
CISCO
SDA
Jan Kaše

Legacy Networks

Konfigurace:

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

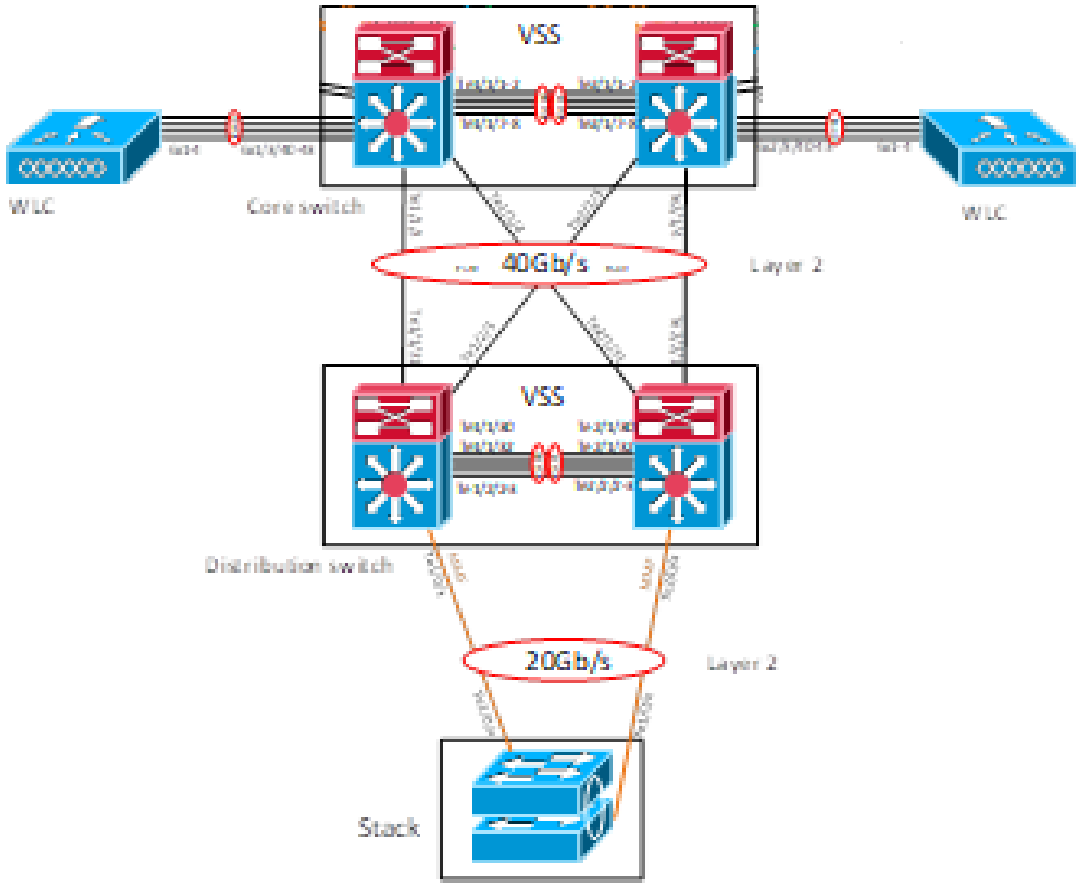
Segmentace a bezpečnost:

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

Wireless (OTT):

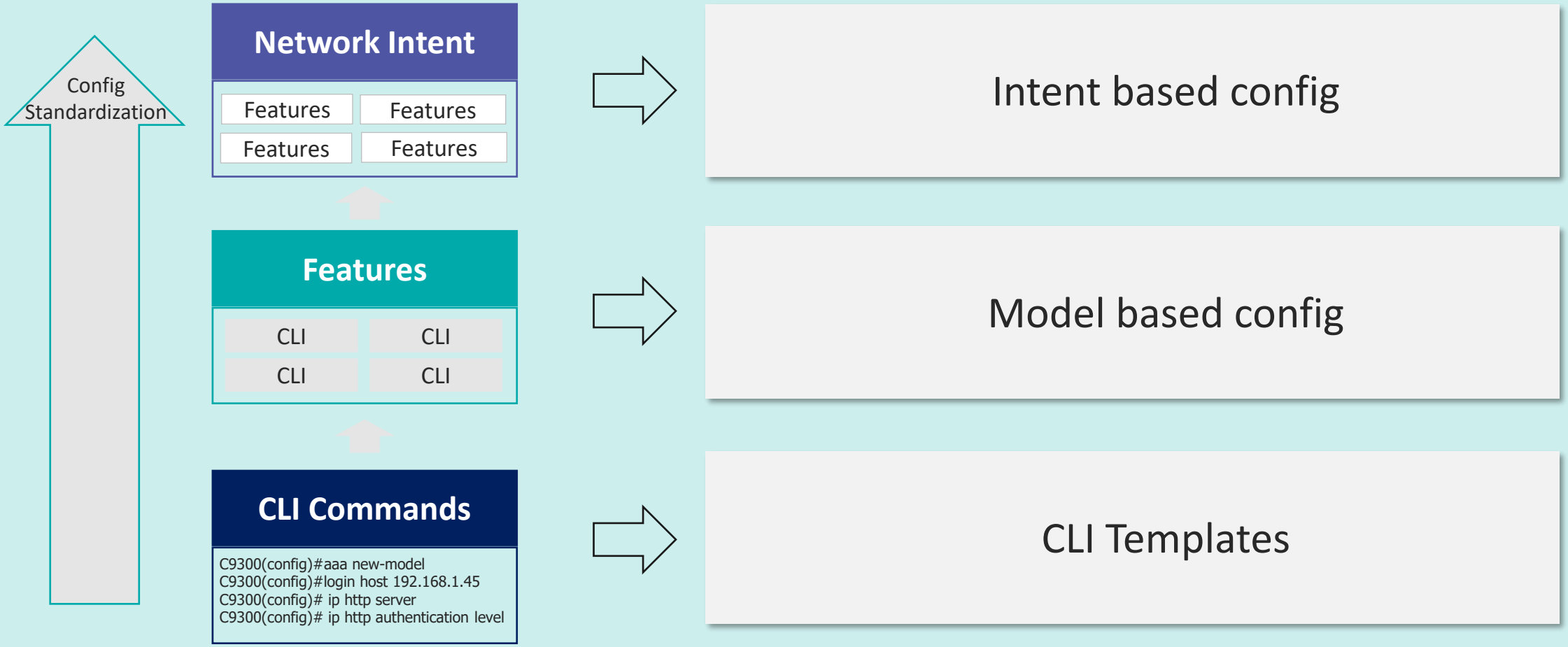
- Oddělená segmentace a konfigurace od wired
- Kde vypadne provoz?
- A co bezpečnost?

Management, monitoring?

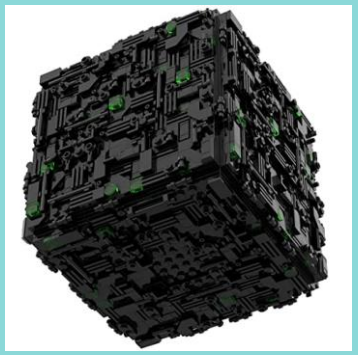


Simplified configuration Management

Network Configuration

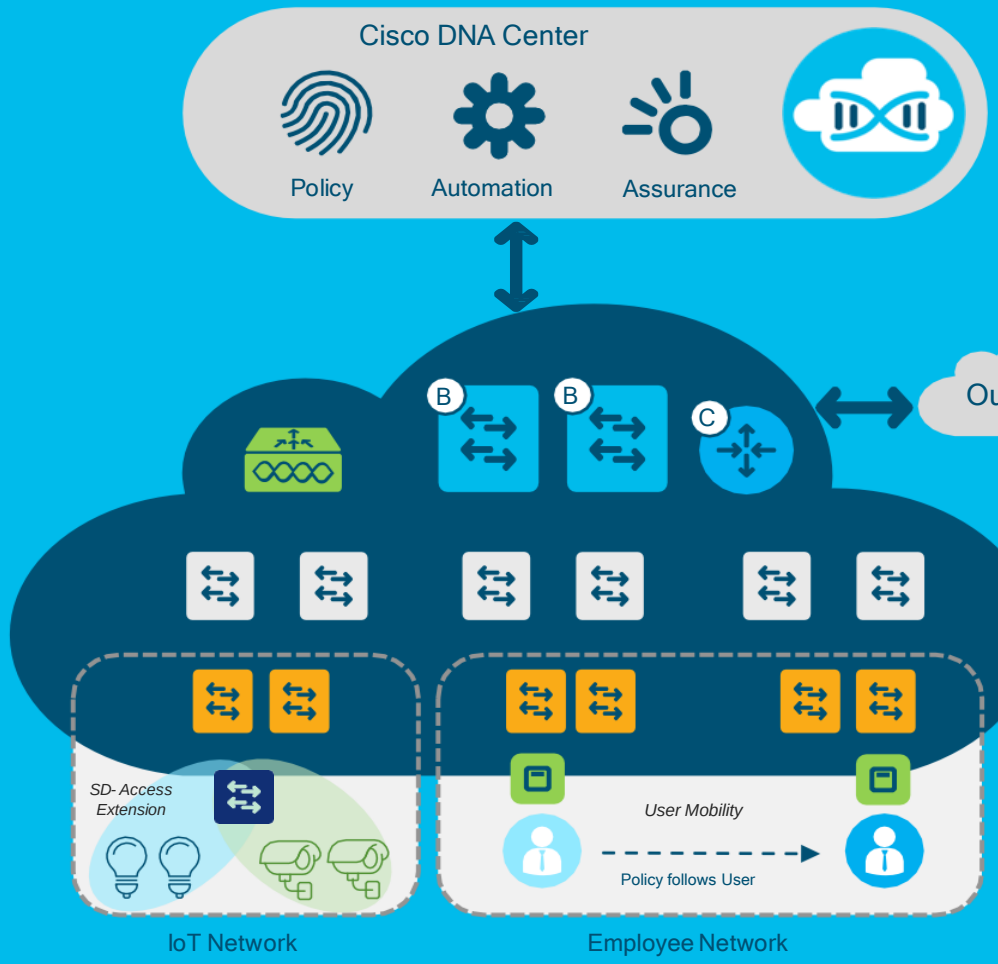


Before SD-Access → After SD-Access



Cisco Software Defined Access

The Foundation for Cisco's Intent-Based Network



Identity-Based Policy and Segmentation

Policy definition decoupled from VLAN and IP address

Automated Network Fabric

Single fabric for Wired and Wireless with full automation

Insights and Telemetry

Analytics and insights into User and Application experience

5

SD-Access Architecture

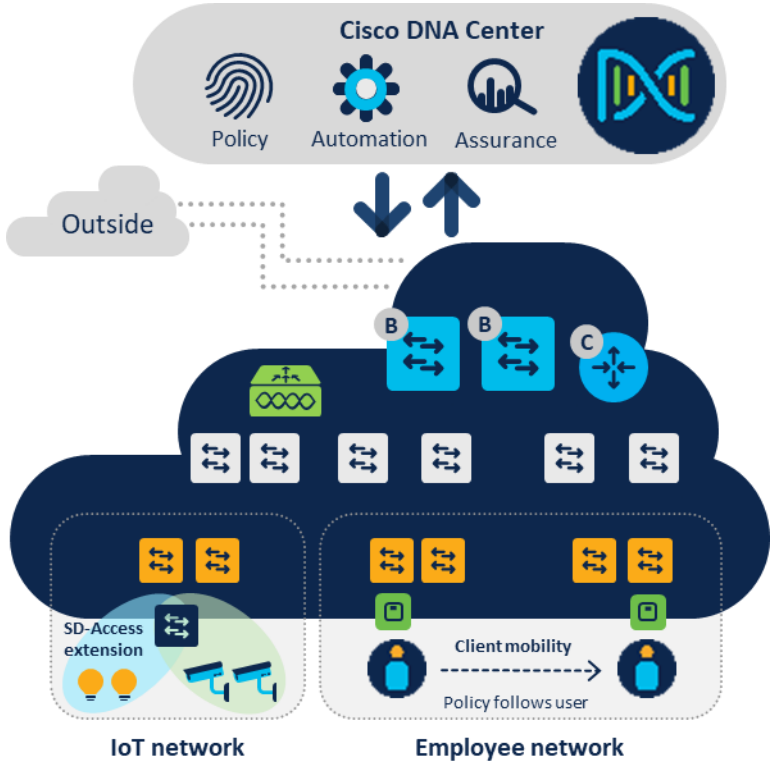
SDA = Campus Fabric + DNA Center

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

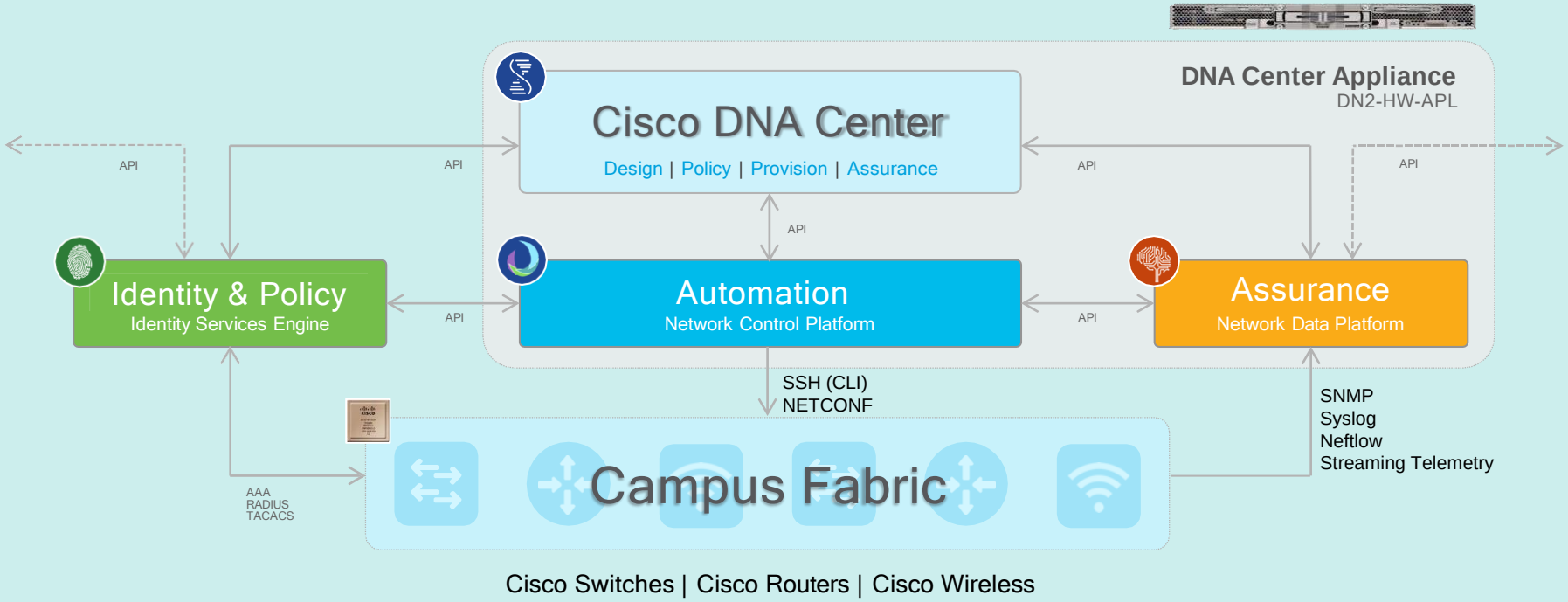
Campus fabric:

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

DNA Center: Management plane

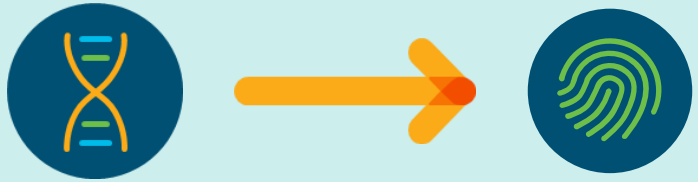


DNA Center Architecture



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

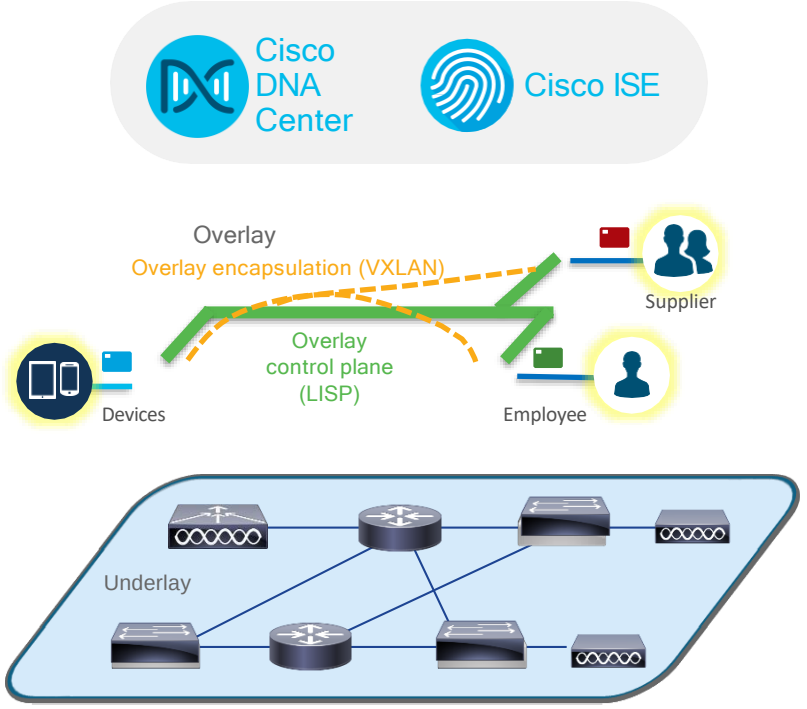
Campus Fabric

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 VLXAN 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

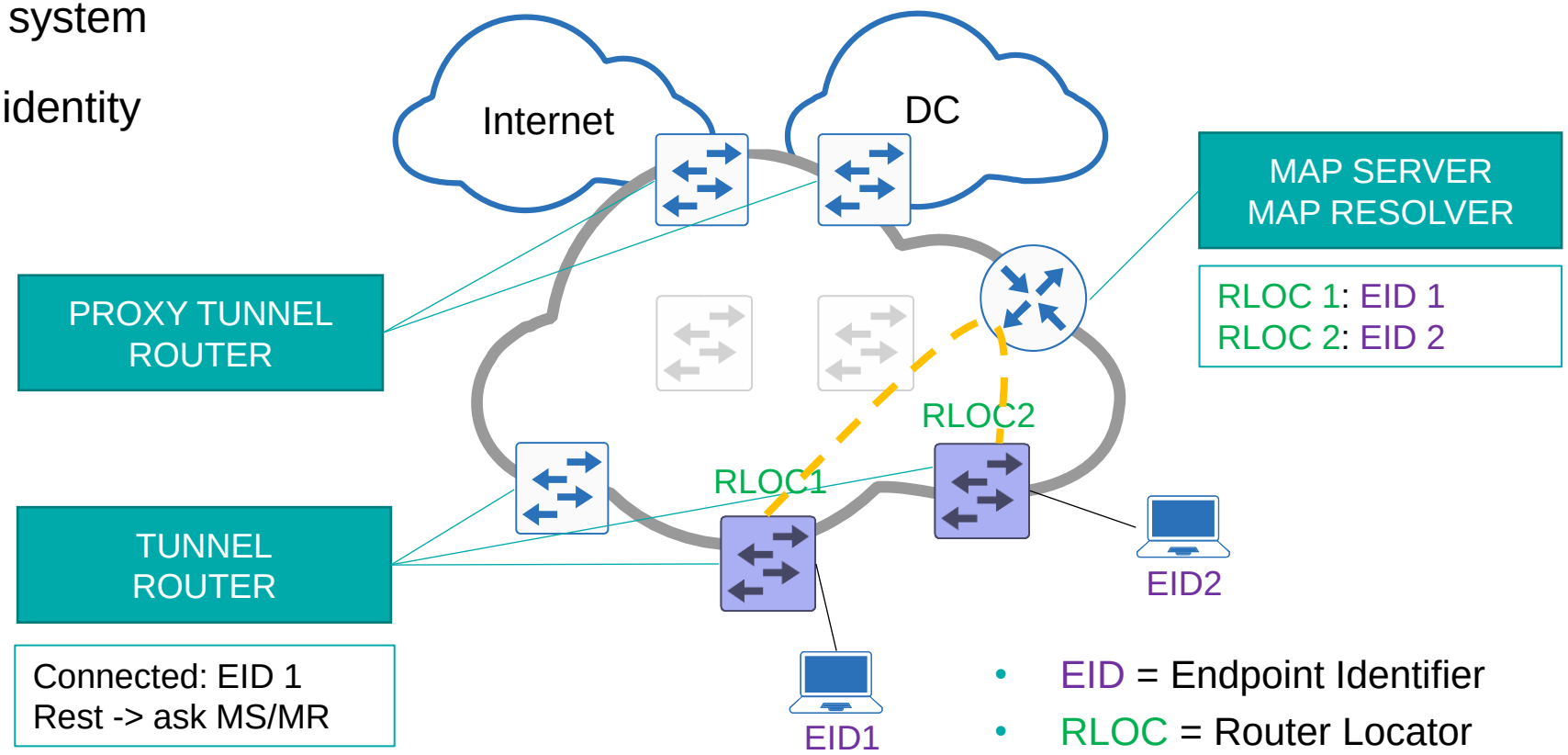
2. LAN Automation – DNA Center

- 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



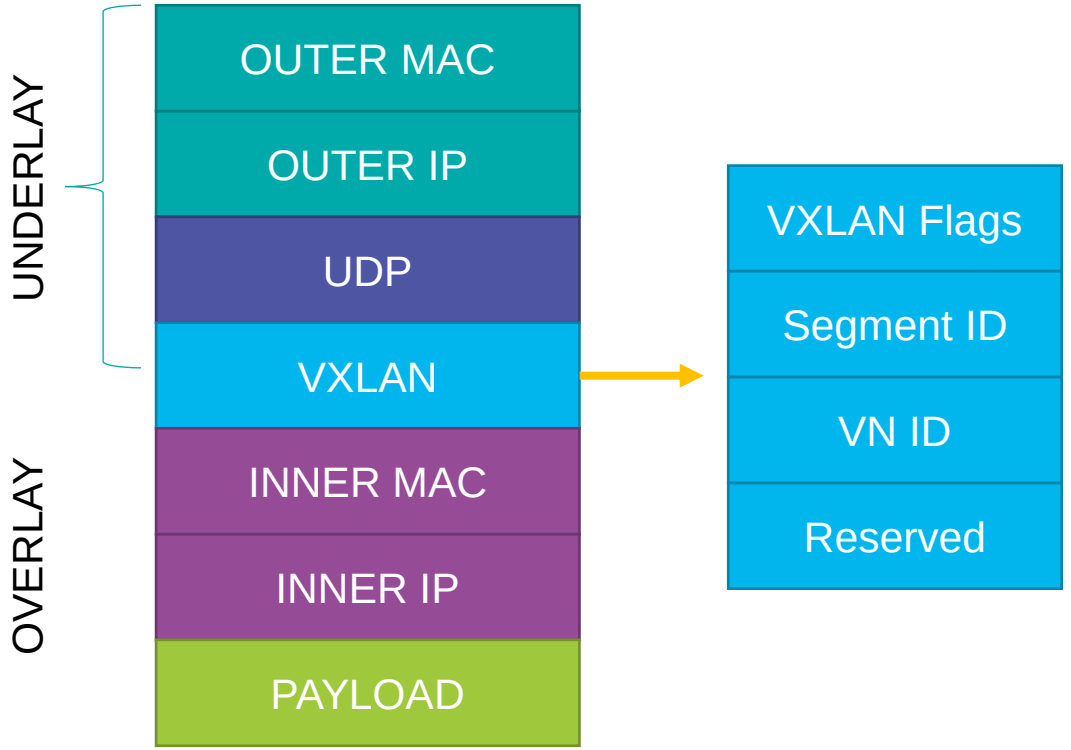
- EID = Endpoint Identifier
- RLOC = Router Locator

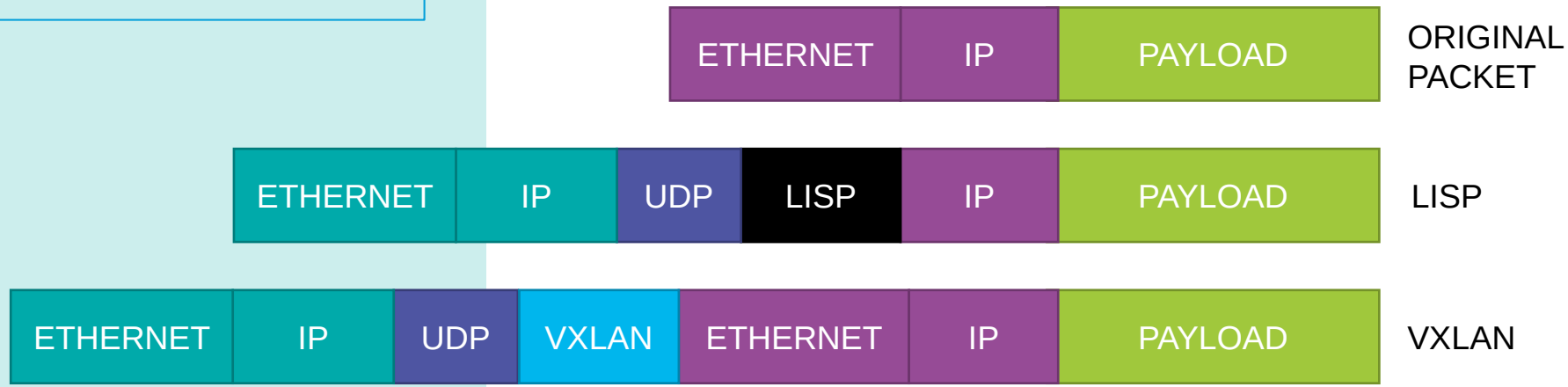
SDA VXLAN Data Plane

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

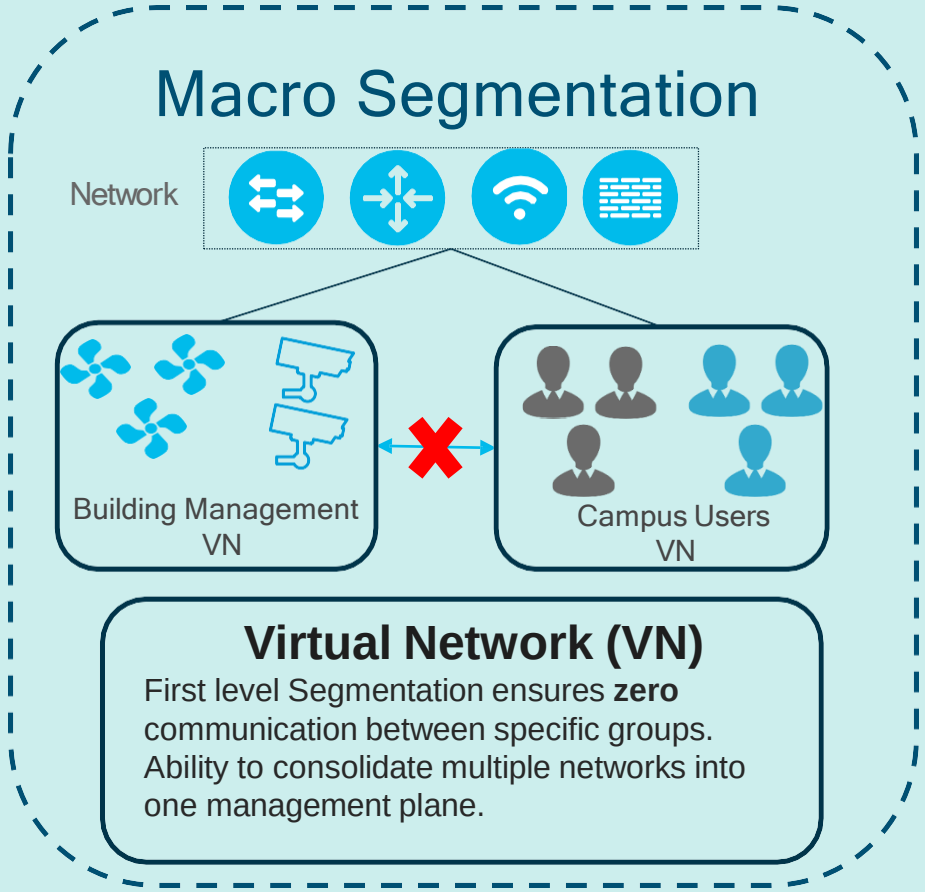
VXLAN header contains VNID (VXLAN Network Identifier) field which allows up to 16 million VRFs.

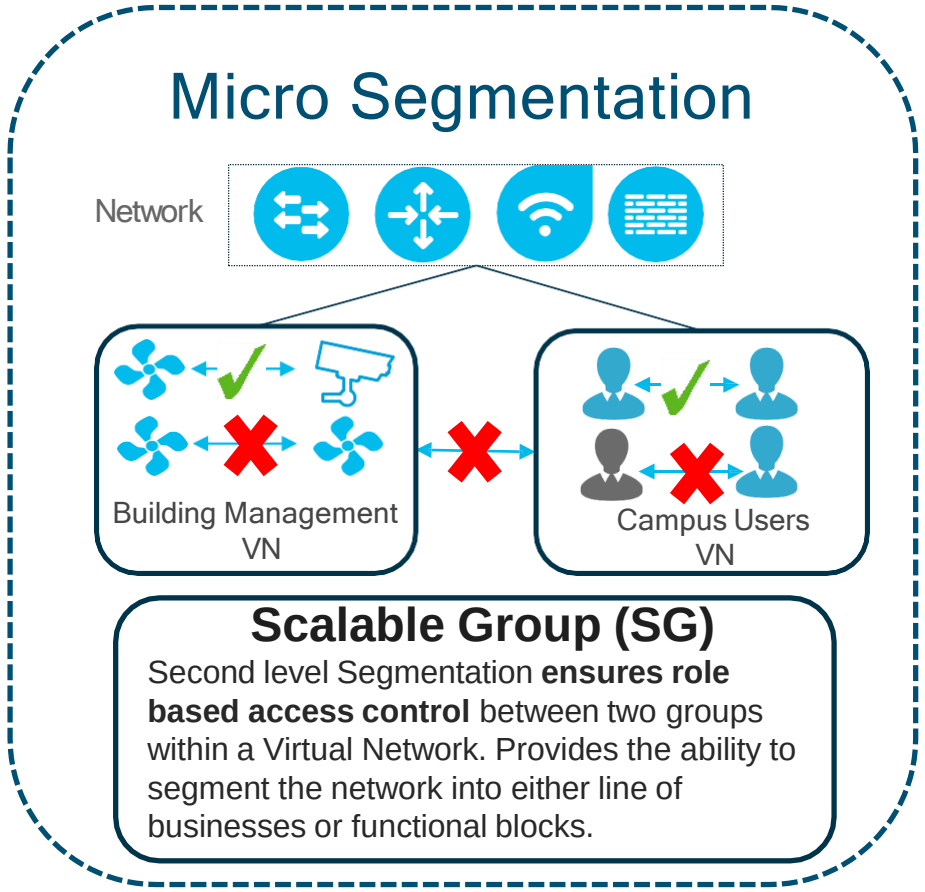
VXLAN header also has Group Policy ID for Scalable Group Tags (SGTs) allowing 64,000 SGTs.





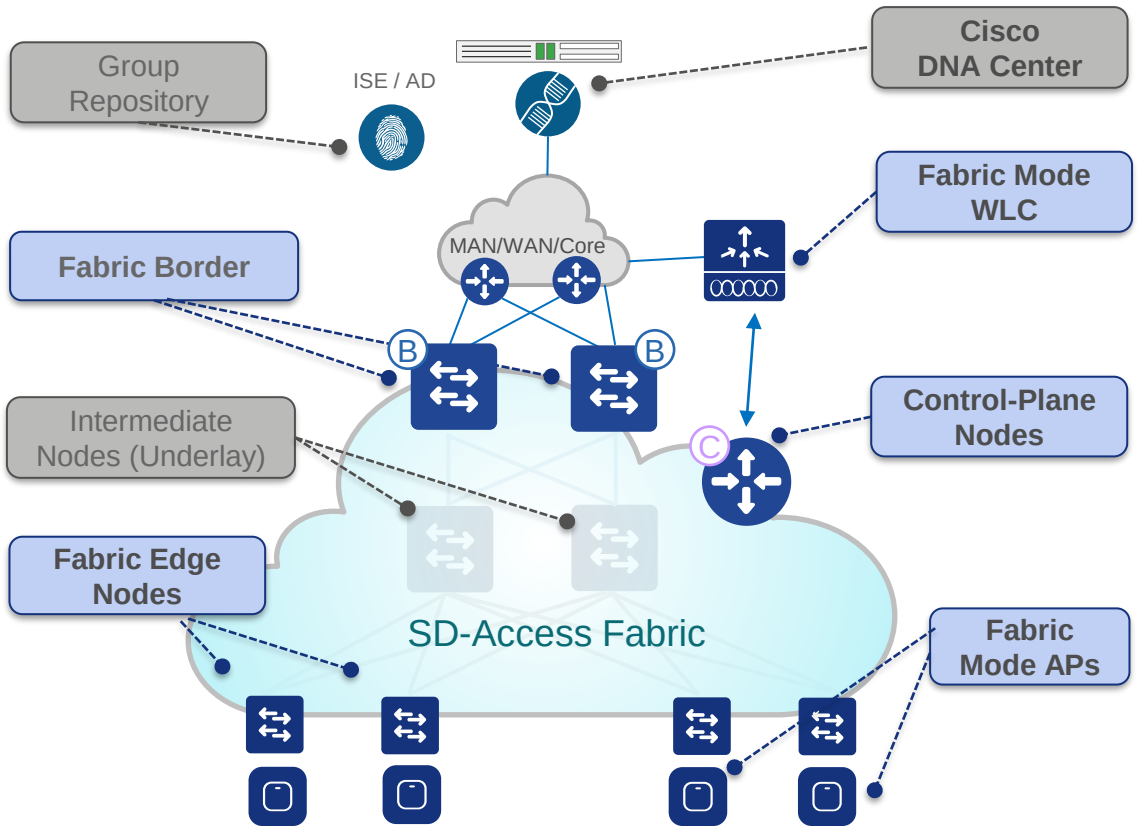
SDA Segmentation and Policy





SDA Fabric Roles

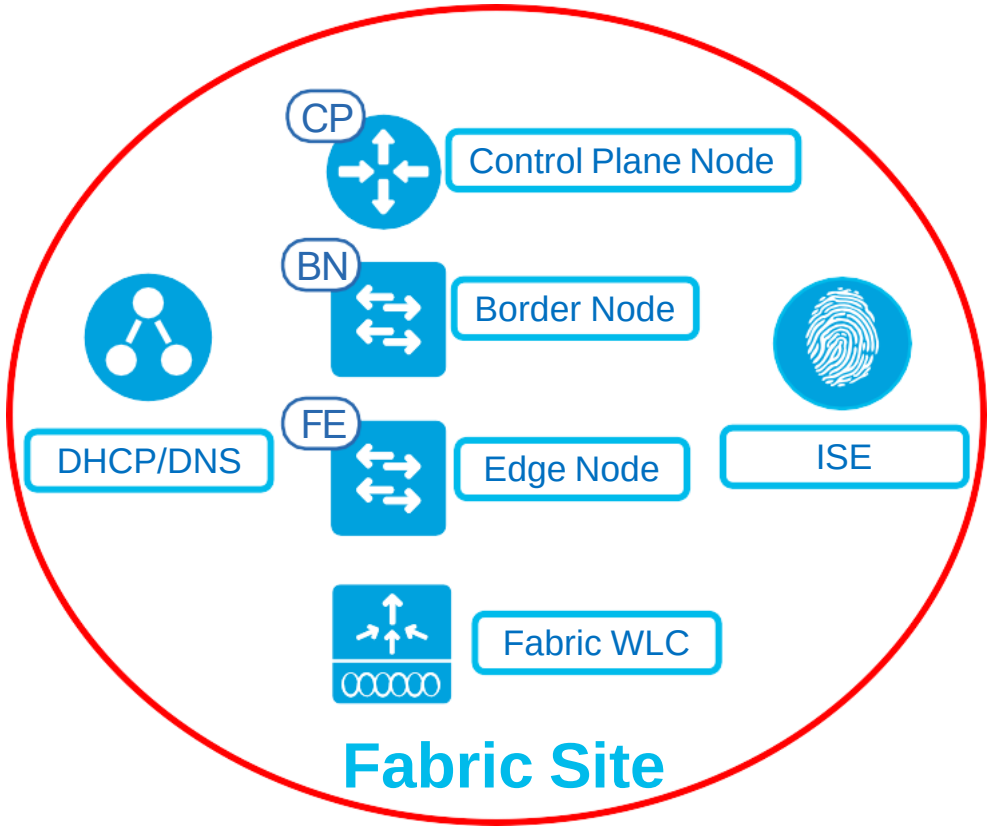
- **DNA Controller** – Enterprise SDN Controller provides GUI management abstraction via multiple Service Apps, which share information
- **Group Repository** – External ID Services (e.g.. ISE) is leveraged for dynamic User or Device to Group mapping and policy definition
- **Control-Plane (C) Node** – 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

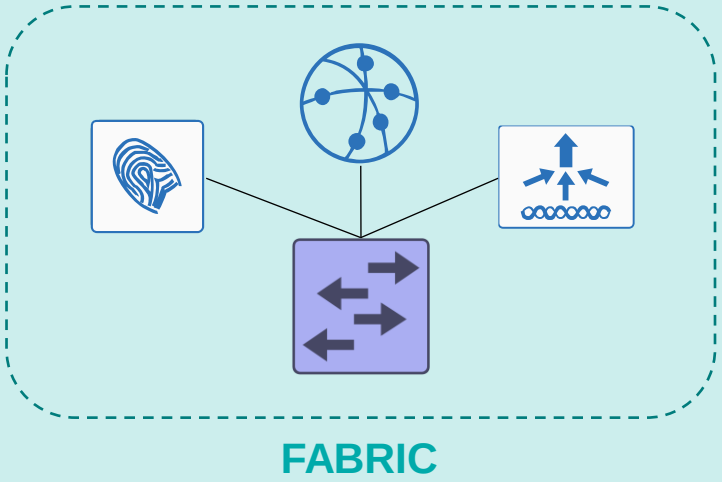
- Contains Control Plane Node, Border Node, and Edge Node
- Contains WLC and ISE Policy Service Node (PSN)
- Fabric Border Node is the ingress and egress device for the site
- A Fabric Site may cover a single physical location, multiple locations, or just a subset of a location
  - Single Location →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



ALEF

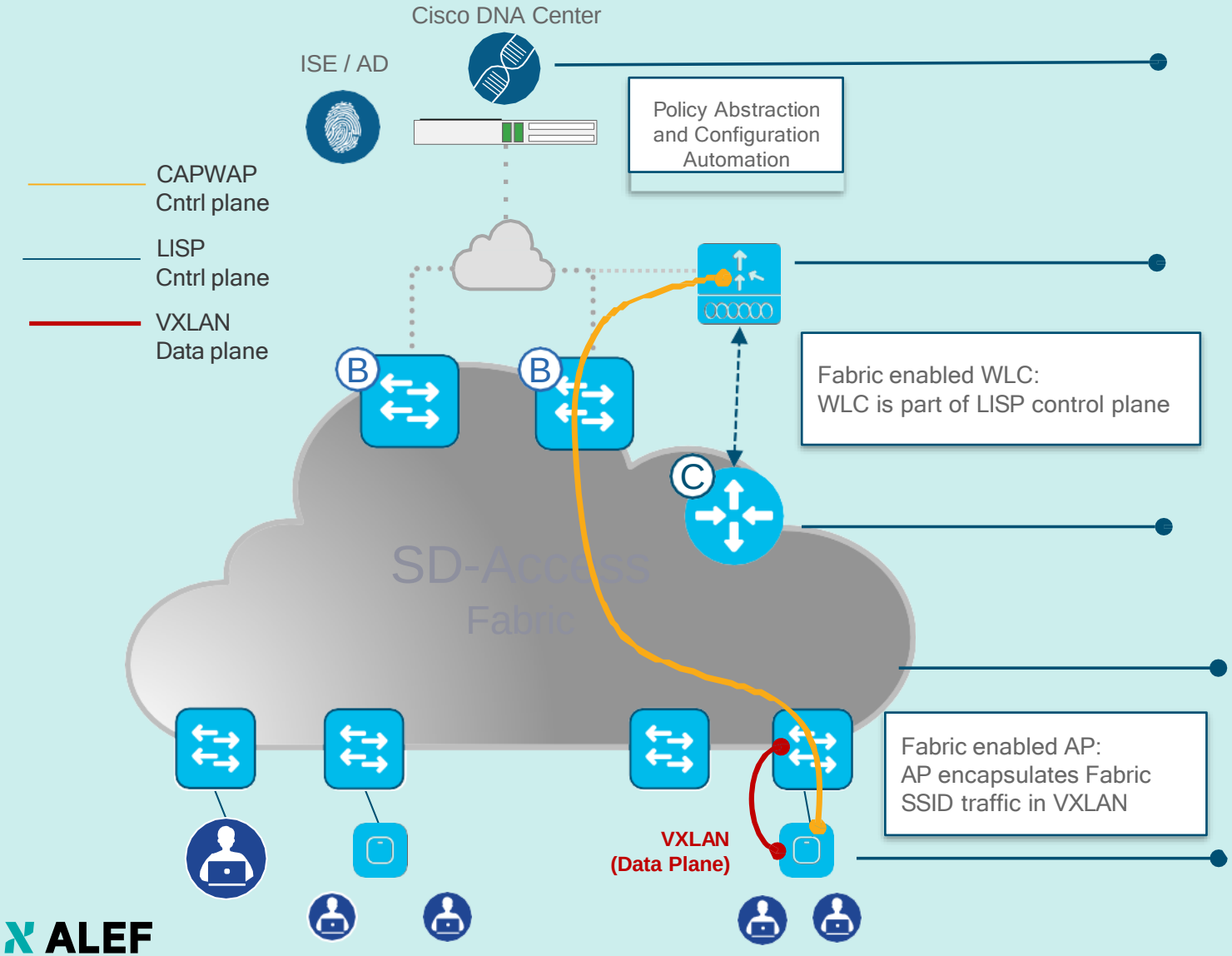
SDA Fabric in a Box

- 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

ALEF

DNA Center Workflow for SD-Access

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
- 360º Views
- FD, Node, Client
- Path Traces

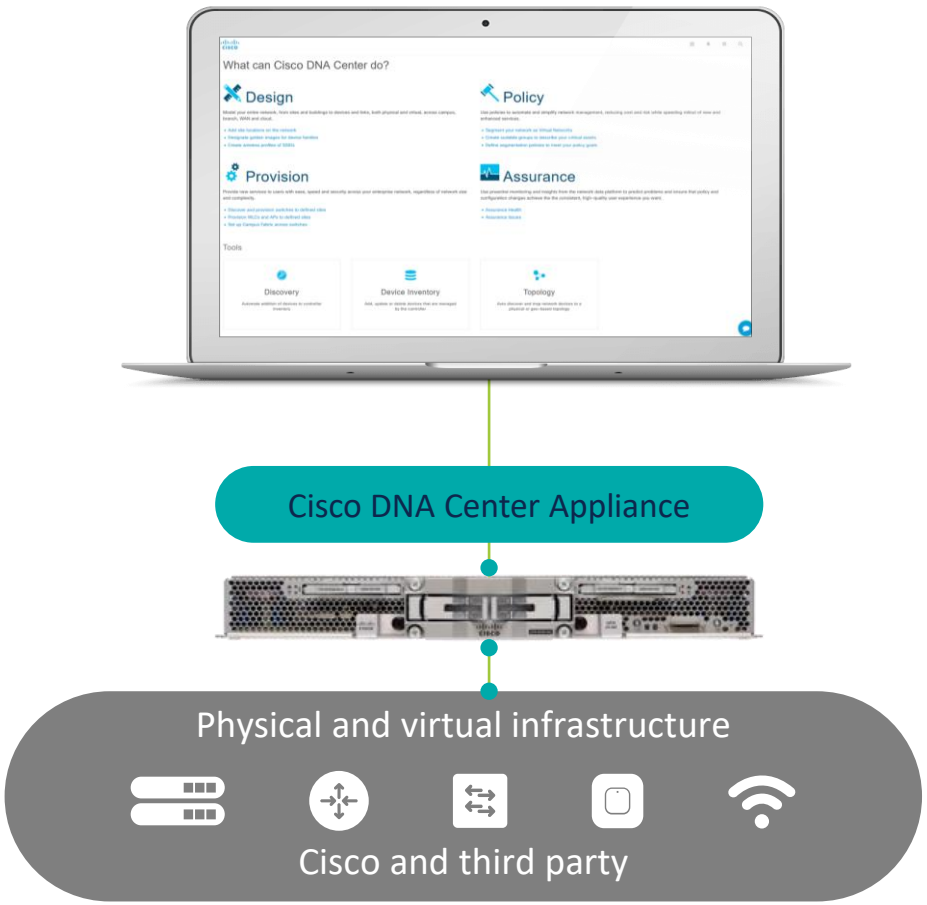
Planning & Preparation

Installation & Integration

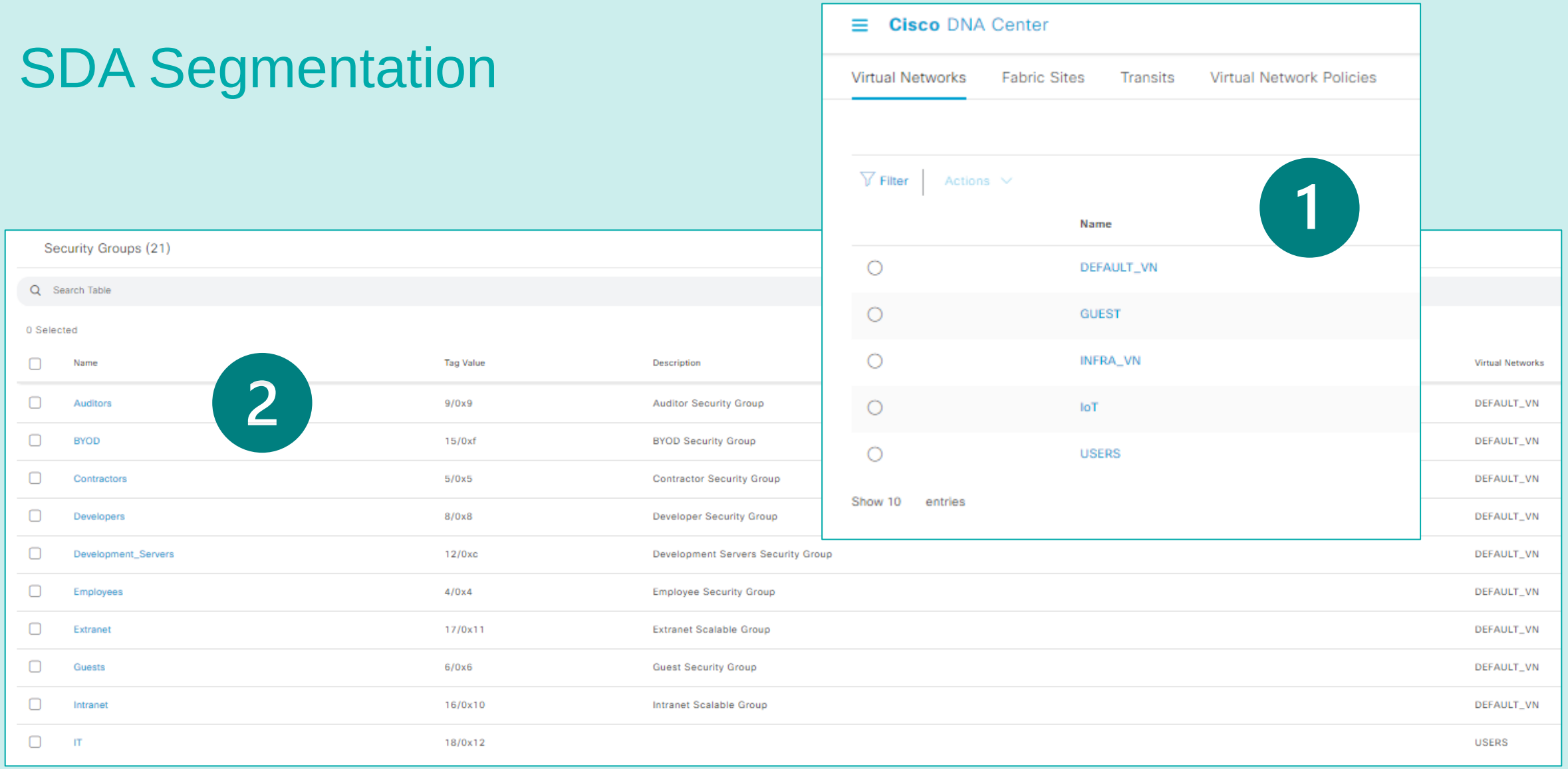
DNA Center Design

- Design your network from GUI

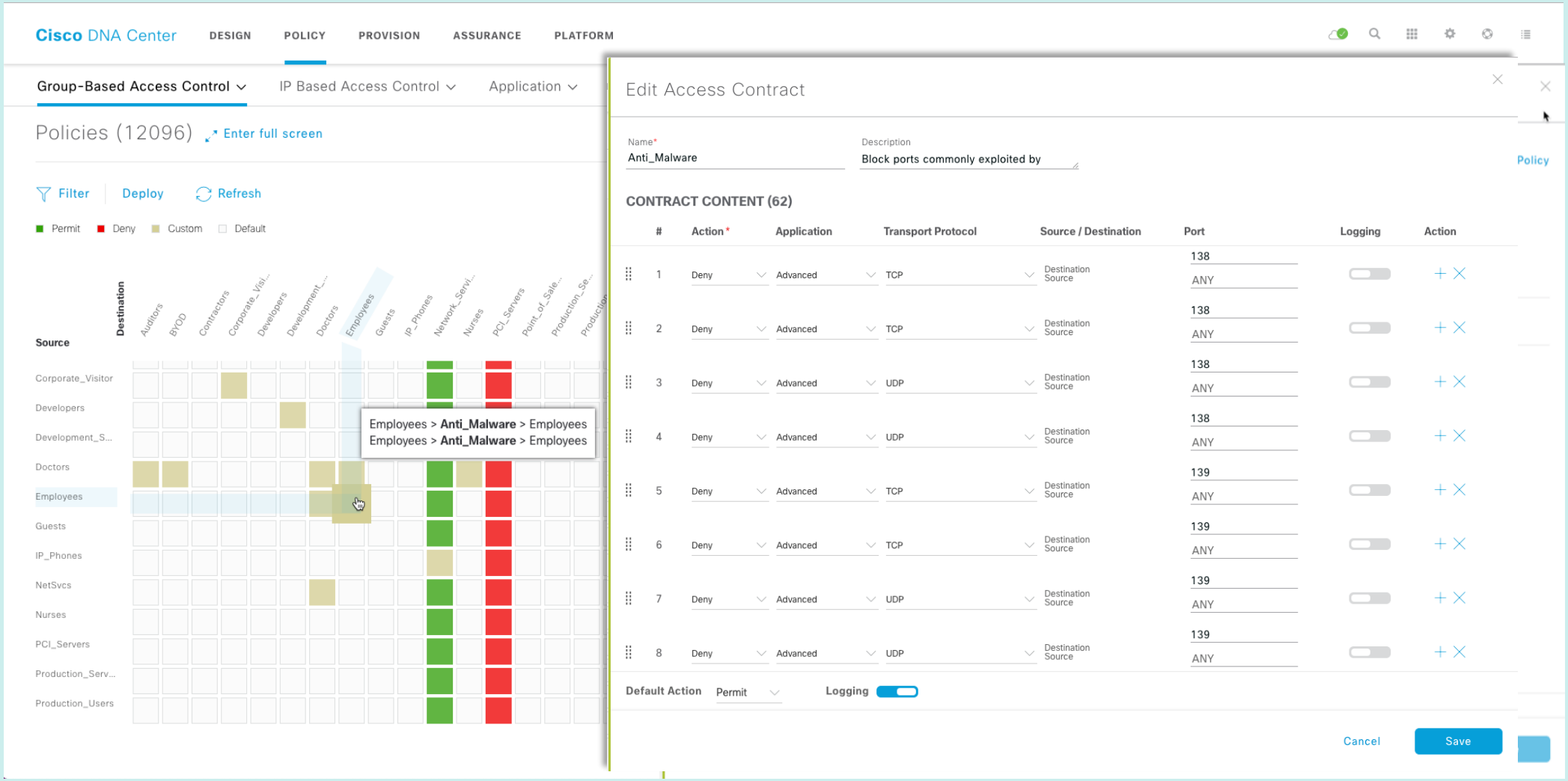
- Network Hierarchy
  - Area > Building > Floor (Maps)
- Network Settings
  - Network: AAA, DHCP, DNS, NTP, MOTD
  - Device Credentials: CLI, SNMP, HTTPS
  - IP Address Pools (SDA)
  - Wireless: SSID, Interfaces, RF Profiles
  - Telemetry: SNMP, Syslog, Netflow, IPDT
- Image Repository
  - Golden Image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



SDA Segmentation

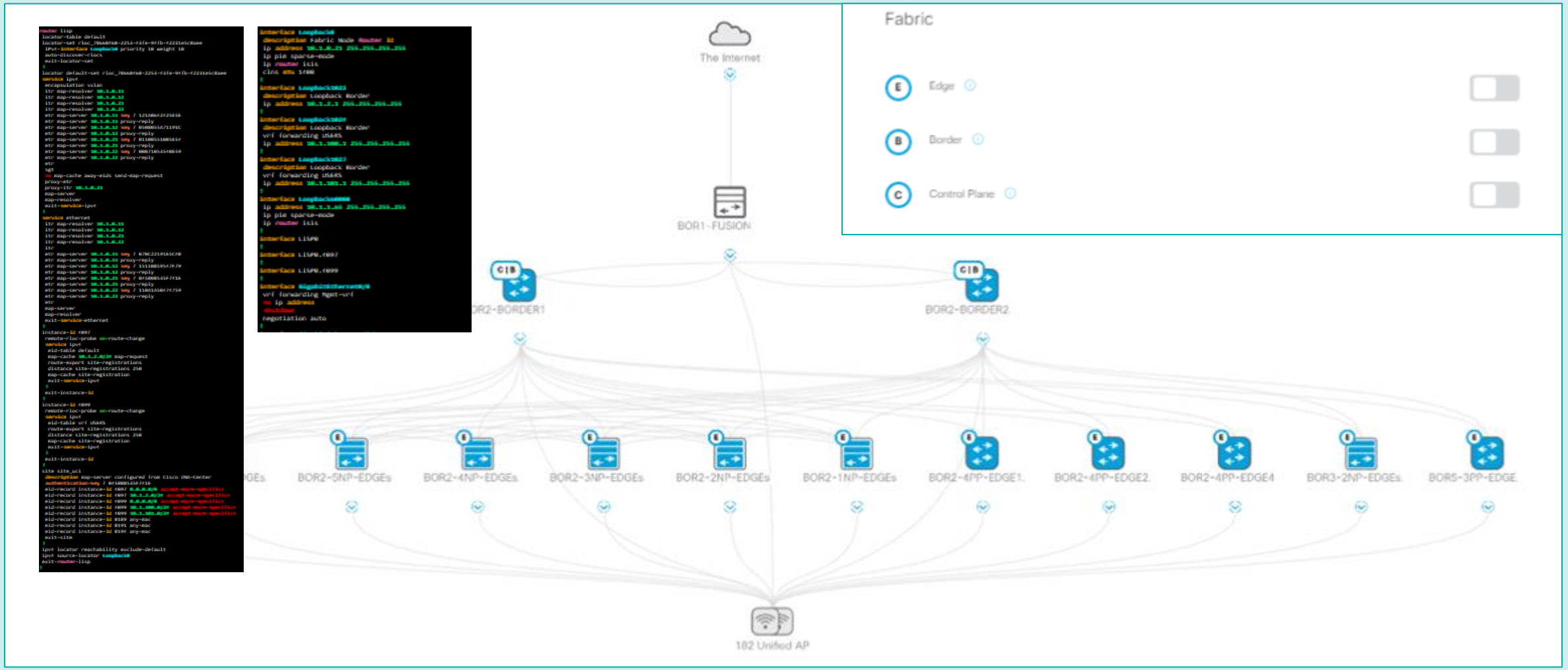


SDA Group-Based Access Control Policy

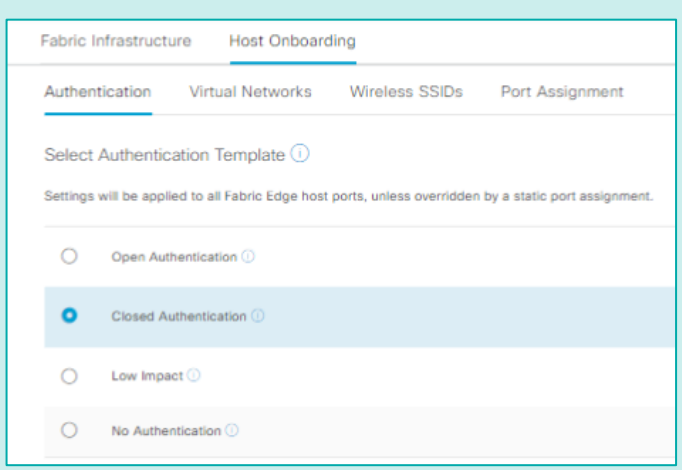


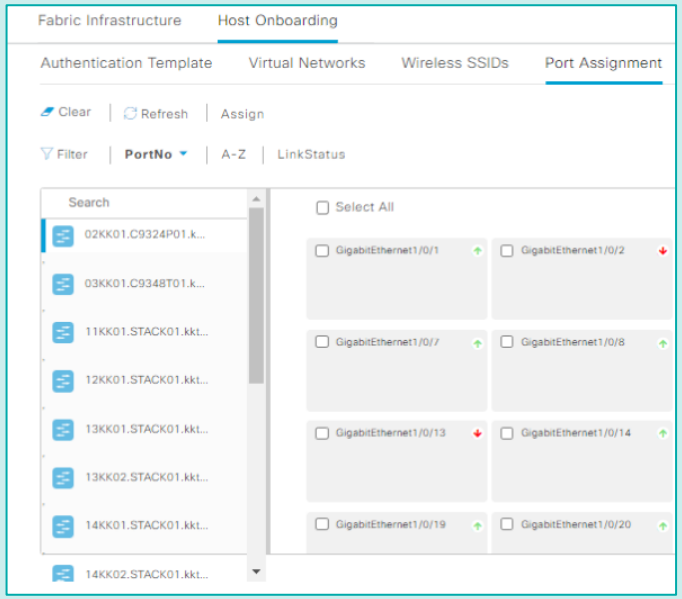
SDA Group-Based Policy Analytics

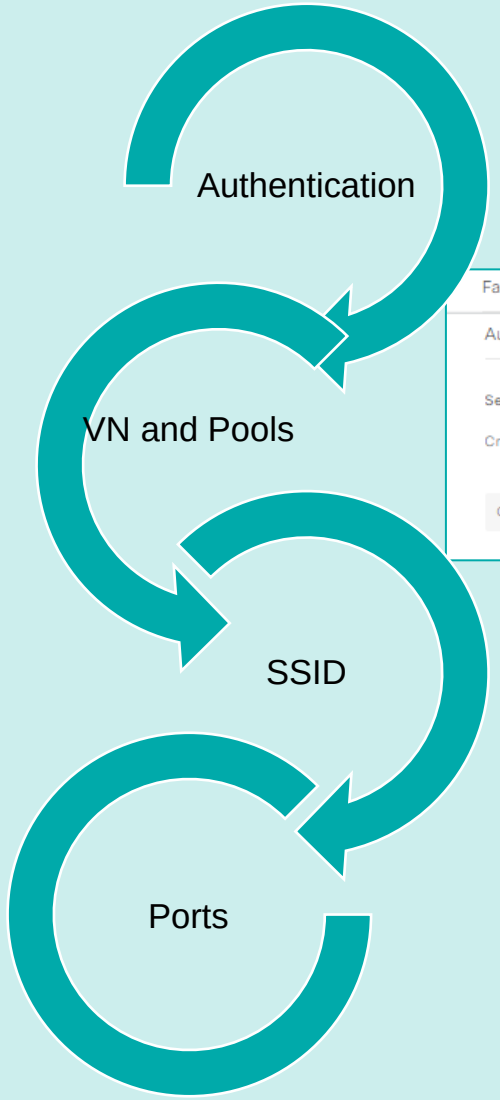
SDA Provisioning – Fabric Infrastructure

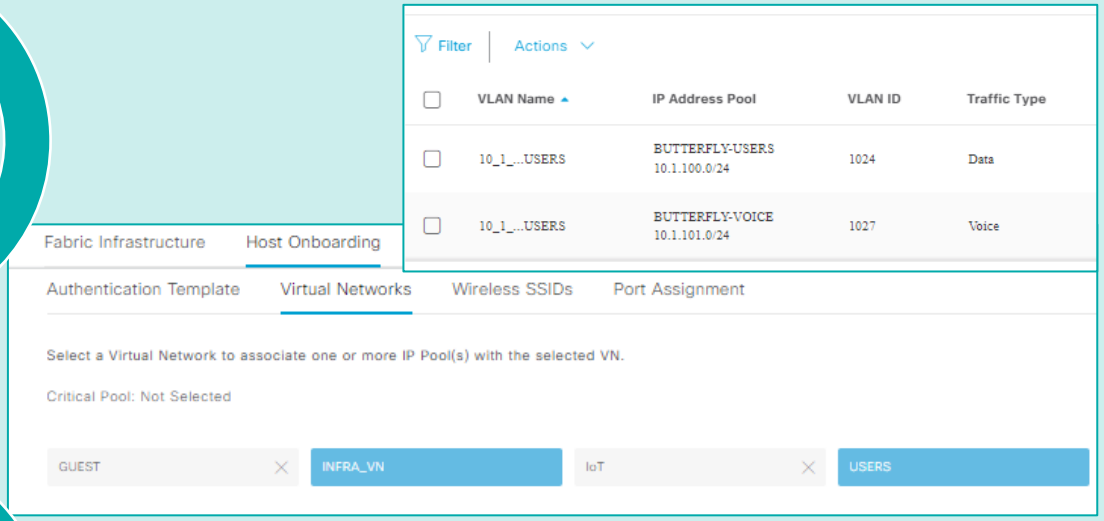


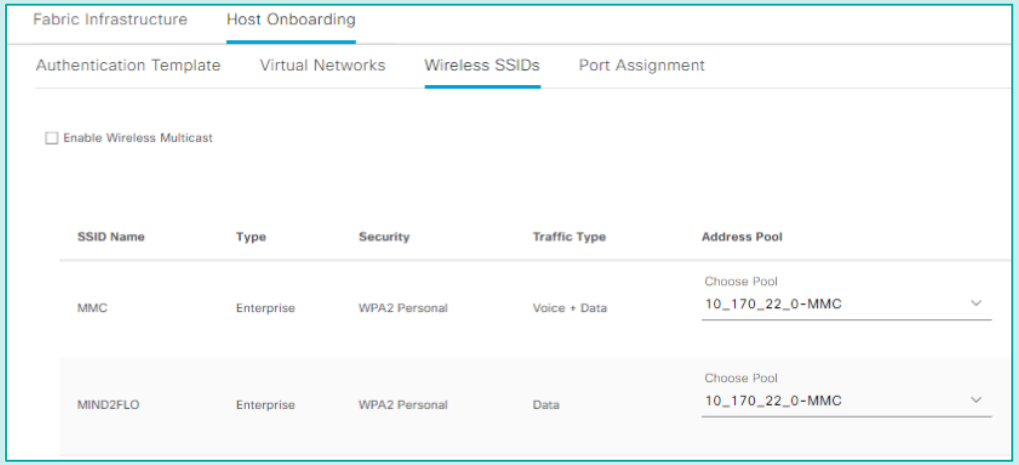
SDA Provisioning – Host Onboarding











Before 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

After SD-Access

- 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

ALEF

Trust the strong and DNA