/HX
- ISR 4300/4400
- 1/10G/40G
- IOS-XE 16.6.3+

### New
- Catalyst 9K
- Catalyst 6K
- Nexus 7K*
Demo
SD-Access Wireless
Under the Hood...
SD-Access Wireless Basic Workflows

Add WLC to Fabric

1. In DNAC, first provision and then add WLC to Fabric Domain
2. Fabric configuration is pushed to WLC. WLC becomes Fabric aware. Most importantly WLC is configured with credentials to established a secure connection to CP
3. WLC is ready to participate in SD-Access Wireless
SD-Access Wireless Basic Workflows

AP Join

Admin configures AP pool in DNAC in INFRA_VN. DNAC pre-provision a configuration macro on all the FEs
SD-Access Wireless Basic Workflows

AP INFRA_VN

- INFRA_VN is introduced to easily onboard APs. APs are in the Fabric overlay but INFRA_VN is mapped to the global routing table.

- AP Provisioning Pool: triggers the AP pool automatic configuration.

- Layer-2 Extension: turns on L2 service in LISP.

- “AP Provision” and “Layer 2 Extension” are automatically enabled on this special VN.
SD-Access Wireless Basic Workflows

AP Join

1. Admin configures AP pool in DNAC in INFRA_VN. DNAC pre-provision a configuration macro on all the FEs.

2. AP is plugged in and powers up. FE discovers it’s an AP via CDP and applies the macro to assign the switch port to the right VLAN.

(*) AP can be connected also through an “Extended node” switch.
SD-Access Wireless Basic Workflows

Automatic AP onboarding

- In DNAC 1.1 the **CDP macro** on the FEs for AP onboarding is pushed **only if** the switchport **No Authentication template** is selected:

  ![Select Devices Host Onboarding Diagram]

  - Select Authentication template
    - Closed Authentication
    - Easy Connect
    - **No Authentication**
    - Open Authentication

- If any other switchport Authentication template is selected, then use static assignment to map the APs’ switch ports to the right IP pool
SD-Access Wireless Basic Workflows

AP Join

1. Admin configures AP pool in DNAC inn INFRA_VN. DNAC pre-provision a configuration macro on all the FEs

2. AP is plugged in and powers up. FE discovers it’s an AP via CDP and applies the macro to assign the switch port the the right VLAN

3. AP gets an IP address via DHCP in the overlay. Next, FE registers the AP as a “special” wired host into the Fabric
SD-Access Wireless Basic Workflows

AP Join

4. Fabric Edge registers AP’s IP address (EID) and updates the Control Plane (CP)
5. AP learns WLC’s IP and joins using traditional methods. Fabric AP joins in **Local mode**
6. WLC checks if it is fabric-capable (Wave 2 or Wave 1 APs)
7. If AP is supported for Fabric, WLC queries the CP to know if AP is connected to Fabric
Control Plane (CP) replies to WLC with RLOC. This means AP is attached to Fabric and will be shown as “Fabric enabled”

WLC does a L2 LISP registration for AP in CP (a.k.a. AP “special” secure client registration). This is used to pass important metadata information from WLC to the FE
**SD-Access Wireless Basic Workflows**

### AP Join

1. **In response to this proxy registration, Control Plane (CP) notifies Fabric Edge and pass the metadata received from WLC (flag that says it’s an AP and the AP IP address)**

2. **Fabric Edge processes the information, it learns it’s an AP and creates a VXLAN tunnel interface to the specified IP (optimization: switch side is ready for clients to join)**
Admin user defines a Pool for wireless clients in DNAC Design phase. The pool is then associated to a VN during “Host Onboarding” phase. For a wireless pool, L2 LISP needs to be enabled.

As soon as the SSID is mapped to the Pool, the WLAN will be enabled and clients will see the Fabric SSID.
SD-Access Wireless Basic Workflows

Client Onboarding

- In DNAC flip the **Layer-2 Extension** toggle to ON to enable L2 LISP and Layer 2 subnet extension on the client Pool/subnet. This is required for wireless to work!
SD-Access Wireless Basic Workflows

Client Onboarding

1. Client authenticates to a Fabric enabled WLAN. WLC gets SGT from ISE, updates AP with client L2VNID and SGT. WLC knows RLOC of AP from internal DB.
Client Onboarding

1. Client authenticates to a Fabric enabled WLAN. WLC gets SGT from ISE, updates AP with client L2VNID and SGT.

2. WLC knows RLOC of AP from internal DB. WLC proxy registers Client L2 info in CP; this is LISP modified message to pass additional info, like the client SGT.

3. FE gets notified by CP and knows it’s a client; FE adds client MAC in L2 forwarding table and go and fetch the client policy from ISE based on the client SGT.
**SD-Access Wireless Basic Workflows**

### Client Onboarding

1. **Client initiates DHCP Request**
2. **AP encapsulates it in VXLAN with L2 VNI info (and SGT)**
3. **Fabric Edge maps L2 VNID to the VLAN interface and forwards the DHCP packet in the overlay (same as for a wired Fabric client)**
SD-Access Wireless Basic Workflows

Client Onboarding

7. Client receives an IP address from DHCP

8. DHCP snooping triggers the client EID registration by the Fabric Edge to the CP.
   
   *(If client has a static IP, then ARP or any other IP packet will trigger the registration)*

This completes Client onboarding process
**SD-Access Wireless Basic Workflows**

**Client Roams**

1. Client roams to AP2 on FE2 (inter-switch roaming). WLC gets notified by AP.
2. WLC updates forwarding table on AP with client info (SGT, L2VNID, RLOC).
3. WLC updates the L2 MAC entry in CP with new RLOC FE2.

---

**Diagram Description:***

- **AP1** and **AP2** are connected to **FE1** and **FE2** respectively.
- **SDA Fabric** is shown connecting both **FE1** and **FE2**.
- **Fabric WLC** is connected to **SDA Fabric**.
- **Fabric client info sent to AP** is shown as an intermediate step between **SDA Fabric** and **AP2**.
- **Client L2 MAC entry update** is shown as an update from **Fabric WLC** to **AP2**.

---

**Notes:**

- The diagram illustrates the workflow of client roaming and updates in an SD-Access Wireless environment.
- The process begins with the client roaming to AP2 on FE2, followed by notification to the WLC, which updates the forwarding table and MAC entry in the CP.
SD-Access Wireless Basic Workflows

Client Roams

CP then notifies
- Fabric Edge FE2 ("roam-to" switch) to add the client MAC to forwarding table pointing to VXLAN tunnel
- Fabric Edge FE1 ("roam-from" switch) to do clean up for the wireless client
- Fabric Border to update internal RLOC for this client

FE will update the L3 entry (IP) in CP data base upon receiving traffic

Roam is Layer 2 as FE2 has the same VLAN interface (Anycast GW)
Wireless and SDA
Deployment Modes
SD-Access Wireless: true integration in Fabric

- True wireless integration with Fabric
- Provides all the advantages of SDA for wireless clients:
  - Full automation with DNAC
  - Hierarchical segmentation (VRF and SGT)
  - Same policy as wired
  - Distributed Data Plane with no drawbacks
  - Optimized traffic path for Guest
- Recommended option

- CAPWAP Control Plane, VXLAN Data plane
- WLC/APs integrated in Fabric, SD-Access advantages
- Requires software upgrade (8.5+)
- Optimized for 802.11ac Wave 2 APs
Wireless on top of SDA Fabric

- No SDA advantages for wireless
- Migration step to full SD-Access
- Customer wants/need to first migrate wired (different Ops teams managing wired and wireless, get familiar with Fabric, different buying cycles, etc.) and leave wireless “as it is”
- Customer cannot migrate to Fabric yet (older APs, need to certify the new software, etc.)

CUWN wireless Over The Top (OTT)

- CAPWAP for Control Plane and Data Plane
- SDA Fabric is just a transport
- Supported on any WLC/AP software and hardware
- Only Centralized mode is supported at FCS
Wireless on top of SDA Fabric

- **FlexConnect Over The Top (OTT)**
  - CAPWAP for Control Plane
  - Data plane is locally switched. Wireless traffic is treated like wired traffic.
  - **Not supported today (1.2)**

- FlexConnect local switching is not supported in SDA 1.2 (today)
- Will it work? Probably yes but it has not been fully tested hence it is not officially supported
- This applies also to 3rd party APs that bridge traffic at the AP
Wireless Integration in SDA Fabric

- **Mixed mode**: mix of Fabric and non-Fabric (centralized) SSIDs
- **Mixed mode** is supported both on the same AP or different APs
- With DNAC 1.1 mixed mode is supported only for greenfield deployments
- Automation for Foreign-Anchor Guest SSID is supported in DNAC 1.2

**Mixed Mode**

- **non-Fabric SSID**: client traffic is CAPWAP encapsulated to WLC
- **Fabric SSID**: client traffic is VXLAN encapsulated
- **Supported in SDA 1.1 in greenfield only**
SD-Access Wireless
Design & Deploy
How to Connect APs and WLC?

**Access Points**
- AP is directly connected to FE (or to an extended node switch)
- AP is part of Fabric overlay
- AP belongs to the INFRA_VN 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 – to talk to CP!
- 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
How to Connect WLC?

Recommnaded WLC Connection to Wired

- WLC is connected outside Fabric to a switch in Service Block or DC

- WLC side:
  - Use multiple ports for redundancy and group them in a LAG (Link Aggregation)
  - Use a pair of boxes and enable Stateful Switch Over – this will double the links to connect to the infrastructure

- Leverage physical redundancy at the switch:
  - Single box solution: modular switch or switch stack and spread WLC links across line cards or stack members
  - Dual switch solution: use VSS and spread links across switches
**AP to WLC Connection**

**South-North Traffic Details**

- **AP to WLC (South to North traffic)**
  - Border Node redistributes the WLC route in the underlay (using the IGP of choice)
  - FE learns the route in the Global Routing Table
  - When FE receives CAPWAP packet from AP, the FE finds a match in the routing table and packet is forwarded directly with no VXLAN encapsulation
  - The AP to WLC traffic travels in the **underlay**

---

**Cisco Live!**

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
AP to WLC Connection
North-South Traffic Details

WLC to AP (North to South traffic)

- The AP subnet is registered in CP
- Border exports AP local EID space from CP to the routing table and also import the AP routes into LISP map-cache entry
- Border to advertise local AP EID space to the external domain
- When Border receives CAPWAP packet from WLC, the LISP lookup happens and traffic is sent to FE with VXLAN encapsulation
- The WLC to AP traffic travels in the overlay
SD-Access Wireless
Design and Deploy considerations

- WLCs connect external to fabric
- Fabric AP joins in Local WLC local to the Site – no support for Flex or WLC over WAN
  - Latency between AP and WLC < 20 ms
- Border advertises WLC Management subnet to the Fabric
- Border advertises Fabric prefixes to the WLC Management network
SD-Access Wireless

Design and Deploy considerations

- Access Points are **directly connected** to the Fabric Edge
- APs are in overlay space on Fabric Edges
- One subnet for APs across the entire Fabric
- APs get registered in the CP database
- Simplified IP design for AP onboarding (one subnet)
SD-Access Wireless

Design and Deploy considerations

- Client subnets are distributed on Fabric Edge switches
- No need to define client subnets on WLC
- Client subnets are mapped to VLAN with Anycast Gateway on all Fabric Edge switches
- All roams are Layer-2 Roams
SD-Access Wireless

Design and Deploy considerations

- Wireless client traffic is distributed
- No hair-pinning to centralized controller
- Communication to wired clients is directly through Fabric
SD-Access Wireless
Design and Deploy considerations

- Fabric capability enabled on a per WLAN basis
- CAPWAP WLAN can co-exist with Fabric-enabled WLAN using same Fabric-enabled WLC. At FCS this is only supported for Greenfield deployments
SD-Access Wireless in Distributed Campus

(Beta in SDA 1.2)
SD-Access for Distributed Campus

Automated Inter-Site Connectivity

Site-Local Services
ISE PSN, WLC, etc.

End-to-End Policy & Segmentation

DNA Center
Policy, Automation, Analytics

Scalable
100s of Sites

Flexible
50 - 100,000 Users/Site

Resilient
Local Control Planes, Borders

High Performance
Local Breakout

Cisco Live! 2020
SD-Access for Distributed Campus

Integrating wireless

* Beta in SDA 1.2

First, build a single Fabric Site as you were building a Fabric Domain in 1.1.x

Then add multiple sites (up to 200 sites) connected via a Transit site

Today (SDA 1.2) each site needs its own physical WLC

WLC only talks to one site Control Plane node (two for redundancy)
SD-Access Wireless
Guest Design
SD-Access Wireless Guest

- One touch Guest solution, DNAC automated
- Backend integration with ISE for Portal and Profiles configuration
- In DNAC 1.2 both Central Web Auth (CWA) with ISE and Local WebAuth (LWA) are supported
- No wired Guest automation in DNAC 1.2
SD-Access Wireless Guest Design
Guest with dedicated Border and Control Plane nodes

- Leverages dedicated Control Plane node and Border for Guest
- Complete Control plane and Data plane separation from Enterprise traffic
- No additional Anchor WLC: Guest traffic is optimized, sent directly to the DMZ
- No Anchor WLC scalability limit (71 tunnels). Scalability depends on Border scale
SD-Access Wireless Guest Design
Using the Enterprise Control Plane & Border

- Guest and Enterprise clients share the same Enterprise CP node
- Guest SSID is associated to a dedicated VN in Fabric
- Leverages Fabric segmentation (VNI, SGT) for guest traffic isolation
SD-Access Wireless Guest Design
Anchor-Foreign CUWN Solution

- Guest WLAN anchored at Guest Anchor in DMZ
- Well proven CUWN solution, protecting investment
- Restriction of 71 Guest Tunnels
- Separate solution for Wired Guest, Anchor WLC managed differently
DNAC 1.2 Guest SSID with Anchor WLC

- DNAC 1.2 now supports Guest Anchor configuration for both Central Webauth (CWA) and Local WebAuth (LWA) with external portal.

- When provisioning the WLC now user has to option to choose Active (Foreign) or Anchor WLC.
SD-Access Wireless
Over the Top (OTT)
CUWN Over the Top (OTT)

• Definition:
  • Wireless OTT: this CAPWAP wireless overlay to Fabric: traditional CAPWAP deployment connected to Fabric overlay. Fabric is a transport for CAPWAP

• Why wireless OTT? As a migration step…
  • Customer wants/need to first migrate wired (different Ops teams managing wired and wireless, get familiar with Fabric, different buying cycles, etc.)
  • Customer doesn’t want/cannot migrate to Fabric (new software, no 802.11n, wireless too critical to make changes)
CUWN Over the Top (OTT)

Design and Deploy considerations

- WLCs connect external to fabric
- Border advertises WLC Management subnet into the Fabric
- Border advertises Fabric prefix for AP to the outside IP network
Access Points are in overlay space on Fabric Edge switches. APs get registered in the Host Tracking Database (CP) as wired clients.

- One subnet for APs across the entire Fabric in Campus => Simplified IP design for AP onboarding
- Use pool in INFRA_VN to onboard OTT APs (*)

(*) assuming whole deployment is OTT
Wireless SSIDs are mapped to VLAN/Subnet at WLC using dynamic interfaces
Border advertises Wireless client subnets to the Fabric
CUWN Over the Top (OTT)
Design and Deploy considerations

- CAPWAP is built from the AP to the WLC
- CAPWAP traffic travels in the underlay from AP to the WLC, and it’s not VXLAN encapsulated. As with Fabric enabled APs, this is because the WLC destination is known in the underlay so the FE forwards this traffic directly.
- The return traffic, from WLC to AP, is encapsulated at the Border
CUWN Over the Top (OTT)

Design and Deploy considerations

- Clients are authenticated and on-boarded by WLC
- Wireless clients are external to fabric in this case
CUWN Over the Top (OTT)
Design and Deploy considerations

- Communication from a wired host in Fabric to Wireless Client outside fabric will occur through Internal Border – JUST LIKE TODAY!!
- For the Fabric, it is a Fabric host communicating to a known destination external to the Fabric
CUWN Over the Top (OTT)

Design and Deploy considerations

- All APs model are supported
- Common subnet for APs – ease AP deployment
- Increase MTU along the path to prevent fragmentation
- External to Fabric. No need to upgrade code. All features work as today
- Can use Cisco Prime or GUI to manage
CUWN Over the Top (OTT)
Design and Deploy considerations

- All APs model are supported
- Common subnet for APs – ease AP deployment
- Increase MTU along the path to prevent fragmentation
- External to Fabric. No need to upgrade code. All features work as today
- If Greenfield, you can manage it using DNAC
Multicast
Important things to know:

- Multicast traffic is transported in the overlay, in the EID space, for both wired and wireless clients.
- To enable multicast for wireless, Global Multicast mode and IGMP snooping need to be enabled globally on the WLC.
- At FCS, multicast traffic leverages head-end replication to forward traffic to the Fabric multicast destination.
SD-Access Fabric
How Multicast Works – Multicast Receiver to RP

- Multicast client (receiver) is in the overlay, multicast source can be outside Fabric or in the overlay as well
- PIM-SM/PIM-SSM needs to be running in the Overlay
- The client sends IGMP join for a specific multicast Group (G)
- AP encapsulates it in VXLAN and send it to the upstream switch.
- The Fabric Edge node (FE) receives it and does a PIM Join towards the Fabric Rendezvous Point RP (assuming PIM-SM is used)
- The RP needs to be present in the Overlay as part of the End point IP space.
How Multicast Works – Multicast Source to RP

- The Multicast source will send the multicast traffic on the interfaces towards the Fabric Border (FB) as it’s the DR for that segment.
- The FB receives it and does a PIM Join towards the RP (assuming PIM-SM is used)
- The RP now has the source and receiver information for that multicast group.
From Earlier, The RP now has the source and receiver information for a particular multicast group.

The FB will send the multicast source traffic over a VXLAN tunnel to the RP and the RP will forward that traffic to the FE over another VXLAN tunnel.

FE receives the VXLAN packets, decapsulates, applies policy and then forwards it again to the AP over an VXLAN tunnel.

The AP removes the VXLAN header and send the original IP multicast packet into the air.
Once the first multicast packet is delivered to the FE the shortest path failover (SPT) happens and the traffic is forwarded between the FB and the FE directly.

The FE knows that the FB owns the multicast source based on the first multicast packet received and send a PIM join directly to the FB for that multicast group.

FB now knows which FEs have clients that requested the specific multicast Group.

It performs headend replication and VXLAN encapsulates the multicast traffic and unicasts it to the interested FEs.

The multicast traffic is sent in the overlay.

FE receives the VXLAN packets, decapsulates, apply policy and then forwards it again to the AP.

The AP removes the VXLAN header and send the original IP multicast packet into the air.
High Availability in SD-Access Wireless
SD-Access Wireless HA
Control Plane Redundancy

Control Plane is based on a LISP Map Server / Resolver

- Host Database, tracks Endpoint ID to Edge Node bindings, along with other attributes (e.g., SGT)
- Redundancy is supported in Active / Active configuration
- WLC (and Fabric Edges) are configured with two CP nodes and synch information to both
- If one fails, all client information is available at the other CP node
SD-Access Wireless HA

CP Redundancy

Control Plane is based on a LISP Map Server / Resolver
**SD-Access Wireless HA**

**WLC Redundancy with SSO**

**Fabric WLC fully supports SSO High Availability**

- Stateful Redundancy with SSO:
  - WLC SSO pair is seen as one node in DNAC
  - Only Active WLC interacts with CP node and CP state is synched between Active and Standby
  - Upon failure, new Active WLC will bulk update Fabric clients to the CP node (LISP refresh)
  - Wireless APs and Clients stay connected

- WLC is connected outside Fabric, so normal best practices apply to connect the SSO pair
Fabric WLC fully supports SSO High Availability

- Stateful Redundancy with SSO:
  - WLC SSO pair is seen as one node in DNAC
  - Only Active WLC interacts with CP node and CP state is synched between Active and Standby
  - Upon failure, new Active WLC will bulk update Fabric clients to the CP node (LISP refresh)
  - Wireless APs and Clients stay connected

- WLC is connected outside Fabric, so normal best practices apply to connect the SSO pair

- SSO using Fabric as L2 transport is not supported

- N+1 redundancy is not supported in DNAC 1.1
SD-Access Wireless HA
WLC Redundancy with N+1

Wireless LAN Controller is part of control plane in Fabric

- Stateless Redundancy with N+1
  - AP is configured with Primary and Secondary
  - AP and associated clients register with Primary
  - Upon Primary failure, AP disconnects and joins Secondary
  - Clients are also disconnected and join Secondary
  - Secondary performs new client registration in CP

- N+1 for SD0-Access Wireless is not automated and not supported as of DNAC 1.2. It’s a feature for future roadmap
Branch Design
SD-Access Wireless – Branch Design

Dedicated Branch Fabric Domain

- Benefits:
  - Support for any WAN link latency
  - Direct Internet Access available

- Considerations
  - Need a local WLC (Today only option is a physical WLC, e.g. 3504)
  - Limited scalability in DNAC1.1 in terms of number of branches (10 Fabric domains). In DNAC 1.2 limitation is removed with Distributed Campus
  - WAN needs to support MTU> 1554f SDA transit
New in DNAC 1.2 / SDA 1.2
New Features in SDA 1.2

- Default RF Profile
- Band Select
- 5GHz only SSID (Radio Policy)
- Hidden SSID
- Override PSK (PSK per site)
### DNAC 1.2 Advanced RF (Default RF Profile)

1. **Admin can pick a custom RF profile to be the Default one**

2. **Easier deployment: during AP provisioning, Default RF profile is shown first**

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Type</th>
<th>5GHz Data Rates</th>
<th>2.4GHz Data Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>advanced_rf_11a_disable</td>
<td>2.4 GHz</td>
<td>-</td>
<td>9.11, 12, 18, 24, 36, 48, 54</td>
</tr>
<tr>
<td>advanced_rf_11g_disable</td>
<td>5 GHz</td>
<td>6, 9, 12, 18, 24, 36, 48, 54</td>
<td>-</td>
</tr>
<tr>
<td>custom_rf</td>
<td>2.4 GHz, 5 GHz</td>
<td>6, 9, 12, 18, 24, 36, 48, 54</td>
<td>9.11, 12, 18, 24, 36, 48, 54</td>
</tr>
<tr>
<td>HIGH</td>
<td>2.4 GHz, 5 GHz</td>
<td>12, 18, 24, 36, 48, 54</td>
<td>9.12, 18, 24, 36, 48, 54</td>
</tr>
<tr>
<td>LOW</td>
<td>2.4 GHz, 5 GHz</td>
<td>6, 9, 11, 12, 18, 24, 36, 48, 54</td>
<td>1, 2, 5, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</td>
</tr>
<tr>
<td>TYPICAL</td>
<td>2.4 GHz, 5 GHz</td>
<td>6, 9, 12, 18, 24, 36, 48, 54</td>
<td>9.12, 18, 24, 36, 48, 54</td>
</tr>
</tbody>
</table>
## DNAC 1.2 Advanced RF (Band Select)

- Create a SSID with “Dual band operation with band select” for the Dual band clients for connecting to the WLAN.
- DNAC configures band-select per-WLAN.
- Global default band select values are not changed from DNAC.

### Wireless Profiles

<table>
<thead>
<tr>
<th>Wireless Network Name (SSID)</th>
<th>TYPE OF ENTERPRISE NETWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAGU11</td>
<td>Voice and Data</td>
</tr>
<tr>
<td></td>
<td>Data only</td>
</tr>
<tr>
<td></td>
<td>Fast Lane</td>
</tr>
</tbody>
</table>

**Broadcast SSID:**
- Off

**Wireless Option**
- Dual band operation (2.4GHz and 5GHz)
- Dual band operation with band select
- 5GHz only

**Level of Security**
- WPA2 Enterprise
- WPA2 Personal
- Open
DNAC 1.2 Advanced RF (5GHz only SSID)

- Radio Policy configuration
- 5GHz only will apply Radio policy 802.11a only to the WLAN.
DNAC 1.2 Advanced RF (Hidden SSID)

- Admin has the option to hide SSID so that SSID is not broadcasted.
- During SSID creation, there is a toggle button for Broadcast SSID - On / Off. The same is reflected on WLAN configuration at WLC.
DNAC 1.2 Advanced RF (Override PSK)

In DNAC 1.2, PSK for SSID can be site specific. Each site can have different PSK SSID.

**Step 1**: Create a PSK SSID under Global

**Step 2**: PSK SSID is created successfully, as shown in below screenshot.
DNAC 1.2 Advanced RF (Override PSK)

Step 3: When traversed to Building or site in the hierarchy, PSK SSIDs are listed and the passphrase for the SSID can be modified.

Step 4: Passphrase updated PSK SSID is shown below in the screenshot and the inheritance is not seen for the updated SSID.
DNAC 1.2 : PnP for AP Provisioning

DNAC 1.2 supports PnP for APs (AP sensor is there already in 1.1.x)

1. AP shows in DNAC -> Provision Page -> Unclaimed Devices. AP will be in Initialized Unclaimed status
Select the AP and claim device

Claim the device which prompts to assign site and RF profile.
DNAC 1.2 : PnP for AP Provisioning (Cont..)

4 AP gets the PnP config with WLC details from DNAC and will be in Onboarding state for a bit and the Success
SD-Access Wireless Adoption/Migration Scenarios
SD-Access Wireless Adoption

The focus for FCS is greenfield

It's a journey....

1 What You Need to Know

2 Supported Adoption Scenarios
SD-Access Wireless Adoption
What You Need to Know

**DNAC 1.2 - General Availability**

- Ideal deployment is still Campus
- Brownfield is now supported: DNAC can read an existing non-Fabric config from WLC
- Mixed mode is supported: Fabric and non-fabric SSIDs on same WLC
- For Over The Top (Fabric as transport) DNAC 1.2 supports AP in Local mode only (no Flex or 3rd party APs)
- Mix deployment of CUWN and SDA wireless: seamless roaming is not supported
SD-Access Wireless Adoption

New Cisco Wireless Customer

**New Wireless customer**

1. Wired SDA?
   - Yes: Value prop for SD-Access Wireless?
     - Yes: Greenfield Fabric wireless integration
       - Full SDA value
       - Tested and supported
       - Recommended
     - No: Greenfield "Overlay to Fabric"
       - Fabric wired first
       - Wireless is an Overlay
       - In DNAC 1.2 only Centralized Wireless is supported
   - No: "Pure CUWN wireless" play
SD-Access Wireless Adoption
Existing Cisco Wireless Customer

- **Existing Cisco Wireless customer**
- **Wired SDA?**
  - No: "Pure CUWN wireless" play
  - Yes: Value prop for SD-Access Wireless?
    - No: "Overlay to Fabric": Brownfield OTT solution "Don't touch my wireless" Prime for Management
    - Yes: Migration to SDA wireless

Brownfield
- Isolated building/Campus in one shot (equivalent to Greenfield)
- Multiple buildings with nomadic roaming (*)

(*) Nomadic and seamless roaming here refers to roaming between Fabric and non-Fabric wireless deployments.
Nomadic Roaming = same SSID, but client’s IP addressing changes
SD-Access Wireless Adoption
Migration for an Existing CUWN Deployment

- Customer has a site with AireOS Centralized wireless
- Assumptions:
  - Migration to Fabric happens in a single area (e.g. building) at the time and migration is in one shot
  - No need for seamless roaming between new SDA area and the existing wireless deployment
SD-Access Wireless Adoption
Migration for an Existing CUWN Deployment

1. Add DNAC and ISE (if not present already)
2. Migrate wired network to Fabric first
3. Wireless is over the top
SD-Access Wireless Adoption
Migration for an Existing CUWN Deployment

1. Discover existing WLC to DNAC – Learn configuration (e.g. SSIDs) and populate DNAC
2. Add a dedicated WLC for SD-Access and provision it to the site (can re-use the configuration inherited from old WLC)
3. on CUWN WLC, configure the APs in the area to join the new Fabric WLC
4. APs in the area will join Fabric WLC. From DNAC provision APs to the Fabric site
SD-Access Wireless Adoption

Brownfield WLC support

Ability for DNA-C to import configuration from a brownfield (existing deployed) Cisco WLC and import parameters into DNA Center Design and Provision module.

Imported configuration: SSID, RF profile, AAA Global settings, AP Groups etc.

Limitations:
- Only configurations recognized by DNA-C will be populated
- DNAC will not be able to learn device credentials
- DNS, webauth redirect url and syslog setting are not currently learnt by DNAC
SD-Access Wireless Adoption
Migration for an Existing CUWN Deployment

Recommendations

- Can use DNAC for both Fabric and non-Fabric
- Dedicated WLC for SD-Access Wireless
- Same SSIDs on Fabric and non-Fabric

- Same RF Groups for CUWN WLC and SDA WLC
- WLCs in different Mobility Group (no seamless roaming between areas)
**SD-Access Wireless Adoption**

**Consideration for Shared WLC for Fabric and non-Fabric**

**Shared controller for SDA and CUWN**
- Shared WLC can manage Fabric and non-Fabric APs but **needs upgrade to 8.5**
- New code = more risk for existing non-Fabric buildings

**Management:**
- **DNAC 1.2 can manage non-Fabric WLC** in brownfield scenarios
- But not all wireless settings are available

**WLAN Design:**
- Fabric is enabled per SSID
- To have same SSID name in both areas:
  1. Need to define and apply AP Groups
  2. APs need to be re-booted

**Guest and Policy:**
- Can leverage existing Guest Anchor also for Fabric area/building
- Can leverage ISE for both

---

**Diagram Notes:**
- Area 1: Traditional Campus
- Area 2: Non-Fabric
- CAPWAP Control
- SD-Access Fabric
- Internal
- Fabric APs
- No roaming between Fabric and non-Fabric
- Shared WLC
- Guest Anchor
- EoIP
- VXLAN
Key Takeaways
Key Takeaways
Software Defined Access Networking at the Speed of Software!

SD-Access brings you...

Identity-based Policy & Segmentation
Decoupled security policy definition from VLAN and IP Address

Automated Network Fabric
Single Fabric for Wired & Wireless with Workflow-based Automation

Insights & Telemetry
Analytics and insights into user and application behavior

...for both wired and wireless!!
Don’t Miss the SD-Access Book…

It’s an e-book and you can download it from the link below

Cisco Enterprise Wireless Book

http://cs.co/wirelessbook
What to Do Next?

SD-Access Capable

DNA Centre

Cisco Services

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

Deploy the DNA Centre
Get DNA Centre Appliances with DNA Centre Software

Engage with Cisco Services
Cisco Services can help you to Test - Migrate - Deploy
Q & A
SD-Access Resources
Would you like to know 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
What to Do Next?

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
Related Sessions
SD-Access Breakouts (Core R&S Track)

Cisco SD-Access - A Look Under the Hood [BRKCRS-2810]
Shawn Wargo, Principal Engineer, Technical Marketing, Cisco
Monday, Jun 11, 01:30 p.m. - 03:30 p.m.

Cisco SD-Access - Connecting to External Networks [BRKCRS-2811]
Satish Kondalam, Technical Marketing Engineer, Cisco
Monday, Jun 11, 04:00 p.m. - 06:00 p.m.

Cisco SD-Access - Integrating with Existing Network [BRKCRS-2812]
Kedar Karmarkar, Technical Leader, Cisco Systems Inc
Tuesday, Jun 12, 04:00 p.m. - 06:00 p.m.
Thursday, Jun 14, 08:00 a.m. - 10:00 a.m.

Cisco SD-Access - Assurance and Analytics [BRKCRS-2814]
Karthik Kumar Thatikonda, Technical Marketing Engineer, Cisco
Wednesday, Jun 13, 10:30 a.m. - 12:00 p.m.

Cisco SD-Access - Deploy Fabric in Large Enterprises [BRKCRS-2815]
Satish Kondalam, Technical Marketing Engineer, Cisco
Wednesday, Jun 13, 08:00 a.m. - 10:00 a.m.
Thursday, Jun 14, 08:00 a.m. - 10:00 a.m.

Cisco SD-Access - Policy Driven Manageability [BRKCRS-3811]
Victor Moreno, Distinguished Engineer, Cisco
Wednesday, Jun 13, 01:30 p.m. - 03:00 p.m.

Cisco SD-Access - Building the Routed Underlay [BRKCRS-2816]
Rahul Kachalia, Sr. Technical Leader, Cisco
Thursday, Jun 14, 10:30 a.m. - 12:00 p.m.

Cisco SD-Access - Extending Segmentation and Policy into IoT [BRKCRS-2817]
Sanjay Hooda, Distinguished Engineer, Cisco
Thursday, Jun 14, 01:00 p.m. - 02:30 p.m.
Related Sessions
SD-Access Breakouts (Other Tracks)

How to setup an SD-Access fabric from scratch [BRKEWN-2021]
Simone Arena, Principal Engineer, Technical Marketing, Cisco
Ramses Smeyers, Principal Engineer, Services, Cisco
Monday, Jun 11, 08:30 a.m. - 10:00 a.m.

Cisco SD-Access Wireless Integration [BRKEWN-2020]
Simone Arena, Principal Engineer, Technical Marketing, Cisco
Tuesday, Jun 12, 08:00 a.m. - 10:00 a.m.

Cisco SD-Access Campus Wired and Wireless Network Deployment Using Cisco Validated Designs [BRKCRS-1501]
Dana Daum, Communications Architect, Cisco
Tuesday, Jun 12, 01:30 p.m. - 03:30 p.m.

Troubleshooting DNA SD-Access from API and Maglev [BRKARC-2016]
Parthiv Shah, Technical Leader, Cisco Systems
Rahul Gupta, Customer Support Engineer, Cisco
Tuesday, Jun 12, 04:00 p.m. - 06:00 p.m.

Cisco SD-Access: Secure Segmentation Design [CCSCRS-2000]
Ankush Arora, Solutions Architect, Cisco
Subodh Gajare, Senior Solutions Architect, Cisco
Thursday, Jun 14, 10:00 a.m. - 11:00 a.m.

Cisco SD-Access – Integration with DC Architectures [BRKDCN-2489]
Karthik Kumar Thatikonda, Technical Marketing Engineer, Cisco
Thursday, Jun 14, 01:00 p.m. - 02:30 p.m.
Related Sessions
SD-Access Hands-On & WISP Labs

A Practical Look at DNA Center: Hands-On Lab [LTRNMS-2500]
Jim Galvez, Technical Solutions Architect, Cisco
Saurav Prasad, Principal Engineer, Technical Marketing, Cisco
Lila Rousseaux, Technical Solutions Architect, Cisco
Monday, Jun 11, 08:00 a.m. - 12:00 p.m.

Cisco SD-Access Hands-On Lab [LTRCRS-2810]
Derek Huckaby, Technical Marketing Engineer, Cisco
Larissa Overbey, Technical Marketing Engineer, Cisco
Wednesday, Jun 13, 01:00 p.m. - 05:00 p.m.
Thursday, Jun 14, 08:00 a.m. - 12:00 p.m.

Cisco Software Defined Access (SD-Access) [LABCRS-2041]
Mariusz Kazmierski, Technical Leader, Services, Cisco Systems

Cisco SD-Access and ACI Integration - Hands-On Lab [LTRACI-2636]
Kaushal Patel, Network Consulting Engineer, Cisco
Ali Haider, Network Consulting Engineer, Cisco
Jaydeepsinh Parmar, Network Consulting Engineer, Cisco
Wednesday, Jun 13, 08:00 a.m. - 12:00 p.m.
DNA Software Subscription

Cisco ONE Suites or Ala Carte Model

Available for Current Catalyst 3K, 4K, 6K and Next Generation Catalyst 9K Series

**ESSENTIALS**
Layer 2, Routed Access, Base Automation and Monitoring

**ADVANTAGE**
Full L3, Segmentation, Software Defined Access, ETA & Assurance

- Ongoing Innovation
- License Portability
- Software Support Included
- OpEx Preference
- Lower Entry Costs

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Questions?
Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session.

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

Webex Teams will be moderated by the speaker until June 18, 2018.
Complete your online session evaluation

Give us your feedback to be entered into a Daily Survey Drawing.

Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.
Continue your education

- Demos in the Cisco campus
- Walk-in self-paced labs
- Meet the engineer 1:1 meetings
- Related sessions
Thank you