

CISCO SDA

Jan Kaše



Legacy Networks

Konfigurace:

- Manuální – „automatizace“?
- Box po boxu
- Lidské chyby
- Troubleshooting
- Kolik času mi to zabere?

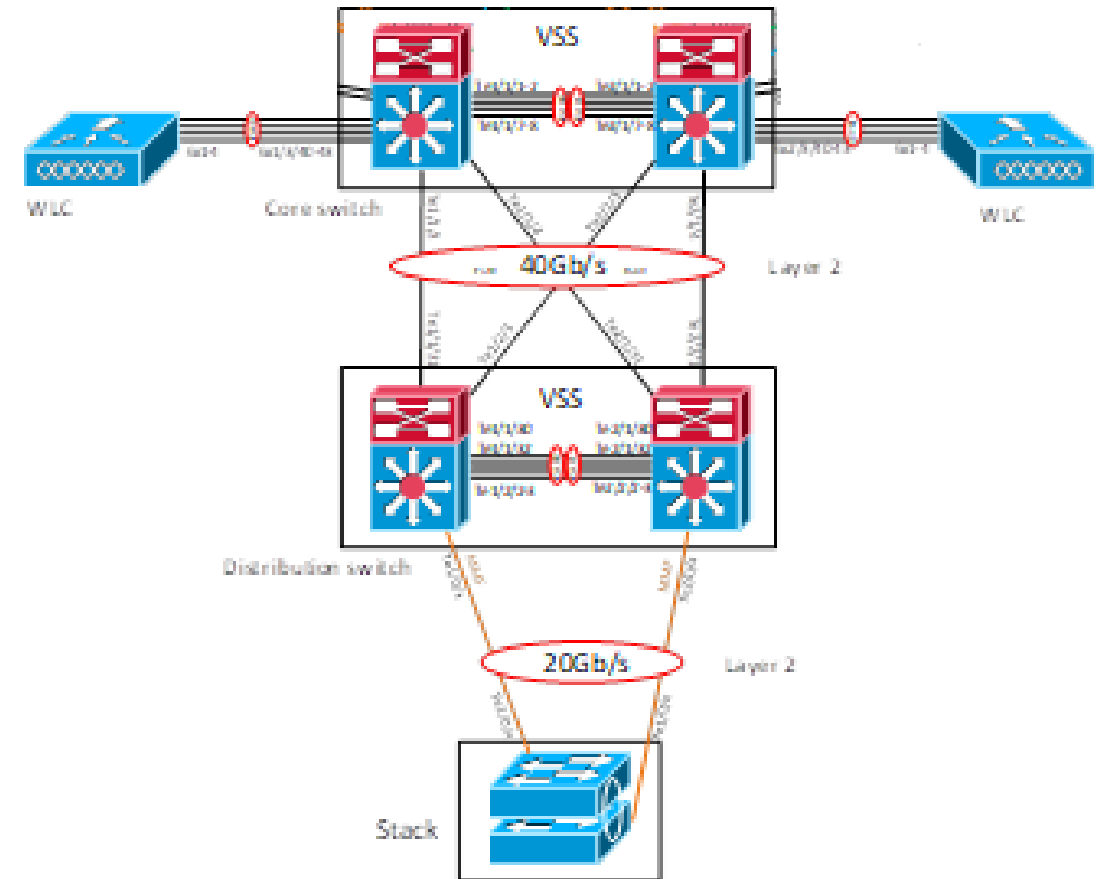
Segmentace a bezpečnost:

- VLANy, VLANy, VLANy a subnety
- Mobilita?
- ACL?

Wireless (OTT):

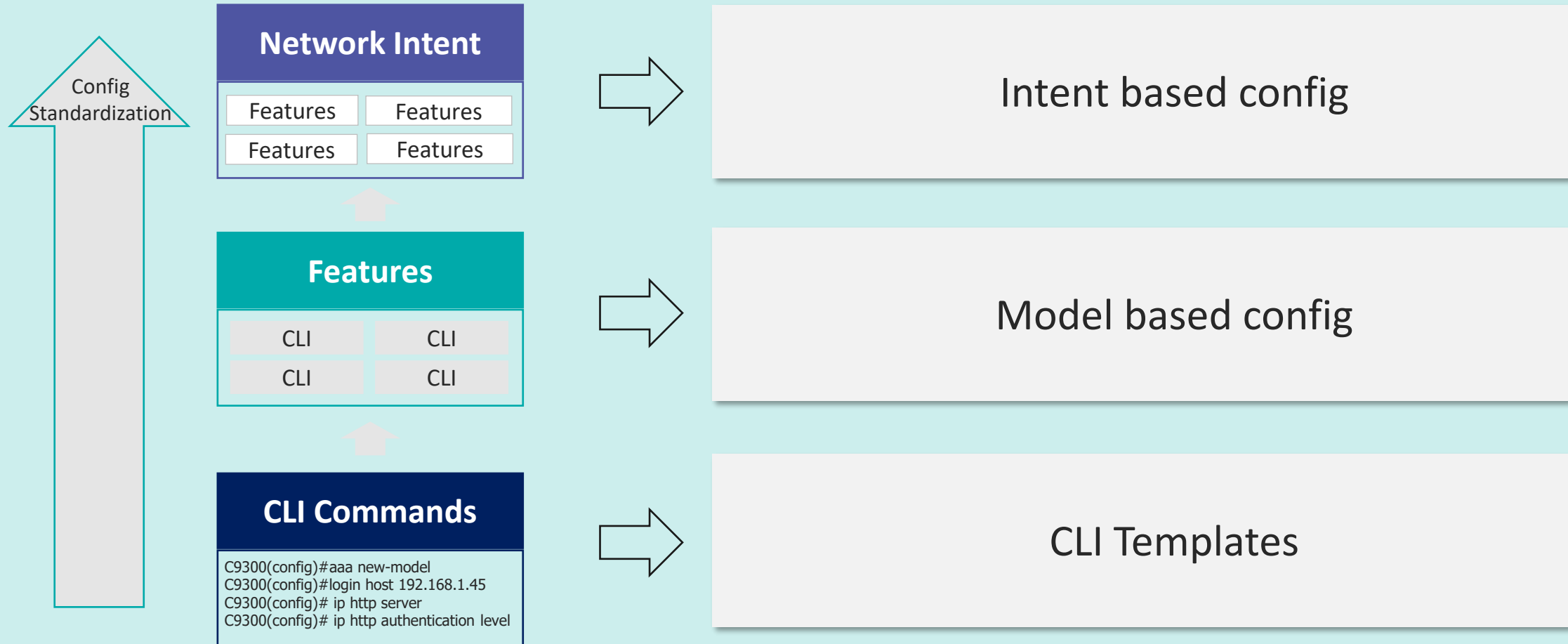
- Oddělená segmentace a konfigurace od wired
- Kde vypadne provoz?
- A co bezpečnost?

Management, monitoring?



Simplified configuration Management

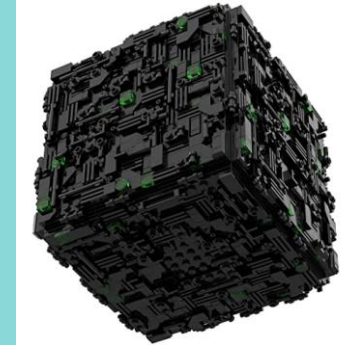
Network Configuration



Before SD-Access

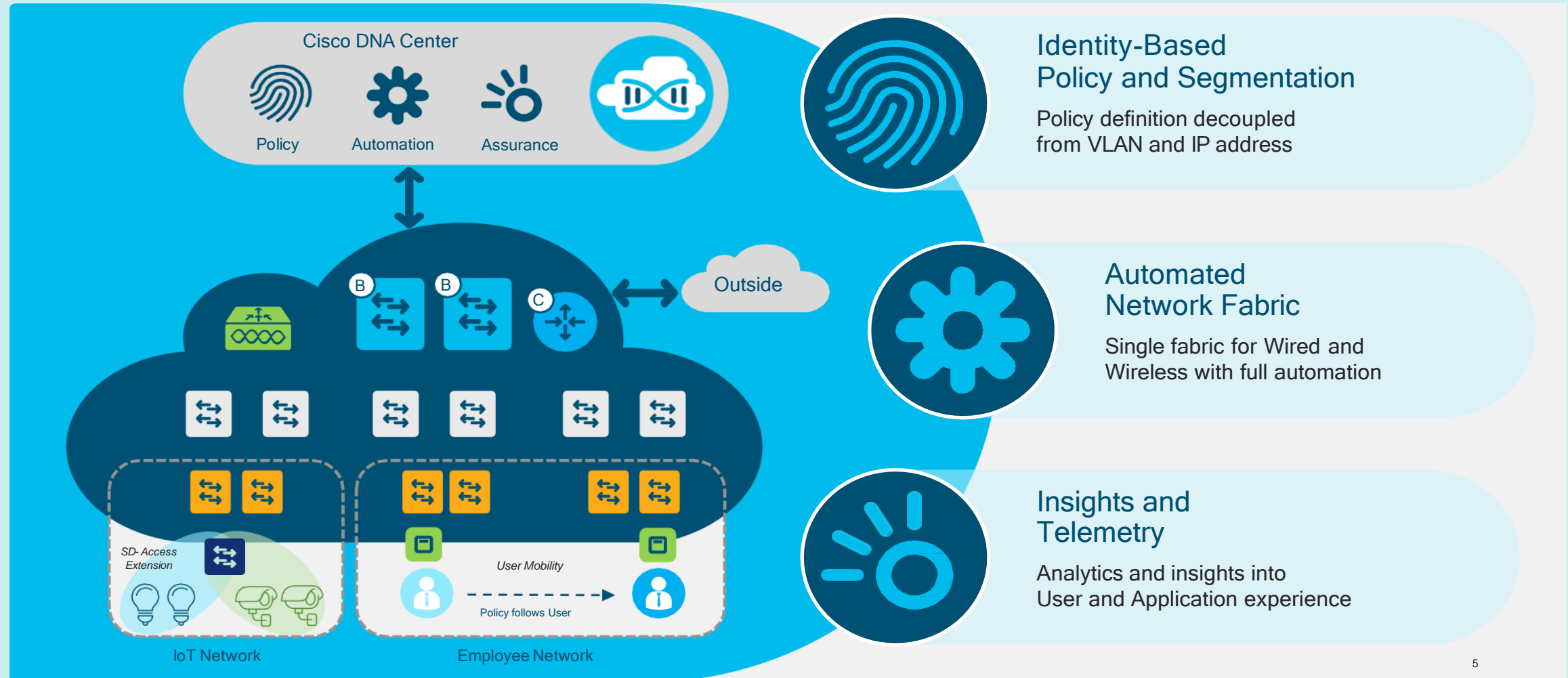


After SD-Access



Cisco Software Defined Access

The Foundation for Cisco's Intent-Based Network



SD-Access Architecture

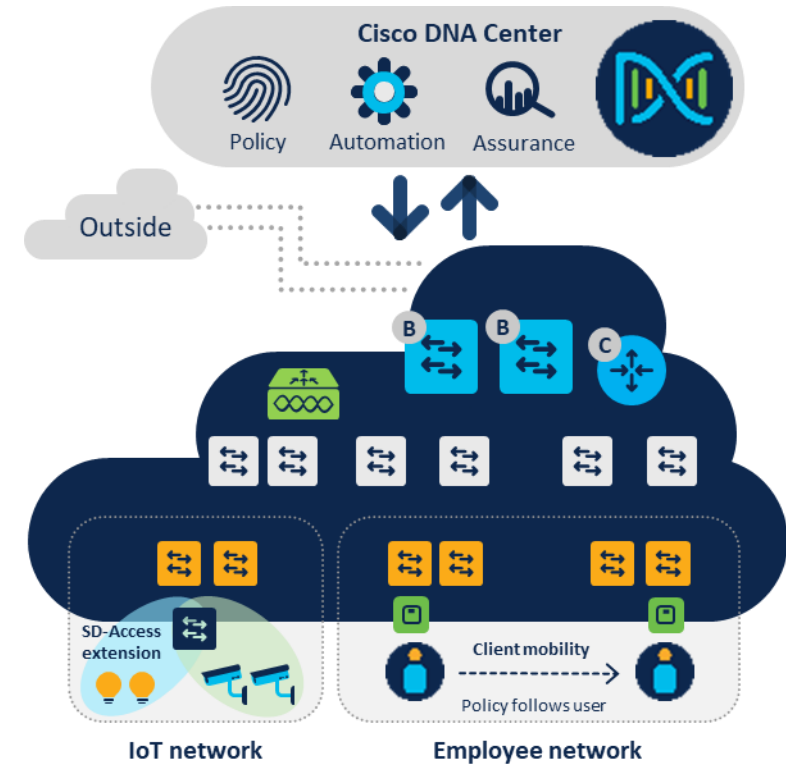
SDA = Campus Fabric + DNA Center

- A new main trend in building access networks
- Old technology:
VRF/VLAN/CTS/VXLAN/ISIS/LISP/BGP
used in a new way:

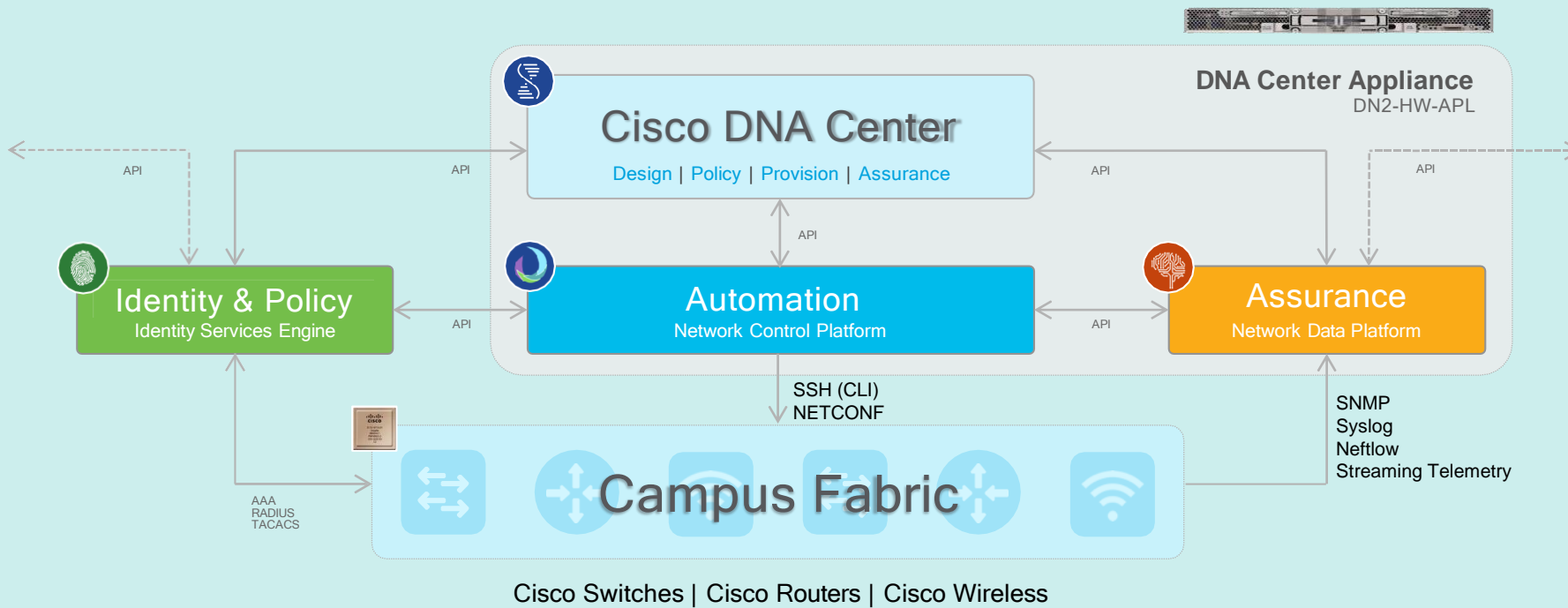
Campus fabric:

- Control-Plane based on LISP
- Data-Plane based on VXLAN
- Policy-Plane based on CTS

DNA Center: Management plane

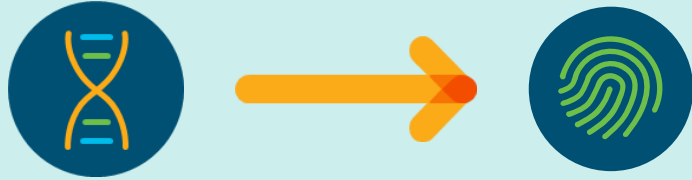


DNA Center Architecture



DNA Center and Identity Service Engine

Configure ISE from DNA Center



- Network Resources
 - Any discovered device > Network Devices
- Segmentation: VNs, SGTs, IP Pools for authorization policies
- Group-Based Access Control
 - Access Contracts
 - Policies

Get user information from ISE to DNA Center



- ISE - Only User IP and MAC address in Assurance
- ✓ ISE – More information in Assurance
 - User Identities:
 - Username
 - Device
 - Operating system

Campus Fabric

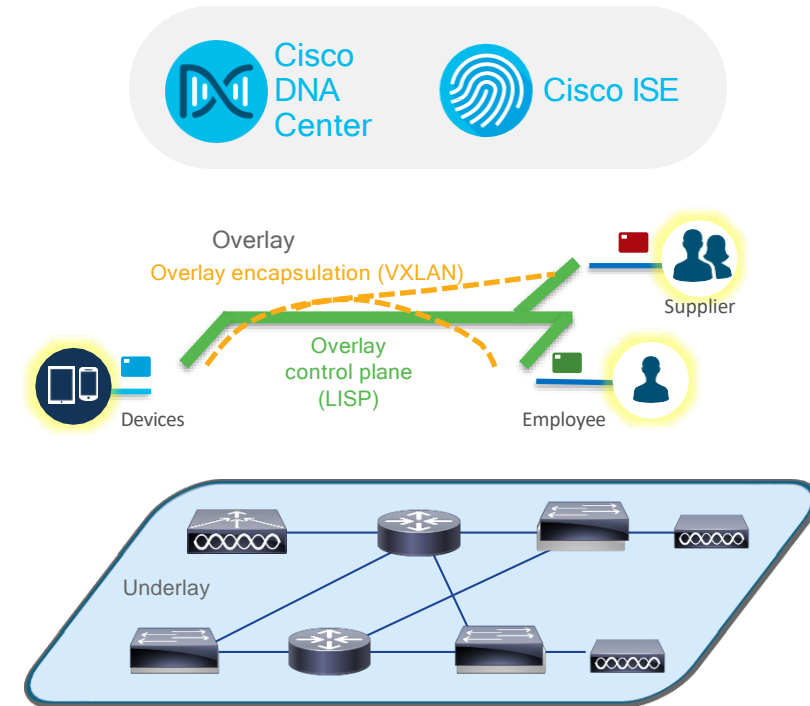
Fabric Overlay – Services plane

- Logical Topology - Dynamically connects Users/Devices/Things
- End to End Policies and Segmentation
- Control Plane (LISP) + Data Plane (VXLAN)
- Point-to-Point/Multipoint (Multicast) On-Demand VXLAN Tunneling Fabric



Fabric Underlay – Forwarding plane

- Physical Topology - Connects the network elements to each other
- Optimized for traffic forwarding (scalability, performance, load-balancing)
- Routed – Connectivity between all Lo0



SDA Fabric Underlay

Two ways how to build the fabric underlay

1. Manually > Discovery

- Manually configure the network devices
- IP connectivity between all nodes
- Custom selection of routing protocol
- Custom IP address plan
- Multicast (Optional)
- Discover the network device via IP address or CDP/LLDP

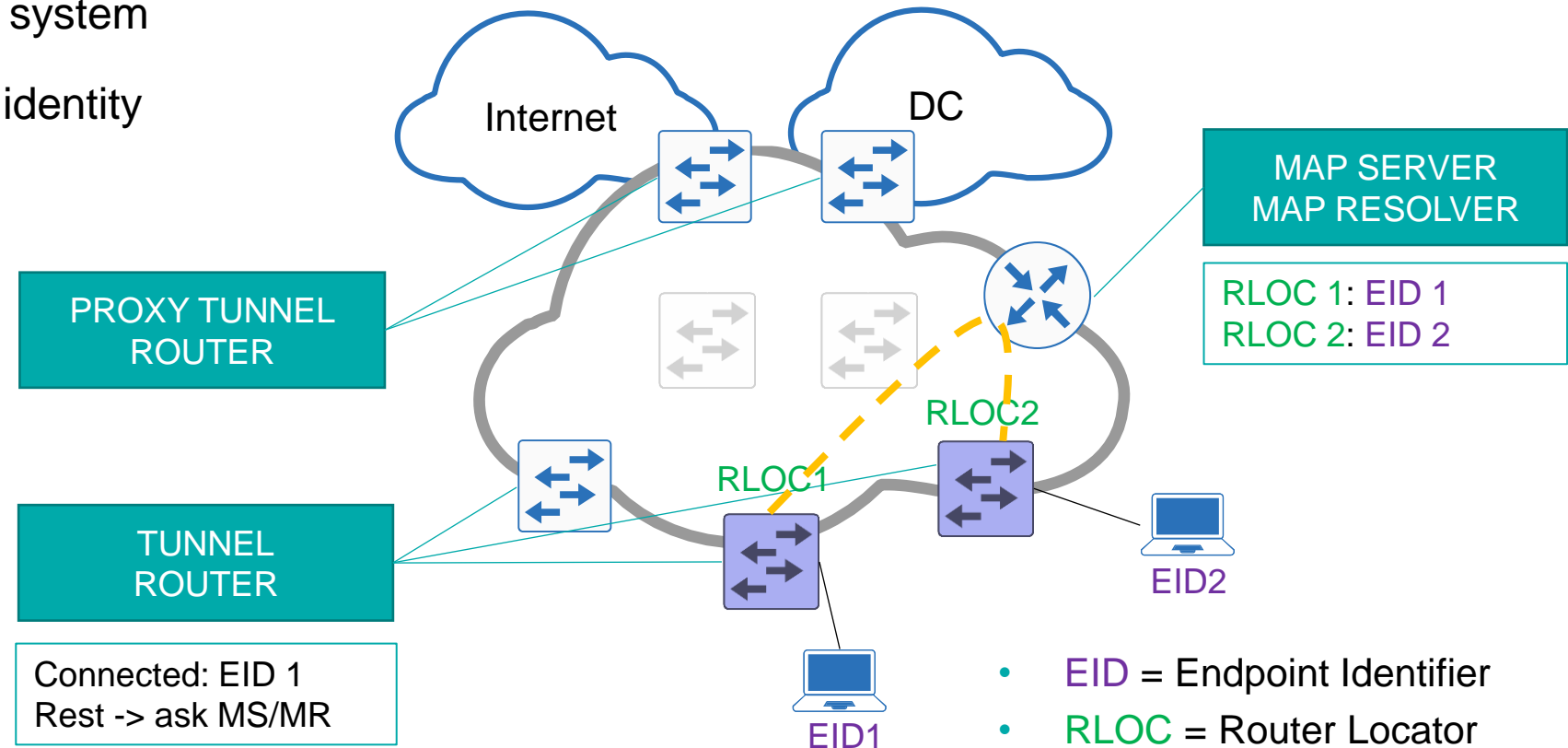
2. LAN Automation – DNA Center

- Configure only the first network device (primary seed = BORDER1 or CORE1) with an IP address
- Optionally configure the second network device (secondary seed = BORDER2 or CORE2) with an IP address (Redundancy)
- Discover the seed devices on the DNA Center
- Let DNA Center configure all other network devices connected (Distribution and Access layer)

LOCATOR/ID SEPARATION PROTOCOL

LISP is used as a Control-Plane protocol

- Traditional routing protocols require big resources (MEM & CPU)
- LISP is on-demand map system
- Separates location from identity

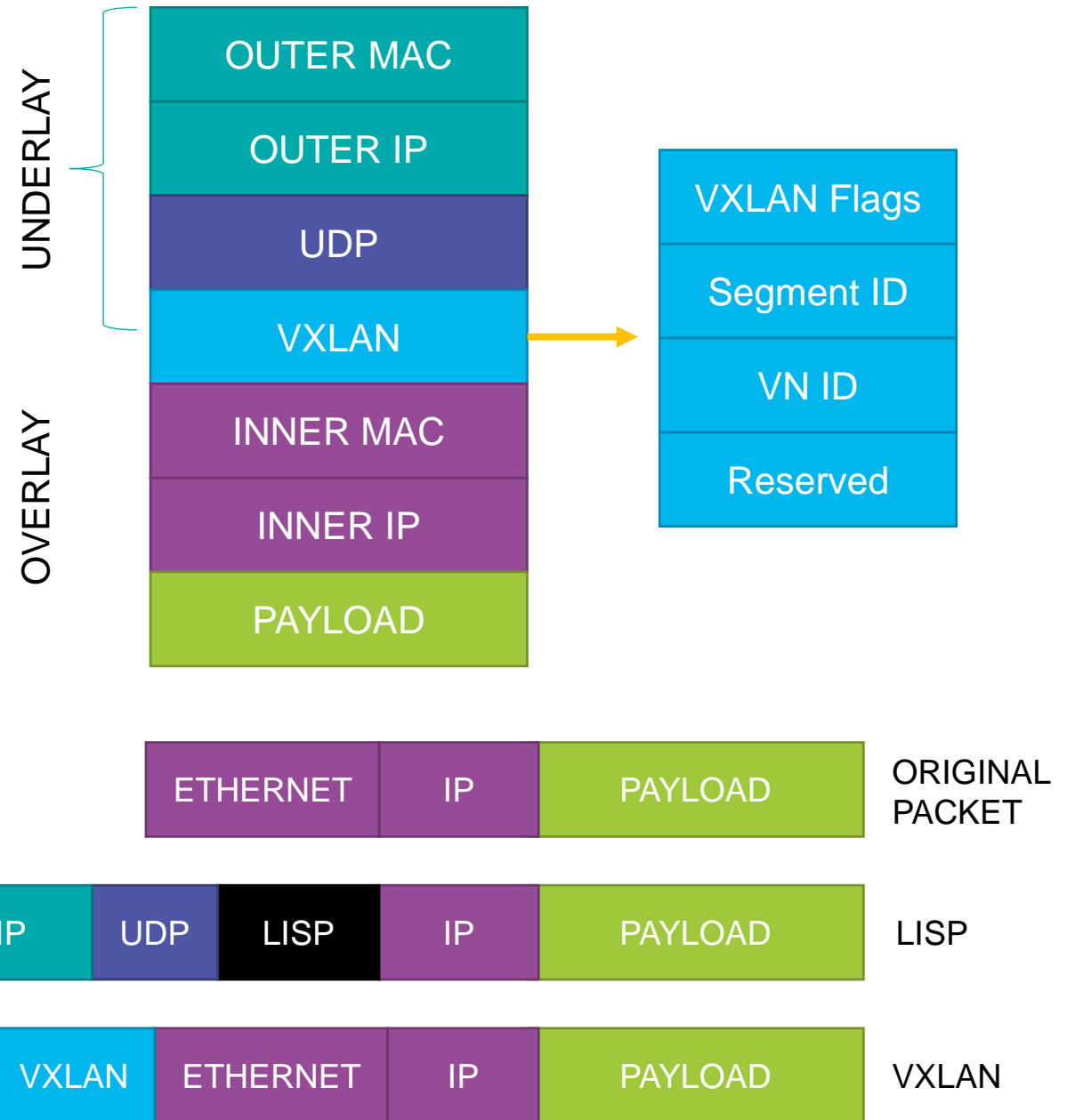


SDA VXLAN Data Plane

Fabric nodes use VXLAN (Ethernet Based) as the data plane which supports both L2 and L3 overlay.

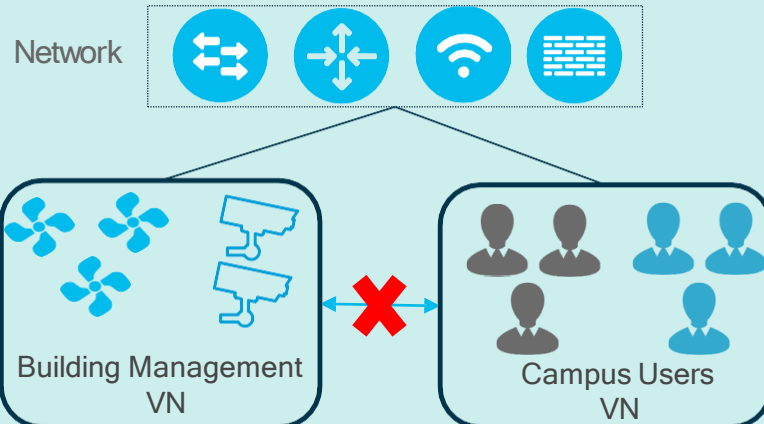
VXLAN header contains VNID (VXLAN Network Identifier) field which allows up to 16 million VRFs.

VXLAN header also has Group Policy ID for Scalable Group Tags (SGTs) allowing 64,000 SGTs.



SDA Segmentation and Policy

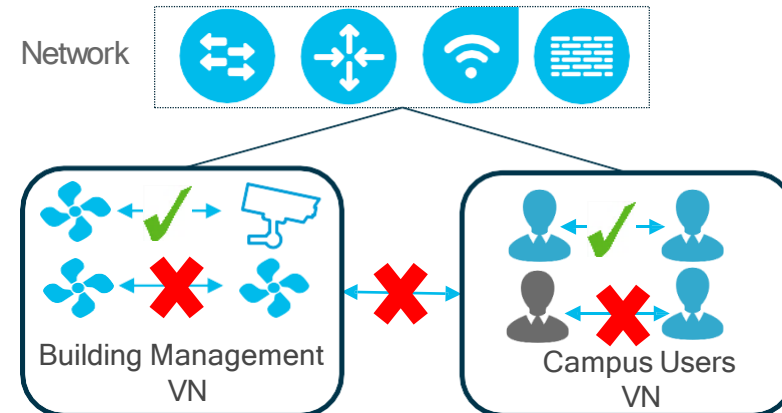
Macro Segmentation



Virtual Network (VN)

First level Segmentation ensures **zero** communication between specific groups. Ability to consolidate multiple networks into one management plane.

Micro Segmentation

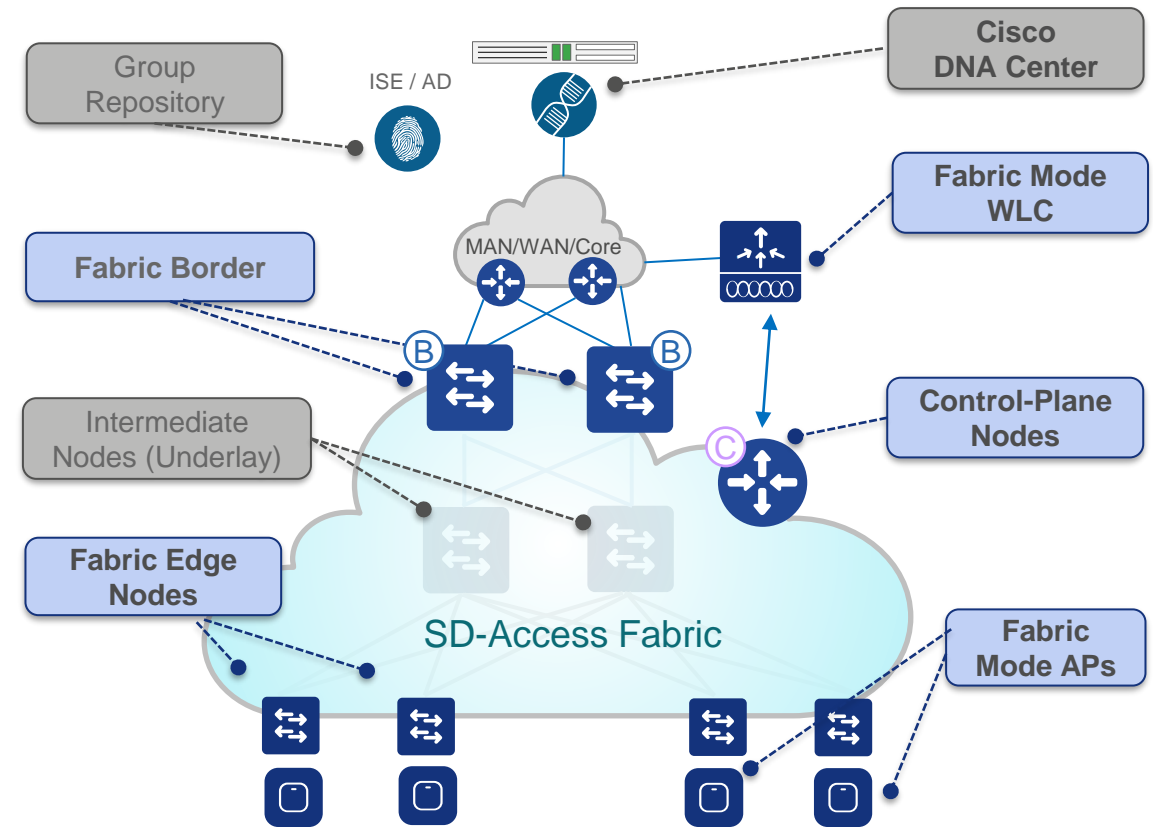


Scalable Group (SG)

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.

SDA Fabric Roles

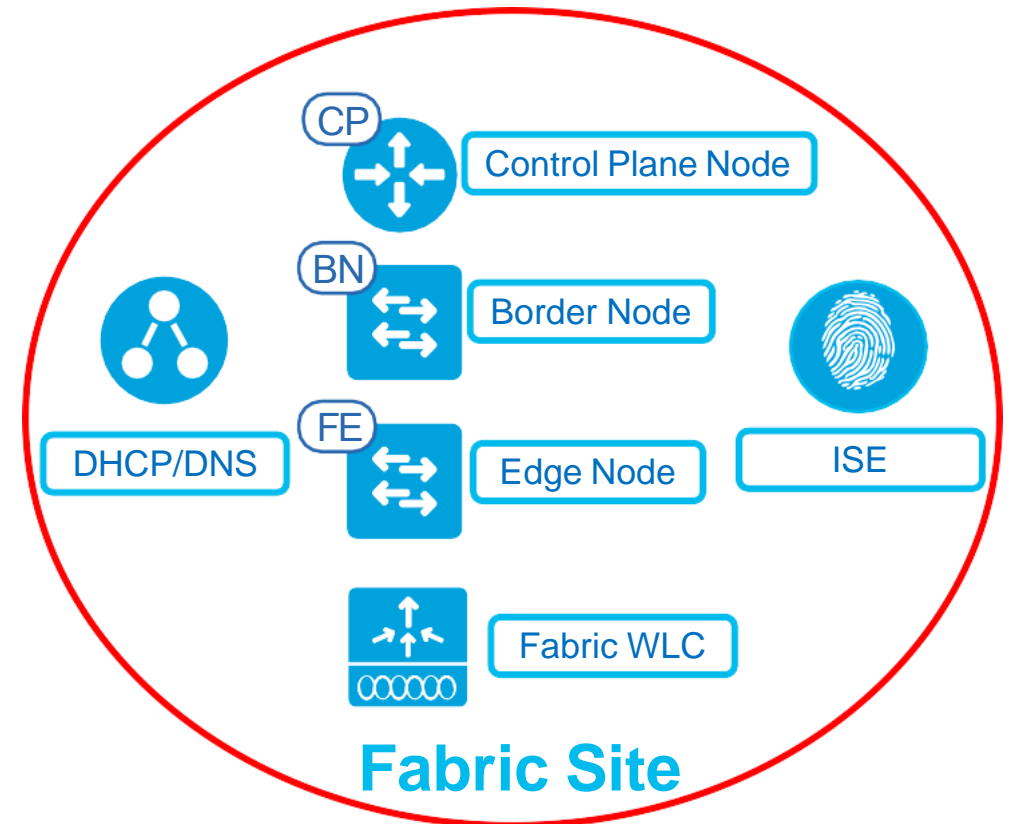
- **DNA Controller** – Enterprise SDN Controller provides GUI management abstraction via multiple Service Apps, which share information
- **Group Repository** – External ID Services (e.g., ISE) is leveraged for dynamic User or Device to Group mapping and policy definition
- **Control-Plane (C) Node** – Map System that manages Endpoint ID to Location relationships. Also known as Host Tracking DB (HTDB)
- **Border (B) Nodes** – A Fabric device (e.g., Core) that connects External L3 network(s) to the SDA Fabric
- **Edge (E) 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



SDA Fabric Sites

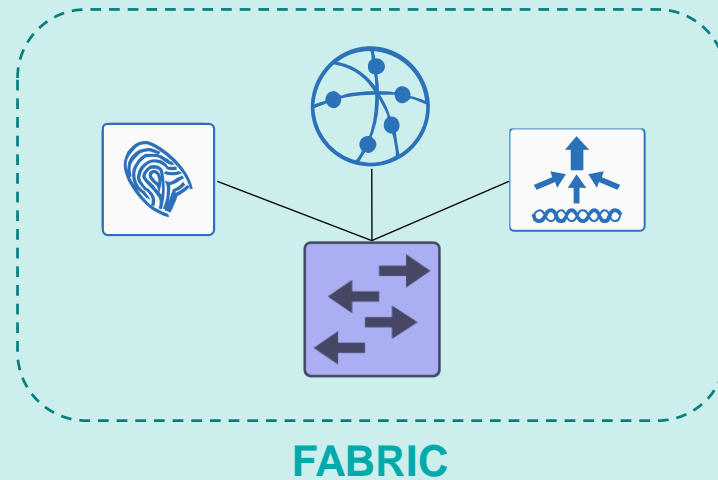
are an independent fabric area with a unique set of network devices

- Contains Control Plane Node, Border Node, and Edge Node
- Contains WLC and ISE Policy Service Node (PSN)
- Fabric Border Node is the ingress and egress device for the site
- A Fabric Site may cover a single physical location, multiple locations, or just a subset of a location
 - Single Location → Branch, Campus, or Metro Campus
 - Multiple Locations → Metro Campus + Multiple Branches
 - Subset of a Location → Building or Area within a Campus



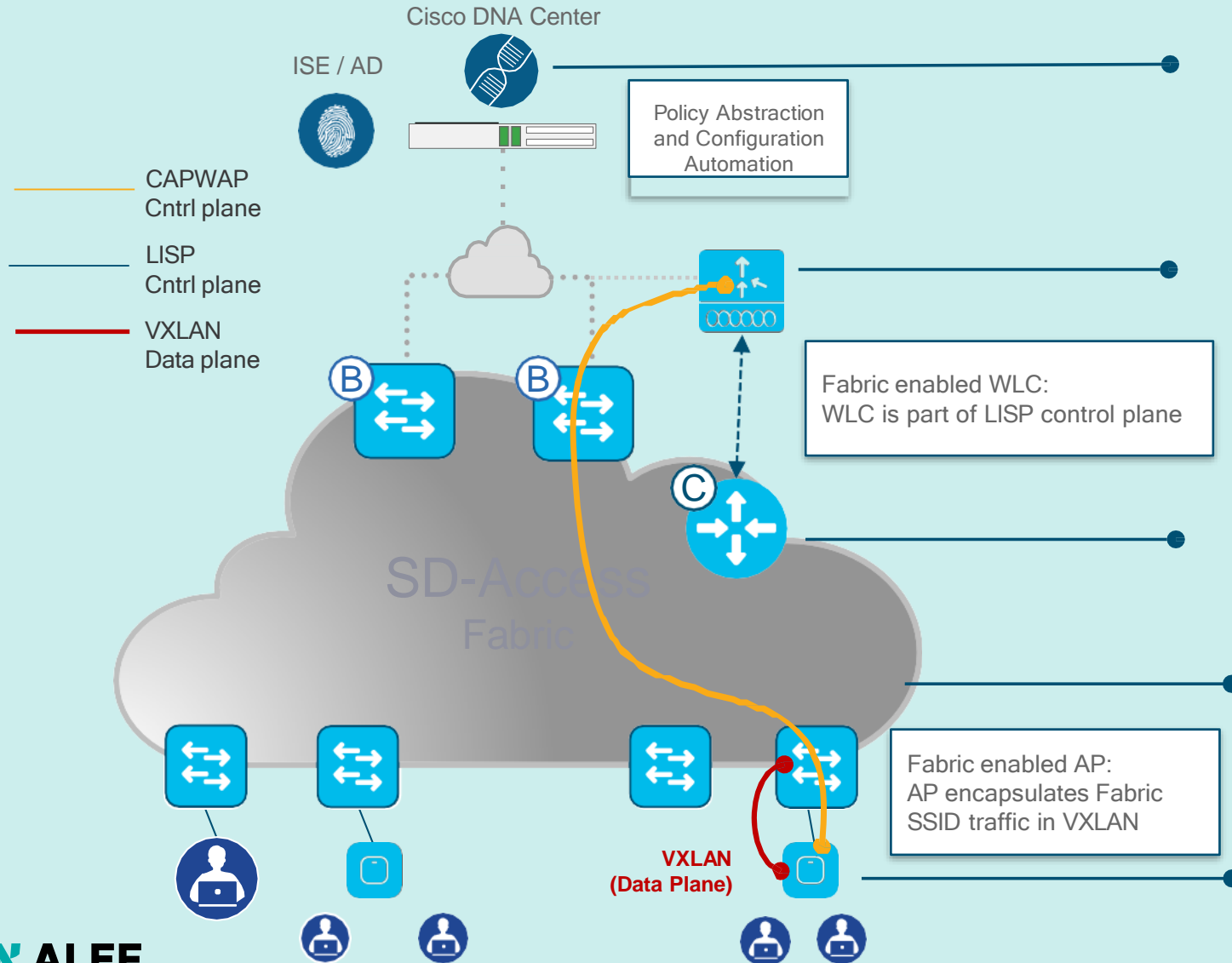
SDA Fabric in a Box

- Single device takes role as CP + Border + Edge
- Single switch, a switch with hardware stacking, or a StackWise Virtual deployment
- Local SD-Access Embedded Wireless, ISE, DHCP, DNS
- Used for remote branches



SD-Access Wireless Architecture

Optimizing the Data Plane



Automation

- Cisco DNA Center 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

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

DNA Center Workflow for SD-Access



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



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



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



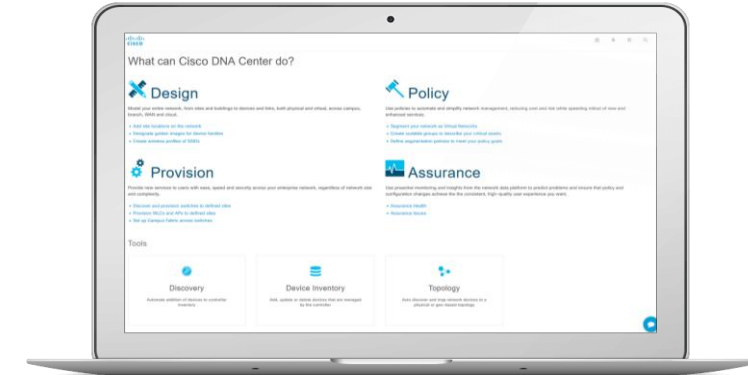
- Health Dashboard
- 360° Views
- FD, Node, Client
- Path Traces

Planning & Preparation

Installation & Integration

DNA Center Design

- Design your network from GUI
- Network Hierarchy
 - Area > Building > Floor (Maps)
- Network Settings
 - Network: AAA, DHCP, DNS, NTP, MOTD
 - Device Credentials: CLI, SNMP, HTTPS
 - IP Address Pools (SDA)
 - Wireless: SSID, Interfaces, RF Profiles
 - Telemetry: SNMP, Syslog, Netflow, IPDT
- Image Repository
 - Golden Image per Site, Device, Role
- Network Profiles
 - Routing, Switching, Wireless
- Authentication Profiles (SDA)
 - 802.1x Configuration



Cisco DNA Center Appliance



Physical and virtual infrastructure



Cisco and third party

SDA Segmentation

Security Groups (21)			
<div><div></div> Search Table</div>			
0 Selected			
<input type="checkbox"/>	Name	Tag Value	Description
<input type="checkbox"/>	Auditors	9/0x9	Auditor Security Group
<input type="checkbox"/>	BYOD	15/0xf	BYOD Security Group
<input type="checkbox"/>	Contractors	5/0x5	Contractor Security Group
<input type="checkbox"/>	Developers	8/0x8	Developer Security Group
<input type="checkbox"/>	Development_Servers	12/0xc	Development Servers Security Group
<input type="checkbox"/>	Employees	4/0x4	Employee Security Group
<input type="checkbox"/>	Extranet	17/0x11	Extranet Scalable Group
<input type="checkbox"/>	Guests	6/0x6	Guest Security Group
<input type="checkbox"/>	Intranet	16/0x10	Intranet Scalable Group
<input type="checkbox"/>	IT	18/0x12	

Cisco DNA Center	
Virtual Networks	Fabric Sites Transits Virtual Network Policies
<div><div>Filter</div><div>Actions</div></div>	
	Name
<input type="radio"/>	DEFAULT_VN
<input type="radio"/>	GUEST
<input type="radio"/>	INFRA_VN
<input type="radio"/>	IoT
<input type="radio"/>	USERS
Show 10 entries	

SDA Group-Based Access Control Policy

Cisco DNA Center

DESIGNPOLICYPROVISIONASSURANCEPLATFORM

Group-Based Access Control

IP Based Access Control

Application

Policies (12096)

Enter full screen

Filter

Deploy

Refresh

■ Permit ■ Deny ■ Custom □ Default

Destination

Source

Auditors

BYOD

Contractors

Corporate_Visi...

Developers

Development_L...

Doctors

Employees

Guests

IP_Phones

Network_Servi...

Nurses

PCI_Servers

Point_of_Sale...

Production_Se...

Corporate_Visitor

Developers

Development_S...

Doctors

Employees

Guests

IP_Phones

NetSvc

Nurses

PCI_Servers

Production_Serv...

Production_Users

Employees > Anti_Malware > Employees

Employees > Anti_Malware > Employees

Edit Access Contract

Name*

Anti_Malware

Description

Block ports commonly exploited by

CONTRACT CONTENT (62)

#	Action*	Application	Transport Protocol	Source / Destination	Port	Logging	Action
1	Deny	Advanced	TCP	Destination Source	138 ANY	<input type="checkbox"/>	+ ×
2	Deny	Advanced	TCP	Destination Source	138 ANY	<input type="checkbox"/>	+ ×
3	Deny	Advanced	UDP	Destination Source	138 ANY	<input type="checkbox"/>	+ ×
4	Deny	Advanced	UDP	Destination Source	138 ANY	<input type="checkbox"/>	+ ×
5	Deny	Advanced	TCP	Destination Source	139 ANY	<input type="checkbox"/>	+ ×
6	Deny	Advanced	TCP	Destination Source	139 ANY	<input type="checkbox"/>	+ ×
7	Deny	Advanced	UDP	Destination Source	139 ANY	<input type="checkbox"/>	+ ×
8	Deny	Advanced	UDP	Destination Source	139 ANY	<input type="checkbox"/>	+ ×

Default Action

Permit

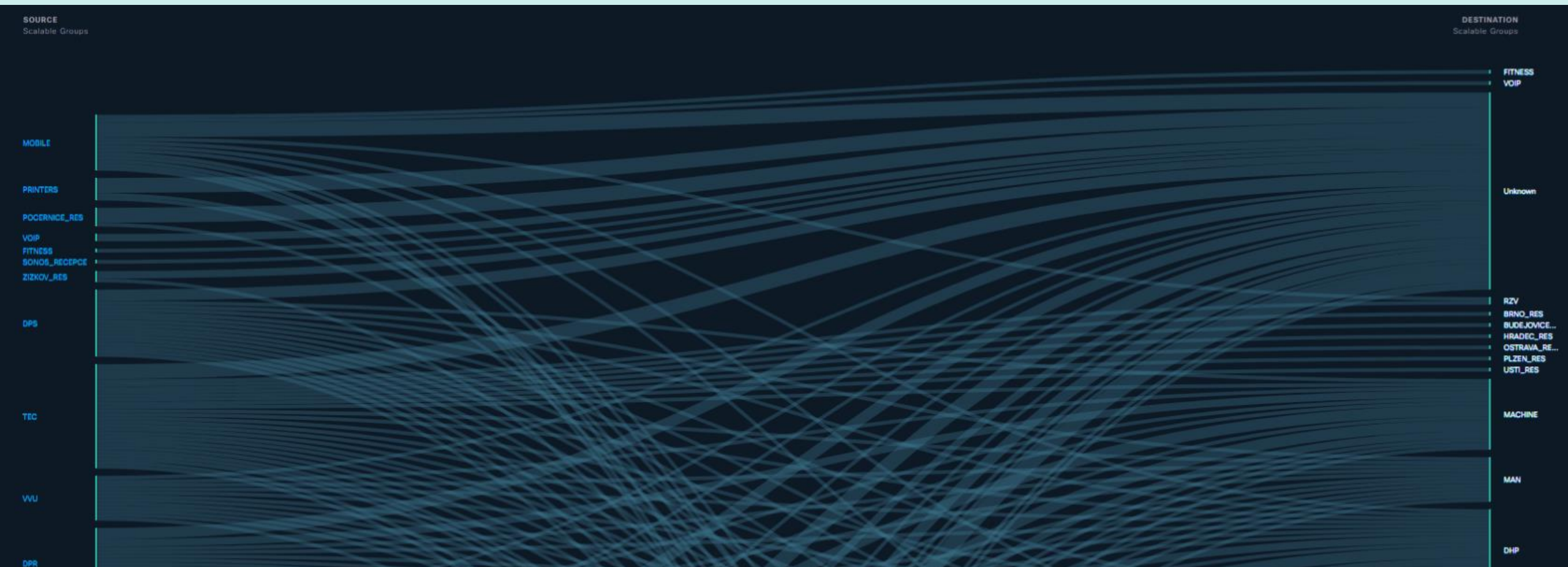
Logging

☒

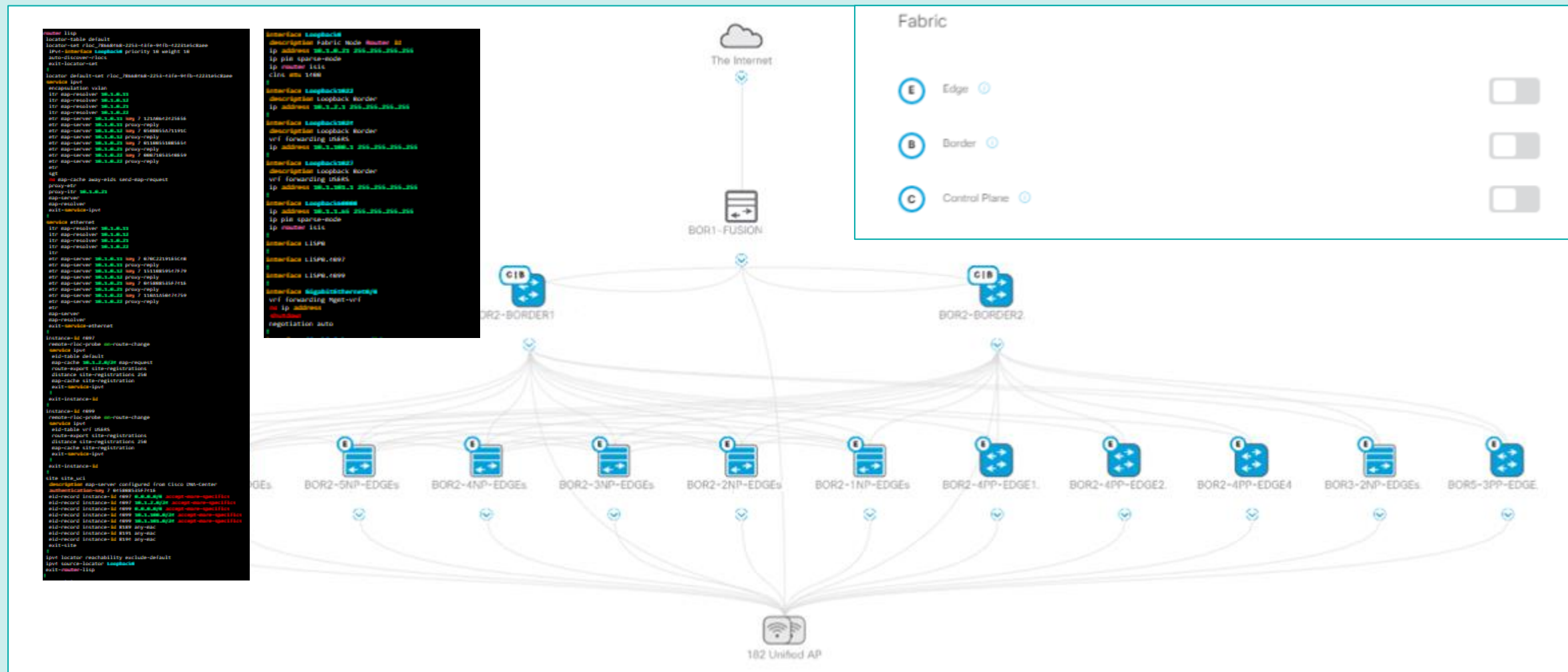
Cancel

Save

SDA Group-Based Policy Analytics



SDA Provisioning – Fabric Infrastructure



SDA Provisioning – Host Onboarding

Fabric Infrastructure Host Onboarding

Authentication Virtual Networks Wireless SSIDs Port Assignment

Select Authentication Template ⓘ

Settings will be applied to all Fabric Edge host ports, unless overridden by a static port assignment.

☐ Open Authentication ⓘ

☒ Closed Authentication ⓘ

☐ Low Impact ⓘ

☐ No Authentication ⓘ

Fabric Infrastructure Host Onboarding

Authentication Template Virtual Networks Wireless SSIDs Port Assignment

Clear Refresh Assign

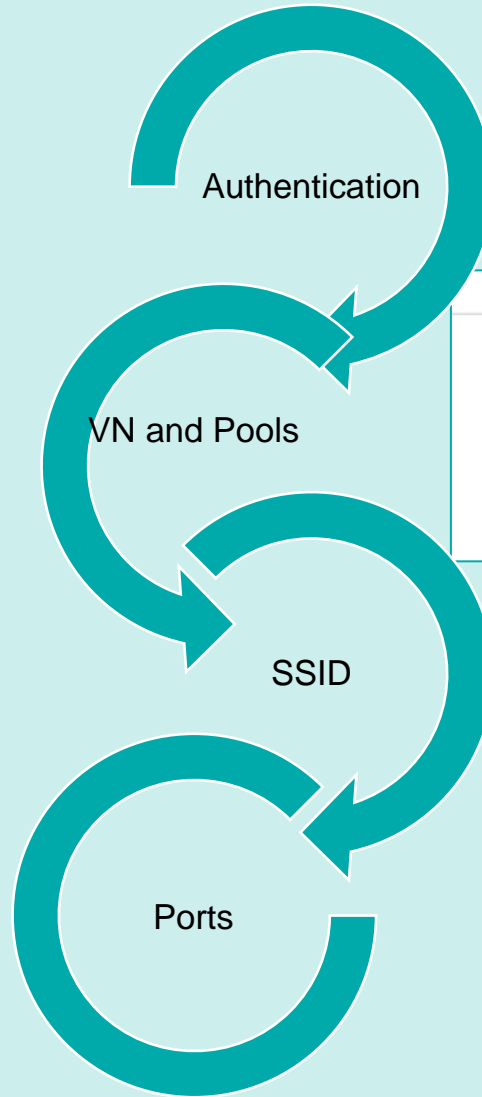
Filter PortNo A-Z LinkStatus

Search

☐ Select All

<input type="checkbox"/> GigabitEthernet1/0/1	<input type="checkbox"/> GigabitEthernet1/0/2
<input type="checkbox"/> GigabitEthernet1/0/7	<input type="checkbox"/> GigabitEthernet1/0/8
<input type="checkbox"/> GigabitEthernet1/0/13	<input type="checkbox"/> GigabitEthernet1/0/14
<input type="checkbox"/> GigabitEthernet1/0/19	<input type="checkbox"/> GigabitEthernet1/0/20

02KK01.C9324P01.k...
03KK01.C9348T01.k...
11KK01.STACK01.kk...
12KK01.STACK01.kk...
13KK01.STACK01.kk...
13KK02.STACK01.kk...
14KK01.STACK01.kk...
14KK02.STACK01.kk...



Fabric Infrastructure Host Onboarding

Authentication Template Virtual Networks Wireless SSIDs Port Assignment

Select a Virtual Network to associate one or more IP Pool(s) with the selected VN.

Critical Pool: Not Selected

GUEST X INFRA_VN IoT X USERS

<input type="checkbox"/>	VLAN Name	IP Address Pool	VLAN ID	Traffic Type
<input type="checkbox"/>	10_1_...USERS	BUTTERFLY-USERS 10.1.100.0/24	1024	Data
<input type="checkbox"/>	10_1_...USERS	BUTTERFLY-VOICE 10.1.101.0/24	1027	Voice

Fabric Infrastructure Host Onboarding

Authentication Template Virtual Networks Wireless SSIDs Port Assignment

☐ Enable Wireless Multicast

SSID Name	Type	Security	Traffic Type	Address Pool
MMC	Enterprise	WPA2 Personal	Voice + Data	Choose Pool 10_170_22_0-MMC
MIND2FLO	Enterprise	WPA2 Personal	Data	Choose Pool 10_170_22_0-MMC

Before SD-Access



After SD-Access

- Manual device configuration (CLI)
- VLANs, VLANs, VLANs, subnets, subnets, subnets
- Security policy based on VLAN and IP address
- Separated configuration wired and wireless
- Limited mobility
- Deploy network in days
- Troubleshoot network in hours
- Human error in configuration

- Fully automated and centralized configuration
- Easy segmentation with VN and SGT
- Security policy definition decoupled from VLAN and IP address
- Management of Wired and Wireless networks from single interface
- Seamless mobility
- Deploy networks in minutes
- Troubleshoot network in minutes
- Ensure consistency in device configuration

Trust the strong and DNA